Министерство науки и высшего
образования Российской Федерации
Федеральное государственное автономное
образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ
ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Сборник материалов
VIII Всероссийской научно-технической конференции
(Ставрополь, 22–23 мая 2018)

Часть 2

Министерство науки и высшего образования Российской Федерации
Северо-Кавказский федеральный университет (г. Ставрополь)
Институт компьютерных технологий и информационной
безопасности Инженерно-технологической академии
Южного федерального университета (г. Таганрог)
Поволжский государственный университет телекоммуникаций
и информатики (г. Самара)
Ростовский государственный экономический университет (РИНХ)
(г. Ростов-на-Дону)

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Сборник материалов VIII Всероссийской научно-технической конференции
(г. Ставрополь, 22–23 мая 2018 года)

Часть 2

Ставрополь
2018

УДК 004.2/.9 (082)
ББК 32.97 я43
С 88

Оргкомитет конференции

Председатель:

Лиховид А. А. – проректор по научной работе и стратегическому развитию СКФУ, доктор географических наук, кандидат биологических наук, профессор

Члены оргкомитета:

Мезенцева О. С. – директор Института информационных технологий и телекоммуникаций (ИИТТ) СКФУ, кандидат физико-математических наук, доцент

Петренко В. И. – заместитель директора по научной работе ИИТТ СКФУ, заведующий кафедрой организации и технологии защиты информации, кандидат технических наук, доцент

Веселов Г. Е. – директор Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета, полномочный представитель ректора по развитию инженерного направления, д-р техн. наук, доцент

Самойлов А. Н. – заместитель директора Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета по научной и международной деятельности, кандидат технических наук, доцент

Паровик Р. И. – декан ФМФ Камчатского государственного университета им. В. Беринга, кандидат физико-математических наук, доцент

Чипига А. Ф. – заведующий кафедрой информационной безопасности автоматизированных систем ИИТТ СКФУ, кандидат технических наук, профессор

Тищенко Е. Н. – заведующий кафедрой информационных технологий и защиты информации Ростовского государственного экономического университета (РИНХ), доктор экономических наук, профессор

Агаханова Я. С. – доцент кафедры высшей математики Московского физико-технического института (МФТИ), кандидат физико-математических наук

Ответственный секретарь:

Лапина М. А. – доцент кафедры информационной безопасности автоматизированных систем ИИТТ СКФУ, кандидат физико-математических наук, доцент

С 88 **Студенческая наука для развития информационного общества:** сборник материалов VIII Всероссийской научно-технической конференции. Ч2. – Ставрополь: Изд-во СКФУ, 2018. – 350 с.

ISBN 978-5-9296-0968-8

Материалы конференции посвящены вопросам развития инновационных образовательных и инфокоммуникационных технологий, проблемам информационной безопасности объектов информатизации, изучению информационных систем и технологий. Изложены результаты научных исследований в области разработки информационных технологий решения экономических задач.

УДК 004.2/.9 (082)
ББК 32.97 я43

ISBN 978-5-9296-0968-8

СОДЕРЖАНИЕ

Раздел 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Раздел 5. РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ

Раздел 6. ИННОВАЦИОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

РАЗДЕЛ 4
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

ОСОБЕННОСТИ ЗАЩИТЫ ИНТЕРНЕТ-ПЛАТЕЖЕЙ

А. А. Агибалов, С. М. Полухин
руководитель – старший преподаватель ***О. В. Криволапова***
Северо-Кавказский федеральный университет, г. Ставрополь

Безопасность платежей не только влияет на владельца карты, который производит оплату товаров в интернет-магазине, но и на сам интернет-магазин и наконец, на платежные системы, которые вкладывают огромные суммы для защиты от мошенничества.

Ключевые слова: SSL, аутентификация, шифрование, безопасная оплата.

Методы, организованные участниками электронной торговли для обеспечения безопасной оплаты в Интернете, всегда были весьма разнообразными.

Прежде всего, это обучение пользователей карт основным навыкам, гарантирующим их собственную безопасность: использование только проверенных Интернет-ресурсов, изучение способа доставки товаров и предоставления услуг, контроль использования сертифицированных протоколов Интернет-торговли, обеспечивающий безопасность информации. Помимо таких не сложных методов защиты от мошенничества, как обучение пользователей, несомненно, используются и технологические методы защиты.

Широко распространенный протокол Secure Sockets Layer (SSL), который является практически обязательным для онлайн-торговли, позволяет всем участникам торгов безопасно передавать даже самую конфиденциальную информацию. Когда злоумышленник пытается перехватить данные, они скрыты специальным шифром, который очень трудно взломать и часто совершенно невозможно.

Протокол SSL обеспечивает безопасный обмен данными из-за следующих двух элементов:

1. Аутентификация.
2. Шифрование.

SSL использует асимметричную систему шифрования для аутентификации ключей при обмене ими, симметричного шифра для обеспечения конфиденциальности и кодов аутентификации для целостности сообщений.

Протокол SSL обеспечивает «безопасный канал», который включает в себя три основных свойства:

1. Канал закрыт. Шифрование используется для всех диалоговых сообщений, предназначенных для идентификации секретного ключа.
2. Канал аутентифицирован. Серверная сторона диалога всегда аутентифицирована, и клиентская сторона определяет это автоматически.
3. Канал надежный. Сообщения включают проверку целостности.

Преимущество SSL заключается в том, что он не зависит от протокола приложения. Такие протоколы, как HTTP, FTP, TELNET и т. д., могут работать вместе с SSL-протоколом, при этом совершенно открыто, то есть протокол SSL может выбрать алгоритм шифрования и ключ сеанса, а также выполнить аутентификацию до принятия или передачи первого байта сообщения.

Протокол SSL использует криптографию и цифровые сертификаты с открытым ключом для идентификации серверов, участвующих в транзакции, и для защиты данных во время передачи с одной страницы на другую через Интернет. Транзакции, использующие SSL, не выполняют аутентификацию клиента. Во-первых, клиент отправляет сообщение серверу. Сервер отвечает и отправляет свой цифровой сертификат клиенту для идентификации. Перед возобновлением транзакции клиент и сервер согласовывают ключи сеанса. Ключи этого сеанса являются симметричными, частными и используются только в этой транзакции. После выбора ключей сеанс продолжается между клиентом и сервером ключей сеанса с цифровыми сертификатами.

Хотя протокол SSL надежно защищает информацию, передаваемую в Интернете, он не может хранить личную информацию, содержащуюся на сервере продавца, такую как номера кредитных карт. Если продавец получает информацию о кредитной карте вместе с запросом на покупку, информация дешифруется и сохраняется на сервере до тех пор, пока запрос не будет завершен. Если сервер не защищен и данные не зашифрованы, возможен несанкционированный доступ к конфиденциальной информации о клиенте.

Наряду с протоколами шифрования для передачи данных участники Интернет-торговли часто используют такие широко известные способы идентификации владельца карты, как использование кода CVV2 / CVC2 (код CVV2 для карт Visa и CVC2 для MasterCard).

Конечно, всех этих мер безопасности определенно недостаточно для обеспечения высокого уровня безопасности электронной торговли в Интернете. Совершенно верно, что процент Интернет-торговли постоянно растет из года в год, объем товаров и услуг в сети растет, а с ними растет число мошеннических транзакций, но мало кто хочет отказаться от Интернет-торговли, поэтому все участники этого процесса все больше обеспокоены безопасностью платежей и расчетов.

Литература

1. Безопасность платежей в Интернете / автор И. Голдовский. Изд-во: Питер; Серия: Электронная коммерция. 2006. 240 с.
2. Журнал «Мир электронной коммерции».

КОМПЛЕКСНАЯ ОЦЕНКА УЯЗВИМОСТЕЙ ИНФОРМАЦИИ В ЗОНЕ ДЗУ СЕТЕВОЙ ФАЙЛОВОЙ СИСТЕМЫ

А. А. Александров, Н. А. Топорков

Северо-Кавказский федеральный университет, г. Ставрополь

В ходе исследования проведена комплексная оценка уязвимостей информации в зоне ДЗУ сетевой файловой системы, проведен анализ типовых нападений на зону ДЗУ сетевой файловой системы. На основе полученных результатов предложены рекомендуемые рубежи защиты.

Ключевые слова: информационная безопасность, ДЗУ, нападения, утечка данных, информация, защита, сетевая файловая система, оценка уязвимостей.

В современном мире широкое распространение получили сетевые технологии. Они используются как частными лицами для познавательно-развлекательных целей, так и компаниями для обмена различного рода информацией. В ходе эксплуатации сетевых технологий для обмена данными встал вопрос удобства передачи и хранения данных, которые могли бы быть использованы разными людьми в одной сети. Для решения этого вопроса был придуман File Transfer Protocol (FTP) сервер. Он позволял скачивать и загружать на него информацию, но не позволял обрабатывать ее непосредственно на нем, что приводило к большим временным затратам.

Этих недостатков были лишены Network File System (NFS) сервера, которые могли быть подключены к компьютерам конечных пользователей, но при этом компьютер воспринимал информацию на нем так, словно это еще один жесткий диск внутри его корпуса. Это позволило значительно облегчить и ускорить обмен и обработку данных в современных сетях.

С развитием сетевых технологий были выявлены множество различных угроз информации, приводящих к её утечке\искажению, в то числе и в NFS. Так как, последние используются почти в каждой корпоративной сети, было необходимо произвести исследования основных угроз и найти способы противостоять им. Существуют различные виды угроз для различных контуров сети. Далее будут рассмотрены основные угрозы сетевой файловой системы в зоне долговременного запоминающего устройства (ДЗУ).

Основными видами угроза сетевой файловой системы в зоне ДЗУ являются:

1) загрузка с несанкционированного носителя;
2) прямой доступ к информации на носителе;
3) перехват информации.

Под загрузкой с несанкционированного носителя подразумевается возможность обхода встроенных сетевых средств защиты файлов путем загрузки с недоверенной операционной системы, которая позволит видоизменять файлы на доверенном ДЗУ или же заносить на него вредоносное ПО.

Данную угрозу можно нейтрализовать несколькими способами: средствами доверенной загрузки, например, Secret Net, блокировка недоверенных устройств при помощи антивирусного ПО, а также ограничением физического доступа к устройству.

Под прямой доступ к информации на носителе подразумевается возможность прочтения информации на носителе, например при похищении ДЗУ.

Данная угроза нейтрализуется шифрованием данных на ДЗУ любым из известных методов. Это может быть, как встроенное шифрование на системах Windows и Unix, так и отдельные шифрование специализированными программными продуктами.

Под угрозой перехвата информации подразумевается возможность считывания информации на выходе серверного или клиентского оборудования, а также перехвата информации во время её транспортировки по линиям связи.

Чтобы избежать этого типа атак необходимо: реализовать end-to-end шифрованные при передаче данных от сервера к клиенту и обратно, что позволить избежать легкого прочтения данных при реализации атаки. Так же необходимо максимально снизить паразитное электромагнитное излучение, что так затруднит попытку перехвата информации.

На основе проведенного исследования были выявлены возможные нападения на зону ДЗУ сетевой файловой системы и необходимые меры для нейтрализации этих угроз.

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М: «Гелиос АРВ», 2010. 336 с.

2. Сагдеев К. М. Физические основы защиты информации: учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург, 2017.

3. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В. С. // Известия ЮФУ. Технические науки. 2009. С. 172-176.

4. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Информационное противодействие угрозам терроризма, 2010. С. 114-118.

5. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.

6. Чипига А. Ф. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев // Фундаментальные исследования, 2015. С. 759.

7. Securelist. Лаборатория Касперского. [Электронный ресурс] URL: https://securelist.ru/spam-and-phishing-in-2017/88630/

8. Infowatch. Аналитика. [Электронный ресурс] URL: https://www.infowatch.ru/analytics

РАЗРАБОТКА МОДУЛЕЙ ФОРМИРОВАНИЯ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С УЧЕТОМ КОРРЕЛЯЦИОННЫХ ЗАВИСИМОСТЕЙ ИНФОРМАЦИИ СЛУЖЕБНЫХ ПРОТОКОЛОВ

А. С. Антипов, Е. А. Емельянов, Ю. А. Андрусенко
руководитель – канд. физ.-мат. наук, доцент ***О. В. Малсугенов***
Северо-Кавказский федеральный университет, г. Ставрополь

Определена модель формирования событий информационной безопасности с учетом корреляционных зависимостей информации служебных протоколов.
Ключевые слова: мониторинг и управление инцидентами информационной безопасности, контроль и учет сетевого трафика, SIEM-системы.

Современные тенденции в области защиты информации стимулируют разработчиков систем безопасности охватывать максимально возможный спектр источников исходной информации, необходимой для анализа состояния безопасности, а также источников индикаторов компрометации, профилей и сигнатур известных информационных угроз. Комплексным решением для обеспечения мониторинга инфокоммуникационных систем и анализа событий безопасности в наше время являются SIEM-системы [1, 2].

Анализ промышленных SIEM систем показал, что большинство известных SIEM систем поддерживают ограниченный набор протоколов и стандартов получения исходной информации, а также не имеют возможности интеграции со сторонними базами индикаторов компрометации. Основной вектор направлен на сбор и анализ информации журналов событий серверов и рабочих станций, сообщений DLP, IDS/IPS систем, межсетевых экранов с DPI, пользовательского трафика сетевого, транспортного и прикладного уровней. Таким образом, большая часть служебных протоколов канального и сетевого уровней остаются за пределами внимания SIEM систем. [3,4] Тем не менее, корреляция событий журналов событий, пользовательского трафика и сообщений служебных протоколов позволяет выявить уязвимости и воздействия на телекоммуникационное оборудование, определить несанкционированное использование служебных протоколов.

Перечень наиболее часто используемых служебных протоколов, а также описание уязвимостей этих протоколов представлен в табл. 1.

Таким образом, представленные служебные протоколы используются для проведения атак типа «отказ в обслуживании» (DNS, NTP, GRE, ICMP, xSTP, IGMP), внедрения ложных объектов сети и перенаправления трафика (ARP, OSPF, RIP, DNS, DHCP, DNS), несанкционированного доступа к технологической информации (CDP, LLDP, VTP, SNMP), создания скрытых каналов связи (ICMP, DNS. [3, 5].

Таблица 1

Уязвимости наиболее часто используемых служебных протоколов стека TCP/IP

Протокол	Название атаки	Описание уязвимости
xSTP	BPDU flood	Отправка ложных BPDU фреймов об изменении топологии на канальном уровне с целью отказа в обслуживании коммутационного оборудования
ARP	ARP-spoofing	Перенаправление трафика через хост злоумышленника с помощью отправки ложного ARP-ответа
	Переполнение CAM-таблицы	Злоумышленник путем отправки большого количества кадров с произвольными MAC-адресами отправителя и получателя переводит коммутатор в режим концентратора.
ICMP	Сканирование сети	Использование некоторых типы сообщений для проведения разведывательной деятельности: определения активности хоста, определения маршрутизатора в сети и. т.д.
	Перенаправление трафика	Возможность формирования ложного ICMP-сообщения о перенаправлении маршрута. С помощью отправки такого сообщения злоумышленник может осуществить изменение таблицы маршрутизации уязвимого хоста с целью перенаправления трафика.
	Атаки типа «отказ в обслуживании»	Возможность отправки ICMP сообщений на широковещательные адреса, а также отсутствие аутентификации позволяют проводить атаки, направленные на отказ работы оборудования
	Создание скрытого канала связи	Возможность внедрения любых нужных данных в эхо-пакет и его пересылки на удаленный хост
OSPF	Затопление LSA-пакетами	Злоумышленник отправляет большое количество LSA-сообщений на OSPF маршрутизатор, вызывая тем самым замедление или даже полную неработоспособность маршрутизатора.
	Внедрение ложного объекта сети	Возможность внедрения ложного OSPF маршрутизатора путем отправки некорректных OSPF-пакетов
	Взлом хеша MD5	Возможность взлома пароля с MD5 шифрованием
RIP	Навязывания ложного маршрута	Перенаправление трафика на подконтрольные узлы, путем отправки маршрутизатору ложной информации о маршрутах
	Понижение версии	Возможность отправки ложного сообщения с целью перевода маршрутизатора на использование уязвимой версии протокола
	Взлом хеша MD5	Возможность взлома пароля с MD5 шифрованием
DNS	Подмена DNS-сервера	Создание обманного DNS-сервера, вследствие перехвата запроса
	Отравление DNS-кэша	Замена корректной записи, хранящейся в кэше DNS-сервера, поддельной записью, с целью направления клиента на ложный узел.
	Атака посредством отраженных DNS-запросов	Возможность отправки DNS-запросов с ложным IP-адресом источника на один или несколько сторонних DNS-серверов. В результате источник принимает большой поток DNS-ответов.

Прото-кол	Название атаки	Описание уязвимости
	DNS-flood	Множество хостов злоумышленника посылают массированный поток запросов на целевой DNS-сервер с ложным SRC IP (IP-адрес источника запроса) с целью выведения DNS-сервера.
DHCP	Подмена DHCP-сервера	Навязывание клиентам ложной службы DNS и сервера WINS, а также использование узла или устройства злоумышленника в качестве шлюза по умолчанию.
	DHCP starvation	Возможность исчерпания пула свободных ip адресов посредством смены MAC адреса атакующего устройства и запроса новых адресов
	DHCP spoofing	Возможность отправки большого количества запросов DHCPDISCOVER с целью вывода из строя DHCP сервера.
NTP	NTP-amplification	Злоумышленник отправляет NTP-запросы с ложным IP-адресом источника на один или несколько сторонних NTP-серверов. В результате источник принимает большой поток NTP-ответов
	NTP-flood	Организация большого количества поддельных NTP-запросов с целью вывода из строя NTP-сервера

Детальный анализ в сообщениях служебных протоколов и их корреляция с основным набором информации по событиям позволит повысить уровень выявления аномалий и вредоносного воздействия, а также реализовать дополнительные действия по контролю состояния и безопасности телекоммуникационной сети и информационных систем. На рис. 1 представлена модель формирования событий информационной безопасности с учетом корреляционных зависимостей информации служебных протоколов.

Сбор сетевых пакетов осуществляется на сервере, использующим библиотеку libpcap, модуль tcpdump и модуль анализа пользовательского трафика Snort. Для этого на вход выделенного сетевого интерфейса, настроенного в режиме неразборчивой обработки пакетов, подается поток данных со span-портов коммутаторов с использованием функции «зеркалирования» трафика от определенного VLAN или группы VLAN. Разделение трафика на пользовательский и служебный происходит на этапе его первичной обработки из PCAP файлов. В качестве критерия используется информация из полей EtherType, SSAP, DSAP в зависимости от типа Ethernet-кадра и поля «Protocol» заголовков IP-пакетов. Детектирование аномального пользовательского трафика осуществляется с помощью IPS/IDS системы с открытым исходным кодом Snort на основе разработанных правил обнаружения из разделенных PCAP файлов пользовательского трафика. Сгенерированные IDS/IPS системой Snort журналы уведомлений обнаружения аномального трафика отправляются в модуль анализа и корреляции [6]. Таким образом, база знаний SIEM системы дополнительно обогащается информацией, позволяющей определить состояние телеком-

муникационной инфраструктуры, корректность функционирования и использования служебных протоколов, выявить источники угрозы и несанкционированные каналы передачи информации.

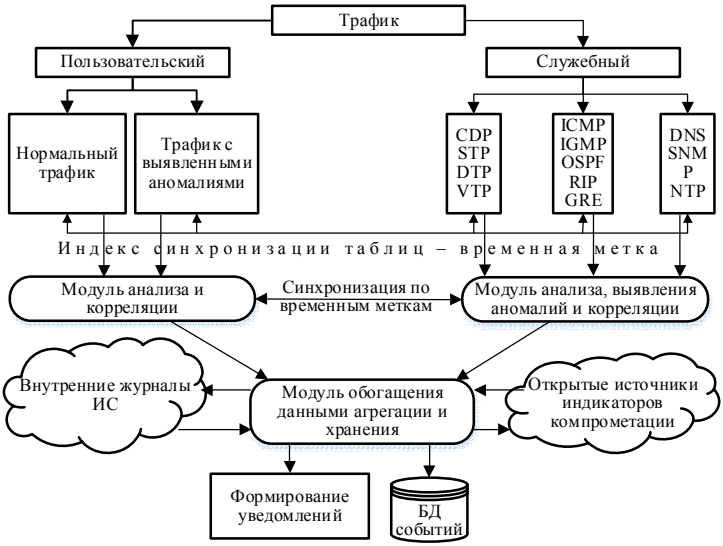


Рисунок 1. Модель формирования событий информационной безопасности с учетом корреляционных зависимостей информации служебных протоколов

Полученные результаты являются основой для дальнейшего изучения трафика служебных протоколов, формирования более точных корреляционных зависимостей событий журналов безопасности, пользовательского и служебного трафика для обнаружения нарушений информационной безопасности.

Литература

1. Обзор мирового и российского рынка SIEM-систем 2017 [Электронный ресурс]: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem#part2, 03.04.18

2. Jeff Edwards 2017 SIEM and Security Analytics Buyer's Guide [Электронный ресурс]: http://solutionsreview.com//dl/2017_Solutions_Review_SIEM_Buyers_Guide_KKM06.pdf, 03.04.18

3. Бирюков А. А. Информационная безопасность: защита и нападение. 2-е издание, перераб. и доп. М.: ДМК Пресс, 2017. 434 с.: ил.

4. Кузнецов А. В., Муравьева Д. С. Создание систем управления событиями и инцидентами ИБ (SIEM) // Журнал "Information Security 2012. № 3. С. 28-29.

5. Норткат Стивен, Новак Джуди Обнаружение нарушений безопасности в сетях, 3-е издание: Пер. с англ. М.: Издательский дома «Вильямс», 2003. 448 с.

6. Dwivedi, Neelam & Tripathi, Aprna. (2015). Event Correlation for Intrusion Detection Systems. Proceedings - 2015 IEEE International Conference on Computational Intelligence and Communication Technology, CICT 2015. 133-139. 10.1109/CICT.2015.111.

ОБЕЗЛИЧИВАНИЕ КАК МЕТОД ПРЕДСТАВЛЕНИЯ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Н. И. Баран-Кешишев, Д. А. Аникин
руководитель – канд. техн. наук, доцент ***Т. В. Минкина***
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье рассмотрены основные проблемы защиты персональных данных. Рассматривается правовая база, регламентирующая правила обработки персональных данных, которая в свою очередь способствует сохранению полноты информации, а также ее конфиденциальности. В результате анализа данной статьи можно сделать вывод, что обезличивание является успешным методом зашиты информации и противодействует утечке персональных данных.

Ключевые слова: информатизация, обезличивание, информационные системы, нормативно-правовая база, анонимность, конфиденциальность, семантичность, несанкционированное использование.

С развитием информатизации современного общества и интеграцией существующих и созданием новых информационных систем, ориентированных на обслуживание граждан, большее внимания уделяется организации обработки персональных данных (ПДн). ПДн составляют достаточно важную часть информационного массива, содержащую сведения о субъектах ПДн. Объединение таких данных в отдельный класс обусловлено особыми требованиями к организации их обработки, связанных с возможностью нанесения ущерба субъектам ПДн.

Поэтому в России развивается и совершенствуется нормативно-правовая база, регламентирующая правила обработки ПДн и реализацию прав граждан на конфиденциальность информации.

Согласно пункту 7 статьи 5 главы 2 ФЗ № 152-ФЗ, Хранение ПДн должно осуществляться в виде, позволяющем определить субъекта ПДн, в той мере, в которой этого требуют цели обработки ПДн. В случае не установления срока хранения ПДн федеральным законом, договором, поручителем или стороной по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению или обезличиванию после достижения целей обработки или в случае утраты необходимости достижении этих целей, если обратное не предусмотрено законом.

Методы и требования обезличивания ПДн, обрабатываемых в информационных системах ПДн, установлены приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 года № 996.

Под обезличиванием ПДн понимаются действия, результатом которых становится невозможность определить принадлежность ПДн конкретному субъекту без использования дополнительной информации.

Обезличивание ПДн, обязано обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки.

Чтобы это реализовать, обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличенных ПДн.

К свойствам обезличенных данных следует отнести:

– структурированность;
– полноту;
– семантичность;
– анонимность;
– применимость;
– релевантность.

Характеристиками методов обезличивания ПДн, определяющими возможность обеспечения заданных свойств, обезличенных данных, являются:

– вариативность;
– обратимость;
– стойкость;
– изменяемость;
– совместимость;
– возможность косвенного деобезличивания;
– параметрический объем;
– возможность оценки качества данных.

Существует ряд методов обезличивания:

– метод декомпозиции;
– метод перемешивания;
– метод изменения семантики или состава;
– метод введения идентификаторов.

Метод введения идентификаторов реализуется путем замена части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия.

Метод перемешивания реализуется путем перемешивания отдельных записей и групп этих записей между собой.

Метод изменения состава или семантики реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта.

Метод декомпозиции реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создание таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением записей, соответствующих этим подмножествам.

Обработка данных включает в себя следующие составные мероприятия:

1. Назначение ответственного сотрудника.

Лицо, ответственное за обработку ПДн (в нашем случае их обезличивание), должно назначаться официальном приказом. После инструктажа

работник подписывает документы о неразглашении конфиденциальной информации.

2. Составление документа о политике в отношении личных данных.

Для чего оператор собирает ПД, где их хранит, в какой срок они должны быть уничтожены и для каких целей применяется обезличивание – ответы на эти и другие вопросы необходимо прописать в документе. Его можно назвать просто «О персональных данных».

3. Получение письменных разрешений владельцев ПД.

4. Следующим организационным документом станет «Распоряжение об обезличивании данных», в нем необходимо прописать выбранный способ обезличивания.

Необходимо провести процедуру и составить акт о выполнении обезличивания. Если речь идет о системе электронных данных, оператору необходимо пройти проверку, после чего класс системы для хранения данных будет понижен.

В заключение можно сделать вывод, что одним из наиболее перспективных и эффективных подходов к защите ПДн в информационных системах является обезличивание. Так как результатом обезличивание ПДн являет не возможность определения принадлежности ПДн конкретному субъекту, то даже при утечке информации вероятность определения принадлежности ПДн конкретному субъекту для дальнейшего неправомерного использования заметно снижается.

Литература

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных"

2. Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных"

3. Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р., Защита персональных данных в организациях. – М.: ФЛИНТА, 2011. – 125 с.

4. Петренко В. И. Мирошников Д. А. Емельянов Е. А. Анализ требований применения систем электронного документооборота // Молодёжный форум: технические и математические науки. Материалы Международной научно-практической конференции, Воронеж, 2015.

5. Петренко В. И., Мирошников Д. А., Емельянов Е. А. Обзор современных средств сетевой защиты информации//Проблемы автоматизации. Региональное управление. Связь и автоматика («ПАРУСА-2015»), Материалы IV Всероссийской научной конференции молодых ученых, аспирантов и студентов, Геленджик, 2015.

6. Донской В.А., Бисюков В.М. Оптимизация процедуры выбора организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных / Сборник научных статей по материалам Всероссийской научно-практической конференции. 2017. С. 58-62.

7. Жук А.П., Петренко В.И., Кузьминов Ю.В., Дорошенко Н.С. Совершенствование математического аппарата синтеза ортогональных дискретных последовательностей для широкополосных беспроводных систем связи//Вестник СевКавГТИ. 2012. № 13. С. 10-15.

АЛГОРИТМ РАБОТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ «АВТОРИЗАЦИЯ ГРАЖДАН»

Р. Г. Белоусов, С. В. Муровятников
Северо-Кавказский федеральный университет г. Ставрополь

Российский рынок систем контроля и управления доступом находится в стадии формирования. Тем не менее, уже существует немало разработок, успешно внедряемых в различных организациях и подразделениях. Системы авторизации существуют, но аналогов мало. Данная система отличается новизной и не высокой стоимостью, поэтому разрабатываемая система имеет практический интерес. В статье приведен алгоритм разрабатываемой системы авторизации граждан для контроля доступа на массовые мероприятия с применением генерации qr кодов из социальных сетей.

Ключевые слова: система авторизации граждан, система контроля управления доступом, защита, авторизация, идентификация.

Российский рынок систем контроля и управления доступом находится в стадии формирования. Тем не менее, уже существует немало разработок, успешно внедряемых в различных организациях и подразделениях.

Системы авторизации существуют, но аналогов мало. Данная система отличается новизной и не высокой стоимостью, поэтому разрабатываемая система имеет практический интерес. Даже в условиях финансового кризиса, данный рынок продолжает формироваться, а темпы роста объемов внедрений только выросли. В настоящее время такой системой заинтересованы государственные органы.

Структура информационной системы «Авторизация граждан» определена требованиями:

- масштабируемость
- интегрируемость с другими информационными системами.

В связи с этим, информационный обмен и взаимодействие между структурными единицами системы происходит в основном через сеть Internet.

К основным структурным единицам данной системы можно отнести:

- сервер базы данных;
- сервер портала регистрации мероприятий;
- сервер регистрации граждан
- клиентский терминал (рабочая станция);
- совокупность автоматизированных рабочих мест.

Принципиальная структурная схема системы отражена на рис.1.

Сервер базы данных выполняет обслуживание и управление базой данных и отвечает за целостность и сохранность данных, а также обеспечивает операции ввода-вывода при доступе к информации.

Основные функции:

– получение данных от сервера портала регистрации и сервера регистрации граждан;

– преобразование полученных данных.

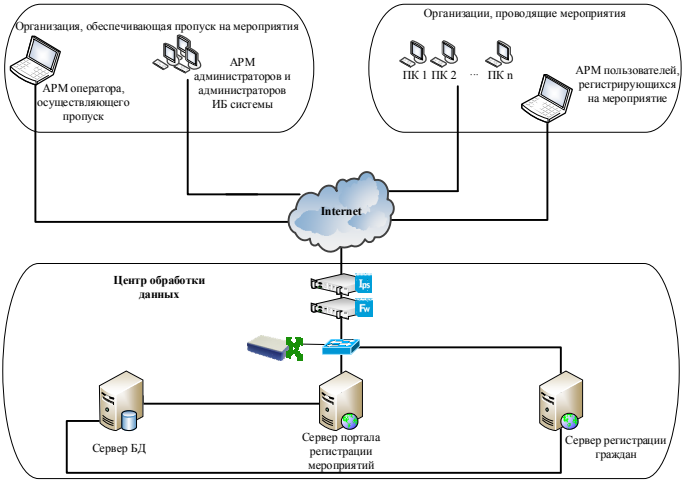


Рисунок 1. Структура системы авторизации граждан для контроля доступа на массовые мероприятия

Сервер может работать с несколькими базами данных, различных клиентов.

Сервер портала регистрации мероприятия служит для регистрации мероприятия на сервере, внесение информации о мероприятии в базу данных и предоставляет информации по запросу от авторизованного автоматизированного рабочего места.

Сервер регистрации граждан предназначен для регистрации людей на мероприятие, созданное в системе и генерации qr кода для пропуска человека на мероприятие.

Автоматизированные рабочие места служат для организации эксплуатации технических и программных средств, контроль работы системы, а также контроль пользователей системы.

Модель взаимодействия системы разработана с учетом уязвимостей, и направлена на минимизацию угроз.

В конечном итоге имеется продукт, направленный на нужды государственных и коммерческих предприятий.

Система является системой контроля и управления доступом и обеспечивает автоматизированный контроль проходов посетителей на территорию объекта по QR-коду и бумажному носителю, изготавливаемому с

применением автоматизированной системой ИС «Авторизация граждан». При изготовлении пропуска, реализуется генерация специального QR-кода, а КПП объекта оснащаются средствами для автоматизированного считывания указанного кода, обеспечивая тем самым учет и идентификацию посетителя при доступе на массовое мероприятие.

При работе с системой реализуется следующий алгоритм:

Регистрация мероприятия в системе «Авторизация граждан». При организации массового мероприятия организатор регистрирует его в системе.

После регистрации в системе – мероприятие вносится в базу данных, где ей присваивается уникальный идентификационный номер и создается уникальная ссылка для регистрации посетителей на мероприятие.

Следующий этап – регистрация участников мероприятия. На данном этапе происходит распространение ссылки на мероприятие для регистрации посетителей. Посетителю предлагается форма для заполнения, в которой необходимо указать фамилию, имя, отчество, указать номер телефона и адрес электронной почты, для отправки сгенерированного QR-кода.

После отправки формы заявки в базу данных сервера вносится информация о посетителе мероприятия и на основе данных происходит генерация уникального идентификатора, на основе которого генерируется QR-код.

Уникальный идентификатор вносится в базу данных с привязкой к конкретному посетителю.

При посещении мероприятия происходит считывание QR-кода, проводится проверка наличия данного QR кода в базе данных, после чего, осуществляется фиксация данных о предъявленном пропуске.

Вывод информации для постового. Одновременно на монитор постового КПП система «Авторизация граждан» выводит признаки, характеризующих результаты проверки наличия информации о пропуске в базе данных, показателей к допуску на объект, а также фамилию, имя, отчество зарегистрированного владельца и его фотографию, если она присутствует.

Разрабатываемая система обеспечит идентификацию посетителей того или иного мероприятия, а также снизит вероятность возникновения террористических актов на мероприятиях.

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М: «Гелиос АРВ», 2010. 336 с.

2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учеб. пособие / А. А. Афанасьев. М.: Горячая линия – Телеком, 2012. 550 с.

3. Исхаков А. Ю. Система двухфакторной аутентификации на основе QR-кодов // Безопасность информационных технологий. 2014 № 3 С. 97–101.

4. Исхаков А. Ю. Методическое и программно-алгоритмическое обеспечение процесса идентификации посетителей в местах массового пребывания людей: автореф. дис. на соиск. учен. степ. канд. тех. наук (05.13.19) Исхаков Андрей Юнусович. Томск, 2015 140 с.

5. Филатова Н. Н. Структурный синтез схем автоматизации в условиях неполных требований к технической реализации / Н. Н. Филатова, А. Г. Требухин // Известия ВолгГТУ. 2012 № 13. С. 72–79.

ПРИНЦИПЫ РАБОТЫ HBM ПАМЯТИ

Э. И. Бережнов
руководитель – старший преподаватель ***О. В. Криволапова***
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье рассмотрены особенности работы технологии HBM, ее особенности и отличия от технологии GDDR5.

Ключевые слова: HBM, GDDR5, AMD, Stack, DRAM, видеопамять, интерфейсы, контроллер, чипы памяти.

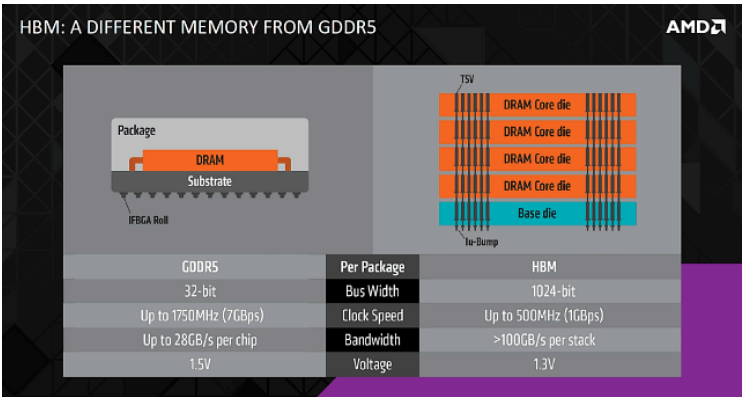
В связи с тем, что дальнейшее развитие и совершенствование GDDR5-памяти и других, подобных ей технологий, сопряжено с большим количеством проблем и сложностей, в последние годы стали появляться «широкие», но медленные интерфейсы. Раньше индустрия шла по пути увеличения частот памяти последовательных интерфейсов, но теперь мы столкнулись с ограничением скорости передачи данных с каждого чипа, а значит нужно переходить к параллельным интерфейсам.

Сравнение HBM и GDDR5.

В отличие от технологии GDDR5, в HBM вместо большого количества быстрых чипов памяти работающих с процессором посредством относительно узкой шины, используют сравнительно медленные чипы памяти, что позволяет увеличить шину в несколько раз. Ширина шины зависит как от конкретного GPU, так и от поколения HBM.

На примере видеоадаптера AMD Fury X, HBM представляет собой многослойную память, разделенную на четыре стека (пачки, стопки), каждый из которых содержит четыре чипа памяти, образующих интерфейс в 1024 бита. Таким образом, общая ширина шины составляет 4096 бит, против 512 бит у GDDR5.

Устройство GDDR5 и HBM



Тем, кто интересуется именно технической стороной вопроса, важно видеть не цифры, а то, откуда эти показатели возникают. Казалось бы, само понятие сверхширокой шины находится где-то на поверхности, но как известно, теория и практика, при близком рассмотрении оказываются вещами, порой, очень разными. Все дело в том, что данная технология вызывает много сложностей, которые раньше не позволяли ее реализовать.

В сравнении со знакомой всем GDDR5, HBM требует гораздо большее количество дорожек на текстолите, в связи с чем возникают проблемы компоновки. Именно из-за проблем с компоновкой, данная технология так сложна в производстве.

Какие же преимущества дает нам технология HBM? На первый взгляд, все кажется просто, благодаря данной технологии увеличивается пропускная способность памяти, но не стоит забывать и о более важных вещах, ведь вместе с тем уменьшается ее размер, снижается энергопотребление, а значит выделяется меньше тепла.

Вывод. Как и любая новая технология, технология HBM еще только выходит на рынок, в связи с чем, не слишком популярна, но имеет большой потенциал и перспективы.

Литература

1. https://www.amd.com - Официальный сайт «AMD».
2. https://www.ixbt.com/video3/amd-hbm.shtml - Интернет ресурс «ixbt».
3. https://ru.wikipedia.org/wiki/GDDR5 - Интернет ресурс «Википедия».

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ПЕРЕГОВОРНОЙ КОМНАТЕ

Т. Б. Блимготов
руководитель – канд. техн. наук, доцент ***В. В. Антонов***
Северо-Кавказский федеральный университет г. Ставрополь

В наши дни особенно актуальна проблема защиты конфиденциальной информации в переговорных комнатах – так называемых выделенных помещениях предприятия. Сегодня можно наблюдать за тем, как все чаще используются переговорные комнаты, ведь каждая крупная фирма встречается с необходимости выделения специально оборудованного помещения для проведения конфиденциальных переговоров. Целью проведения мероприятий по обеспечению безопасности проведения переговоров в переговорных комнатах является исключение доступа злоумышленника к конфиденциальной информации.

В статье разработана модель угроз для конфиденциальной информации и приведены методы обеспечения защиты от несанкционированных действий злоумышленника.

Ключевые слова: выделенное помещение, акустический канал, модель угроз, рекомендации по защите.

Как известно, существует множество различных физических каналов утечки информации, которыми может воспользоваться злоумышленник.

Первостепенными задачами обеспечения безопасности информации являются:

1. Защита от утечки информации по акустическому каналу.
2. Защита от утечки информации по виброакустическому каналу.
3. Защита от утечки информации за счет электроакустического преобразования.
4. Защита от утечки информации за счет ВЧ-навязывания.
5. Защита от утечки информации по оптическому каналу.

В данной статье мы подробно остановимся на акустическом канале утечки информации, так как данный канал наиболее подвержен атакам со стороны злоумышленников.

Модель угроз для информации через акустический канал утечки

Злоумышленник может осуществить несанкционированный доступ к конфиденциальной информации по акустическому каналу утечки информации:

– при помощи непосредственного прослушивания;
– при использовании технических средств.

Доступ к информации злоумышленника посредством прослушивания может быть осуществлен следующими способами:

– сквозь открытое окно;
– сквозь дверь;
– через вентиляционные каналы;
– сквозь стены, перегородки.

Следует подметить, что осуществить доступ к информации по акустическому каналу утечки не составляет труда, так как помещение имеет много уязвимостей.

Злоумышленник может использовать специальные технические средства – микрофоны различных типов. К таким специальным средствам относятся:

– направленные микрофоны;
– проводные микрофоны;
– радиомикрофоны;
– устройство «Электронное ухо».

Рекомендации по защите

При разработке рекомендаций по защите следует ожидать, что злоумышленник – хорошо подготовленный человек.

Поэтому необходимо разработать и реализовать комплекс мероприятий, обеспечивающих надежную защиту во время ведения переговоров.

1. Особо важным аспектом является выбор места для переговорной комнаты. Ее рекомендуется разместить по возможности на верхних эта-

жах. Желательно, чтобы окна переговорной комнаты выходили во двор, или же отсутствовали вовсе.

2. Вход в переговорную комнату следует оборудовать тамбуром, внутренняя сторона которого должна быть оббита звукоизоляционным материалом. Технология не должна допускать даже значительных щелей, так как они значительно снижают звукоизоляцию.

3. При наличии в комнате для переговоров вентиляционных каналов, необходимо оборудовать их специальными, позволяющими закрывать отверстие вентиляционного канала при ведении переговоров.

4. При наличии окон в переговорной комнате, следует принять следующие меры предосторожности:

– проведение переговоров должно осуществляться при закрытых форточках.

– на окнах должны иметься шторы либо жалюзи.

– оконные стекла должны быть оборудованы вибродатчиками.

5. Для защиты переговорной комнаты от проводных микрофонов, рекомендуется использовать специальные технические средства. К таким техническим средствам относится генератор типа «Соната-С1», эффективно выполняющий функции защиты.

Важно периодическое проведение специальных обследований и аттестаций, призванное осуществлять контроль состояния безопасности в переговорной комнате. Это обусловлено возможностью злоумышленника при случайном нарушении целостности системы защиты воспользоваться «брешью» и осуществить несанкционированный доступ к конфиденциальной информации.

Таким образом, предложенные рекомендации позволят обеспечить безопасность переговоров, проводимых в специально выделенных для этой цели помещениях. Для повышения стойкости переговорных комнат к действиям злоумышленников рекомендуется комбинировать меры защиты, тем самым осложнив злоумышленнику задачу преодоления защитных мер.

Литература

1. URL – http://bre.ru/security/11635.html

2. Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия. М.: Дашков и К, 2006.

3. URL - http://studbooks.net/2197138/informatika/zaschita_informatsii_vydelennyh_pomescheniyah.

ЗАЩИТА ОТ ПРОСЛУШИВАЮЩИХ УСТРОЙСТВ

Т. Б. Блимготов
руководитель – канд. техн. наук, доцент ***В. Е. Рачков***
Северо-Кавказский федеральный университет, г. Ставрополь

Защита бизнеса или же персональной информации – залог успешности любого мероприятия. Однако в современном мире десятки недоброжелателей, конкурентов или же просто корыстных людей, применяют различные технологические устройства для получения конфиденциальной информации третьих лиц. Вероятность утечки коммерческих данных становится все более распространенной в современном бизнесе, не всегда опирающемся на закон, авторские права и добропорядочность. Проверка на прослушку помещения требует индивидуального и комплексного подхода, позволяющего гарантированно выявлять и устранять каналы утечки.

Целью проверки помещений на предмет наличия прослушивающих устройств является исключение возможности получения информации конфиденциального характера злоумышленником, а следовательно возникновению убытков, связанных с этим. В статье будет разработан план мероприятий по поиску и устранению прослушивающих устройств.

Ключевые слова: прослушивающие устройства, утечка, жучки, закладки.

Описание проблемы

Несанкционированный доступ к конфиденциальной информации на предприятии может быть осуществлен при помощи установки в помещении скрытых видеокамер, или же установке шпионского ПО в компьютер пользователя. Но на практике все чаще всего сводится к прослушке – эффективном методе скрытной записи разговоров или же мониторинга в реальном времени. Особенность заключается в том, что прослушивающее устройство может быть доставлено в помещение любым человеком и может не требовать особой установки. Так же «жучок» может быть замаскирован под какой-либо предмет.

В данной статье мы рассмотрим несколько действенных рекомендаций и полезных советов по защите помещения от жучков.

Рекомендации по проверке помещений на наличие «жучков»

Прежде чем приступить к разработке рекомендаций по проверке помещений на наличие прослушивающих устройств, следует отметить, что практически все они делаются вручную. Каждый отдельно взятый «жучок» оригинален и уникален. Это осложняет задачу поиска.

Следует придерживаться следующих рекомендаций, которые являются универсальными:

– необходимо тщательно исследовать всякого рода розетки (как электрические, так и телефонные), провода и другие предметы, способные предоставить постоянный источник питания прослушивающему устройству. Жучки, имеющие источник питания, такого рода могут работать постоянно и бесперебойно, в отличие от шпионских устройств на батарейках.

– следует внимательно осматривать все подарки, которые попадают в помещение от клиентов, партнеров по бизнесу или коллег. Довольно часто под видом подарка преподносится прослушивающее устройство. Такой жучок может оставаться без внимания годами, передавая конфиденциальную информацию злоумышленнику.

– следует внимательно относиться к случайно забытым в помещении вещам, а также случайно появившимся предметам. Распространена ситуация, в которой злоумышленник может подкинуть прослушивающее устройство под видом случайно оставленного предмета (ручки, флешки), или же заменяют предмет, находившийся в помещении таким же, но с жучком внутри. Отличить предмет с закладкой по внешнему виду невозможно.

– не следует озвучивать конфиденциальную информацию в помещении, если нет уверенности что оно безопасно. Для проведения конфиденциальных переговоров следует использовать специально подготовленные переговорные комнаты.

Таким образом, чтобы минимизировать возможность утечки конфиденциальной информации благодаря прослушивающему устройству, следует придерживаться вышеперечисленных рекомендаций. Стоит добавить, что следует периодически проводить проверки помещений на наличие жучков. Лучше всего предоставить это профессионалу. Так же при проверке следует максимально сузить круг лиц, присутствующих в это время в помещение, во избежание «заметания» следов злоумышленником.

Литература

1. URL - http://www.shpionam.net/recomend-po-proverke-ghuchkov.htm
2. URL - http://audiospy.ru/rec_articles/proslushivayuwie_ustrojstva/
3. URL - https://www.forter.com.ua/experts/kak-najti-proslushku-amatorskie-i-professionalnye-sposoby-obnaruzhenija-zhuchkov/

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПЛАТЁЖНОЙ СИСТЕМЫ

М. А. Брехов
руководитель – канд. техн. наук, доцент ***В. В Антонов***
Северо-Кавказский федеральный университет, г. Ставрополь

На сегодняшний день остается ряд спорных вопросов по обеспечению безопасности электронных платежных систем, поэтому для нормальной работы она должна иметь высокий уровень защищенности. С появлением электронных платежных систем вопрос обеспечения безопасности в платежных системах стоял не так глобально, как сейчас. Целью статьи является исследование обеспечения системы защиты электронных банковских услуг.

В соответствии с этим, сформулированы и решены следующие задачи исследования:

1) изучение статистики ущерба от случаев мошенничества с банковскими картами в России;

2) рассмотрение видов мошенничества с пластиковыми картами;

3) выявление мер защиты информации с банковскими картами;

4) предложение путей совершенствования системы электронных платежей.

Ключевые слова: система безналичных расчетов, пластиковая карта, банковская карта, банковские операции, информационная безопасность, электронные платежи, шифрование операции, интернет-мошенничество, легитимная пластиковая карта.

Система безналичных расчетов с помощью пластиковых карт называется электронной платежной системой [1]. Банковская карта – пластиковая карта, привязанная к расчётным счетам в банке и использующаяся для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных. Банковские операции, сделки с денежными средствами и взаимные платежи нельзя представить без расчетов с использованием пластиковых карт.

Наиболее уязвимым местом в системе электронных платежей является передача платежных и иных сообщений между банками, банком и банкоматом, банком и клиентом [2].

Нужно отметить тот факт, что тема информационной безопасности в контексте дистанционных банковских услуг затрагивается все чаще. На данный момент важнейшим является вопрос об эффективном совершенствовании банковских систем.

Проанализировав данные статистики, касающиеся ущерба от случаев мошеннических операций, нужно сказать, что, как таковой фактической статистики по мошенничеству с банковскими картами в нашей стране нет. Во-первых, это связано с тем, что банки не хотят демонстрировать свои потери от злоумышленников. А во-вторых, граждане наиболее часто отказываются от обращений в полицию, чтобы зафиксировать факт происшествия.

Исходя из этого, можно сказать, что статистика бывает как официальной, по данным министерства внутренних дел, так и неофициальной, полученная от должностных лиц. Статистика ущерба от случаев мошенничества с банковскими картами (табл. 1) [7].

Таблица 1

Статистика ущерба от случаев мошенничества с банковскими картами

Год		2009	2010	2011	2012	2013
Ущерб, (руб.)	Официальные данные МВД	77,2 млн	38,6 млн	32,2 млн	140 млн	150 млн
	Неофициальные данные	1,25 млрд	1,46 млрд	2,7 млрд.	3,6 млрд	4,6 млрд

Полагаясь на данные (табл. 1) можно отметить, что официальные и неофициальные данные отличаются друг от друга. Но даже несмотря на это стоит отметить, что с каждым годом наблюдается рост убытков, по сравнению с предшествующими годами. Всё это, безусловно, связано с тем, что количество пользователей карт становится с каждым годом больше.

Для обеспечения нормальной работы электронная платежная система должна быть надежно защищена.

Меры защиты делятся на два типа: внутренние и внешние. К внутренним мерам безопасности относят механизмы защиты, которые осуществляются со стороны платежной системы без участия пользователя [1].

К внешним мерам безопасности относят все действия пользователя, осуществляемые им для защиты своих финансов [1].

Для совершенствования информационной системы, в первую очередь, необходимо повысить эффективность обеспечения безопасности пластиковых платежных средствах с помощью технологических и организационных методов защиты [6].

Банкам следует совершенствовать механизмы защиты банкоматов: периодически изменять конфигурацию, увеличивать количество камер видеонаблюдения, производить установку банкоматов в общественных местах и крупных учреждениях [3].

Таким образом, для повышения эффективности механизмов защиты следует вести работу с владельцами банковских карт, ведь их бдительность поможет избежать потерь денежных средств. Уровень обеспечения безопасности банковской системы зависит от «честности» граждан, принимающих участие в финансовых отношениях, эффективности работы службы безопасности кредитных организаций, профессионализма сотрудников правоохранительных служб, задачей которых является предупреждение и выявление мошенничества в сфере банковских услуг, а также объема разъяснительной работы с владельцами пластиковых карт.

Литература

1. https://vkoshelek.com/bezopasnost-pri-rabote-s-elektronnymi-platezhnymi-sistemami-pravila-i-sovety-novichkam/

2. https://studfiles.net/preview/299340/

3. https://fundamental-research.ru/ru/article/view?id=38141

4. https://cyberleninka.ru/article/n/informatsionnaya-sistema-opredeleniya-moshennichestva-po-platezhnym-kartam-v-rezhime-realnogo-vremeni

5. http://docplayer.ru/63915641-Ekonomicheskie-nauki-problemy-bezopasnosti-raschetov-plastikovymi-kartami.html

6. http://arhivinfo.ru/2-89747.html

7. https://applied-research.ru/ru/article/view?id=6598

ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ В 2018 ГОДУ

А. С. Борисенков
руководитель – канд. техн. наук, доцент ***В. В. Антонов***
Северо-Кавказский федеральный университет, г. Ставрополь

Киберпреступники постоянно находят новые методы и средства для совершения кибератак. В данной статье рассмотрены основные виды киберугроз, с которыми могут столкнуться пользователи по всему миру и методам борьбы с ними. Проведен анализ отчета мониторинга информационной безопасности за 2017 год, выявлены развивающиеся угрозы, которые могут стать значимыми в 2018 году.

Ключевые слова: киберугрозы, вредоносное программное обеспечение, автоматизированное рабочее место, вирусы-шифровальщики, криптомайнинг, WannaCry, Petya/notPetya, удаленный браузер.

Изучив наиболее подверженные атакам злоумышленников сегменты сети за прошлый год (рис. 1) можно сделать вывод, что приоритетными целями являются простые пользователи автоматизированного рабочего места (АРМ) [1, 2].

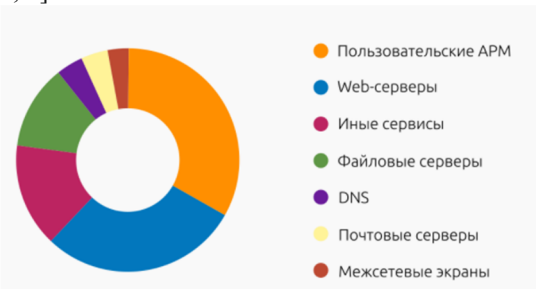


Рисунок 1. Топ подверженных инцидентам сегментов информационной безопасности за 2017 год

Самым большим классом является вредоносное программное обеспечение (ВПО) (рис. 2) [1]. За 2017 год наблюдались следующие тенденции:

1. Происходило заражение АРМ семейством вредоносов WannaCry и Petya/notPetya.

2. Появились новые виды ВПО, в котором используются компоненты WannaCry.

3. Рост ВПО для майнинга криптовалют увеличился в несколько раз.

Наиболее приоритетными направлениями для злоумышленников стали программы вымогатели и программы для майнинга криптовалют.

1) WannaCry и Petya/notPetya являются наиболее яркими представителями вирусов вымогателей. Вымогатель представляет собой относительно простую форму вредоносной программы, шифрующей файлы на целевом

компьютере и требующей выкуп за ключи расшифровки. Процент выплаченных выкупов достаточно высок, так как в большинстве случаев жертвы не имеют в своем распоряжении резервных копий.

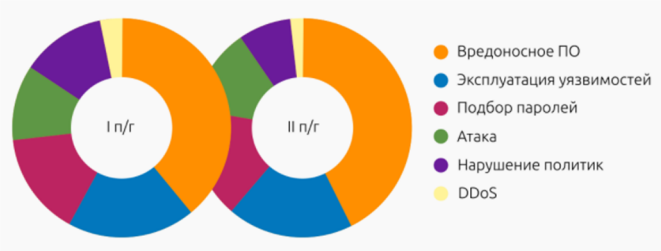


Рисунок 2. Статистика по классам инцидентам угроз информационной безопасности за 2017 год

Для борьбы с вирусами-шифровальщиками есть два наиболее эффективных способа:

1. Регулярно делать резервные копии всех важных файлов, при этом желательно, чтобы у вас было два бэкапа: один в облаке, а другой на сменном носителе.

2. Регулярно устанавливать обновления операционной системы (ОС), браузера, антивируса и другого программного обеспечения (ПО).

2) Майнинг криптовалюты. Киберпреступники, в последнее время нацеливаются на владельцев биткойнов и других цифровых валют. Однако более серьезной угрозой является кража вычислительной мощности компьютера. Такое положение вещей побуждает хакеров компрометировать миллионы компьютеров, чтобы использовать их для майнинга.

Для предотвращения вредоносного криптомайнинга также можно выделить два наиболее эффективного способа:

1. Использование удаленного браузера. Технология изоляции удаленного браузера (RBI) предлагает виртуальный браузер, который находится в одноразовых контейнерах вне сети. Для пользователей браузер выглядит как их обычный Firefox, Chrome, Opera или Edge и обеспечивает те же функции.

2. Программная защита. Защиту от несанкционированного майнинга можно реализовать также на самих устройствах или на уровне корпоративной сети, например, с помощью антивирусных программ или шлюза сетевой безопасности. Производители антивирусных программ и сетевых шлюзов сейчас встраивают функции детектирования криптомайнинга.

Таким образом, в 2018 году самыми опасными угрозами станут вирусы шифровальщики и майнеры криптовалют. Именно с этих направлений будут происходить основные угрозы для информации пользователей. Следует пользоваться качественным антивирусом, своевременно обновлять ПО и с осторожностью выходить в сеть интернет.

Литература

1. https://habrahabr.ru/company/pm/blog/349000/
2. https://habrahabr.ru/company/pm/blog/326810/
3. https://www.anti-malware.ru/analytics/Threats_Analysis/six-cyber-threats-to-really-worry-about-in-2018
4. https://www.anti-malware.ru/analytics/Threats_Analysis/cryptojacking-new-threat
5. https://www.anti-malware.ru/analytics/Technology_Analysis/technologies-that-could-win-the-battle-against-cybercrime

ТЕХНОЛОГИИ, СПОСОБНЫЕ ПОБЕДИТЬ КИБЕРПРЕСТУПНОСТЬ

А. С. Борисенков
руководитель – канд. техн. наук, доцент ***В. Е. Рачков***
Северо-Кавказский федеральный университет, г. Ставрополь

С развитием информационной безопасности (*ИБ*) *появляются все новые способы, позволяющие контролировать киберпреступность. В данной статье рассмотрены технологии, применяя которые можно свести на нет киберпреступность. Приведены значимые виды угроз, а также технологии для борьбы с ними.*

Ключевые слова: аналитика, вредоносные программы, вирусы-вымогатели, вирусы-шифровальщики, DDoS-атаки, уязвимости программ, кража личности, машинное обучение.

Сегодня интернет изобилует ресурсами, посвященным способам и технологиям предотвращение кибератак. Изучив их можно сделать вывод, что приоритетными являются три направления:

1. Предотвращение атак нулевого дня (0-day). Атаки нулевого дня являются самой опасной формой кибератак. Они используют не устранённые уязвимости, а также вредоносные программы, против которых еще нет методов защиты. Это значит, что антивирусы и брандмаузеры не могут защитить предприятие от таких атак. По мнению организаций и предприятий в области защиты информации для противодействия вредоносным программам и устранения уязвимостей в системе необходимо использовать машинное обучение как долгосрочное решение проблемы 0-day-атак. Система, построенная на машинном обучении, мониторит сайты даркнета, на которых злоумышленники создают, а затем модернизирую вредоносные программы. В среднем в неделю на таких сайтах обнаруживается до 305 высокоприоритетных предупреждений об угрозах. Другой способ предотвращения атак нулевого дня можно рассмотреть на основе Chronicle, компании организованной Google X обеспечивающей защиту информации [2]. Эта компания фокусируется на обнаружении угроз на крупных предприятиях путем хранения и анализа данных, связанных с безопасностью. Используя развитую инфраструктуру Google, Chronicle может быстро обна-

руживать угрозы и делать это в более широких масштабах, чем существующие системы.

2. Самостоятельная идентификация. Сейчас в сети интернет существует множество онлайн-сервисов, а также государственных онлайн-услуг, которые собирают личную и финансовую информацию граждан. Из-за этого стало возможным такое понятие, как «кража личности». Кража личности – означает незаконное использование чужих персональных данных для получения выгоды. Выделяют несколько способов, благодаря которым злоумышленники могут получить необходимые для них данные: взлом и хищение баз данных у государственных структур, получение информации из социальных сетей, заражение устройств вредоносными программами, а также физическая кража документов. Однако самым эффективным способом является компрометация крупного хранилища, которое содержит огромное количество данных пользователей. Для защиты персональных данных можно использовать такую технологию блокчейн, как Decentralized.id (DID), позволяющую пользователям хранить личную информацию в децентрализованной публичной записи. Для того, чтобы получить доступ к своим данным, а затем воспользоваться услугами онлайн сервиса, гражданам необходимо подтвердить свою личность с помощью личного устройства. Модель self-sovereign identity будет хранить ваши данные в неизменном блокчейне. Такая информация, как паспортные данные или банковские реквизиты хранятся в зашифрованном виде, а платформы вроде DID позволяют управлять вашими идентификаторами и использовать их для различных транзакций, например, для входа в веб-сервисы или покупок.

3. Противодействие DDoS-атакам. DDoS-атаки являются самыми распространенными формами кибератак. Эта технология представляет собой атаку, которая происходит сразу с многих компьютеров, задачей которой является выведения из строя сервера за счет огромного количества запросов, которые он не может обработать. Данная киберугроза влечет за собой потери доходов, а также создает возможность для дальнейших нарушений, таких как заражение вредоносными программами, или утечка информации. Результатом может быть потерянная репутация компании. По данным «Лаборатории Касперского», поставщики услуг DDoS-as-a-service получают до 95 процентов прибыли на веб-рынках «глубокой сети». Для того, чтобы противостоять таким атакам можно использовать DDoS-фильтр – это программно-аппаратный комплекс, отсеивающий «мусорный» интернет-трафик, который формируют организаторы DDoS-атак. Из-за его дороговизны целесообразней использовать специальные сервисы, например Cloudflare или Incapsula. Помимо этого, существуют услуги веб-хостинга, которые обеспечивают защиту от DDoS на уровне сети, а также позволяют блокировать трафик из подозрительных источников.

Таким образом, специалистам в области защиты информации необходимо применять активный подход к кибербезопасности. Предприятиям нужно уделить особое внимание машинному обучению и защите сети от DDoS атак, а онлайн сервисам переходить на технологии блокчейна. Применяя отмеченные технологии для борьбы с киберпреступностью можно со временем свести на нет ее основные проявления.

Литература

1. https://www.anti-malware.ru/analytics/Technology_Analysis/technologies-that-could-win-the-battle-against-cybercrime#part2
2. https://chronicle.security/technology/
3. https://www.anti-malware.ru/analytics/Threats_Analysis/protection-against-zero-day-vulnerabilities#part2
4. https://www.anti-malware.ru/threats/identity-theft
5. https://www.anti-malware.ru/analytics/Threats_Analysis/what-is-a-ddos-attack#part1
6. https://habr.com/company/hosting-cafe/blog/324848/

ВИДЫ МЕЖСЕТЕВЫХ ЭКРАНОВ ИХ РАЗЛИЧИЯ И ПРИМЕРЫ ПРИМЕНЕНИЯ

Г. В. Бушной
руководитель – преподаватель ***В. А. Гогуля***
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье описаны отличительные черты межсетевых экранов относительно других сетевых устройств. Будут даны базовые знания о межсетевых сетях, их особенностях, различиях, преимуществах и недостатках, а также реальные примеры их применения.

Ключевые слова: Firewall, шлюзы, сети, межсетевые экраны, фильтры, хост, маршрутизатор, прокси.

Межсетевой экран (сетевой экран) – специализированный программный или программно-аппаратный элемент компьютерной сети, который осуществляет фильтрацию и контроль сетевого трафика, проходящего через него, в соответствии с заданными правилами. Межсетевой экран так же ещё называют Firewall иди Брандмауэр.

Основной задачей межсетевых экранов является защита сегментов сети или отдельных хостов от несанкционированного доступа в протоколах сетевой модели OSI (от англ. open systems interconnection basic reference model, что в переводе означает Базовая Эталонная Модель Взаимодействия Открытых Систем) посредством использования уязвимых мест или же в программном обеспечении, установленном на компьютерах сети.

Маршрутизаторы можно считать первой программно-аппаратной реализацией межсетевого экрана. Маршрутизатор – это устройство, пересы-

лающее пакеты между различными сегментами сети на основе правил и таблиц маршрутизации. Маршрутизатор может связывать различные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором. Маршрутизаторы работают на «сетевом» -третьем уровне сетевой модели OSI. Принцип работы маршрутизатора заключается в том, находящиеся что маршрутизатор использует адрес получателя указанный в заголовке пакета, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса, нет описанного маршрута, пакет отбрасывается.

Программные межсетевые экраны появились намного позже и являются более молодым средством защиты, нежели антивирусные программы. Например,проект Netfilter/iptables (одиниз первых программных межсетевых экранов, встраиваемых в ядро Linux с версии 2.4), который был основан в 1998 году. Такое «позднее» появление было обусловлено тем, что, антивирус достаточно долго решал проблему защиты персональных компьютеров от вредоносных программ. Однако в конце 1990-х вирусы стали очень активно использовать уязвимость в виде отсутствия межсетевых экранов на компьютерах, что привело к увеличению интереса пользователей к данному классу устройств.

Существует несколько различных классов межсетевых экранов, каждый из которых выполняет свою функцию:

1. **Фильтрующие маршрутизаторы**. Они представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать исходящие и входящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов. Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета: IP-адрес отправителя; IP-адрес получателя; порт отправителя; порт получателя. Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации. Фильтрация может быть реализована различными способами для блокирования соединений с определенными компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех компьютеров и сетей, которые считаются враждебными или ненадежными.

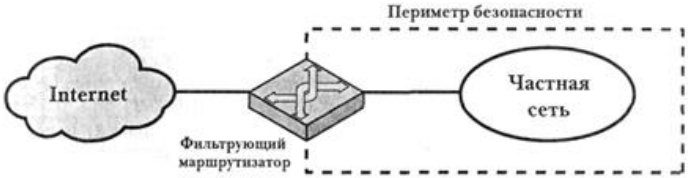


Рисунок 1. Фильтрующий маршрутизатор

Правила фильтрации пакетов формулируются сложно и обычно не существует средств для проверки их корректности, кроме ручного тестирования. При этом в отсутствие фильтрующего маршрутизатора средств протоколирования такие пакеты не смогут быть выявлены до обнаружения последствий проникновения. Даже если администратору сети удастся создать эффективные правила фильтрации, их возможности останутся ограниченными. Например, администратор задает правило, в соответствии с которым маршрутизатор будет отбраковывать все пакеты с неизвестным адресом отправителя. Однако в данном случае хакер для проникновения внутрь защищенной сети может осуществить атаку, которую называют подменой адреса. В таких условиях фильтрующий маршрутизатор не сумеет отличить поддельный пакет от настоящего и пропустит его.

К положительным качествам фильтрующих маршрутизаторов можно отнести следующие: сравнительно невысокая стоимость; гибкость в определении правил фильтрации; небольшая задержка при прохождении пакетов.

Недостатки фильтрующих маршрутизаторов: внутренняя сеть видна (маршрутизируется) из сети Интернет; правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP; при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными; отсутствует аутентификация на пользовательском уровне.

2. **Шлюзы сеансового уровня.** Этот класс маршрутизаторов пре дставляет собой транслятор TCP-соединения.

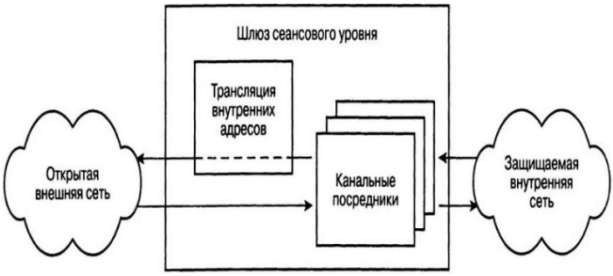


Рисунок 2. Шлюзы сеансового уровня

Шлюз принимает запрос авторизованного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом), далее шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации. Как правило, пункт назначения задается заранее, в то время как источников может быть много. Используя различные порты, можно создавать разнообразные конфигурации соединений. Данный тип шлюза позволяет создать транслятор TCP-соединения для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к

этому сервису и сбор статистики по его использованию. Шлюз следит за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы выявить допустимость запроса на сеанс связи, шлюз выполняет следующую процедуру. Когда авторизованный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации. Затем, действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за выполнением процедуры квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число. Внешний хост, получивший этот пакет, посылает в ответ другой, помеченный флагом ACK и содержащий число на единицу большее, чем в принятом пакете, подтверждая тем самым прием пакета SYN от клиента. Далее осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом, а клиент подтверждает его получение передачей пакета ACK, содержащего число на единицу больше. На этом процесс квитирования связи завершается.

Шлюз сеансового уровня признает завершенное соединение допустимым только в том случае, если при выполнении процедуры квитирования связи флаги SYN и ACK, а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными между собой. После определения того, что доверенный клиент и внешний хост являются авторизованными участниками сеанса TCP, и проверил его допустимость, он устанавливает соединение. С этого момента шлюз копирует и перенаправляет пакеты туда и обратно, не проводя никакой фильтрации. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает сеть, использовавшуюся в текущем сеансе.

Недостатком шлюзов сеансового уровня является отсутствие проверки содержимого передаваемых пакетов, что дает возможность нарушителю проникнуть через такой шлюз.

3. **Шлюзы уровня приложений.** С целью защиты ряда уязвимых мест, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как Telnet и FTP.

Рисунок 3. Шлюзы уровня приложений

Подобное приложение называется proxy-службой, а хост, на котором работает proxy-служба, – шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне. Шлюзы прикладного уровня позволяют обеспечить надежную защиту, поскольку взаимодействие с внешним миром реализуется через небольшое число уполномоченных приложений, полностью контролирующих весь входящий и исходящий трафик. Следует отметить, что шлюзы уровня приложений требуют отдельного приложения для каждого сетевого сервиса.

Преимущества шлюзов прикладного уровня: невидимость структуры защищаемой сети из глобальной сети Интернет. Имена внутренних систем можно не сообщать внешним системам через DNS, поскольку шлюз прикладного уровня может быть единственным хостом, имя которого будет известно внешним системам надежная аутентификация и регистрация. Прикладной трафик может быть аутентифицирован, прежде чем он достигнет внутренних хостов, и зарегистрирован более эффективно, чем с помощью стандартной регистрации приемлемое соотношение цены и эффективности. Дополнительные программные или аппаратные средства аутентификации или регистрации нужно устанавливать только на шлюзе прикладного уровня простые правила фильтрации. Правила на фильтрующем маршрутизаторе оказываются менее сложными, чем на маршрутизаторе, который самостоятельно фильтрует прикладной трафик и отправляет его большому числу внутренних систем.

К недостаткам шлюзов уровня приложений можно отнести: относительно низкая производительность по сравнению с фильтрующими маршрутизаторами. В частности, при использовании клиент-серверных протоколов, таких как Telnet, требуется двухшаговая процедура для входных и выходных соединений; более высокая стоимость по сравнению с фильтрующими маршрутизаторами.

Межсетевой экран, основанный на ***фильтрации пакетов***, является самым распространенным и наиболее простым в реализации, представляя собой фильтрующий маршрутизатор, расположенный между защищаемой сетью и Интернетом. Фильтрующий маршрутизатор сконфигурирован для блокирования или фильтрации входящих и исходящих пакетов на основе анализа их адресов и портов. Компьютеры, находящиеся в защищаемой сети, имеют прямой доступ в Интернет, в то время как большая часть доступа к ним из Интернета блокируется. В принципе, фильтрующий маршрутизатор может реализовать любую из политик безопасности, описанных ранее. Однако если маршрутизатор не фильтрует пакеты по порту источника и номеру входного и выходного порта, то реализация политики «запрещено все, что не разрешено» в явной форме может быть затруднена. Межсетевые экраны, основанные на фильтрации пакетов, имеют те же недостатки, что и фильтрующие маршрутизаторы.

Межсетевой экран на базе ***двухпортового прикладного шлюза*** представляет собой хост с двумя сетевыми интерфейсами. При передаче информации между этими интерфейсами и осуществляется основная фильтрация. Для обеспечения дополнительной защиты между прикладным шлюзом и Интернетом размещают фильтрующий маршрутизатор. В результате между прикладным шлюзом и маршрутизатором образуется внутренняя экранированная подсеть. Ее можно использовать для размещения доступного извне информационного сервера. Размещение информационного сервера увеличивает безопасность сети, поскольку даже при проникновении на него злоумышленник не сможет получить доступ к системам сети через шлюз с двумя интерфейсами. В отличие от схемы межсетевого экрана с фильтрующим маршрутизатором, прикладной шлюз полностью блокирует трафик IP между Интернетом и защищаемой сетью. Только уполномоченные приложения, расположенные на прикладном шлюзе, могут предоставлять услуги и доступ пользователям. Данный вариант межсетевого экрана реализует политику безопасности, основанную на принципе «запрещено все, что не разрешено в явной форме»; при этом пользователю доступны только те службы, для которых определены соответствующие полномочия. Такой подход обеспечивает высокий уровень безопасности, поскольку маршруты к защищенной подсети известны лишь межсетевому экрану и скрыты от внешних систем. Рассматриваемая схема организации межсетевого экрана относительно проста и достаточно эффективна. Поскольку межсетевой экран использует хост, то на нем могут быть установлены программы для усиленной аутентификации пользователей. Межсетевой экран может также протоколировать доступ, попытки зондирования и атак системы, что позволяет выявить действия злоумышленников.

Отличие межсетевых экранов от других устройств:

1. В отличии от маршрутизатора или NAT межсетевой экран не пересылает пакеты из одной сети в другую, а лишь фильтрует их.

2. В отличии от системы обнаружения/предотвращения вторжений (IDS/IPS) классический межсетевой экран не проводит глубокий анализ содержимого пакетов с целью обнаружения вредоносного содержимого.

3. Если рассматривать технологию Deep Packet Inspection (DPI), то в отличии от классического межсетевого экрана DPI производит более глубокий анализ содержимого пакетов для их фильтрации.

На практике маршрутизатор для удобства совмещен с другими сетевыми устройствам, т.к. вместе они выполняют дополняющие друг друга функции.

К основным недостаткам применения межсетевых экранов можно отнести:

1. Неудовлетворительная защита от атак сотрудников компании. Межсетевые экраны обычно не обеспечивают защиту от внутренних угроз

2. Ограничение пропускной способности.

3. Большое количество остающихся уязвимых мест. Межсетевые экраны не защищают от черных входов (люков) в сети. Например, если можно осуществить неограниченный доступ по модему в сеть, защищенную межсетевым экраном, атакующие могут эффективно обойти межсетевой экран.

4. Ограничение в доступе к нужным сервисам. Самый очевидный недостаток межсетевого экрана заключается в том, что он может блокировать ряд сервисов, которые применяют пользователи, – Telnet, FTP и др. Для решения подобных проблем требуется проведение хорошо продуманной политики безопасности, в которой будет соблюдаться баланс между требованиями безопасности и потребностями пользователей;

Существует два варианта исполнения межсетевых экранов: программный и программно-аппаратный. В свою очередь программно-аппаратный вариант имеет две разновидности – в виде отдельного модуля в коммутаторе или маршрутизаторе и в виде специализированного устройства.

На сегодняшний день чаще используется программное решение, которое на первый взгляд выглядит более привлекательным. Это вызвано тем, что для его применения достаточно, казалось бы, всего лишь приобрести программное обеспечение межсетевого экрана и установить на любой имеющийся в организации компьютер. Однако, как показывает практика, в организации далеко не всегда находится свободный компьютер, да ещё и удовлетворяющий достаточно высоким требованиям по системным ресурсам. После того, как компьютер всё-таки найден (чаще всего — куплен), следует процесс установки и настройки операционной системы, а также, непосредственно, программного обеспечения межсетевого экрана. Нетрудно заметить, что использование обычного персонального компьютера далеко не так просто, как может показаться. Именно поэтому всё большее распространение стали получать специализированные программно-аппаратные комплексы, называемые security appliance, на основе, как правило, FreeBSD или Linux, «урезанные» для выполнения только необходимых функций.

Литература

1. Дэвид В. Чепмен, мл., Энди Фокс Брандмауэры Cisco Secure PIX = Cisco® Secure PIX® Firewalls. М.: «Вильямс», 2003. С. 384.

2. Мэйволд Э. Лекция 10 «Межсетевые экраны» // Безопасность сетей: Информация. ИНТУИТ, 2006.

3. Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. МГТУ им. Н. Э. Баумана, 2002. 306 с.

4. https://compress.ru/article.aspx?id=10145#02

5. http://dorlov.blogspot.de/2010/06/issp-05-7.html

6. Лапина М. А., Лапин В. Г. MICROSOFT OFFICE: EXCEL, POWERPOINT/ Практикум. Ставрополь, 2009. Том Часть 2.

7. Соколов А.И., Стадник В.А., Минкина Т.В. Системное описание научной проблемы // Студенческая наука для развития информационного общества: сборник материалов IV Всероссийской научно-технической конференции: в 2х томах, 2016. С. 178-179.

8. Петренко В. И., Мирошников Д. А., Емельянов Е. А. Обзор современных средств сетевой защиты информации//Проблемы автоматизации. Региональное управление. Связь и автоматика («ПАРУСА-2015»), Материалы IV Всероссийской научной конференции молодых ученых, аспирантов и студентов, Геленджик, 2015.

9. Nemkov R., Mezentseva O., Mezentsev D., Brodnikov M. Image recognition by a second-order convolutional neural network with dynamic receptive fields// CEUR Workshop Proceedings 2. Сер. "YSIP2 2017 - Proceedings of the 2nd Young Scientist's International Workshop on Trends in Information Processing" 2017. С. 147-151.

10. Забокрицкий Е. И., Заводнов В. С., Минкина Т. В. Предпосылки угроз информационной безопасности объекта // Материалы III Всероссийской научно-технической конференции «Студенческая наука для развития информационного общества». СКФУ(Ставрополь), 2015. С.181-182.

11. Домашенко А.А., Беспутнев В.В., Минкина Т.В. Актуальность защиты информации в сети интернет // Материалы III Всероссийской научно-технической конференции «Студенческая наука для развития информационного общества». СКФУ(Ставрополь), 2015. С.174-176.

АНАЛИЗ УЯЗВИМОСТЕЙ СОВРЕМЕННЫХ ПРОЦЕССОРОВ

С. С. Васильченко, С. М. Полухин
руководитель – канд. физ.-мат. наук, доцент ***М. А. Лапина***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрены обнаруженные на момент написания уязвимости современных процессоров и основные атаки, эксплуатирующие их, а также методы защиты.

Ключевые слова: процессоры Intel, процессоры AMD, spectre, meltdown, уязвимость, атака, блок TLB, оперативная память.

4 января 2018 года были опубликованы сведения об атаках spectre (англ. Призрак) и meltdown (англ. Расплавление). Аппаратная уязвимость, позволяющая осуществить эти атаки, имеется у подавляющего числа процессоров Intel и AMD, произведёнными после 1995 года, за исключением Intel Itanium и Intel Atom до 2013 года выпуска [1].

Meltdown была независимо обнаружена и представлена тремя командами:

– Янн Хорн (Google Project Zero),

– Вернер Хаас, Томас Прешер (Cyberus Technology),

– Дэниел Грюсс, Мориц Липп, Стефан Мангард, Майкл Шварц (Технологический университет Граца).

Spectre была независимо обнаружена двумя людьми:

– Джанн Хорн (Google Project Zero),

– Paul Kocher в сотрудничестве с Даниэль Генкин (Университет Пенсильвании и Университет Мэриленда), Майк Гамбург (Rambus), Мо-

риц Липп (Технологический университет Грац) и Юваль Яром (Университет Аделаиды и Data61).

Данные атаки используют уязвимость блока управления памятью процессора, который выполняет задачу трансляции адресов виртуальной памяти в адреса физической памяти, и воздействуя на него, можно получить доступ к любому участку оперативной памяти компьютера, таким образом злоумышленники способны завладеть персональными данными пользователей (пароли, идентификаторы, номера карт и случайные документы), обрабатывающиеся в данный момент. Из-за специфики уязвимости, упомянутые атаки осуществимы любые ОС и устройства, использующие современные процессоры [1].

Spectre нарушает изоляцию между различными приложениями. Это позволяет злоумышленнику обманывать безошибочные программы, которые следуют лучшим методам по предотвращению утечки их секретов. Проверки безопасности увеличивают поверхность атаки и могут сделать приложения более восприимчивыми к данной атаке.

Meltdown нарушает самую фундаментальную изоляцию между пользовательскими приложениями и операционной системой. Эта атака позволяет программе получать доступ к памяти, а также к секретам других программ и операционной системы. Если ваш компьютер имеет уязвимый процессор и запускает незагруженную операционную систему, небезопасно работать с конфиденциальной информацией без возможности утечки информации. Это относится как к персональным компьютерам, так и к облачной инфраструктуре [1].

Атаку Spectre сложнее реализовать, чем Meltdown, но её также трудно нейтрализовать.

Основной принцип атак. Сначала создаётся буфер размером 2 мегабайта, причем в этот буфер нельзя писать/читать до проведения атаки и он должен располагаться на границе 4К блока. Этот размер принципиален, в буфере должны разместиться ровно 256 страниц по 4К.

В программе после команды Mov al, (адрес ядра ОС); произойдет прерывание и значение регистра al не изменится.

В буфере TLB из-за прямого запроса выполнения операции произойдет запоминание вычисленного соответствия физического адреса и виртуального адреса.

Если злоумышленники узнают адрес страницы размером 4К в буфере размером 2М, записанный в блоке TLB, то они заполучат и значения прочитанные из ядра ОС [2].

Анализ блока TLB. Для этого требуется один раз прочитать все его страницы по 4К, их ровно 256, выполняются 256 операций чтения. При этом измеряется время выполнения операции чтения. Номер страницы, которой будет читаться быстрее остальных, и будет получен номер в буфере размером 2М соответствующий прочитанному значению байта из

ядра ОС. Это произойдет потому, что в буфере TLB для этой страницы уже вычислено соответствие между физическим и виртуальным адресом, а для всех остальных страниц этой операции выполнено еще не было [2].

Меры защиты. Единственная возможность программного воздействия на блок TLB, – это полный сброс всех его. Все патчи уязвимостей Spectre и Meltdown предложенные производителями ПО это и делают, перезагружая в обработчике исключения GP регистр CR3. После сброса TLB процессору приходится заново выполнять трансляции всех используемых страниц виртуальной памяти, это и снижает производительность системы.

Производители программного обеспечения и процессоров, выпускают обновления и патчи закрывающие эту уязвимость, в ущерб производительности. Apple для обеспечения безопасности они выпустили обновления операционной системы на всех устройствах до macOS 10.13.2, iOS 11.2 и tvOS 11.2 (или старше), а также обновление Safari версии 11.0.2. Старые устройства, которые не получили обновления своих ОС до этих версий, останутся уязвимыми. Для ОС Android исправления операционной системы выпускают производители устройств. Из-за этого нет единого решения для всех устройств. Так же многие производители бюджетных смартфонов не способы устранить уязвимость самостоятельно. Microsoft выпустила обновления только для Windows 7 SP1, Windows 8.1 и Windows 10, а также для браузеров Internet Explorer и Edge. Также защитные обновления вышли для браузеров: Security Update, Monthly Rollup и IE Cumulative [3].

Уязвимость затронула почти все современные процессоры и представляет опасность, но атака требует больших ресурсов со стороны злоумышленника, поэтому обычные пользователи будут редко целью злоумышленников, им следует соблюдать основные правила информационной безопасности [2, 3, 4].

Литература

1. Электронный ресурс - meltdownattack.com
2. Электронный ресурс - habr.com
3. Электронный ресурс - 3dnews.ru
4. П. С. Довгий, В. И. Поляков “Прикладная архитектура базовой модели процессора Intel.

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ИСПОЛЬЗОВАНИЮ КОМПЛЕКСА «КАССАНДРА К21» ДЛЯ ВЫЯВЛЕНИЯ НЕСАНКЦИОНИРОВАННЫХ РАДИОИЗЛУЧЕНИЙ

М. В. Вепаев
руководитель – канд. техн. наук, доцент ***В. В. Антонов***
Северо-Кавказский федеральный университет, г. Ставрополь

Статья посвящена настройке комплекса «Кассандра К21», и разработке рекомендаций по выявлению средств негласного съема информации, использующих для передачи информации радиоэлектронный канал. Усовершенствование устройств негласного съема информации вынуждает использование подобного рода комплексов, которые ведут постоянный контроль радиообстановки и моментально извещает о возможном появлении радиоэлектронного канала утечки информации на охраняемом объекте.

Ключевые слова: Кассандра К21, радиоэлектронный канал, закладные устройства, канал утечки информации, методы защиты, устройства перехвата, информационная безопасность.

На сегодняшний день велик риск утечки информации по радиоэлектронному каналу с помощью различного рода устройств негласного съема информации («жучков»), особенно остро этот вопрос стоит в государственных учреждениях, но в нынешнее время, в условиях конкурентной борьбы на рынке, не только государственные, но и коммерческие организации задались этим вопросом.

Сейчас существует огромное количество таких устройств, и самое главное, с каждым годом их разнообразие увеличиваются, так как злоумышленник становится умнее и придумывает более ухищренные методы. Одну из наиболее опасных групп представляют электронные устройства негласного получения информации, не производящие непрерывной передачи информации по радиоканалу, а накапливающие ее в течении продолжительного периода времени (несколько часов и дней), а затем передающие накопленную информацию в течение короткого промежутка времени, а также существуют радиозакладки, постоянно меняющие частоту несущего сигнала или генерирующие шумоподобные сигналы, размытые по частотному спектру. Усовершенствование техники негласного съема информации предъявляет все более высокие требования к аппаратуре поиска.

Актуальность данной статьи определяется тем, что для успешного предотвращения утечки информации по радиоэлектронному каналу на предприятии необходимо осуществлять поиск и обнаружение радиоизлучения в целях предотвращения несанкционированного перехвата информации. В этой статье для достижения поставленной цели будет использоваться комплекс радиомониторинга «Кассандра К21».

Конечно, нет никакого смысла приобретать данный комплекс, если у вас маленькое предприятие и вопрос утечки информации стоит не в приоритете. Но в больших корпорациях, или в учреждениях, где циркулирует информация, составляющая государственную тайну риск утечки (даже хоть «мизерной») информации может очень сильно оказать влияние.

Рисунок 1. Комплекс радиомониторинга и цифрового анализа сигналов «Кассандра К21»

«Кассандра К21» это уникальное сочетание новейших технических решений, а современное специализированное программное обеспечение комплекса позволяет обнаруживать и идентифицировать сигналы от различных типов устройств негласного съема информации, в том числе использующих цифровые виды модуляции, шумоподобную структуру, режим псевдослучайной перестройки рабочей частоты и т.д. [3].

Алгоритм настройки работы комплекса в режиме сбора данных представлен ниже (рис. 2).

Сканирование радиообстановки лучше оставлять круглосуточным, заранее подумав о размере хранилища.

Комплекс радиомониторинга «Кассандра К21» работает с ПО «Radio-Inspector», который позволяет вести журнал событий всех зафиксированных сигналов и превысивших порог.

Каждый из зафиксированных сигналов может быть подробно осмотрен вызвав соответствующее меню. Такое меню предполагает:

- визуальный вид самого сигнала;
- время появления сигнала;
- уровень сигнала.

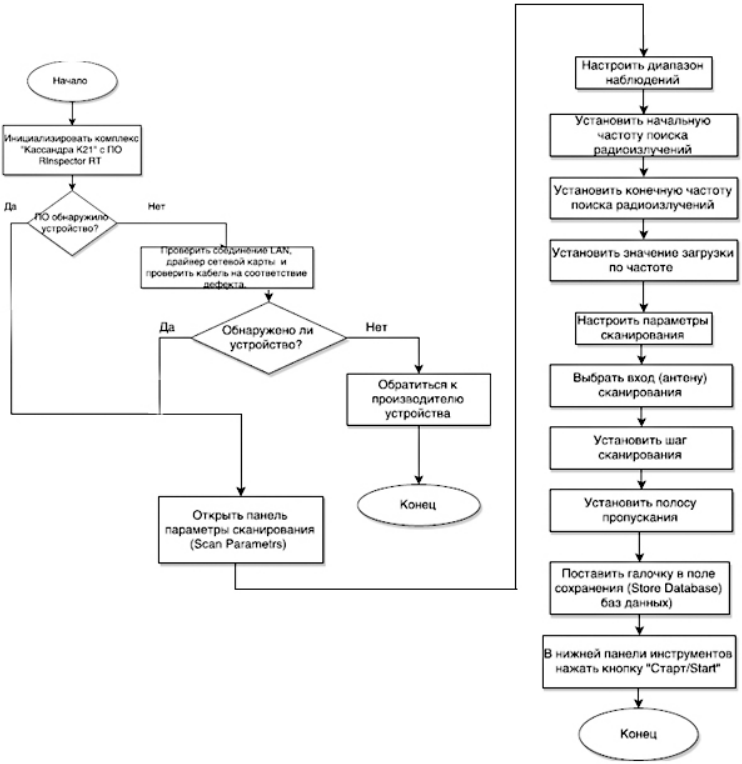


Рисунок 2. Алгоритм настройки сканирования комплекса

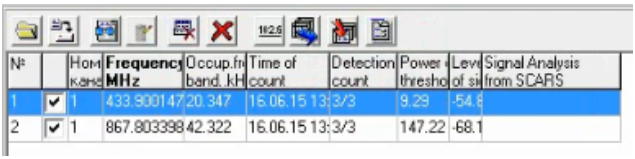


Рисунок 3. Листинг сигналов, превысивших порог

Если будет выяснено, что данный сигнал является не опасным, то мы можем откорректировать линию порога и удалить данный сигнал из списка обнаруженных. При необходимости, можно прослушать данный сигнал или же посмотреть на форму сигнала через низкочастотный осциллограф.

Комплекс позволяет автоматически классифицировать различные стандарты связи (WIFI, DECT, TETRA, GSM, UMTS, DMR, Bluetooth, APCO25, DMR) для дальнейшего их анализа [3].

Очевидно, что в данной статье не представляется возможным описание всех функций и возможностей данного комплекса.

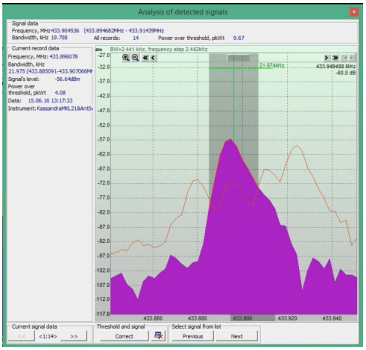


Рисунок 4. Окно подробной справки о сигнале, превысившего порог

На рис. 5 написан алгоритм для выявления радиозакладных устройств в выделенном помещении на предприятии.

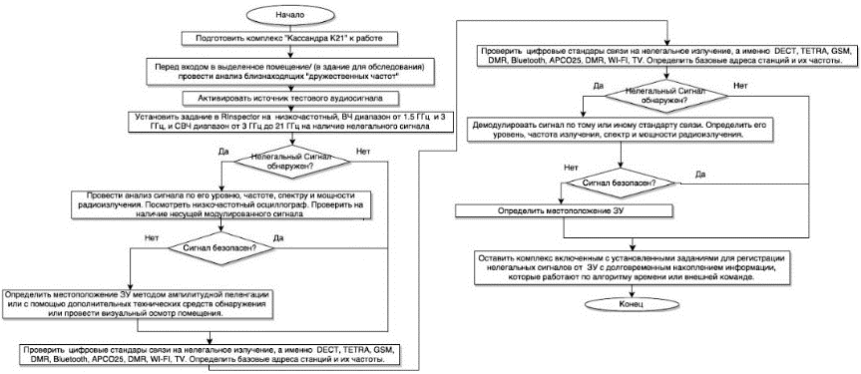


Рисунок 5. Алгоритм по выявлению радиозакладных устройств в выделенном помещении с комплексом «Кассандра К21»

Комплекс «Кассандра К21» имеет расширенный спектр возможностей, а программное обеспечение является многозадачным, интерфейс довольно гибким и позволяет производить оператору большое количество настроек.

Литература

1. Хорев А. А. Техническая защита информации: Учебное пособие для студентов вузов. М.: НЦП «Аналитика»2012. 436 с.

2. «Комплексы радиоконтроля » // Сайт Федеральное Государственное Унитарное Предприятие «Научно-производственное предприятие» URL: http://www.nppgamma.ru/-catalog/third_party/kompleksy_radiokontrolya// (дата обращения 13.04.2018).

3. «Руководство к эксплуатации » // Сайт бюро STT GROUP Специальная техника и технологии URL: http://detektor.ru/files/Opisanie/kassandra.pdf (дата обращения 15.04.2018).

ОСОБЕННОСТИ РАЗВИТИЯ КЛЕПТОГРАФИИ

Р. Л. Выговский, Д. М. Барышев
руководитель – аспирант кафедры ИБАС ***Н. А. Топорков***
Северо-Кавказский федеральный университет г. Ставрополь

С увеличением роста криптографических систем защиты был обнаружен новый вид атак – клептографический, использующий в основе само устройство обеспечения безопасности. В статье приведено описание и основные способы защиты.

Ключевые слова: клептография, криптография, шифрование, защита, атака, безопасность, backdoor.

Для обеспечения конфиденциальности деловой переписки будет использовано оборудование со стойким алгоритмом шифрования. В теории, такой способ связи является защищённым. Но может случиться ситуация, при которой разработчик, являющийся в этом случае нарушителем, заранее видоизменил криптосистему и тем самым обеспечил себе возможность скрытного доступа к информации. Кажется, что пересылаемые сообщения доступны только абонентам, на деле же злоумышленник нарушил тайну переписки.

Именно такого рода проблема называется клептографической атакой. Алгоритм шифрования генерирует закрытый и открытый ключ при условии, что закрытый ключ известен только владельцу, но можно создать псевдослучайную числовую последовательность, при которой будут сгенерированы ключи, похожие на настоящие, но открывающие разработчику доступ к корреспонденции.

Проблемой таких атак занимается наука клептография – изучение способов незаметного для пользователя похищения информации. Клептография является подкатегорией криптовирологии и охватывает безопасные и скрытые коммуникации через криптосистемы и криптографические протоколы. Впервые была описана в 1996 году Адамом Янгом и Моти Юнгом, показавшие на практике возможность компрометации канала связи без обнаружения. Из-за отсутствия теоретического метода обнаружения подобных атак и сомнений в их существовании, в 90-ые данная проблема мало принималась во внимание. Более остро вопрос клептоатак начал рассматриваться в наше время после заявлений Эдварда Сноудена и появления конкретных примеров, например скандала с автомобилями Volkswagen.

Причин для применения уязвимости достаточно: государственные агентства хотят превысить свои полномочия и получить информацию о гражданах, на которую по закону они не имеют права – об этом и говорил Сноуден. Компании заинтересованы в сборе информации о своих пользователях, которая в наше время стоит больших денег.

В основе механизма клептографической атаки работает backdoor – внедрённый при изготовлении механизм системы, позволяющий в фоновом режиме передавать данные с пользовательского устройства злоумыш-

леннику незаметно. Получается, криптография работает против криптографии: backdoor не является ещё одним каналом связи с внешним миром за пределами криптосистемы, поэтому при нелегальном получении конфиденциальных данных нет нужды передавать дополнительную информацию. backdoor может быть встроен в процессе разработки криптосистемы таким образом, чтобы предоставить нарушителю доступ к закрытому ключу, что даёт возможность расшифрования секретной информации, подделывания подписи. Целью клептографических атак является не ПО компьютера, а детали среды системы шифрования.

Борьбой с такими атаками и занимается наука клептография. Существует два способа: создание модульной системы и обратная разработка.

Первый связан с внедрением систем. При работе со структурой устройств одного производителя возможность клептографической атаки сильно возрастает. Суть метода в использовании программных решений различных разработчиков, собранных в единый модуль самостоятельно. При такой работе шанс обнаружения backdoor увеличивается.

Вторым способом является реверс-инжиниринг – исследование некоторого готового устройства или программы, а также документации с целью разбора принципа его работы. Используется при отсутствии официального описания разработчиком работы устройства; в случае применения для борьбы с клептографическими атаками – вычисление алгоритма, генератора псевдослучайных чисел криптографической системы. Главная проблема состоит в том, что независимый аудитор не получит доступ к просматру проприетарного программного кода; единственное, что они могут, – это попытаться написать аналогичную программу, если их не остановит механизм безопасности «чёрного ящика» криптосистемы, и сравнить результаты.

Потенциальной опасностью заражения пользовательского устройства для последующего возникновения клептоатаки может являться вирусная программа. Логичным решением будет использование лицензированного антивирусного ПО и файрвола.

Проблема клептографии сильно затрагивает интересы IT-корпораций, страдает международный экспорт оборудования. В главном случае – из-за недоверия: иностранные правительства не хотят рисковать, связываясь с компаниями, которые теоретически могут продать оборудование с backdoor и полкчить несанкционированный доступ к информации.

Но самый главный вопрос – это интересы отдельных людей, которые ежедневно пользуются десятками сервисов, передают конфиденциальные данные, в том числе и финансовые.

В итоге, подробно разбирая уязвимость, видится одна из задач информационной безопасности на будущее – решение проблемы клептографических атак. Уже сейчас IT-сообщество активно занимается поиском средств клептозащиты.

Литература

1. https://postnauka.ru/faq/82154
2. http://www.itsec.ru/articles2/crypto/temnaya-storona-kriptografii
3. https://protos.su/licensing/statyi-o-licenzirovanii/kleptografija-novaja-ugroza-dlja-konfidencianoj-nformacii/
4. Петренко В. И. Мирошников Д. А. Емельянов Е. А. Анализ требований применения систем электронного документооборота//Молодёжный форум: технические и математические науки. Материалы Международной научно-практической конференции, Воронеж, 2015.
5. Петренко В. И., Мирошников Д. А., Емельянов Е. А. Обзор современных средств сетевой защиты информации//Проблемы автоматизации. Региональное управление. Связь и автоматика («ПАРУСА-2015»), Материалы IV Всероссийской научной конференции молодых ученых, аспирантов и студентов, Геленджик, 2015.
6. Донской В. А., Бисюков В. М. Оптимизация процедуры выбора организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных /Сборник научных статей по материалам Всероссийской научно-практической конференции. 2017. С. 58-62.
7. Жук А. П., Петренко В. И., Кузьминов Ю. В., Дорошенко Н. С. Совершенствование математического аппарата синтеза ортогональных дискретных последовательностей для широкополосных беспроводных систем связи // Вестник СевКавГТИ. 2012. № 13. С. 10-15.

АРХИТЕКТУРНЫЕ ИЗМЕНЕНИЯ В МИКРОПРОЦЕССОРАХ AMD

Ф. А. Гаврилов
руководитель – старший преподаватель ***О. В. Криволапова***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье будут рассмотрены архитектурные изменения в микропроцессорах компании AMD двух поколений Piledriver и Zen, а также изменения в производительности данных процессоров.

Ключевые слова: Микропроцессор, архитектура, AMD, Zen, Piledriver, Hypertransport, Infinity Fabric, Ryzen, Vishera.

Первые процессоры на архитектуре AMD Piledriver появились в конце 2012 года и кардинально отличались от своих предшественников возросшим количеством ядер, а также частотным потенциалом вплоть до 5Ghz.

До начала 2017 года решения на данной архитектуре были единственными в сегменте для настольных ПК, столь долгий по меркам IT-индустрии жизненный цикл данных процессоров обуславливается инженерными особенностями архитектуры.

В марте 2017 года на смену AMD Piledriver пришла новая архитектура – AMD Zen, она также внесла свои значительные изменения и инновационные разработки в процессоры AMD. Возникает вопрос что же именно изменилось и какие решения были применены в каждой из архитектур?

AMD Piledriver на примере процессоров серии FX(Vishera)

При детальном рассмотрении архитектуры восьми ядерных процессоров семейства Vishera, можно обратить внимание на то, что ядра скомпо-

нованы в модули по два ядра, каждое ядро имеет в своем распоряжении блок ALU и кэш первого уровня L1. Однако рассматривая данный модуль более детально можно отметить, что ядра одного модуля делят между собой один блок FPU, что несомненно ведет к повышению задержек при обращении к нему одновременно двух ядер одного модуля. Каждый модуль обладает своим персональным FEP.

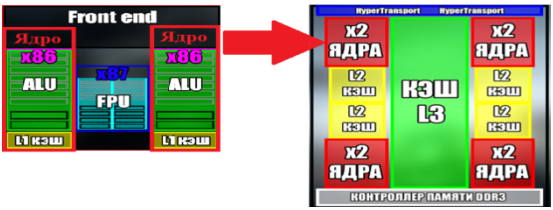


Рисунок 1. Архитектура микропроцессоров AMD FX(Vishera)

Кристалл имеет четыре двухъядерных модуля связанных между собой двунаправленной последовательно-параллельной шиной Hyper-Transport 3.1. Каждый двухъядерный модуль имеет свой собственный кэш второго уровня L2 и общим для всех модулей кэшем третьего L3.Также на кристалле расположен контроллер памяти DDR3 способный работать в двухканальном режиме.

AMD Zen на примере процессоров серии Ryzen 7(Ryzen)

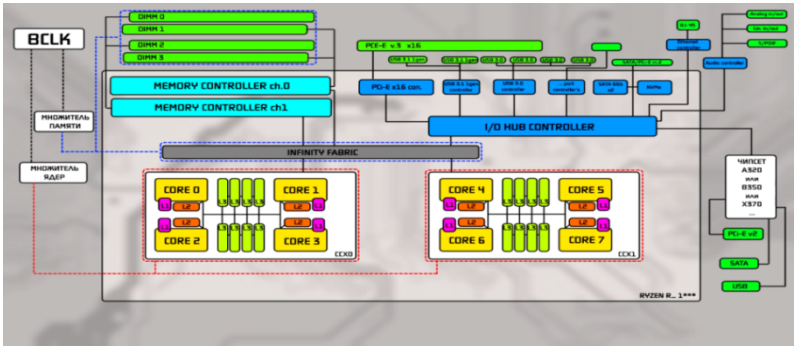


Рисунок 2. Архитектура микропроцессоров AMD Ryzen

Процессоры Ryzen 7 базируются на архитектуре Zen первого поколения. При детальном рассмотрении кристалла процессора можно выделить следующие изменения по сравнению с архитектурой AMD Piledriver. Процессоры Ryzen состоят из двух четырех ядерных модулей. Каждый модуль Zen содержит в себе четыре ядра, которым в отличие от AMD FX предоставляется по одному блоку ALU и FPU, также они имеют свой персо-

нальный кэш первого L1 и второго L2 уровня, кэш третьего уровня L3 общий для всех 4х ядер одного модуля. Претерпела изменения, и внутренняя шина HyperTransport ее пропускная способность значительно возросла и напрямую зависит от эффективной частоты оперативной памяти или же частоты BCLK (тактового генератора), также претерпел изменения и контроллер памяти, который теперь работает с новым более скоростным видом памяти DDR4. Также стоит отметить улучшенные алгоритмы работы FEP, что тоже значительно повлияло на производительность. Однако наиболее весомым изменением стало внедрение на аппаратном уровне технологии SMT (Simultaneous Multithreading), что позволило каждому ядру одновременно обслуживать два потока. Данная технология значительно повышает производительность в мультипоточных задачах.

Новая шина получила Infinity Fabric ее пропускная способность возросла в 10 раз по сравнению с HyperTransport 3.1, из-за масштабируемости данная шина может использоваться и в дискретных графических решениях от AMD, к примеру в AMD Vega 64 данная шина может обеспечивать пропускную способность в 512Гбайт/сек что более чем в 10 раз превосходит пропускную способность Hyper Transport 3.1. Данные изменения в архитектуре должны значительно повысить производительность процессора.

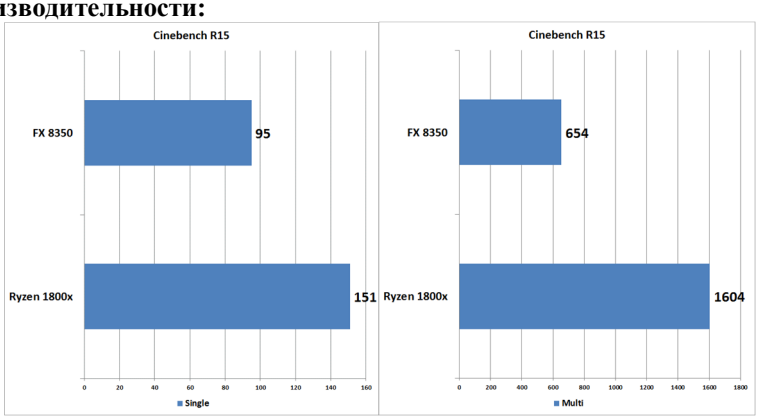
Сравнение процессоров AMD FX 8350 и AMD Ryzen 7 1800x

Для оценки производительности данных архитектур на практике были выбраны два процессора принадлежащие к данным архитектурам – это AMD FX 8350 и AMD Ryzen 7 1800x. Ознакомимся с их техническими характеристиками:

Тип процессора	AMD FX-8350 Piledriver	AMD Ryzen 7 1800x Zen
Количество ядер/потоков	8 (4 модуля)/8	8/16
Тактовая частота	4,0 ГГц	3,6 ГГц
Частота с учетом Turbo	до 4,2 ГГц	до 4,0 ГГц
Техпроцесс	32nm	14nm
Объем кэша L3	8MB	16MB
Контроллер памяти	DDR3-1866 2 Channel	DDR4-2667 2 Channel
Тепловое энергопотребление	125 Вт	95 Вт

Для тестирования данных процессоров было решено использовать бэнчмарк Cinebench R15, так как он позволяет определить производительность процессора как и в одногопоточных, так и в мультипочных задачах.

Тестирование однопоточной и мультипоточной производительности:



Исходя из тестов даннных процессоров в Cinebench R15 производительность архитектуры Zen значительно выше.В однопоточных задачах разница в производительности составила 59 %, в мультипоточных задачах производительность возросла на колосальные 145 %.

Литература

1. https://www.amd.com -Официальный сайт “AMD”
2. http://itndaily.ru/2017/03/06/sravnenie-proizvoditelnosti-amd-ryzen-7-1800x-i-fx-8350 - Интернет ресурс “itndayly”.
3. https://en.wikipedia.org/wiki/Piledriver_(microarchitecture). Интернет ресурс «Википедия»

КОМПЛЕКСНАЯ ОЦЕНКА УЯЗВИМОСТЕЙ ИНФОРМАЦИИ В ЗОНЕ ОЗУ СЕТЕВОЙ ФАЙЛОВОЙ СИСТЕМЫ

А. С. Горлов
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье рассмотрены уязвимости информации в зоне ОЗУ сетевой файловой системы, а также способы их перекрытия.

Ключевые слова: автоматизированная система, сетевая файловая система, ОЗУ, группа угроз, уязвимость, устранение уязвимости.

Самое ценное в автоматизированной системе – циркулирующая в ней информация. Потеря информации может нанести серьезный материальный ущерб как для организации, так и для ее клиентов [1, с. 157].

Автоматизированная система включает в себя множество основных компонентов, которые в совокупности образуют информационную инфраструктуру предприятия. Одним из таких компонентов является сетевая

файловая система в зоне ОЗУ [2, с. 115]. Обеспечение информационной безопасности сетевой файловой системы является необходимым мероприятием, которое лежит в основе комплексной защиты информации всех подсистем информационной инфраструктуры [3, с. 175].

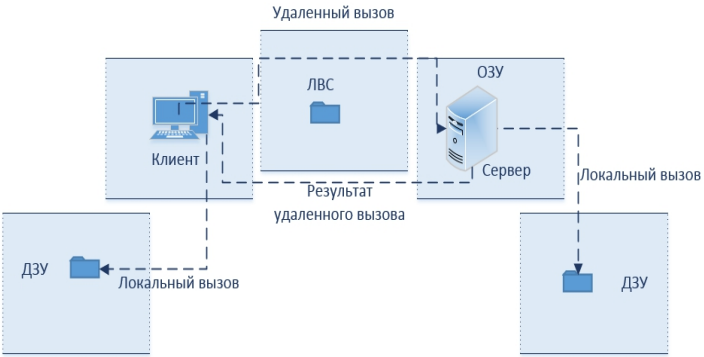


Рисунок 1. Функциональная структура процедур взаимодействия в сетевой файловой системе, на основании которой составляется таблица уязвимостей информации в зоне ОЗУ

Таблица 1

Сводная таблица уязвимостей информации в зоне ОЗУ сетевой файловой системы

Группа угроз	Уязвимость	Перекрытие уязвимости
Физические угрозы для информации в зоне ОЗУ сетевой файловой системы	Отсутствие контроля доступа за помещением, где находится оборудование	Внедрение систем контроля доступа
Использование ОЗУ сетевой файловой системы сотрудниками не по назначению	Игнорирование прямых обязанностей	Внедрение организационных мер, которые строго разделяет обязанности и контролируют их исполнение
Угрозы вывода оборудования из строя	Место, где находится оборудование не оснащено должным образом	Оснащение помещения: источниками бесперебойного питания, системой охлаждения, пожарной сигнализацией
	Ошибки программного обеспечения или системные сбои	Своевременное обновление операционной системы и программного обеспечения
Модификация системных и прикладных программ	Уязвимости системных и прикладных программ	Антивирусные программы
		Программы контроля целостности
Подмена доверенного объекта сети	Сетевые уязвимости	Системы предотвращения вторжений
		Межсетевые экраны
		Системы обнаружения вторжений

Проведя анализ угроз от ее параметров с помощью калькулятора cvss v3 (обычный калькулятор системы оценки уязвимости) будут выявлены метрики, влияющие на конфиденциальность, целостность и доступность информации крайне критично [4, с. 125].

Рисунок 2. Выявление метрик, оказывающих негативное влияние на конфиденциальность, целостность и доступность информации

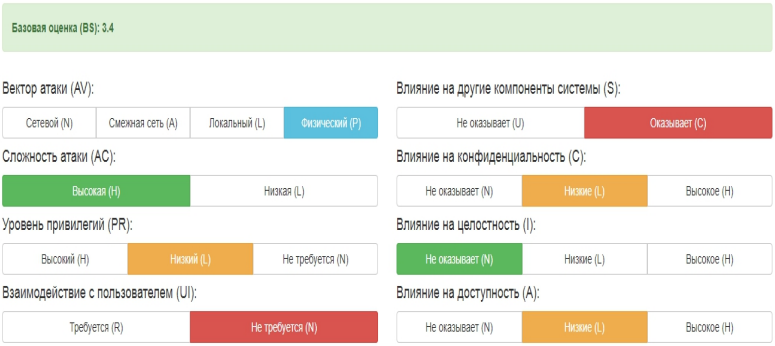


Рисунок 3. Выявление метрик, оказывающих негативное влияние на конфиденциальность, целостность и доступность информации

На основании проведенных расчетов с использованием различных метрик выявлено, что наибольшее влияние на сетевую файловую систему в зоне ОЗУ оказывают уязвимости, которые негативно сказываются на целостности, доступности и конфиденциальности информации [5, с. 761].

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем: учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем». М., 2010.

2. Чипига А. Ф., Пелешенко В.С. Методология обнаружения и предотвращения угроз и компьютерных атак на информационную систему и психику людей/ А. Ф. Чипига, В. С. Пелешенко. Информационное противодействие угрозам терроризма. 2010. № 15. С. 114-118.

3. Чипига А. Ф., Ерещенко Ф. Ф., Пелешенко В. С. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, В. С. Пелешенко. Известия ЮФУ. Технические науки. 2009. № 11 (100). С. 172-176.

4. Чипига А. Ф., Ерещенко А. А. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко. Информационное противодействие угрозам терроризма. 2005. № 5. С. 122-128.

5. Чипига А. Ф., Марков Д. В., Слюсарев Г. В. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. В. Марков, Г. В. Слюсарев. Фундаментальные исследования. 2015. № 11-4. С. 759-762.

6. Сагдеев К. М., Петренко В. И., Чипига А. Ф. Физические основы защиты информации: учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург 2017. (2-е издание, исправленное и дополненное).

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ WI-FI СЕТЕЙ

А. В. Горохов, И. Р. Евдокимов
руководитель – канд. физ.-мат. наук, доцент ***М. А. Лапина***
Северо-Кавказский федеральный университет, г. Ставрополь

Беспроводные технологии – подкласс информационных технологий, служат для передачи информации на расстояние между двумя и более точками, не требуя связи их проводами. Для передачи информации может использоваться инфракрасное излучение, радиоволны, лазерное излучение. Стандарты защиты беспроводной сети WPA2, WEP, WPA защищают по-разному. Стандарт WPA2 считается самым надежным. В нём реализовано CCMP и шифрование AES, за счёт чего WPA2 стал более защищённым, чем свой предшественник WPA.

Ключевые слова: Wi-Fi, WPA2, WEP, безопасность сети.

В настоящее время на беспроводные сети Wi-Fi переходят не только частный сектор и малые компании, но и крупные предприятия. Беспроводные сети очень удобны для пользования, но при этом они более уязвимы. Ключевая проблема безопасности таких сетей – это то, что пароль подключения передается по радиоканалу, таким образом, злоумышленник может его перехватить. Для обеспечения безопасности Wi-Fi сетей используют 2 основных способа подключения к ней. Первый способ подключения к Wi-Fi – это wps. Для подключения пароль не нужен, нужно нажать кнопку и подключиться. WPS позволяет пользователю подключиться к сети по 8-символьному коду, который состоит из цифр. Из-за ошибки в этом стандарте можно угадать 4 первых символа, после чего еще 3 последующих символа, а 8 символ является контрольной суммой, и вычисляется по подобранным 7 символам. Таким образом, злоумышленнику достаточно перебрать всего 10^4+10^3 комбинаций вместо 10^8. Для защиты, ко-

личество запросов на вход ограничено по 10-50 запросов в секунду, но в любом случае время для подбора кода колеблется от 3 до 15 часов.

Второй способ – это подключение с помощью пароля, этот способ является наиболее безопасным. Существует несколько таких стандартов защиты как WPA, WPA2, WEP. Рассмотрим WPA2 и WEP.

Стандарт WPA2 на данный момент является наиболее безопасным из-за длины ключа (от 8 символов) и самого шифрования данных. WPA шифрует данные каждого пользователя по отдельности, чем и отличается от WEP. А после авторизации пользователя генерируется временный ключ, который используется для кодирования передачи только этого пользователя. При помощи этого механизма злоумышленник не сможет читать пакеты всех пользователей, взломав один из них.

WEP – это первый стандарт защиты Wi-Fi, был разработан в конце 90-х, но некоторые пользователи используют его сейчас, но этот стандарт имеет парольную фразу (всего 5 символов), но также имеет ошибку в проектировании – несколько байт парольной фразы передается с каждым переданным пакетом в сети, что облегчает процесс расшифровки пароля.

Взломать сеть, можно перехватив пакеты авторизации пользователя и подобрав пароль, поэтому время, за которое злоумышленник подберет пароль, прямо зависит от его длины и используемых символов. Средняя скорость подбора паролей составляет 1800 ключей в секунду, такая скорость достигается на обычном компьютере. Например, в случае с WEP, алфавит содержит 10 цифр, а длина равна 5 символам, отсюда следует, что количество размещений равно 10^5 = 100000, делим это число на скорость подбора ключей 1800 и получаем 55 секунд. С WPA2, алфавит содержит 10 цифр, а длина равна 8 символам, 10^8/1800=55555 секунд – 15 часов. Если в пароль добавить буквы и цифры, то время подбора значительно увеличится.

Следовательно, нужно всегда отключать технологию WPS, и использовать только протокол шифрования WPA2. Для лучшей защиты с шифрованием WPA2 нужно иметь пароль длиной от 10 символов, с использованием цифр и букв. Также, рекомендуется менять пароль 1-2 раза в 3 месяца. При соблюдении данных рекомендаций можно считать технологию Wi-Fi вполне безопасной.

Литература

1. RFC 4764. The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method.

2. RFC 5416. Control and Provisioning of Wireless Access Points (CAPWAP) ProtocolBinding for IEEE 802.11

3. Пролетарский А. В., Баскаков И. В., Чирков Д. Н.Беспроводные сети Wi-Fi.

КОМПЛЕКСНАЯ ОЦЕНКА УЯЗВИМОСТЕЙ ИНФОРМАЦИИ В ЗОНЕ ЛВС СЕТЕВОЙ ФАЙЛОВОЙ СИСТЕМЫ

С. Н. Горшков
руководитель – канд. техн. наук, профессор ***А. Ф. Чипига***
Северо-Кавказский федеральный университет, г. Ставрополь

Комплексная оценка уязвимостей информации является одной из основных задач при построении сетевой инфраструктуры. Одним из важнейших компонентов сетевой инфраструктуры является сетевая файловая система.

Ключевые слова: информационная безопасность, сеть, сетевая инфраструктура, файл, файловая система, уязвимость, оценка уязвимости, локальная вычислительная сеть, угроза информационной безопасности.

Сетевая файловая система (Network File System) обеспечивает хранение файлов в сети, не занимая ресурсов на устройствах пользователей. Архитектура NFS основывается на модели клиент-сервер. Сервером выступает машина, которая импортирует, экспортирует и хранит файлы. Клиентами являются устройства, которые имеют доступ к этим файлам. Файлом является некоторый абстрактный интерфейс, который инкапсулирует операции ввода-вывода информации при решении различных задач обработки, передачи и хранения информации. В основе проектирования сетевой файловой системы лежит принцип «Redirect», то есть переадресация запросов. На практике обращения к файлам выполняются посредством механизма RPC (удаленного вызова процедур). Данный подход позволяет использовать один и тот же набор системных функций как для обращения к файлам на удаленных файловых системах, так и для доступа к локальным файлам.

Комплексная оценка уязвимостей информации основывается на использовании моделей общей оценки угроз, которые являются основой оценки угроз безопасности. Типовыми угрозами информационной безопасности являются:

- прямой доступ к информации на носителе;
- перехват;
- загрузка с несанкционированного носителя.

Целью угрозы прямого доступа к информации на носителе является похищение носителя информации для изучения хранящейся на нем информации с помощью специальных или стандартных программно-аппаратных средств.

Смыслом перехвата является получение доступа к отдельным объектам файловой системы при помощи конструкторских недостатков или специальных технических средств.

Загрузка с несанкционированного носителя осуществляется для обхода встроенных средств защиты файлов сетевой ОС при отсутствии необходимых данных для доступа.

Уязвимости информации в зоне ЛВС разделяют по следующим классам:

– объективные;
– случайные;
– субъективные.

Случайные уязвимости зависят от непредвиденных обстоятельств и особенностей окружения информационной среды. Для зоны ЛВС актуальны следующие случайные угрозы:

– сбои и отказы работы систем;
– ослабляющие информационную безопасность факторы.

Сбои и отказы работы систем влияют на доступность информационных ресурсов. Устранить такие уязвимости можно при помощи периодической диагностики всех компонентов сетевой инфраструктуры.

К ослабляющим информационную безопасность факторам можно отнести: повреждение коммуникаций и неисправности в работе ограждающих устройств. Данную уязвимость необходимо устранять при помощи проведения инженерно-технического разбирательства.

Объективные уязвимости напрямую зависят от технического проектирования оборудования на объекте защиты и его характеристик. Последствиями таких уязвимостей является утечка информации, что зачастую является критической проблемой предприятия. К ним относятся уязвимости:

– связанные с техническими средствами излучения;
– активизируемые.

Уязвимости, связанные с техническими средствами излучения, возникают при побочных ЭМ излучениях, акустических вибросигналах или по наводкам на линии от объектов зоны ЛВС.

Активизируемые уязвимости – это вредоносные ПО, нелегальные программы или закладки аппаратуры. Последним являются факторы, внедряющиеся напрямую в электрические сети, телефонные линии или в помещения.

Субъективные уязвимости представляют собой результат неверных действий сотрудников на этапе разработки систем хранения и защиты информации. Данные уязвимости могут нарушить конфиденциальность и целостность информационных ресурсов. Такие уязвимости необходимо устранять при помощи методик с использованием ПО и аппаратуры.

При комплексной оценке уязвимостей информации в зоне ЛВС сетевой файловой системы оцениваются следующие уязвимости, представленные в следующей таблице:

Уязвимость	Угроза
Незащищенное хранение	Кража
Нестабильное электропитание	Флуктуация электропитания
Неадекватное управление сетью	Перегрузка трафика
Отсутствие процедур резервного копирования	Потеря информации
Неадекватный контроль изменений	Сбой системы безопасности

Передача или повторное использование средств хранения информации без надлежащей очистки	Несанкционированный доступ к информации
Неконтролируемое копирование	Кража
Незащищенные соединения с сетями общего пользования	Использование программного обеспечения неавторизованными пользователями
Недостаточная защита криптографических ключей	Раскрытие информации
Неконтролируемая загрузка и использование программного обеспечения	Вредоносное программное обеспечение
Неправильное разграничение доступа в сетях	Несанкционированные подключения к сетям
Отсутствие механизмов идентификации и аутентификации, таких как аутентификация пользователей	Присвоение чужого пользовательского идентификатора
Отсутствующая или некорректная политика контроля доступа	Несанкционированный доступ к информации, системам или программному обеспечению

Таким образом, комплексная оценка уязвимостей в зоне ЛВС сетевой файловой системы подразумевает полное исследование возможных угроз для всех компонентов сетевой инфраструктуры, для дальнейшего определения уязвимостей, специфичных для данной сетевой файловой системы. По результатам исследования необходимо предпринять меры по устранению выявленных уязвимостей.

Литература

1. Информационная безопасность автоматизированных систем / А.Ф.Чипига. М.: «Гелиос АРВ», 2010. 336 с.
2. Петренко В.И. Теоретические основы защиты информации: учебное пособие. – Ставрополь: Изд-во СКФУ, 2015г. - 222 с.
3. Модель трехмерной структуры объектов с матрицей доступа / Чипига А. Ф., Ерещенко А. А., Пелешенко В. С. // Известия ЮФУ. Технические науки. 2009. С. 172-176.
4. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / Чипига А. Ф., Пелешенко В. С. // Информационное противодействие угрозам терроризма. 2010. С. 114-118.
5. Объектный подход к модели разграничения доступа в компьютерных системах / Чипига А. Ф., Ерещенко А. А. // Информационное противодействие угрозам терроризма. 2005. С. 122-128.
6. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / Чипига А. Ф., Марков Д. М., Слюсарев Г. В. // Фундаментальные исследования. 2015. 759 с.
7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных // ФСТЭК России, 2008 г.
8. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

ЗАЩИТА ПРИЛОЖЕНИЙ ОТ ДЕФЕКТА ФОРМАТНЫХ СТРОК

С. Н. Горшков
руководитель – старший преподаватель ***Д. В. Соломонов***
Северо-Кавказский федеральный университет, г. Ставрополь

Дефекты форматных строк – одна из немногочисленных действительно новых атак, появившихся за последние годы. Как и во многих проблемах безопасности, первопричиной дефектов форматных строк становится использование введенных пользователем данных без проверки. В C/C++ дефекты форматных строк могут использоваться для записи в произвольные адреса памяти, причем самый опасный аспект заключается в том, что это может происходить без махинаций со смежными блоками памяти.

Ключевые слова: дефект форматных строк, форматная строка, спецификатор.

Дефект форматных строк – это проблема одной из самых распространенных функций вывода информации – printf, и ее семейства. Многие разработчики используют именно эту функцию для вывода информации на экран, но ее применение в приложениях, работающих по сети Интернет, может привести к серьезным последствиям, таким как получение контроля над устройством, подмена информации, кража конфиденциальных данных, возможность выполнения произвольного кода на целевом устройстве.

Форматная строка – это константная строка с заполнителями, определяющими место подстановки переменных. Например, для включения числа типа double в форматную строку применяется спецификатор формата %f. Спецификаторы состоят из нескольких компонентов – флаг, ширина и точность, определяющих формат вывода. Дефект форматных строк происходит при включении данных, вводимых пользователем, в форматную строку семейства printf (fprintf, sprint, snprintf, vprintf и другие). Следующих пример выведет квадратный корень из 2 с точностью до 4 цифр:

printf(“sqrt(2) = %.4f\n”, sqrt(2));

Но если передать программе форматную строку, но не указать подставляемые переменные, то происходят вывод информации из стека.

Следующий код показывает, как работает дефект форматной строки:

```
#include <iostream>
using namespace std;
int main(int argc, char *argv[])
{
if (argc != 2)
{
printf("Error\n");
return 1;
}
printf(argv[1]);
```

```
printf("\n");
return 0;
}
```

Результат выполнения этой программы представлен на рис. 1.

Рисунок 1. Дефект форматной строки

Программа вывела некоторые данные из стека. Но если увеличить количество спецификаторов, то получится следующий результат, представленный на рис. 2.

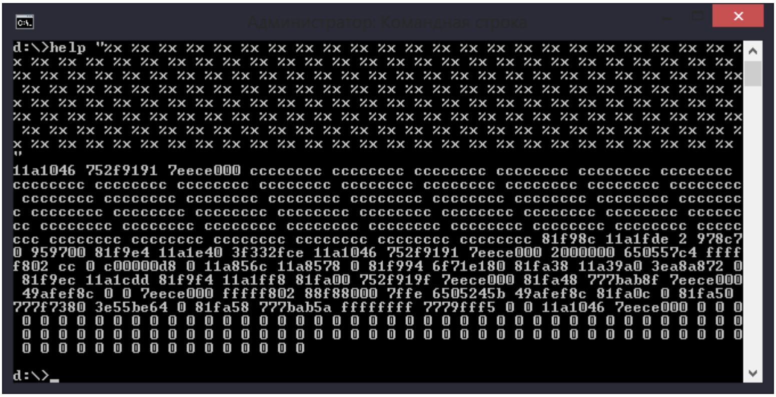


Рисунок 2. Увеличение количества спецификаторов

Программа вывела данные за границей стека. При использовании спецификатора %s можно выводить строку из ячейки, %d – число. Но более опасным будет занесение информации в ячейки памяти, это происходит при вводе спецификатора %n. Это может привести к неприятным последствиям, поэтому необходимо выводить информацию при помощи функции printf следующим образом:

```
printf("%s", argv[1]);
```

Как видно на рис. 3, теперь нельзя вывести данные таким способом.

Рисунок 3. Невозможность выведения данных приведенным способом

Таким образом, уязвимость дефекта форматных строк является достаточно опасной, так как может привести как к утечке данных, так и к утере контроля над исполнением приложения, но защита от данной уязвимости выполняется достаточно просто. Поэтому при разработке необходимо думать не только о функциональной составляющей приложения, но и о его безопасности.

Литература

1. Джек Козиол, Искусство взлома и защиты систем. Питер, 2006. 416 с.
2. Майкл Ховард, Двадцать четыре смертных греха компьютерной безопасности. Питер, 2010. 400 с.

КИБЕРБЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

Н. В. Горяйнова
руководитель – канд. экон. наук, доцент ***И. В. Лебедева***
Северо-Кавказский федеральный университет, г. Ставрополь

Данная статья рассказывает о том, что в связи с развитием информационных и компьютерных технологий возникают проблемы, которые связаны с информационной безопасностью. На современном этапе развития общества киберпреступность приобрела глобальный характер. Рассматриваются проблемы организации противодействия преступлениям, которые совершаются в сфере информационных технологий. Для эффективной борьбы предлагается совершенствовать правовую базу и разработать концепцию организации противодействия киберпреступности.

Ключевые слова: киберугроза, киберпространство, кибертерроризм, информационное пространство, киберпреступления, киберзащита, защита информации.

В современном мире наблюдается резкий рост инцидентов в области информационной безопасности. Они широко распространяются и как правило, носят угрожающий характер. Большинство из таких атак затрагивают частные, корпоративные и государственные интересы. Причины развития угроз очень разнообразны, например: возрастание числа атак, ведущих к большим потерям; воздействие на все электронные устройства, в особенности мобильные телефоны; применение наиболее развитыми странами технологических средств и методов кибернападения на другие государства.

Все это подтверждается ежедневными сводками новостей, где постоянно сообщают о новых атаках преступников в сфере информаций.

Ежегодно в сети обнаруживают миллиарды вредоносных объектов. За их распространение отвечает более чем 100 миллионов адресов. И каждый год это число увеличивается на 40%. Все атаки в информационном пространстве наносят колоссальный ущерб. За минувший год проведено 73% хакерских атак по экономическим причинам. На 2017 год убытки состави-

ли три триллиона долларов. А на 2021 год прогнозируют убыток шесть триллионов долларов.

В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)» [3, с. 4]. Если говорить о кибербезопасности, то можем сказать, что это совокупность условий, при которой все составляющие киберпространства защищены от максимально возможного числа угроз и действий с нежелательными последствиями.

Киберпространство – это сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, ПО, интернет сервисов посредством технологических устройств и сетевых связей. Его мы можем рассмотреть, как триаду, в которую входят три составляющие: информация в цифровом представлении (файлы, записанные на носители данных; пакеты, команды и т.д. передаваемые по различным сетям); техническая инфраструктура, с помощью которых осуществляется реализация основных действий с информацией (сбор, обработка, хранение и передача); информационное взаимодействие [2, с. 340].

Каждый день вирусы-вымогатели атакуют 4000 компьютеров. Если рассматривать в глобальном масштабе, то киберпреступность стала вторым наиболее частым преступлением. В течение нескольких минут происходят 93% хищения данных и из них 83% утечек не обнаруживаются владельцами на протяжении несколько недель. Самым крупным хищением данных был инцидент с Yahoo, когда в 2013 году злоумышленники похитили три миллиарда телефонных номеров. На (рис. 1) представлена статистика по количеству киберпреступлений по наиболее частым видам кибератак.

Рисунок 1. Количество киберпреступлений по видам (март – апрель 2017 год)

Статистика компании Positive Technologies дает право утверждать, что в течение всего 2017 года финансовые компании входили в пятерку наиболее атакуемых киберпреступниками типов организации. В этом же году киберпреступники выработали основные схемы по быстрой монети-

зации. Самые распространенные атаки на АТМ (логические атаки на банкоматы). Такой тип демонстрирует драматический рост в этом году: за первое полугодие 2017 года общий объем атак такого типа в странах Европы вырос на 500% [4, с. 7].

Существует ряд требований по защите от кибервоздействий. Система киберзащиты сетевого коммуникационного оборудования (КЗСКО) предназначена для защиты сетевого коммуникационного оборудования (коммуникаторов, маршрутизаторов, модемов). Эта система обеспечивает: защиту сетевого коммуникационного оборудования от кибервоздействий из внешних сетей; защиту от компьютерных вирусов и иного вредоносного ПО.

В рамках киберпреступности можно выделить отдельный вид – это кибертерроризм. Так называемые, современные преступники – террористы используют все возможные и легкодоступные средства и способы для достижения желаемого результата. С каждым годом профессионализм кибертеррористов в использовании информационных сетей растет. Следовательно, кибербезопасность является проблемой государственной важности. Масштабность угрозы требует внимания и применения решительных мер ведущими государствами мира и объединения в целях предотвращения преступлений, которые совершаются в киберпространстве.

Литература

1. Гриняев С.Н., Поле битвы – киберпространство. М., 2004. 426 с.

2. Климов С.М. Методы и модели противодействия компьютерным атакам// КАТАЛИТ. Люберцы, 2008. 316 с.

3. Тонких И. М., Комаров М. М., Ледовской В. И., Михайлов А. В. Основы кибербезопасности // Описание курса для средних школ, 2-11 классы. М., 2016. 113 с.

4. Positive cinema cyberdocumentary// Кибербезопасность 2017-2018: цифры, факты, прогнозы. URL https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2017-2018-rus.pdf

АНАЛИЗ УЯЗВИМОСТИ МИКРОАРХИТЕКТУРЫ СОВРЕМЕННЫХ ЦЕНТРАЛЬНЫХ ПРОЦЕССОРОВ НА ПРИМЕРЕ АТАКИ MELTDOWN

М. А. Гражданкин, И. А. Коваль
руководитель – канд. физ.-мат. наук, доцент ***М. А. Лапина***
Северо-Кавказский федеральный университет, г. Ставрополь

Безопасность компьютерных систем фундаментально зависит от механизма изоляции памяти, т.е. диапазоны адресов на уровне ядра должны быть отмечены как недоступные и, тем самым, защищены от произвольного пользовательского доступа. Целью данной статьи является рассмотрение уязвимостей архитектуры центральных процессоров (ЦП) на примере реализации атаки Meltdown. Meltdown эксплуатирует побочные эффекты технологии внеочередного исполнения, которая используется в современных ЦП. С помощью эксплуатации недоче-

тов данной технологии становится возможным применить уязвимость, которая позволяет считывать произвольные участки памяти ядра, включая парольную и другую конфиденциальную информацию.

Ключевые слова: центральный процессор, информационная безопасность, уязвимость, ядро, память, аппаратное обеспечение, программное обеспечение, инструкции, внеочередное исполнение, Meltdown.

Одной из центральных функций обеспечения безопасности в современных ОС является изоляция памяти. ОС обеспечивают разграничение областей памяти, таким образом, при котором пользовательские приложения не имеют возможностей для записи и чтения памяти сторонних приложений на уровне ядра. Такая изоляция является основополагающей концепцией современных компьютерных систем и позволяет множеству различных приложений функционировать одновременно.

В современных ЦП изоляция между ядром и пользовательскими процессами традиционно осуществляется частью процессора, называемой супервизор. Супервизор использует бит, который определяет, разрешен доступ к определенному участку памяти ядра или нет. Основная идея заключается в том, что значение данного бита может быть установлено только в процессе ввода кода на уровне ядра, а при переключении на пользовательские приложения значение бита сбрасывается. Данная аппаратная особенность позволяет ОС обозначить участок ядра в адресном пространстве каждого процесса и, тем самым, получать крайне эффективные переходы между пользовательскими процессами и ядром, т.е. обработку прерываний. Следовательно, на практике отсутствует необходимость производить переназначение участков памяти при переключении между пользовательскими процессами и ядром.

При исследовании уязвимостей на базе центральных процессоров текущего поколения была обнаружена уязвимость, получившая название Meltdown. Meltdown является неизвестной доселе атакой, которая позволяет полностью обходить механизм изоляции памяти путем предоставления любому пользовательскому процессу простого пути для чтения всей памяти ядра на функционирующем оборудовании, включая все участки физической памяти, назначенные в области ядра. Meltdown не базируется на программных уязвимостях, т.е. работает на всех крупных и популярных ОС. Напротив, Meltdown основывается на использовании побочной информации, доступной на большинстве современных ЦП (например, процессоры Intel начиная с 2010 года выпуска и позднее).

Хотя атаки через побочный канал обычно требуют точных знаний в области их применения и направлены на получение информации в узкой сфере их реализации, Meltdown позволяет злоумышленнику, который имеет возможность исполнения кода на уязвимом ЦП, полностью выгрузить данные из адресного пространства ядра, включая назначенные участки

физической памяти. Корневой причиной такой простоты и опасности Meltdown являются побочные эффекты, вызванные недочетом в механизме внеочередного исполнения.

Технология внеочередного исполнения является важной особенностью современных ЦП, которая позволяет избежать замедлений, вызванных занятостью исполняющих блоков (например, блок обмена данными с памятью вынужден ожидать получения данных из памяти). Вместо остановки процесса исполнения, современные ЦП выполняют операции вне очереди, т.е. анализируют предстоящие операции и распределяют их между простаивающими блоками исполнения. Однако, такие операции часто обладают нежелательными побочными эффектами. Например, отсутствие синхронизации может приводить к утечке информации, как при последовательном, так и при внеочередном исполнении.

С точки зрения безопасности, важно следующее наблюдение: при использовании внеочередного исполнения уязвимые процессоры позволяют неуполномоченному процессу выгружать данные из привилегированного адреса во временный регистр ЦП. Более того, ЦП использует значение данного регистра для выполнения дальнейших вычислений, например, для получения доступа к массиву на основе значения регистра. Процессор обеспечивает корректное исполнение программ путем простого отброса результатов поиска в памяти (к примеру, изменений состояний регистра) в том случае, если исполнение инструкции не должно осуществляться. Таким образом, на уровне архитектуры (т.е. базируясь на абстрактном представлении о том, как процессор должен проводить вычисления) не возникает проблем безопасности.

Тем не менее, наблюдения показывают, что процесс поиска в памяти, осуществляемый вне очереди, оказывает влияние на кэш, который, в свою очередь, может быть раскрыт через побочный канал кэша. В результате, злоумышленник может выгрузить всю память ядра путем чтения привилегированного участка памяти в рамках потока внеочередного исполнения и передать полученные данные во внешние каналы через микроархитектурные каналы утечки информации. На принимающей стороне канала утечки информации значение регистра воссоздается. Следовательно, на микроархитектурном уровне (т.е. на уровне аппаратной реализации) существует реальная проблема безопасности.

Meltdown разрушает все представления о безопасности, основанные на возможностях изоляции памяти, которые предоставляются центральным процессором.

Атака Meltdown состоит из 3-х шагов:

Содержимое желаемого участка памяти, недоступное для злоумышленника, выгружается в регистр.

Мимолетная инструкция получает доступ к линии кэша на основании скрытого содержимого регистра.

Злоумышленник использует побочный канал утечки информации (такой как атака типа FLUSH+RELOAD) для определения линии кэша, к которой был получен доступ и, следовательно, к скрытому содержимому выбранного участка памяти.

Таким образом, в результате данного исследования можно сделать вывод о серьезности и практической значимости уязвимостей физической архитектуры современных процессоров. Технологии, применяемые для эффективного функционирования процессора и наиболее быстрого исполнения инструкций, несут в себе потенциальный риск для безопасности любых систем, которые используют уязвимые ЦП. Следует отметить, что зависимость от применяемого на системах ПО отсутствует, а соответственно, отсутствует необходимость применения программных уязвимостей для реализации атак, направленных на архитектуру микропроцессора.

Литература

1. Moritz L. [Мориц Л.]. Meltdown [Электронный ресурс]. URL: https://meltdownattack.com/meltdown.pdf (дата обращения: 04.04.2018).

АНАЛИЗ И СОДЕРЖАНИЕ ПОЛНОГО МНОЖЕСТВА ФУНКЦИЙ ЗАЩИТЫ В КОНТУРЕ КЛИЕНТА СЕТЕВОЙ ФАЙЛОВОЙ СИСТЕМЫ

М. А. Гражданкин, А. П. Львова, И. А. Коваль
Северо-Кавказский федеральный университет, г. Ставрополь

В ходе исследования было проанализировано полное множество функций защиты в контуре клиента файловой системы. Клиент сетевой файловой системы разделен на три части. Для каждой части были предложены различные соответствующие средства и системы защиты, обеспечивающие необходимый уровень информационной безопасности.

Ключевые слова: сетевая файловая система, информационная безопасность, сетевой доступ, клиент файловой системы, средства защиты информации, network file system, хранение информации, обработка информации.

Сетевая файловая система – метод размещения файлов в системе посредством протокола сетевого доступа NFS (Network File System). В модели организации информационной системы предприятия сетевая файловая система является ключевым элементом.

Клиент файловой системы разделяется на две основных зоны. Первая зона – долговременное запоминающее устройство (ДЗУ). В ДЗУ располагаются аппаратные средства хранения и ввода/вывода информации: стационарные и сменные накопители информации, устройства печати и т.п.

Угрозы информационной безопасности в области ДЗУ: загрузка с несанкционированного носителя, прямой доступ к информации на носителе, перехват.

Программные и технические средства нападения: аппаратные закладки, средства перехвата ПЭМИН.

Для обеспечения защиты целесообразно применять аппаратное шифрование информации, аппаратный контроль целостности, средства борьбы с ПЭМИН.

Вторая зона – оперативное запоминающее устройство (ОЗУ). Здесь размещаются временные файлы чтения/записи.

Угрозы информационной безопасности в области ОЗУ: модификация системных и прикладных программ, использование уязвимостей системных и прикладных программ, внедрение программных закладок, использование чужих или похищенных реквизитов доступа.

Программные и технические средства нападения: вредоносные программы.

Защита: программное шифрование информации, антивирусные программы, средства безопасности ОС, программы контроля целостности.

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М: «Гелиос АРВ», 2010. 336 с.

2. Сагдеев К. М. Физические основы защиты информации: учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург, 2017.

3. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В. С. // Известия ЮФУ. Технические науки. 2009. С. 172-176.

4. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Информационное противодействие угрозам терроризма, 2010. С. 114-118.

5. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.

6. Чипига А. Ф. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев // Фундаментальные исследования, 2015. С. 759.

7. Securelist. Лаборатория Касперского. [Электронный ресурс] URL: https://securelist.ru/it-threat-evolution-q3-2017-statistics/87982/

РАЗРАБОТКА МОДЕЛИ СБОРА И ОБРАБОТКИ ДАННЫХ ОТКРЫТЫХ ИСТОЧНИКОВ ПОКАЗАТЕЛЕЙ КОМПРОМЕТАЦИИ ДЛЯ SIEM-СИСТЕМ

Е. А. Емельянов, А. С. Антипов, Ю. А. Андрусенко
руководитель – канд. физ.-мат. наук, доцент ***О. В. Малсугенов***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье описаны способы и модели сбора и обработки данных для формирования базы индикаторов угроз в системах мониторинга и управления событиями информационной безопасности(*SIEM-системах*).

Ключевые слова: SIEM-система, показатель компрометации, IOC, база показателей компрометации, информационная безопасность.

Анализируя современные требования к качеству и эффективности работы SIEM-систем, следует отметить, что их эффективная работа существенно зависит от уровня точности детектирования инцидентов информационной безопасности, а также их своевременного расследования.

Значительную роль в повышении точности детектирования инцидентов информационной безопасности играет формирование и поддержание в актуальном состоянии комплексной базы показателей компрометации на основе анализа открытых источников. Особенностью использования открытых источников является необходимость разработки уникальных модулей сбора и обработки данных для каждого источника в связи с отсутствием единых форматов и стандартов представления информации о показателях компрометации.

Вышесказанное определяет актуальность разработки, внедрения и использования технологий сбора и обработки данных для последующего использования в SIEM-системах.

В результате анализа предметной области сформирован набор исходных данных для разработки структуры базы данных. В табл. 1 приведены основные параметры трафика, используемые в качестве показателей компрометации, предоставляемые открытыми источниками.

Таблица 1

Параметры трафика, используемые в качестве показателей компрометации

Показатель	Описание
IP	Адреса узлов и сетей в сети Интернет, содержащие и распространяющие вредоносное ПО или распространяющие нежелательный контент.
DNS	Доменные имена узлов, содержащие и распространяющие вредоносное ПО или распространяющие нежелательный контент.
URL	Адреса страниц веб-серверов в сети Интернет, содержащие и распространяющие вредоносное ПО или распространяющие нежелательный контент.
ASN	Уникальный номер автоматизированной системы

Информацию открытых источников показателей компрометации можно классифицировать по типам угроз.

Таблица 2

Классификация источников показателей компрометации

Тип угрозы	Источник
Botnet	Alienvault OTX Public Malware Domain List Feodotracker Zeustracker Malwaredomains C1fapp Bambenekconsulting
Malware	Alienvault OTX Public Malware Domain List Clean MX Malc0de Malwaredomains Nothink C1fapp Talos
Suspicious	Alienvault OTX Public Malware Domain List Dshield Malwaredomains C1fapp
Phishing	Alienvault OTX Public Clean MX Malware Domain List C1fapp
Spam	SpamHaus Alienvault OTX Public Projecthoneypot C1fapp

Описание типов угроз:

Botnet – хост используется для управления другим хостом или вредоносным процессом. Соответствующий трафик указывает на заражение, используемое для идентификации скомпрометированных хостов.

Malware – вредоносные программное обеспечение; хост используется для эксплуатации и/или распространения вредоносных программ.

Suspicious – используется как тип «по умолчанию», в сочетании с исходным описанием для более детального анализа. Также содержит узлы Tor Exit и анонимные прокси соединения.

Phishing – хост используется с целью получения конфиденциальной информации обманным путем с помощью электронной почты или фишинговых сайтов.

Spam – хост используемый для массовой рассылки сообщений, распространения вредоносных программ, троянских загрузчиков, контроллеров ботнета.

Описание технической реализации.

В качестве инструментального средства сбора информации из открытых источников используются разработанные PHP-скрипты, реализующие взаимодействие на основе протоколов HTTP/HTTPS методом GET, взаимодействие через интерфейсы REST API или специализированный API интерфейс ресурса. Полученные данные передаются модулям синтаксического анализа в зависимости от формата представления информации (JSON, XML, TXT, HTML и т.д.). С выхода модулей структурированная информация передается в модуль нормализации формирования базы источников компрометации. Скрипт модуля нормализации приводит данные к единому формату. Дополнительно в модуле нормализации реализован функционал первичного обогащения расширенными данными с использованием открытых сервисов (библиотека SxGeo для получения геоинформации по ip-адресу, сервисы robtex, whois и т. д.). После нормализации и обогащения скрипт формирует запись в базе данных, а также создает выходные данные для загрузки в SIEM систему с учетом требуемого формата, принятого в SIEM-системе. База данных индикаторов компрометации содержит дополнительно весовые коэффициенты для каждого из объектов, характеризующие степень достоверности информационной записи.

Модель SIEM системы с модулем технического сбора и обработки данных открытых источников показателей компрометации представлена на рис. 1.

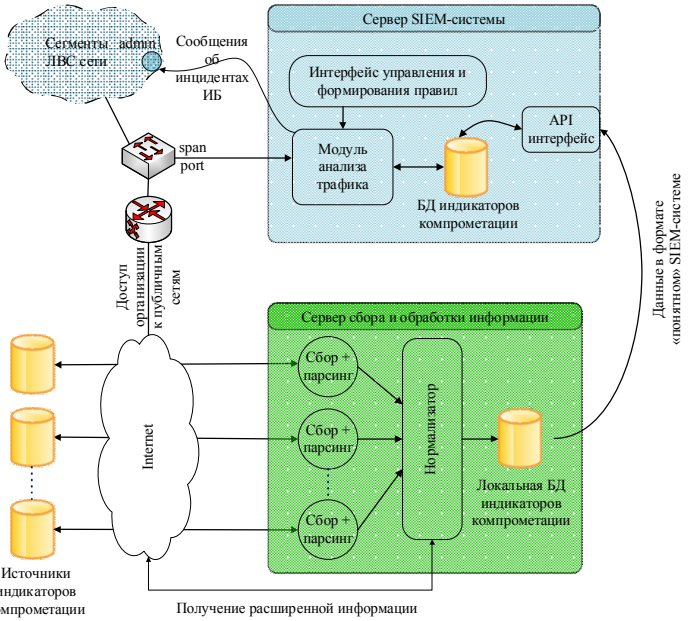


Рисунок 1. Модель SIEM системы с модулем технического сбора и обработки данных из открытых источников

В качестве СУБД для управления базой индикаторов компрометации используется MySQL. MySQL обеспечивает достаточный уровень безопасности, а благодаря открытому коду существует возможность расширения функционала, при этом MySQL является достаточно эффективной на небольших объемах данных.

Разработанная модель сбора и анализа индикаторов компрометации на основе открытых источников позволяет сформировать независимую от производителей базу данных, обеспечить ее наполняемость и поддержание в актуальном состоянии из большого количества открытых независимых источников, расположенных в различных доменных зонах сети интернет. Использование проприетарных решений иностранных производителей приводит к зависимости организаций, эксплуатирующих SIEM системы, от доступа к внешним базам данных производителя в режиме реального времени, слабой проверяемости актуальности базы и ее полноты.

Литература

1. Kotenko I., Chechulin A. Attack modeling and security evaluation in SIEM systems // Intern. Transact. on Systems Science and Applications. 2012. Vol. 8, Dec. P. 129-147.
2. Kotenko I. V., Stepashkin M. V. Network Security Evaluation Based on Simulation of Malefactor's Behavior // Proc. of the Intern. Conf. on Security and Cryptography, (SECRYPT 2006), Portugal, Aug. 7–10, 2006. P. 339–344.
3. Ruiz J. F., Harjani R., Maña A., Desnitsky V., Kotenko I., Chechulin A. A methodology for the analysis and modeling of security threats and attacks for systems of embedded components // Proc. of the 20th Euromicro Intern. Conf. on Parallel, Distributed and Network-Based Processing (PDP 2012). Garching, Germany. 2012. C. 261-268.
4. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 7-24.
5. Kotenko I. V., Chechulin A. A. Common framework for attack modeling and security evaluation in SIEM systems // IEEE Intern. Conf. on Green Computing and Communications, Conf. on Internet of Things, and Conf. on Cyber, Physical and Social Computing; Besançon, France, 11-14 Sept., 2012; Los Alamitos, CA: IEEE Computer Society, 2012. P. 94-101.

КОМПЛЕКСНАЯ ОЦЕНКА УЯЗВИМОСТЕЙ ИНФОРМАЦИИ В КОНТУРЕ ЗАЩИТЫ КЛИЕНТА СЕТЕВОЙ ФАЙЛОВОЙ СИСТЕМЫ

Е. В. Ермолаева

Северо-Кавказский федеральный университет, г. Ставрополь

В связи с высокой актуальностью защиты информации в сетевых файловых системах в статье в данной статье рассматривается структура контура защиты клиента сетевой файловой системы, приводится список угроз и средств защиты для зон ДЗУ и ОЗУ, рассматриваются способы оценки уязвимости информации, на их основе сделаны выводы.

Ключевые слова: сетевая файловая система, ДЗУ, ОЗУ, файл, информация, уязвимость, угроза.

Сетевая файловая система является одним из важнейших компонентов информационной инфраструктуры предприятия. Этот факт подразумевает необходимость решения задачи ее защиты. На сегодняшний день при наличии огромного списка угроз информационной безопасности решение этой задачи невозможно без применения комплексного подхода к использованию технологий и средств защиты информации.

Контурзашиты клиента сетевой файловой системы представляет из себя совокупность зоны ДЗУ и зоны ОЗУ. В зоне ДЗУ расположены аппаратные средства хранения информации, устройства вводы и вывода информации и т.д. В Зоне ОЗУ располагаются прикладные программные средства. Структура контура защиты клиента изображена на рис. 1.

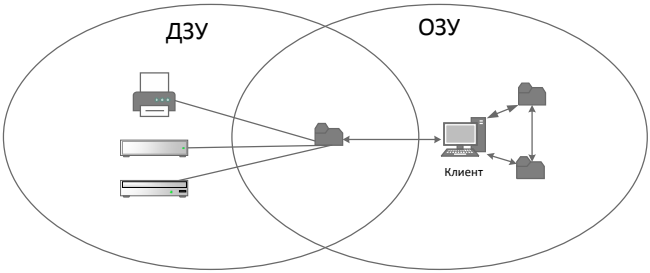


Рисунок 1. Структура контура защиты клиента сетевой файловой системы

Зона ДЗУ подвержена следующим видам угроз:

- загрузка с несанкционированного носителя;
- прямой доступ к информации на носителе;
- перехват.

Средства безопасности в зоне ДЗУ предназначенные для предотвращения угроз:

- аппаратный контроль целостности;
- аппаратное шифрование информации;
- средства борьбы с ПЭМИН.

Угрозы, которым подвержена зона ОЗУ:

- модификации системных и прикладных программ;
- использование уязвимостей системных или прикладных программ;
- внедрение программных закладок;
- использование чужих или похищенных реквизитов доступа.

Средства безопасности:

- программы контроля целостности;
- средства безопасности ОС;
- антивирусное ПО;
- программное шифрование информации.

Влиянию побочных электромагнитных излучений подвержены обе зоны.

Поскольку воздействие на информацию различных факторов в значительной мере является случайным, то в качестве количественной меры уязвимости информации целесообразно принять вероятность нарушения защищаемых характеристик ее при тех условиях обработки и хранения, которые имеют место в сетевой файловой системе, а также потенциально возможные размеры (математическое ожидание) нарушения защищенности информации.

Множество разновидностей различных показателей уязвимости определяется декартовым произведением чисел, характеризующих количество значений всех значащих параметров.

Для исследования и практического решения задач защиты информации наряду с рассмотренными выше необходимы еще такие показатели, которые характеризуют наиболее неблагоприятные ситуации с точки зрения уязвимости информации. Такими являются: самый уязвимый структурный компонент АСОД, самый опасный дестабилизирующий фактор, самый опасный нарушитель. Эти показатели могут быть названы экстремальными.

При том, что существует несколько способов оценки уязвимостей информации, для получения правильных показателей необходима оценка группой экспертов. Только тогда на основе полученных значений удастся реализовать надежную защиту информации в сетевой файловой системе.

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М: «Гелиос АРВ», 2010. 336 с.

2. Сагдеев К. М. Физические основы защиты информации: учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург, 2017.

3. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В.С. //Известия ЮФУ. Технические науки. 2009. С. 172-176.

4. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Информационное противодействие угрозам терроризма, 2010. С. 114-118.

5. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.

6. Чипига А. Ф. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев // Фундаментальные исследования, 2015. С. 759.

7. Securelist. Лаборатория Касперского. [Электронный ресурс] URL: https:// securelist.ru/spam-and-phishing-in-2017/88630/

8. Infowatch. Аналитика. [Электронный ресурс] URL: https://www.infowatch.ru/analytics

ТИПОВЫЕ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЕВОЙ ФАЙЛОВОЙ СИСТЕМЕ

П. А. Жолобов, А. П. Львова, А. Е. Костянов
Северо-Кавказский федеральный университет, г. Ставрополь

Приведена общая структура сетевой файловой системы и проанализированы типовые нарушения ее информационной безопасности. На основе последних статистических данных выявлены наиболее опасные и часто встречающиеся, а также обозначены средства, способные предотвратить утечку информации из сетевой файловой системы.

Ключевые слова: сетевая файловая система, NFS, утечка, типовые нарушения, информационная безопасность, криптоалгоритмы, антивирусное ПО, сетевые протоколы.

Сетевая файловая система является важнейшим компонентом информационной структуры предприятия. Она позволяет централизовать информацию, обеспечивать контролируемый доступ и экономить вычислительные ресурсы узлов сети.

Принцип работы заключается в том, что множество клиентов объединяются в большую сеть, а функции над файлами, такие как управление, хранение и другие делегируются серверу или нескольким серверам. Получение доступа к информации основывается на запросах к серверу с помощью протокола вызова удаленных процедур ОТС RPC (Open Network Computing Remote Procedure Call).

Логическая структура сетевой файловой системы представляет собой совокупность трех зон: оперативное запоминающее устройство (ОЗУ), долговременное запоминающее устройство (ДЗУ) и линии вычислительных сетей (ЛВС). Каждая из трех зон присутствует на узлах системы и обеспечивает исправную работу с файлами. Однако, любая система, проводящая операции с информацией, нуждается в защите.

В более подробном рассмотрении можно сделать вывод, что всем зонам присущи свои специфические уязвимости и их устранение необходимо проводить в зависимости от ситуации и характера обрабатываемой информации. При общем анализе выявлены следующие типовые нарушения информационной безопасности в сетевой файловой системе:

1. Получение удаленного контроля над узлами вычислительной сети;
2. Перехват информации в телекоммуникационной системе;
3. Распространение вредоносного программного обеспечения;
4. Подавление сетевых средств защиты и управления;

Одной из причин, которая может вызвать сразу несколько типовых нарушений является отсутствие защитного программного или аппаратного обеспечения. Необходимость установки антивирусов и межсетевых экранов обуславливается официальными статистическими данными. Так,

например, согласно информации компании Kaspersky, зафиксировано 72012219 уникальных URL, на которых происходило срабатывание веб-антивируса. Попадание вируса на компьютер, подключенный к сети ставит под угрозу всех участников информационного обмена.

Кроме того, перехват информации в телекоммуникационной системе возможен по причине уязвимостей протоколов, используемых при передаче данных. Если сервера и узлы связываются посредством сети «Интернет» необходимо применять протоколы скрытия адресов, например NAT (Network Address Translation – «преобразование сетевых адресов»), организовывать защищенную передачу данных с помощью GRE-туннеля или технологии VPN. Кроме того, телекоммуникационная система подвержена такой уязвимости как анализ сетевого трафика, при которой можно перехватить пароль и логин и осуществить доступ к конфиденциальной информации. Защита от данной атаки может заключаться в сильной аутентификации (одноразовые пароли, двойная аутентификация), анти-снифферы, криптографические методы (протоколы IPSec, SSL, SSH).

В заключение, можно сделать вывод, что основной причиной типовых нарушений информационной безопасности сетевой файловой системы являются уязвимости протоколов передачи данных. Для решения этой проблемы необходимо применять надежно защищенные криптоалгоритмами протоколы. Кроме того, доступ к информации должен предоставляться посредством аутентификации, в том числе и двухфакторной. От защиты узлов и линий вычислительных сети зависит качество работы с информацией и ее безопасность.

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М: «Гелиос АРВ», 2010. 336 с.

2. Сагдеев К. М. Физические основы защиты информации: учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург, 2017.

3. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В. С. // Известия ЮФУ. Технические науки. 2009. С. 172-176.

4. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Информационное противодействие угрозам терроризма, 2010. С. 114-118.

5. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.

6. Чипига А. Ф. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев // Фундаментальные исследования, 2015. С. 759.

7. Securelist. Лаборатория Касперского. [Электронный ресурс] URL: https://securelist.ru/it-threat-evolution-q3-2017-statistics/87982/

ПУТИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В МЕДИЦИНЕ

Н. Ю. Журавлев, Е. С. Пелешенко
руководитель – старший преподаватель ***О. В. Криволапова***
Северо-Кавказский федеральный университет, г. Ставрополь

В наше время компьютерные технологии являются неотъемлемой частью во всех сферах человеческой деятельности, не исключая и в медицине. С каждым днем количество медицинской информации растет, поэтому применение компьютерных технологий в медицине на данном этапе необходимо, а также для более верных результатов исследований в этой сфере. Средства коммуникации между людьми и организациями на сегодняшний день прогрессируют большими шагами.

Ключевые слова: компьютерные технологии, информационные технологии, медицинская информация, медицинская информатика.

Телемедицина – это использование телекоммуникационных технологий для обеспечения медицинской информацией и медицинским обслуживанием потребителей, которые находятся на расстоянии от медицинского персонала. Данное определение используется в сегодня как совокупность проведения консультаций и установления диагноза дистанционно.

Телемедицину можно определить, как систему, обеспечивающую доступ к новейшим медицинским источникам, как локальным, так и мировым. Такая система является совокупностью, обеспечивающая возможность развития информационных и телекоммуникационных технологий в медицине, а также финансово-правовое оснащение. Телемедицина совместно с интернет технологиями обеспечивает рациональное использование научных и практических возможностей медицинской сферы. Таким образом, прогресс в области телемедицины исключает необходимость в физическом присутствии.

В наше время телемедицина преследует следующие цели, добившись которых, поднимет на ступень выше медицину:

– постоянное профилактическое обследование граждан;

– большие перспективы по снижению стоимости оказания медицинских услуг;

– обеспечение обследование удаленных граждан;

– увеличение уровня медицинских работ.

Современные телемедицинские методы дают возможность проводить удалённые консультации врачей и их пациентов, которые находятся в отдалённых районах. Применение технологий для видеосвязи, которые позволяют контактировать в режиме видео, обеспечивает современные возможности в разных видах врачебной деятельности. Например, если доктор сталкивается с трудной задачей в практике, он советуется со своими коллегами, нередко есть необходимость в консультации с коллегами за рубе-

жом. На данном этапе развития информационных технологий такие возможности как обмен электронными документами, общение в соц. сетях интернета, общения при помощи устройств видеосвязи. Для организации видеоконференцсвязи необходимы персональный компьютер, настроенный для выхода в Интернет, со звуковыми и видео возможностями, кодер-декодер (для сжатия/декомпрессии видео и звуковых сигналов), видео камеры, микрофоны, и подключение к выделенной линии через высокоскоростной модем, к локальной сети или сети Интернет. В роли медицинской информации передаются и обсуждаются данные эхокардиограмм, кривые ЭКГ, видеоматериалы диагностических процедур и этапов операций. Постепенно в жизнь входит дистанционное консультирование. Ситуации, когда необходимо вносить правку в назначениях для постоянного пациента, такая услуга может показаться наиболее эффективной и быстрой. Например, часто поступают эндокринологи, при лечении сахарного диабета регулируют дозировку лекарств в зависимости от показателя уровня глюкозы в крови. Кроме того, возможность дистанционного консультирования с врачом оказывается важной, когда больной живёт в удалённом регионе.

Развитие телемедицина облегчает и улучшает эффективность лечения и обследование на высшем уровне. Дистанционное общение предоставляет новые возможности для консультирования, но стоит помнить, что полномочия врача при онлайн консультации чаще всего ограничиваются предоставлением информации справочного характера. Невозможно получить точный диагноз и план лечения, описав претензии на форуме. В этом случае предоставляется информация о причинах, симптомах заболевания, показании к применению тех или иных препаратов, но правильного диагноза и более эффективного результата в лечении добиться не получится. При удаленной постановке диагноза вероятность ошибки увеличивается, поэтому администраторы медицинских сайтов используют различные формы ограничения способов консультирования. Подобное ограничение диктуется и кодексом этики врачей, но поскольку этот кодекс не имеет законодательного подкрепления, в сети появляются разнообразные ресурсы, предоставляющие услуги некомпетентными специалистами.

Таким образом, телемедицина – это направление объединяющая несколько областей: медицина, телекоммуникации, информационные технологии, образование. Телемедицина прогрессирует во многих государствах мира, показала на практике свою высокую эффективность, повышает качество медицинской помощи и увеличивает возможности врачей опыта работы. Обеспечивает взаимодействие между здравоохранительными учреждениями, для решения определенной проблемы. Выделены цели для развития телемедицины, среди которых названы стандартизация применяемых медицинских, компьютерных и телекоммуникационных технологий, а также развитие медицинских информационных ресурсов.

Литература

1. Буравков С. В., Григорьев А. И. Основы телемедицины. М.: Фирма «Слово», 2001. 112 с.

2. Григорьев А. И., Орлов О. И. Клиническая телемедицина. М.: Фирма «Слово», 2001. 144 с.

3. Лях Ю. Е., Владимирский А. В. Введение в телемедицину. Серия «Очерки медицинской и биологической информатики». Донецк: ООО «Лебедь», 1999. 134 с.

СИСТЕМНАЯ ОЦЕНКА ТИПОВЫХ НАПАДЕНИЙ НА ЗОНУ ДЗУ КЛИЕНТА ЭЛЕКТРОННОЙ ПОЧТЫ

Н. Г. Заргаров, А. П. Львова

Северо-Кавказский федеральный университет, г. Ставрополь

В ходе исследования выполнена системная оценка типовых нападений на зону ДЗУ клиента электронной почты. Приведены данные аналитики центров информационной безопасности и выявлены основные причины возникновения типовых нападений. По результатам исследования даны рекомендации по обеспечению защиты зоны ДЗУ клиента электронной почты.

Ключевые слова: электронная почта, информационная безопасность, ДЗУ, клиент, нападения, утечка данных, информация, защита.

Представить современный мир без электронной почты уже невозможно. Сотни миллионов почтовых ящиков, триллионы сообщений ежегодно, терабайты данных ежедневно. Адрес электронной почты стал для современного общества столь же обязательным, как домашний адрес, а для многих организаций является неотъемлемой частью электронного документооборота.

Структуру почтовой системы составляют два основных узла:

1. Компьютер с базой данных сообщений пользователя (клиент ЭП).
2. Сервер, выполняющий роли шлюза, концентратора и сервера пересылки электронной почты.

Клиент формирует, отправляет, принимает, хранит сообщение, а также поддерживает справочник адресов электронной почты. Память клиента разделяется на долговременную (ДЗУ) и оперативную (ОЗУ). ДЗУ вызывает интерес у зломышленников, так как здесь находятся базы данных сообщений и адресов. Исходя из этого типовыми нападениями на зону ДЗУ клиента являются:

1) Утечка классифицированной информации. Возможными причинами возникновения являются попадание файлов во временные области памяти почтовой системы, в область оперативной памяти, которые могут быть доступны другим пользователям или программам.

Проблема решается строгой регламентацией работы с определенными категориями информации. Согласно статистике центра аналитики информационной безопасности InfoWatch, за первое полугодие 2017 года про-

изошло 925 утечек конфиденциальных данных, 520 из которых результат внутренних нарушений (например, вина сотрудников).

2) Хищение баз данных электронной почты или ее несанкционированное копирование.

Актуальность этой проблемы подтверждается периодической информацией СМИ о том, что хакерам стали известны пароли от почтовых ящиков. Кроме того, проходят активные фишинговые атаки, в ходе которых загружается вредоносное ПО.

Защитой от этой атаки могут являться антифишинговые средства, фильтры спама.

Аналитический центр Лаборатории Касперского Securelist сообщает, что за 2017 год было зафиксировано 246231645 срабатываний системы «Антифишинг», а доля почтового спама составила 56,63% от общего почтового трафика.

3) Хищение адресных справочников электронной почты. Результат – рассылка большого количества спама, который забивает память почтовой системы.

В заключении можно сделать вывод, что одними из основных причин типовых нападений являются некомпетентность сотрудников при работе с классифицированной информацией и фишинг.

Таким образом, защиту электронной корреспонденции в зоне ДЗУ необходимо осуществлять криптографическими средствами операционных систем и программного обеспечения электронной почты, средствами контроля целостности и антифишинговыми программами. Проведение работы с сотрудниками и регламентация процесса отправки конфиденциальной информации посредством почтовой системы также сыграет важную роль при построении системы защиты.

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М: «Гелиос АРВ», 2010. 336 с.

2. Сагдеев К. М. Физические основы защиты информации: учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург, 2017.

3. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В.С. //Известия ЮФУ. Технические науки. 2009. С. 172-176.

4. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Информационное противодействие угрозам терроризма, 2010. С. 114-118.

5. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.

6. Чипига А. Ф. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев // Фундаментальные исследования, 2015. С. 759.

7. Securelist. Лаборатория Касперского. [Электронный ресурс] URL: https://securelist.ru/spam-and-phishing-in-2017/88630/

8. Infowatch. Аналитика. [Электронный ресурс] URL: https://www.infowatch.ru/analytics

ПРОБЛЕМЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

М. Н. Иванов
Северо-Кавказский федеральный университет, г. Ставрополь

Рассмотрены проблемы биометрической идетификации.
Ключевые слова: защита информации, аутентификация, идентификация.

В наше время количество и ценность информации играют важную роль в жизни каждого человека. В связи с этим актуальна проблема ее защиты. Однако создавая «надежные» много символьные пароли велика вероятность их попросту забыть, да и они не гарантируют 100% безопасность. Однако даже в этой ситуации было принято инновационное решение и введены биометрические системы идентификации. Рассмотрим проблемы различных методов биометрической идетификации.

Обращаясь к подобным методам нужно сразу принять несколько фактов во внимание: биометрические системы по своей природе представляют почти полностью чисто математические данные. И что бы определить качество и безопасность нужно выявить все аспекты, влияющие на работу подобных систем.

Аутентификация по отпечаткам пальцев. Технология сканирования отпечатков пальцев – одна из самых распространенных. Отпечатки уникальны для каждого человека и не постоянны на протяжении всей жизни, поэтому они входят в группу статических методов распознавания.

Существует 3 типа сканеров отпечатков: оптические (FTIR, оптоволоконные, оптические протяжные и др.), полупроводниковые (термосканеры, протяжные термо-сканеры, емкостные и др.) и ультразвуковые. Они работают по разным принципам, но в итоге получают аналогичные данные, которые в соответствии с определенными математическими алгоритмами преобразуются в контрольную сумму. Возможные уязвимости:

1.Создание муляжа на основе высокоточного снимка пальца. Подобный муляж может сработать на простых сканерах.

Устранение:

1) установка многофункционального сканера, фиксирующего температуру и уровень пота.

2) Комбинирование с другими биометрическими системами защиты.

2. Перехват отпечатка в случае, если сканер связан с основной системой проводным интерфейсом.

Устранение: использование методов криптографии при передаче сигналов.

3. Восстановление конденсатом (направление струи теплого воздуха на сканер и, как результат, восстановление последнего отпечатка).

Устранение: уязвимость актуальна только для не дорогих оптических сканеров. Как еще один фактор, есть проблема идентификации пальца с

порезами, "сморщиванием" кожи и иными дефектами, ее можно обойти с помощью повторного идентифицирования отпечатков. Однако нужно не допустить избыточности биометрической информации в системе, потому что это является нарушением ФЗ "О персональных данных" и постановления "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных".

Идентификация по голосу. Внедрение этой технологии связано с быстрым ростом и распространением аналоговых линий разного типа. Этот вид биометрии основан на анализе характеристик голоса: высоте, частоте, тембре, скорости, манере речи и др.

Основные проблемы данного вида идентификации:

– изменение голоса (эмоции, состояние здоровья);

– помехи в микрофоне и линиях связи;

– перехват конфиденциальной информации нарушителем.

Решение: использование ларингофона может дать звуковой сигнал, индивидуальный для каждого человека и весьма трудно дискредитируемый. Значительное развитие данного способа аутентификации может дать использование вейвлет-преобразования, которое позволяет уменьшить количество ошибок первого рода при фиксированной ошибке второго рода.

Идентификация по геометрии лица. Системы по распознаванию геометрии лица работают на основе физиологических признаков (формы лица, симметрии/асимметрии лица, формы и размера губ, носа, глаз и т.д.). Приняв картину лица, система генерирует уникальный шаблон, который сравнивается с образцом, находящимся в базе данных. Такие системы используются на улицах и в аэропортах многих городов мира.

Недостатки метода:

1. Изменение света, выражения лица, волос, наличие или отсутствие дополнительных факторов (макияжа и др.) мешают идентификации.

Устранение: дорогие системы используют наблюдение в инфракрасном диапазоне (термография лица). Так можно установить, что качество прямо пропорционально зависит от цены.

2. Обход метода путем использования изображения лица зарегистрированного пользователя или подбор фотографий с разными типами лиц.

Устранение: использование 3D-распознавания.

3. Система не может отличить близнецов.

Устранение: комбинирование методов идентификации.

Литература

1. https://ru.wikipedia.org/wiki/Биометрия

2. https://www.speechpro.ru/product/sistemy-upravleniya-kachestvom-i-avtomatizatsii/voice-key/specification

СИСТЕМНАЯ ОЦЕНКА ТИПОВЫХ НАПАДЕНИЙ НА ЗОНУ ОЗУ СЕРВЕРА ЭЛЕКТРОННОЙ ПОЧТЫ

К. А. Каграманов
Северо-Кавказский федеральный университет, г. Ставрополь

В ходе исследования изучена структура системы электронной почты, проведен анализ типовых нападений на зону ОЗУ сервера электронной почты. На основе полученных результатов предложены рекомендуемые рубежи защиты.

Ключевые слова: защита, утечка, сервер, электронная почта, информационная безопасность, ОЗУ, информация.

В последнее время процент атак, связанных с электронной почтой неумолимо растет, ведь зачастую электронные послания содержат в себе особо ценную информацию для злоумышленников.

Не вдаваясь в подробности, условимся, что электронная почта, это сервис, позволяющий обмениваться сообщениями между адресатами и получателями.

Структура электронной почты представляет собой 3 основных элемента: ЛВС, клиент и сервер.

Клиент – это компьютер с соответствующим ПО для получения, отправки и чтения электронных сообщений. Также клиент занимается хранением почты в специальной почтовой базе данных.

Сервер – специальный компьютер, работающий на серверной архитектуре, выполняющий функции шлюза, концентратора электронной почты и занимающийся ее пересылкой.

ЛВС (линия вычислительной сети) обеспечивает передачу сообщений между адресатом и получателем через почтовый сервер.

В последние годы, в связи с более глубоким внедрением интернет технологии во все сферы жизни, в том числе использование электронных денег, количество утечек и скомпрометированной информации сильно возросло. По данным аналитического центра InfoWatch наиболее популярные сценарии утечки платежных данных через электронную почту (44,1%).

Клиент и сервер используют 2 типа памяти ДЗУ (долгосрочная) и ОЗУ (краткосрочная). Мы будем рассматривать краткосрочную. На зону ОЗУ сервера осуществляются следующие типовые нападения:

1. **Перехват электронной почты в оперативной памяти:**

Суть заключается в том, чтобы получить доступ к передаваемым сообщениям до того, как они будут зашифрованы различными средствами криптографической защиты. При использовании изъянов ПО это нападение значительно упрощает процесс получения информации из-за того, что не приходится расшифровывать перехваченное сообщение.

2. **Навязывание электронной почты в оперативной памяти:**

Используются программные закладки, которые формируют сообщения для передачи в процесс обработки электронной почты и принуждают

сервер принять их к отправке. Целью является очередь отправки в оперативной памяти

3. **Обход фильтров электронной почты**

Сообщение преобразуется таким образом, что становится невозможным их фильтрация по известным признакам

4. **Навязывание маршрутизации электронной почты**.

Как видно из названия, нападение принуждает систему доставить сообщение по определенному адресу. Реализуется за счет служебных функций системы и особенностей заголовочных файлов на основе масок и шаблонов.

Всех этих угроз можно избежать, если установить и правильно настроить следующие рубежи защиты:

1. **Рубеж фильтрации**, который борется с утечкой классифицированной информации, с распространением вредоносного ПО и спама.

2. **Рубеж преобразования на основе системы правил**, который модифицирует заголовки и содержимое электронных сообщений. Этот рубеж скрывает от злоумышленника внутреннюю структуру организации и реализует криптографическую защиту сообщений.

3. **Рубеж маршрутизации**, который управляет всеми информационными потоками и решает по какому каналу связи отправить сообщение. Дополнительной задачей этого рубежа является реализация отказоустойчивости системы за счет использования избыточных каналов связи.

На основе проведенного исследования были выявлены возможные нападения на зону ОЗУ сервера и необходимые меры для нейтрализации этих угроз.

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010. 336 с.

2. Сагдеев К. М. Физические основы защиты информации: учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург, 2017.

3. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В.С. // Известия ЮФУ. Технические науки. 2009. С. 172-176.

4. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Информационное противодействие угрозам терроризма, 2010. С. 114-118.

5. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.

6. Чипига А. Ф. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев // Фундаментальные исследования, 2015. С. 759.

7. РБК [Электронный ресурс] URL: https://www.rbc.ru

8. Infowatch. Аналитика. [Электронный ресурс] URL: https://www.infowatch.ru/analytics.

АНАЛИЗ ТИПОВЫХ НАПАДЕНИЙ НА ЗОНУ ОЗУ СЕРВЕРА ЭЛЕКТРОННОЙ ПОЧТЫ

В. А. Калашникова
Северо-Кавказский федеральный университет, г. Ставрополь

Глобальные информационные сети – одно из основных достижений человечества в области информационных технологий, главная примета вхождения в эпоху информационного общества. Делая возможным оперативное общение на огромных расстояниях, глобальные сети уже изменили для многих людей характер и возможности образования и профессиональной деятельности. В связи с растущим количеством пользователей растет и количество атак на них, поэтому система электронной почты нуждается в защите. Для организации мероприятий по обеспечению информационной безопасности необходимо ясно представлять структуру объекта защиты и характер связей и взаимодействий, составляющих основу электронного документооборота. Целью исследования является изучение компонентов электронной почты, нуждающихся в защите информации. Задача исследования выявление типовых нападений на зону ОЗУ сервера электронной почты и методов защиты от них.

Ключевые слова: электронная почта, информационная безопасность, оперативная память, сервер, нападения, программное обеспечение, информация, доступ.

Электронная почта (ЭП) – технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой компьютерной сети.

Основными компонентами системы являются:

- линия вычислительной сети (ЛВС);
- сервер;
- клиент.

Сервер – специализированное оборудование и/или специализированный компьютер для выполнения на нём сервисного программного обеспечения. Представляет собой компьютер, выделенный из группы рабочих станций для выполнения какой-либо сервисной задачи без физического участия человека. Сервер и рабочую станцию различают их лишь по присутствию человека в работе за консолью, так как они имеют одинаковую аппаратную конфигурацию. Сервер обеспечивает максимальную защищенность и безопасность выполняемых задач, а также их сохранность. Существует сервер для хранения файлов и веб-сайтов пользователей Интернета (хостинг), их используют для поиска ответа на запросы и выдачи запрашиваемой информации, обработки и выполнения скриптов на вебсайтах, работы с базой данных и большим количеством пользователей. За работу сервера отвечает системный администратор организации.

Различают два вида атак на сервер. Такие как, атаки зоны оперативного запоминающего устройства (ОЗУ) и атаки долговременного запоминающего устройства (ДЗУ).

Атаки зоны ДЗУ сервера бывают следующих типов:

1. Доступ с носителя информации к электронной почте. Происходит несанкционированное копирование или хищение информации.

2. Внедрение электронной почты на носитель информации. Цель: путем замены или модификации носителей с сообщениями электронной почты и внедрением опасной ситуации добиться замены подлинной информации с сервера электронной на фиктивную с носителя информации электронной почты.

В зоне ОЗУ сервера осуществляются следующие нападения:

1. Перехват электронных сообщений в оперативной памяти (ОП). Цель: с помощью вредоносной программы получить доступ к электронным сообщениям пользователя в ОП сервера на этапе сохранения на внешнем носителе информации.

2. Внедрение мнимой электронной почты в оперативную памяти для передачи сообщений, сформированных средствами вредоносных программ, в процесс обработки и принуждения сервера ЭП принять их к отправке через каналы межпроцессорного взаимодействия. Основной целью нападающей стороны является очередь сообщений для отправки, чтобы заполнить память процессора;

3. Метод обхода фильтров электронной почты путём использования служебных или других преобразований полученных сообщений ЭП делает невозможной фильтрацию по известным признакам в почтовой системе;

4. Внедрение ложного маршрута ЭП заставляет почтовую систему доставлять электронное сообщение по определенному маршруту за счет использования служебных функций системы ЭП, особенностей обработки заголовков на основе масок и шаблонов [1, с. 61]

Несовершенство систем передачи данных приводит к хищению информации и каждая новая уязвимость предоставляет доступ злоумышленникам. Однако именно это несовершенство и двигает вперед информационную безопасность, мотивируя создавать более надежные средства защиты. ОЗУ сервера можно защитить установкой следующих рубежей защиты:

– аутентификации и криптографическая защита канала передачи данных;
– рубеж фильтрация;
– рубеж преобразование на основе системы правил;
– рубеж маршрутизации.

На основе проведенного исследования можно сделать вывод, что каждый элемент системы электронной почты нуждается в надежных средствах защиты. Дополнительным уровнем безопасности, помимо защиты клиентов, является защита серверов. Для их защиты используются различные методы защиты данных. А также рубежи фильтрации, маршрутизации и т.д.

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010. 336 с.
2. Сагдеев К. М. Физические основы защиты информации: учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург, 2017.
3. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В. С. / /Известия ЮФУ. Технические науки. 2009. С. 172-176.
4. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Информационное противодействие угрозам терроризма, 2010. С. 114-118.
5. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.
6. Чипига А. Ф. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев // Фундаментальные исследования, 2015. С. 759.

КОНСАЛТИНГ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. Н. Карабанова
руководитель – канд. техн. наук, доцент ***В. В. Антонов***
Северо-Кавказский федеральный университет, г. Ставрополь

Тема консалтинга в области информационной безопасности (ИБ) очень актуальна в наши дни, потому что большинство компаний предпочитают обращаться именно к консалтинговым фирмам при необходимости построения собственной системы информационной безопасности. Целью данного исследования является обоснование предназначения консалтинговых фирм в области ИБ. В ходе исследования консалтинга в области ИБ были применены такие научные методы как анализ и синтез. В результате было выявлено назначение консалтинговых фирм в области ИБ, а также их характеристики, применяемые при оценке таких фирм.

Ключевые слова: IT-консалтинг, «Инфосистема Джет», организация защиты информации, система защиты предприятия, информационная безопасность, консалтинговые компании.

В условиях хозяйственной самостоятельности, финансовой нестабильности и жесткой конкуренции современные предприятия вынуждены использовать комплекс мероприятий и средств, одним из которых является привлечение к решению существующих проблем специалистов – консультантов, способствующих поиску выхода из затруднительного положения. В настоящее время в нашей стране развивают свою деятельность более 500 крупных консалтинговых фирм. В структуре российского рынка консалтинговых услуг наибольший удельный вес принадлежит информационным технологиям (47 %).

Консалтинг в области ИБ – это оказание услуг различным организациям, фирмам и компаниям по направлению развития ИБ, противодействию

текущим угрозам, анализу и обоснованию перспектив дальнейшего развития системы обеспечения ИБ. Большинство консалтинговых компаний работает со следующими системами: связи, информационные системы, автоматизированные системы общего назначения, автоматизированные системы управления технологическим процессом, инженерные системы, системы обеспечения физической защиты [1].

Из-за того, что в настоящее время отношение к ИБ во многих организациях достаточно формальное, услуги консалтинга необходимы для руководителей российских компаний, не уделяющих должного внимания развитию ИБ ресурсов своей компании. Менеджмент таких организаций предпочитает сократить расходы на систему и обойтись одним специалистом в этой сфере. Существующий уровень компетенции сотрудников службы безопасности организации может быть недостаточен для решения поставленных задач по построению эффективной системы безопасности. IT-консалтинг необходим для решения задач, связанных с совершенствованием системы управления предприятием с использованием информационных технологий как современного инструмента субъекта управления. Если пренебречь безопасностью информационных систем и надеяться на то, что «как-нибудь обойдётся», то крупные финансовые потери как от реализации внутренних, так и внешних угроз, неизбежны. По оценкам и данным опросов, проведенных SANS Institute, убыток только от одной атаки на корпоративную систему для банковского и IT-секторов экономики США, где безопасности уделяется особое внимание, составляет в среднем около 500 тыс. долларов [2].

По данным компании «Инфосистема Джет», спрос на консалтинг в сфере ИБ, по сравнению с прошлыми годами, вырос. Создание проектов для ИБ постепенно переходит из теоретической плоскости в практическую. Меняется также само понимание организациями существующих и потенциальных рисков ИБ, всё чаще они считаются чем – то обыденным при использовании информационных технологий. Ведь в современном мире безопасность бизнеса – это прежде всего информационная безопасность.

Важнейшей задачей для консалтинга является рациональное распределение ресурсов организации, которые выделяются на систему защиты, с учётом выявленных тенденций её внешнего и внутреннего роста. Естественно, создание целиком и полностью защищенной системы невозможно. А возможно формирование такой системы защиты, затраты на которую и размер теоретически возможного ущерба при атаке злоумышленника был бы допустимым.

На сегодняшний день деятельность консалтинговых компаний в РФ никак не регламентирована. Признаки, по которым приходится оценивать компании, являются неформальными, это: стоимость услуг, сроки реализации проекта, объём оказываемых услуг, известность компании, количество сотрудников, уровень их подготовки, рекомендации [3].

Так как консалтинговый проект – интеллектуальная продукция, то оценить качество данного проекта сложно. Поэтому критерии качества организации, принимаемой подготовленный проект, должны быть внесены в договор между организацией и консалтинговой компанией.

Таким образом, целью создания консалтинговых компаний в области ИБ является выявление проблем, а именно их причин, и, как следствие, разработка практических рекомендаций, направленных на их решение.

Литература

1. Страница компании ASP Labs. – URL: http://asplabs.ru/information-security-consulting.
2. Ю. Самохин, Д. Шепелявый. Консалтинг в информационной безопасности. Журнал сетевых решений/LAN, 2000, №11.
3. Г.А. Левочкина, Г.Н. Калянов, Р.Б. Васильев. Управление развитием информационных систем: учеб. курс/ Национальный открытый Университет. Электронная книга. М.: ИНТУИТ, 2016. 521 с.

КРИПТОГРАФИЧЕСКИЕ ХЭШ-ФУНКЦИИ

И. А. Коваль, М. А. Гражданкин
руководитель – магистр направления подготовки
«Информационная безопасность» ***С. М. Полухин***
Северо-Кавказский федеральный университет, г. Ставрополь

В современном мире проблема защиты информации очень актуальна. Поэтому все время появляются все новые методы и способы ее решения. В данной статье рассматривается использование криптографических хэш-функций.

Ключевые слова: криптография, целостность информации, хэш-функция, свертка, эмитовставка, аутентификация, ключевые хэш-функции, коллизия, секретный ключ.

Для обеспечения возможности проверки целостности информации в криптографии используются хэш-функции.

Хэш-функция – это функция, предназначенная для сжатия произвольного сообщения или набора данных, записывания, как правило, в двоичном алфавите в некоторую двоичную комбинацию фиксированной длины. Такая комбинация называется сверткой. Хэш-функция – это односторонняя функция, предназначенная для получения дайджеста файла, сообщения или некоторого блока данных.

С помощью хэш-функции сообщения различной длины преобразуются к блоку, длина которого, как правило, равна 128, 256, 512 бит.

В криптографии хэш-функции применяются для решения следующих задач:

1. Построение системы контроля целостности данных при их передаче или хранении.
2. Аутентификация источника данных.

При решении первой задачи для каждого набора данных вычисляется значение хэш-функции, называемой кодом аутентификации сообщения или эмитовставкой. Вычисленное значение хэш-функции передается или хранится вместе с этими данными. При получении данных пользователь вычисляет значение свертки и сравнивает его с полученным значением. Несовпадение этих значений говорит о том, что данные были изменены.

Хэш-функция, служащая для выработки эмитовставки, должна позволять проводить обнаружение не только случайных ошибок, возникших при хранении и передаче данных, но и сигнализировать об активных атаках злоумышленника по навязыванию ложной информации.

Для того, чтобы злоумышленник не смог вычислить значение свертки и, тем самым, осуществить успешную подмену данных, хэш-функция должна зависеть от секретного ключа, неизвестного злоумышленнику. Этот ключ должен быть известен только передаваемой и проверяющей стороне. Такие хэш-функции называются ключевыми.

Эмитовставки, формируемые при помощи ключевых хэш-функций, противостоят атакам типа имитация или модификация передаваемого сообщения.

При решении второй задачи имеет место ситуация, когда стороны не доверяют друг другу. Значит, использовать один секретный ключ нельзя. Для аутентификации, в этом случае, используется цифровая подпись, при этом подпись ставят на результат сжатие сообщения с помощью хэш-функции.

Большинство хэш-функций строится на основе однонаправленной функции, которая образует выходное значение, длиной n бит.

Алгоритм реализации хэш-функции на основе суммирования блоков:

1. На передающей стороне вычисляется хэш-функция
2. Вычисленная хэш-функция и исходное сообщение передается на приемную сторону.
3. На приемной стороне вычисляется эмитовставка.
4. Происходит сравнение полученной на приемной стороне эмитовставки и хэш-функции, вычисленной на передающей стороне.
5. Если значения совпадают, то исходное сообщение не модифицировано.

Далее рассмотрена реализация хэш-функции на основе суммирования блоков длиной n=4 бит передаваемого сообщения M.

$$M=1011110111110101$$

Абонент A вычисляет хэш-функцию H:

$$H\_((свертки))=h\ (M)$$

Для этого разбиваем исходный текст на блоки по 4 бита. Тогда

$$H\_0=M\_0=1011$$

$$H\_1=H\_0 \oplus M\_1=1011 \oplus 1101=0110$$

$$H\_2=H\_1 \oplus M\_2=1001$$

$$H\_3=H\_2 \oplus M\_3=1100$$
$$H=H\_3=1100$$
$$H\_((\text{свертки}))=h\ (M)=1100$$

На приемную сторону передается M и H.

Абонент B вычисляет эмитовставку принятого сообщения. Вычисленное значение совпадает со значением H, значит передаваемое сообщение не модифицировано.

В данном примере хэш-функция является неудовлетворительной, так как ее значения могут совпасть для различных сообщений M, такое совпадение называется коллизией.

Хэш-функция должна удовлетворять следующим условиям:

1. Хэш-функция должна быть чувствительной ко всем изменения в тексте M, таким как: вставка, перестановка, выброс элементов.
2. Хэш-функция должна обладать свойством необратимости.
3. Вероятность того, что значение хэш-функции двух различных сообщений M и M* совпадет должна быть ничтожно мала.

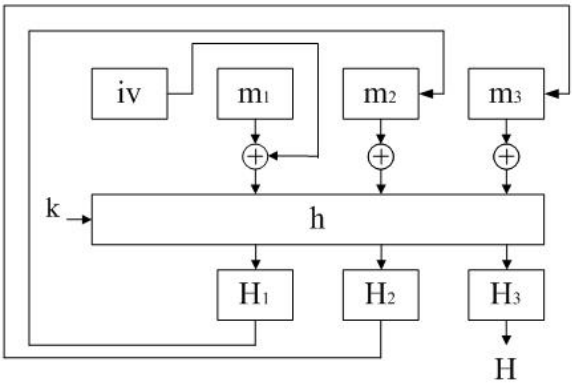


Рисунок 1. Структура ключевой хэш-функции

На рисунке представлена ключевая хэш-функции, которая использует секретный ключ k, известный передаваемой и принимающей стороне. Информация представлена в виде наборов блоков определенной длины l бит. Результат последовательной итерации является ключевой эмитовставкой передаваемого сообщения.

Литература

1. Введение в криптографию / В. В. Ященко. М.: Изд-во МЦНМО, 2012.
2. Основы криптографии / А. П. Алферов. Изд-во Гелиос АРВ, 2002.
3. https://ru.wikipedia.org/
4. https://habrahabr.ru/

ТИПОВЫЕ НАПАДЕНИЯ НА ЗОНУ ЛВС МЕЖСЕРВЕРНОГО ВЗАИМОДЕЙСТВИЯ ЭЛЕКТРОННОЙ ПОЧТЫ

И. А. Коваль, Д. А. Дзюба, А. П. Львова, М. А. Гражданкин
Северо-Кавказский федеральный университет, г. Ставрополь

Надежная защита электронной почты – важнейшая задача при проектировании системы информационной безопасности организации. Проанализированы типовые нападения на зону ЛВС межсерверного взаимодействия электронной почты. Предложены возможные рубежи защиты.

Ключевые слова: электронная почта, безопасность, линии вычислительной сети, криптография, аутентификация, сервер, рубеж защиты.

Структура системы электронной почты (ЭП) состоит из трех компонентов: клиента, сервера, линий вычислительной сети. Каждый из элементов выполняет свои специфические функции. Формирование сообщений происходит на уровне клиента, гарантированную доставку обеспечивают сервера, а линии вычислительной сети предназначены для объединения выше перечисленных программных и аппаратных средств.

Из анализа общей структуры электронной почты видно, что ее защиту необходимо осуществлять в нескольких зонах, таких как ОЗУ и ДЗУ клиента, зоне «клиент-сервер», а также между серверами.

Анализ современного состояния систем ЭП показывает, что типовыми нападениями на зону ЛВС являются:

1) Подмена серверов-получателей и серверов-отправителей. Злоумышленник имитирует сеанс отправки сообщения с своего сервера выдавая его за санкционированный.

Такой вид атаки применяется в виде подмены адресов-отправителей для рассылки вредоносных спам-сообщений. При этом мошенники используют формат почтового адреса в качестве отображаемого имени отправителя, и вместо "Microsoft Corporation" может присутствовать, например, "support@microsoft.com", которому будет соответствовать реальный адрес "microsoft491@gmail.com", который явно не имеет никакого отношения к корпорации Microsoft.

Подмена сервера-получателя может привести к тому, что важная информация вместо нужного получателя попадет к злоумышленнику.

2) Подмена и перехват сообщений электронной почты.

Почтовые серверы и почтовые клиенты работают как минимум используя два прикладных протокола, без которых обмен почтой невозможен. Это протокол SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты), и протокол приема сообщений POP3 (Post Office Protocol ver 3, протокол почтового офиса). На основе уязвимостей данных протоколов возможен несанкционированный захват сервера и перехват или подмена сообщений, которые через него проходят.

Например, одним из методов данного нападения является e-mail инъекция – используется для эксплуатации почтовых серверов и почтовых приложений, посредством конструирования IMAP/SMTP выражений из выполняемого пользователем ввода, который не проверяется должным образом. IMAP / SMTP инъекции позволяют получить доступ к почтовому серверу, к которому ранее доступа не было.

3) Блокирование сообщения электронной почты. Цель атаки - с помощью служебных сообщений электронной почты или подконтрольного злоумышленнику телекоммуникационного оборудования нарушить штатную работу электронной почты, сделать невозможным электронный документооборот.

Одним из самых распространенных способов выведения сервера из строя являются Dos-атаки. На оборудование присылается большое количество ложных запросов и система отказывает в обслуживании.

Проведенный анализ показывает, что большинство из представленных типовых нападений основаны на уязвимостях протоколов передачи информации по линиям вычислительной сети и недостатком средств аутентификации отправителей и получателей.

На рис. 1 изображена общая схема установки рубежей защиты в зоне ЛВС. Рубежами защиты для линий вычислительных сетей между серверами могут служить криптографические средства защиты сетевых операционных систем, межсетевых экранов и телекоммуникационного оборудования.

Важно своевременно устанавливать обновления защиты для протоколов, применять в дополнение более защищенные протоколы передачи данных (например, TSL – криптографический протокол защиты транспортного уровня).

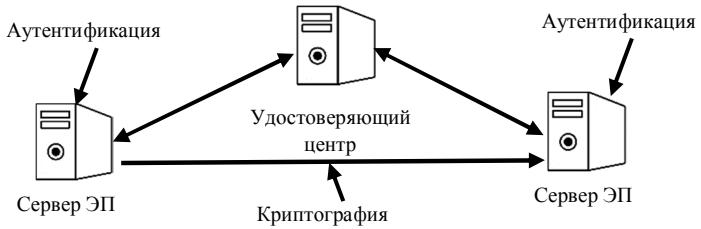


Рисунок 1. Рубежи защиты в зоне ЛВС

Применение взаимной аутентификации посредством инфраструктуры открытого ключа на основе общего удостоверяющего центра повысит надежность отправителей и гарантированную доставку до санкционированных получателей.

Кроме того, использование фильтров сообщений существенно повышают качество безопасности почтовой системы. Они защищают от вредоносного спама и служат рубежом защиты от несанкционированных отправителей.

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010. 336 с.
2. Сагдеев К. М. Физические основы защиты информации: учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. Санкт-Петербург, 2017.
3. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В. С. // Известия ЮФУ. Технические науки. 2009. С. 172-176.
4. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко // Информационное противодействие угрозам терроризма, 2010. С. 114-118.
5. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.
6. Чипига А. Ф. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев // Фундаментальные исследования, 2015. С. 759.

АНАЛИЗ ИДЕНТИФИКАТОРОВ ПОЛЬЗОВАТЕЛЕЙ И МОДЕЛЬ ИСПОЛЬЗОВАНИЯ ГОРЯЧИХ КЛАВИШ

О. О. Колеватов,
руководитель – магистр направления подготовки «Информационная безопасность» ***В. С. Пелешенко***
Северо-Кавказский федеральный университет, г. Ставрополь

В наш век информационных технологий информация – это самый дорогой товар, а ее защита является одной из самых наиважнейших задач для обладателя. Целью исследования является анализ идентификаторов пользователей и модели использования горячих клавиш (ИГК). В определенных случаях на обладателя возлагается обязанность по защите информации, в случае нарушение которой, предусматривается дисциплинарная, административная или уголовная ответственность. Требуется обустроить безопасность важной для учреждения или предприятия информации, то есть такое ее состояние, при котором защищенность характеризуется умением персонала обеспечивать конфиденциальность и сохранение информации в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Ключевые слова: информационные технологии, защита информации, идентификация, идентификатор, несанкционированный доступ, системой обеспечения информационной безопасности (СОИБ), модель используемых горячих клавиш (ИГК).

Идентификация напрямую связана с аутентификацией: субъект обязан проходить процедуру аутентификации, и если аутентификация удовлетворяет необходимым критериям, то информационная система, основанная на факторах аутентификации, в обязательном порядке, определяет иден-

тификатор, присущий субъекту. Классификация идентификаторов пользователей представлена на рис. 1.

Рисунок 1. Классификация идентификаторов пользователей

Одним из способов аутентификации является применение цифровых следов. Использование горячих клавиш (ИГК) является активным элементом цифрового следа, оставляемым теми пользователями, которые знают и применяют горячие сочетания клавиш при работе с клавиатурой. Подразумевает под собой статистический идентификатор, так как пользователи используют разные сочетания. Для использования данного цифрового следа необходимо обозначить определенный набор сочетаний клавиш, которых будет считываться системой обеспечения информационной безопасности (СОИБ). Назначения горячих клавиш делится на: работу с текстом; работу с файлами; работу в проводнике; работу с окнами; работу с диалоговыми окнами; работу в Internet Explorer; горячие клавиши общего назначения. Для экономии информационного ресурса СОИБ будут применяться горячие клавиши общего назначения, приведенные в табл. 1.

Таблица 1

Примеры горячих клавиш общего назначения

Сочетание клавиш	Описание	Частота применения
Ctrl плюс Esc Win	Открыть меню «Пуск» (Start)	8%
Ctrl плюс Shift плюс Esc	Вызвать диспетчер задач	9%
Win плюс E	Запустить проводник (Explore)	5%
Win плюс R	Отобразить диалог «Запуск ПО» (Run), аналогичная команда «пуск» — «выполнить»	6%
Win плюс D	Свернуть все открытые окна	4%
Win плюс L	Выполнить блокировку рабочей станции	3%
Ctrl плюс C Ctrl плюс Insert	Копировать в буфер обмена (объекты, текст)	14%
Ctrl плюс X Shift плюс Delete	Вырезать в буфер обмена (объекты, текст)	11%
Ctrl плюс P	Напечатать документ	32%
Ctrl плюс Z	Отменить предыдущее действие	8%

Благодаря данному элементу цифрового следа можно повысить уровень эффективности системы защиты информации (СОИБ). При применении данного элемента в составе цифрового следа можно частично отследить вреждебные действия пользователя. В совокупности с другими элементами, при выявлении враждебных действий, можно своевременно заблокировать подозрительного юзера системы.

Литература

1. Бирюков А. А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2013. 474 с.
2. Громов Ю. Ю. Информационная безопасность и защита информации: Учебное пособие / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. Ст. Оскол: ТНТ, 2010. 384 с.
3. Семененко В. А. Информационная безопасность: учебное пособие. М.: МГИУ, 2010. 277 с.

МЕТОДЫ ИДЕНТИФИКАЦИИ И ВЫЯВЛЕНИЯ ИДЕНТИФИКАТОРОВ ПОЛЬЗОВАТЕЛЕЙ

О. О. Колеватов
руководитель – доцент ***В. С. Пелешенко***
Северо-Кавказский федеральный университет, г. Ставрополь

В наш век информационных технологий информация – это самый дорогой товар, а ее защита является одной из самых наиважнейших задач для обладателя. Целью исследования является анализ идентификаторов пользователей и модели использования горячих клавиш (ИГК). В определенных случаях на обладателя возлагается обязанность по защите информации, в случае нарушение которой, предусматривается дисциплинарная, административная или уголовная ответственность. Требуется обустроить безопасность важной для учреждения или предприятия информации, то есть такое ее состояние, при котором защищенность характеризуется умением персонала обеспечивать конфиденциальность и сохранение информации в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Ключевые слова: информационные технологии, защита информации, идентификация, идентификатор, несанкционированный доступ, биометрические идентификаторы, аппаратные идентификаторы, логические идентификаторы.

Идентификация – процедура, во время действий которой для субъекта идентификации присваивается его идентификатор. Для выполнения процедуры в информационной системе необходимо предварительно быть назначен соответствующий идентификатор, то есть должна произойти регистрация в ИС. Примеры выявления идентификаторов приведены в табл. 1.

Таблица 1

Примеры выявления идентификаторов

Вид идентификации	Факторы аутентификации	Результат
Пользовательская идентификация	1) Логин / пароль	Логин
Пользовательская идентификация по банковской карте	1) Банковская карта (микропроцессорная), 2) ПИН-код	PAN – учетный номер карты (считывается с банковской карты)
Пользовательская идентификация по банковской карте с биоверификацией	1) Банковская карта (микропроцессорная), 2) Биометрический фактор (отпечаток пальца)	PAN – учетный номер карты (считывается с банковской карты)
Идентификация товара по штрих-коду	1) Штрих-код	Учетный номер товара
Идентификация файла по контрольной сумме	1) Хэш-сумма	Наименование файла
Пользовательская идентификация по электронной подписи	1) Носитель электронной подписи, 2) Пароль для доступа к носителю	Идентификатор сертификата (например, для сертификата ключа проверки квалифицированной электронной подписи – СНИЛС)

Идентификация и аутентификация связаны напрямую: субъект (например, физическое лицо) проходит процедуру аутентификации, и если данная процедура прошла успешно, то на основе аутентификационных факторов информационная система определяет для субъекта идентификатор. Достоверность идентификации при этом полностью определяется уровнем достоверности выполненной процедуры аутентификации. Классификация идентификаторов пользователей представлена на рис. 1.

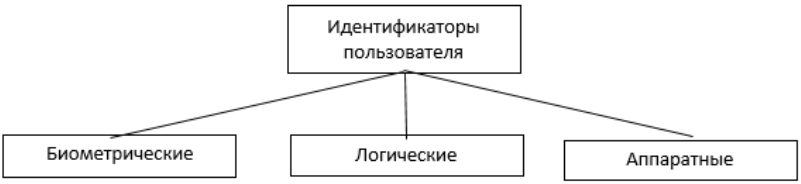


Рисунок 1. Классификация идентификаторов пользователей

Биометрическая идентификация – процесс, в результате которого доказывается и проверяется подлинность имени, заявленного пользователем, через предъявление этим пользователем своего биометрического образа и путём преобразования данного образа в соответствии с протоколом аутентификации, определенным заранее.

Логическими идентификаторами являются придуманные пользователем последовательности букв, цифр и знака подчеркивания, которые начинается с буквы или символа подчеркивания и не содержат пробелов, а также относящиеся к парольным системам идентификации.

Существует три типа аппаратных идентификаторов, специальных устройств для хранения файла-ключа – USB-токены, смарт-карты и контактная память.

Идентификатор-токен представляют собой устройство, размером с Flash-накопитель, имеющее чип, в котором хранятся зашифрованные данные и подключается к компьютеру через USB. Смарт-карты похожи на «визитку», имеют такой же чип, но для работы требуют специальные считыватели, внешние или интегрированные в устройство. Контактная память, называемая на сленге «таблетка», также требует отдельного устройства для чтения.

Контактная память работает по более простому принципу, выступая в роли хранилища небольшого объема данных. Она не защищена от клонирования и подделки данных, является на порядок менее безопасной.

Литература

1. Бирюков А. А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2013. 474 с.

2. Громов Ю. Ю. Информационная безопасность и защита информации: Учебное пособие / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. Ст. Оскол: ТНТ, 2010. 384 с.

3. Семененко В. А. Информационная безопасность: учебное пособие. М.: МГИУ, 2010. 277 с.

4. Галатенко В. А. Основы информационной безопасности: курс лекций: учебное пособие. М.: ИНТУИТ.РУ, 2012. 208 с.

РАДИОЧАСТОТНАЯ ИДЕНТИФИКАЦИЯ

Р. С. Корниенко, Е. С. Пелешенко

руководитель – д-р техн. наук, профессор ***И. А. Калмыков***

Северо-Кавказский федеральный университет, г. Ставрополь

В настоящее время российский и мировой рынки испытывают на себе влияние такого понятия, как контрафактная продукция. Можно утверждать, что почти все виды товаров так или иначе подделываются, создана и развивается целая индустрия производства и внедрения населению неоригинальной продукции. Очевидно, что с контрафактным товаром необходимо бороться. Одним из методов борьбы с контрафактной продукцией является технология RFID (*Radio Frequency Identification – радиочастотная идентификация*). *Подобно любому коммуникационному устройству, технология RFID состоит из передатчиков и приемников в виде RFID-меток. Это микрочипы, хранят всю необходимую информацию. Информация считывается с помощью RFID-считывателя. Антенна, присутствующая в тегах, используется в передаче, а также при приеме сигналов.*

Ключевые слова: радиочастотная идентификация, RFID-метка, RFID-ридер, радиосигнал, считывающее устройство, интегральная схема, интеллектуальное поведение.

Технология радиочастотной идентификации (RFID) существует уже много десятилетий, но только сейчас RFID все чаще используется во многих различных приложениях - и список растет.

RFID – это технология, которая использует теги для приема и передачи радиосигналов считывающим устройствам / запросчикам, которые принимают сигнал. Эти метки содержат антенны, позволяющие им получать и отвечать на радиочастотные запросы, в которых хранится информация, которая может использоваться для идентификации элемента, к которому он прикреплен.

Существуют два основных видов меток:

– активные;

– пассивные.

Активные теги имеют источник питания, обычно аккумулятор. Они, как правило, относительно дорогие. Пассивные метки получают питание, когда они перемещаются радио-поле, генерируемое считывателем. Эта технология экономически эффективна по сравнению с активными тегами.

Система радиочастотной идентификации состоит из основных компонентов:

– RFID-меток –устройств для хранения и передачи данных;

– считывающих устройств – специальных приборов для распознавания и записи данных на метки;

– антенны – устройства для приема и передачи радиосигнала. С помощью антенны метки и считыватели могут обмениваться данными;

– программное обеспечение − программы, с помощью которых осуществляется сбор и анализ информации, получаемой с RFID-меток [10].

Существует несколько способов систематизации RFID-меток и систем:

– по источнику питания;

– по рабочей частоте;

– по типу памяти;

– по исполнению.

По дальности считывания RFID-системы можно подразделить на системы:

– ближней идентификации (считывание производится на расстоянии до 20 см);

– идентификации средней дальности (от 20 см до 5 м);

– дальней идентификации (от 5 м до 300 м)

Большинство RFID-меток состоит из двух частей:

– интегральная схема (ИС) для хранения и обработки информации, модулирования и демодулирования радиочастотного сигнала (RF) и некоторых других функций;

– антенна для приёма и передачи радиосигнала.

Таблица 1

Сравнительная характеристика RFID со штрих-кодом и защитной голограммой [3, 10]

Характеристики технологии	RFID	Штрих-код	Защитные голограммы
Необходимость в прямой видимости метки	Чтение даже скрытых меток	Чтение без прямой видимости невозможно	Чтение без прямой видимости невозможно
Объём памяти	От 10 до 512 000 байт	До 100 байт	До 100 байт
Возможность перезаписи данных и многократного использования метки	Есть	Нет	Нет
Дальность регистрации	До 100 м	До 4 м	До 4 м
Одновременная идентификация нескольких объектов	До 200 меток в секунду	Невозможна	Невозможна
Устойчивость к воздействиям окружающей среды: механическому, температурному, химическому, влаге	Повышенная прочность и сопротивляемость	Зависит от материала, на который наносится	Зависит от материала, на который наносится
Срок жизни метки	Более 10 лет	Зависит от способа печати и материала, из которого отмечаемый объект	Зависит от способа печати и материала, из которого состоит отмечаемый объект
Безопасность и защита от подделки	Подделать возможно	Подделать легко	Подделать легко
Работа при повреждении метки	Невозможна	Затруднена	Затруднена
Идентификация движущихся объектов	Да	Затруднена	Затруднена
Подверженность помехам в виде электромагнитных полей	Есть	Нет	Нет
Идентификация металлических объектов	Возможна	Возможна	Возможна
Использование как стационарных, так и ручных терминалов для идентификации	Да	Да	Да
Возможность введения в тело человека или животного	Возможна	Затруднена	Затруднена
Габаритные характеристики	Средние и малые	Малые	Малые
Стоимость	Средняя и высокая	Низкая	Низкая

Ежегодно RFID начинает применяться большим числом кампаний, поскольку технология продолжает развиваться. Это связано с тем, что пре-

имущества технологии RFID можно увидеть в самых разных отраслях промышленности – от розничной торговли до сферы здравоохранения, транспортировки и логистики. У каждой отрасли есть свои требования, которые RFID-технология помогает удовлетворить. Например, розничные компании часто используют метки RFID для отслеживания количества одежды на складе в каждом магазине. Компании здравоохранения используют технологию RFID для управления распределением лекарств в больницах. Логистические компании ежедневно используют RFID для создания обновленного списка того, что было наложено и изъято из его грузовиков.

Преимущества радиочастотной идентификации:

– низкая стоимость и высокая производительность: приложения RFID могут автоматизировать сбор информации о движении и местоположении товаров, компонентов, акций или других предметов; делая это быстрее, уменьшая затраты и с большей точностью и надежностью, чем это возможно с помощью других методов аутентификации таких, как штриховое кодирование. Идентификация продуктов с использованием RFID выполняется быстрее, чем сканирование штрих-кодов или чем ручной ввод сведений о продукте;

– улучшенное качество сбора данных: использование RFID означает, что данные можно быстро и точно записывать. Электронный сбор данных с помощью RFID позволяет избежать ошибок транскрипции данных и позволяет избежать «пропущенных элементов» при использовании сбора данных по большому количеству элементов одновременно;

– снижение капитальных затрат: технологии RFID помогают снизить затраты, обеспечивая лучший контроль над запасами или активами. Они могут помочь отслеживать различное оборудование, вычислительную технику и другие портативные устройства;

– лучшая безопасность: системы контроля доступа с использованием RFID способствуют повышению безопасности.

– увеличение доходов;

К недостаткам технологии радиочастотной идентификации можно отнести:

– RFID слишком дорогостоящее по сравнению с другими методами отслеживания и идентификации, такими как простой штрих-код;

– тяжело считывать нформацию с RFID метки, если метки установлены в жидких или металлических изделиях. Проблема в том, что жидкие и металлические поверхности имеют тенденцию отражать радиоволны, что делает метки нечитаемыми;

– помехи наблюдаются в RFID-системах, когда поблизости находятся такие устройства, как рации. Было обнаружено, что наличие мобильных телефонов также мешает хорошему сигналу;

– частоты сигналов RFID по всему миру не стандартизированы. Например, США и Европа имеют разные диапазоны частот, с которыми функционируют метки RFID. Это делает необходимым, чтобы международные судоходные компании и другие организации знали о рабочей структуре в других странах;

– RFID рассматривается многими как инвазивная технология. Потребители склонны беспокоиться о своей конфиденциальности. И когда покупают продукты с этими метками, то существует опасение, что с помощью этих меток продолжается отслеживание человека. В результате чего, его личная информация может быть украдена. Поэтому, хотя многие магазины заявляют, что деактивируют теги после покупки продукта, покупатели по-прежнему продолжают опасаться этой технологии.

Литература

1. Бхуптани Маниш, Морадпур Шахрам RFID-технологии на службе вашего бизнеса; Альпина Паблишер. М., 2007. 290 с.
2. В. В. Чеклецов. Чувство планеты. Интернет Вещей и следующая технологическая революция. М.: Российский исследовательский центр по Интернету Вещей, 2013. 132 с.
3. Клаус Финкенцеллер. Rfid-технологии. М.: ДМК Пресс, Додэка XXI, Hanser Publishers, 2016. 490 с.
4. Максим Власов. RFID. 1 технология – 1000 решений. Практические примеры использования RFID в различных областях. М.: Альпина Паблишер, 2015. 218 с.
5. Маниш Бхуптани, Шахрам Морадпур RFID-технологии на службе вашего бизнеса = RFID Field Guide: Deploying Radio Frequency Identification Systems / Троицкий Н. М.: Альпина Бизнес Букс, 2007. 290 с.
6. Николай Филинюк, Елена Войцеховская und Людмила Лищинская. Информационные устройства на комбинированных динамических негатронах. М.: LAP Lambert Academic Publishing, 2013. 160 с.
7. Сандип Лахири RFID. Руководство по внедрению = The RFID Sourcebook / Дудников С. М.: Кудиц-Пресс, 2007. 312 с.
8. Финкенцеллер Клаус RFID-технологии; Додэка XXI. М., 2010. 496 с.
9. Э. А. Кирсанов, А. А. Сирота. Обработка информации в пространственно-распределенных системах радиомониторинга. Статистический и нейросетевой подходы. М.: ФИЗМАТЛИТ, 2013. 344 с.
10. http://ru-wiki.org/wiki/RFID

К ВОПРОСУ О ПРОЦЕДУРЕ ВЫБОРА ОПЕРАТОРОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ПЕРЕЧНЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Д. А. Коробейников, А. А. Османов
руководитель – доцент ***В. М. Бисюков***
Северо-Кавказский федеральный университет, г. Ставрополь

Актуальность темы обусловлена тем, что ст. 19 ФЗ №152 требует от оператора персональных данных (ПДн) применения организационных и

технических мер для защиты ПДн обрабатываемых в информационных системах персональных данных (ИСПДн), а также оценки эффективности принимаемых мер по обеспечению безопасности ПДн [1, с. 14].

Проблема заключается в том, что:

– порядок выбора оператором организационных и технических мер для защиты ПДн изложен в различных нормативных документах, регламентирующих технологию построения системы защиты ПДн в ИСПДн, что затрудняет полный учёт всех требований при проведении данной работы;

– утверждённой методики оценки эффективности принимаемых мер защиты ПДн для ИСПДн нет.

Целью исследования является оптимизация технологии выбора организационных и технических мер защиты ПДн в ИСПДн с учётом требований всех нормативных документов, регламентирующих данный процесс, а также предложение методики оценки эффективности принятых мер.

При проведении исследования применялся метод экспертных оценок.

В результате проведённых исследований предложен алгоритм работы оператора ПДн, позволяющий оптимизировать технологию выбора организационных и технических мер защиты ПДн с учётом требований различных нормативных документов, регламентирующих данную работу, а также методика оценки эффективности принимаемых мер по обеспечению безопасности ПДн по критерию оценки риска информационной безопасности для ИСПДн.

Ключевые слова: персональные данные, информационная система персональных данных, технические меры защиты персональных данных, организационные меры защиты персональных данных.

В соответствии с требованиями нормативных документов, построение системы защиты ПДн в ИСПДн необходимо начинать с разработки перечня персональных данных подлежащих защите, который является базой, при определении актуальных угроз для ИСПДн, а также правовой основой системы защиты ПДн в ИСПДн.

Требуемый уровень защищённости ИСПДн определяется на основании требований постановления правительства № 1119 [2. с. 16], (табл. 1).

Предлагаемые рекомендации оператору, по выбору организационных и технических мер по обеспечению безопасности ПДн при их обработке ИСПДн, можно представить в виде алгоритма (рис. 1).

Таблица 1

Выбор уровня защищённости для ИСПДн

№	Категория ПДн	Тип угроз				
		1	2		3	
1	Специальные	УЗ-1	УЗ-1 При обработке ПДн >100 тыс др. субъектов	УЗ-2 При обработке ПДн сотрудников оператора или < 100 тыс др. субъектов	УЗ-2 При обработке ПДн>100 тыс др. субъектов	УЗ-3 При обработке ПДн сотрудников оператора или < 100 тыс др.

№	Категория ПДн	Тип угроз				
		1	2		3	
						субъектов
2	Биометрические	УЗ-1	УЗ-2		УЗ-3	
3	Иные категории ПДн	УЗ-1	УЗ-2 При обработке ПДн>100 тыс др. субъектов	УЗ-3 При обработке ПДн сотрудни-ков оператора или < 100 тыс др. субъектов	УЗ-3 При обработке ПДн>100 тыс др. субъектов	УЗ-3 При обработке ПДн сотрудни-ков оператора или < 100 тыс др. субъектов
4	Общедоступные	УЗ-2	УЗ-2 При обработке ПДн>100 тыс др. субъектов	УЗ-3 При обработке ПДн сотрудни-ков оператора или < 100 тыс др. субъектов	УЗ-4	

Базовый набор мер определяется на основе определённого уровня защищённости ИСПДн, с учётом требований приказа ФСТЭК №21 [3, с. 11].

Для определения адаптированного базового набора мер необходимо провести анализ структурно-функциональных характеристик ИСПДн, используемые информационные технологии, физические, логические, функциональные и технологические взаимосвязи в ИСПДн.

Уточнение базового адаптированного набора мер производится по перечню актуальных угроз, полученному на основании построенной частной модели угроз для ИСПДн в следующей последовательности [4, с. 4]:

– построение базовой модели угроз для ИСПДн и определение на её основе потенциальных угроз безопасности ИСПДн;

– выявление актуальных угроз для ИСПДн;

– уточнение адаптированного базового набора мер по защите ПДн в ИСПДн.

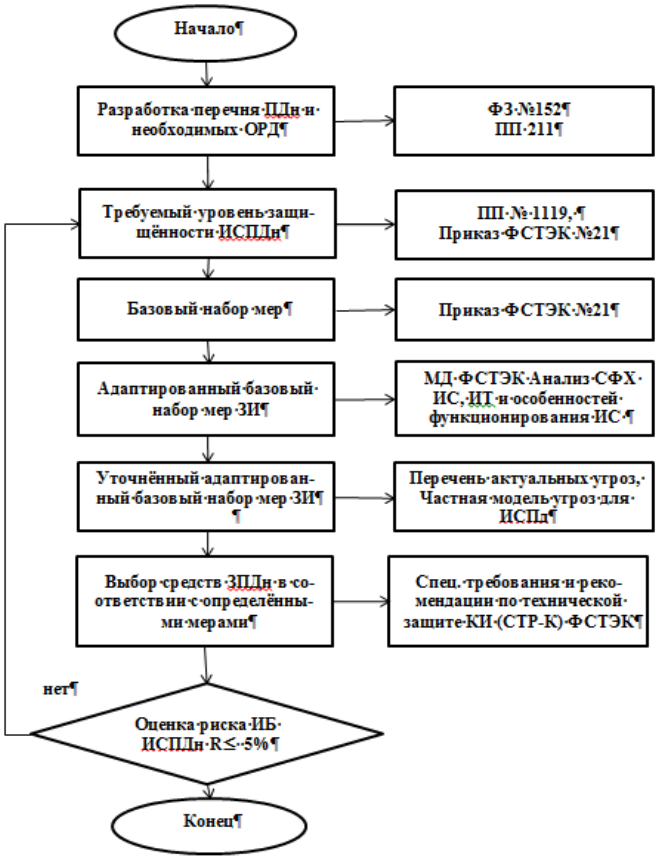


Рисунок 1. Алгоритм выбора и реализации организационных и технических мер по обеспечению безопасности ПДн, при их обработке в ИСПДн

Дополнение уточнённого адаптированного базового набора мер производится с учётом требований последних нормативных документов, ценности сведений и материальных возможностей предприятия.

Проведение оценки эффективности системы защиты ПДн в ИСПДн предприятия предлагается проводить по критерию количественной оценке риска информационной безопасности для ИСПДн [5, с.12].

Этапы оценки риска ИБ для ИСПДн:

– оценка степени учёта требований нормативных документов в области информационной безопасности для ИСПДн;

– определение вероятности реализации хотя бы одной из актуальных угроз;

– определение коэффициента оценки ценности ПДн обрабатываемых в ИСПДн;

– определение степени использования организационных и технических мер защиты ПДн в ИСПДн;

– определение количественного значения риска ИБ.

В результате реализации предложенных рекомендаций получаем перечень организационных и технических мер для защиты ИСПДн. С учетом определенного уровня защищённости ПДн выбираются технические средства для реализации выбранных организационных и технических мер.

Литература

1. Закон РФ «О персональных данных» от 27.07.2006 № 152 - ФЗ Бюллетень нормативных актов министерств и ведомств. № 7. 2006. С.15-32.
2. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
3. Приказ ФСТЭК от 18.02.2013. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах ПДн, утвержденная приказом ФСТЭК РФ 15.02.2008.
5. Плетнёв А.В. Методика количественной оценки риска информационной безопасности. М.: ЗАО «Бизнес-школа «Интел-Синтез», 2013. 126 с.

РАЗРАБОТКА АЛГОРИТМА ДЛЯ ОПРЕДЕЛЕНИЯ МЕР ПО ЗАЩИТЕ ПЕРИМЕТРА И КАНАЛОВ СВЯЗИ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

А. Е. Костянов, А. П. Львова

Северо-Кавказский федеральный университет, г. Ставрополь

Статья посвящена разработке алгоритма, который позволит сократить временные затраты при определении требований и реализации мер. Разработан алгоритм, позволяющий определить актуальные угрозы для периметра и каналов связи в информационной системе, а также перечень мер, которые необходимо реализовать при построении подсистемы защиты периметра и каналов связи.

Ключевые слова: персональные данные, информационная система, требования к информационной системе персональных данных, защита информации, защита периметра и каналов связи.

Требования Федерального закона «О персональных данных» №152-ФЗ обязательны к исполнению для всех государственных и коммерческих

организаций, обрабатывающих персональные данные (ПД) физических лиц, независимо от размера и формы собственности.

Согласно статье 19 ФЗ-152 оператору при обработке персональных данных необходимо принимать определенные меры и технические средства для защиты ПД от случайного доступа к ним, каких-либо модификаций, а также иных неправомерных действий.

Для того чтобы упростить формирование перечня требований и мер при построении подсистемы защиты информации (ЗИ) в периметре и каналах связи информационной системы персональных данных, необходимо разработать унифицированный алгоритм, который можно использовать как в государственных, так и в коммерческих организациях.

При разработке алгоритма необходимо поставить следующие задачи: определение актуальных угроз ИБ и формирование перечня требований и мер, которые будет реализованы в информационной системе.

Определение актуальных угроз включает в себя:

1. Анализ структурно-функциональных характеристик информационной системы;

2. Построение модели нарушителя, которая содержит в себе: типы потенциальных нарушителей, анализ информации, которой может обладать нарушитель, потенциальные средства атак, возможные каналы атак, классификацию потенциального нарушителя согласно [1].

3. Построение модели угроз, содержащую анализ исходной защищенности информационной системы, анализ вероятности и опасности реализации угроз, анализ возможности реализации угроз, перечень актуальных угроз.

При проектировании подсистемы защиты периметра и каналов связи, после построения модели угроз необходимо выбрать угрозы, которые относятся к защите периметра и каналов связи. Остальные угрозы, в данном случае, не рассматриваются. Определение актуальных угроз, позволяет перейти к решению следующей задачи – формированию перечня требований и мер, которые будет реализованы в подсистеме.

Этапы её решения включают:

1. Определение уровня защищенности информационной системы персональных данных согласно [3];

2. Определение базового набора мер ЗИ для установленного уровня защищенности информационной системы в соответствии с базовыми наборами мер защиты информации, приведенными в приложении к [7].

3. Адаптацию базового набора мер ЗИ применительно к структурно-функциональным характеристикам информационной системы;

4. Уточнение адаптированного базового набора мер ЗИ с учетом не выбранных ранее мер защиты информации, приведенных в приложении к [7];

5. Дополнение уточненного адаптированного базового набора мер ЗИ мерами, обеспечивающими выполнение требований о ЗИ, установленными

нормативно-правовыми актами, которые действуют на территории Российской Федерации [1, 2, 4, 5, 6, 8].

На рис. 1 представлен алгоритм формирования набора требований к информационной системе персональных данных.

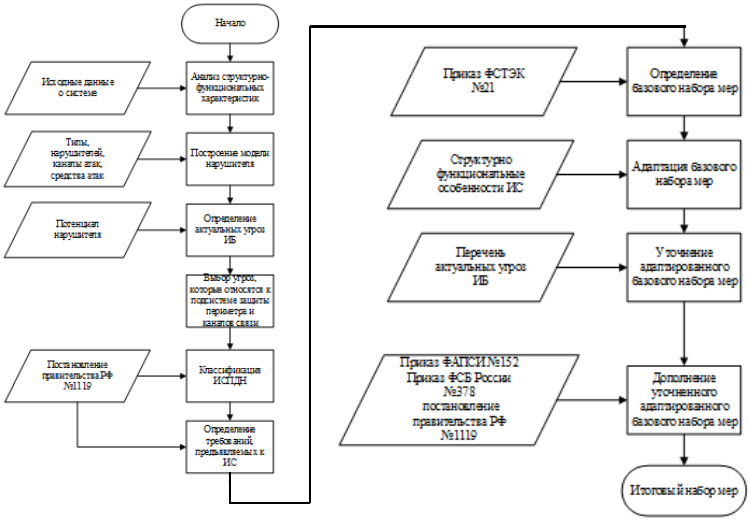


Рисунок 1. Алгоритм формирования набора требований к информационной системе персональных данных

Согласно нему, можно проводить проектирование подсистем защиты данных как в государственных, так и в коммерческих организациях.

Решение поставленных задач позволит полностью сформировать требования и меры, которые обеспечат защиту персональных данных в соответствии с нормативно-правовой базой, действующей на территории Российской Федерации.

Литература

1. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ РФ 21.02.2008 №149/54-144).

2. Методические рекомендации 8 Центра ФСБ России «по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» от 31 марта 2015 года №149/7/2/6-432.

3. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4. Приказ ФАПСИ от 13 июня 2001 г. №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с ис-

пользованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

5. Приказ ФСБ РФ от 9 февраля 2005 г. №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

6. Постановление Правительства РФ от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

7. Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

8. Решение Коллегии Гостехкомиссии России №7.2/02.03.2001г. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К).

9. Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ.

ОСНОВНЫЕ ТИПЫ УГРОЗ НА ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ, ИХ КЛАССИФИКАЦИЯ И МЕТОДЫ РЕШЕНИЯ УГРОЗ

М. С. Кочанов
руководитель – канд. техн. наук, доцент ***Т. В. Минкина***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье проводится анализ локальных вычислительных сетей, изучены цели злоумышленников, методы и типы атак. Предоставлены решения, связанные с защитой локальных вычислительных сетей.

Ключевые слова: защита информации, безопасность, информация, локальные вычислительные сети, угроза локальных вычислительных сетей, дублирование, удаление, задержка, модификация, пассивный перехват, виртуальные частные сети, аутентификация, двухфакторная аутентификация, коммутируемая инфраструктура. сниффинг, криптография.

В настоящее время проблемы информационной безопасности встают наиболее остро. Это связанно с тем, что при использовании автоматизированных систем обработки информации появились угрозы, которые могут привести к несанкционированному доступу. Главной проблемой защиты информации является отсутствие жёсткого носителя. Её можно быстро и легко скопировать и передать по каналам связи. Информационная система доступна как внешним, так и внутренним угрозам со стороны нарушителей.

На данное время, информационная безопасность компьютерных систем от несанкционированного доступа представлена как возрастание роли программных механизмов по сравнению с аппаратными. Новые проблемы в области защиты информации требуют использования протоколов и механизмов с высокой вычислительной сложностью.

Теперь перейдем к рассмотрению угроз локальных вычислительных сетей. В локальных вычислительных сетях различают две угрозы: актив-

ный и пассивный перехват. При активном перехвате происходит непосредственное изменение и воздействие с пакетами, включающее: дублирование, удаление задержку и модификацию. Пассивный перехват предполагает чтение информации, анализ трафика.

Данные угрозы наиболее четко раскрываются, при взаимодействии с огромным количеством приложений, связанных с взаимодействием электронной почты. Почтовые серверы действуют, как локальные почтовые отделения, обеспечивая пользователям возможность посылать и получать сообщения через локальные вычислительные сети. Благодаря широкому спектру возможностей пользователи подвергаются угрозам со стороны злоумышленников. Один из примеров угроз – сниффинг.

Сниффинг – это перехват пакетов между двумя компьютерами и дальнейшим взаимодействием с ними. Для ликвидации угрозы сниффинга используют различные методы по организации защиты информации на локальных вычислительных сетях. Основные из них: криптография, аутентификация, коммутируемая инфраструктура. Один из самых полезных методов защиты – криптография. При использовании криптографии на локальных вычислительных сетях не предотвращается перехват пакетов, но результат полученный злоумышленником, в результате кражи пакета не принесет продуктивных результатов. Криптография Cisco на сетевом уровне базируется на протоколе IPSec. IPSec представляет собой стандартный метод защищенной связи между устройствами с помощью протокола IP.

Использование персональных компьютеров в локальных вычислительных сетях также увеличивает риск. Для решения этой угрозы приходится использовать метод аутентификации. Чаще всего используется технология двухфакторной аутентификации. При использовании двухфакторной аутентификации в случае кражи пароля, злоумышленник не может получить доступ к файлам, находящимся в локальной сети. Данный метод эффективен при перехвате паролей. При перехвате программных пакетов данный метод не рационален. В настоящее время локальные вычислительные сети являются одним из самых безопасных сетей за счет коммутируемой инфраструктуры. При использовании данного метода борьбы с угрозами в локальных вычислительных сетях злоумышленники могут получить доступ только к тому трафику, который поступает на порт, к которому подключены злоумышленники. Коммутируемые структуры не убирают угрозы полностью, но значительно их снижают.

В заключение можно сделать следующие выводы: причиной высокого риска безопасности в локальных вычислительных сетях является отсутствие знаний у пользователей по теме информационной защиты локальных сетей. Отсутствие осведомленности пользователей в отношении безопасности ЛВС значительно увеличивает риск. Не зная алгоритмов защиты, пользователи допускают ряд ошибок, которыми злоумышленники пользуются в дальнейшем. Использование вышесказанных способов защиты

приведет к повышению безопасности пользователей и снижению риска в локальных вычислительных сетях.

Литература

1. Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 №351.

2. Безбогов А. А. Безопасность операционных систем. М., 2015. 20 с.

3. Гайкович В. Г., Першин А. Л. Безопасность электронных систем. М., 2017. –36 с.

4. Запечников С.В. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите. М., 2016. 536 с.

5. Запечников С. В. Информационная безопасность открытых систем. В 2 томах. Том 2. Угрозы, уязвимости, атаки и подходы к защите. М., 2016. 560 с.

6. Лопатин В. Н. Информационная безопасность России / Серия: Безопасность человека и общества. М., 2017. 176 с.

7. Макарова Н. В. Информатика. М., 2015. 87 с.

8. Партыка Т. Л., Попов И. И. Информационная безопасность / Форум, Инфра. М., 2012. 368 с.

9. Олифер В. Г., Олифер Н. А. Сетевые операционные системы: Учебник для вузов.– СПб., 2015. 125 с.

10. Острейковский В. А. Информатика: Учебник для вузов. М., 2016. 174 с.

11. Степанов Е. А., Корнеев И. К. Информационная безопасность и защита информации. Учебное пособие. М., 2013. 304 с.

12. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М., 2016. 65 с.

13. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. М., 2014. 102 с.

К ВОПРОСУ ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ПРИНИМАЕМЫХ МЕР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

М. Р. Курачинова, А. А. Шхануков, Д. Е. Юдин
руководитель – доцент ***В. М. Бисюков***
Северо-Кавказский федеральный университет, г. Ставрополь

Актуальность темы обусловлена тем, что ст. 19 ФЗ №152 требует от оператора персональных данных (ПДн) оценки эффективности принимаемых мер по обеспечению безопасности ПДн в информационных системах персональных данных (ИСПДн) [1, с. 14].

Проблема заключается в том, что на сегодняшний день, утверждённой федеральными органами исполнительной власти (ФОИВ), уполномоченными в области обеспечения безопасности ПДн, методики оценки эффективности принимаемых мер защиты ПДн в ИСПДн нет.

Целью исследования является разработка методического обеспечения процедуры оценки эффективности предложенных организационных и технических мер защиты ПДн в ИСПДн.

При проведении исследования применялся метод экспертных оценок.

В результате проведённых исследований, в качестве методики оценки

эффективности принимаемых организационных и технических мер защиты ПДн в ИСПДн предложена методика количественной оценки риска информационной безопасности (*ИБ*) *для информационных систем [2 с. 1-3], которая позволит провести сравнительный анализ эффективности системы защиты ПДн в ИСПДн* до и после реализации предложенных организационных и технических мер.

Ключевые слова: информационная безопасность, риск информационной безопасности, персональные данные, оператор персональных данных, информационная система персональных данных, технические меры защиты персональных данных, организационные меры защиты персональных данных, модель угроз информационной системы персональных данных.

Этапы оценки риска ИБ для ИСПДн (табл. 1).

Таблица 1

Этапы оценки риска ИБ для ИСПДн

Этапы	Название этапов
Этап 1	Оценка уровня учёта требований нормативных документов в области ИБ для ИСПДн
Этап 2	Определение вероятностей реализации хотя бы одной из актуальных угроз в ИСПДн
Этап 3	Определение степени использования организационных и технических мер защиты ПДн в ИСПДн
Этап 4	Определение количественного значения риска ИБ для ИСПДн

При выполнении первого этапа необходимо учесть, что в перечень нормативных документов, обязательных для выполнения, при создании системы защиты ПДн в ИСПДн, входят федеральные законы и приказы ФОИВ в сфере ИБ, а также перечень организационно-распорядительных документов (ОРД), в обязательном порядке, разрабатываемых оператором ПДн. В соответствии с требованием ФОИВ, регулирующих вопросы защиты ПДн, минимальный комплект ОРД разрабатываемых оператором ПДн должен состоять из 29 документов [1, с. 2-16].

Перечень актуальных угроз и вероятности их реализации получены из частной модели угроз для ИСПДн [3 с.1-14]. Вероятность реализации хотя бы одной из актуальных угроз определяется по формуле:

$$P_{\text{угр}} = 1 - \Pi\left(1 - P_{\text{у1}}\right)\left(1 - \text{P}_{\text{у2}}\right)\left(1 - \text{P}_{\text{у3}}\right) \ldots (1 - \text{P}_{\text{у}n}), \qquad (1)$$

где $\text{P}_{\text{угр}}$ - вероятность реализации хотя бы одной из актуальных угроз;

$\text{P}_{\text{уn}}$ – вероятность реализации n- ой актуальной угрозы.

Перечень необходимого набора организационных и технических мер защиты ПДн в ИСПДн получен на основании реализации приказа ФСТЭК №21 [4 с.1-24]. Фрагмент результатов исследований, для ИСПДн (табл. 2).

В ходе проведения анализа степени использования организационных и технических мер защиты ПДн в ИСПДн всем требованиям, которые выполняются, присваивается значение «1», частично выполняются – «0,5» не выполняются – «0». С полученной суммой результатов (1 и 0,5) входим в таблицу и получим коэффициент использования организационных $\text{R}_{\text{о}}$ и

технических Rt мер защиты ПДн в ИСПДн (табл. 3).

Таблица 2

Перечень организационных и технических мер защиты ПДн в ИСПДн

Угрозы безопасности ПДн	Меры защиты	
	Организационные меры	Технические меры
1.1 Угрозы утечки акустической информации	ЗТС. 2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации	ЗТС. 1 Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам.
1.2 **Угрозы утечки видовой информации**	ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее её несанкционированный просмотр	ЗТС.1 Защита информации, обрабатываемой техническими средствами, от её утечки по техническим каналам

Таблица 3

Порядок определения степени использования организационных и технических мер защиты ПДн в ИСПдн

% выполнения организационных мер защиты в ИС	Риск несоответствия требованиям законодательства (Ro,Rt)
61-90	0,25
21-60	0,5
≤ 20	0,9

Для определения количественного значения риска информационной безопасности используется формула [2 с. 3]:

$$R = P_{\text{угр}} \cdot R_n \cdot \frac{K_o + K_т}{2} \cdot 100\% \qquad (2)$$

где R – численная величина риска реализации угроз ИБ для ИСПДн;

Ругр - вероятность реализации хотя бы одной из актуальных угроз;

Rn – показатель уровня выполнения требований нормативных документов по защите ПДн в ИСПДн;

Ko – коэффициент использования организационных мер защиты ПДн в ИСПДн;

Kt – коэффициент использования технических мер защиты ПДн в ИСПДн.

Таким образом, реализация предложенных рекомендаций позволит провести оценку эффективности предложенных мер защиты ПДн по критерию сравнительной оценки величины риска ИБ для ИСПДн.

Литература

1. Закон РФ «О ПДн» от 27.07.2006 № 152 - ФЗ Бюллетень нормативных актов министерств и ведомств. № 7. 2006. С.15-32.

2. Плетнёв А. В. Методика количественной оценки риска информационной безопасности. М.: ЗАО «Бизнес-школа «Интел-Синтез», 2013. 26 с.

3. Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн, утвержденная приказом ФСТЭК РФ 14.02.2008.

4. Приказ ФСТЭК от 18.02.2013. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн».

РАЗРАБОТКА ПРОЕКТА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ АВТОМАТИЗИРОВАННЫМ СПОСОБОМ В КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

Д. С. Лебедев
руководитель – преподаватель ***Д. П. Киселев***
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье рассмотрены меры для построения системы защиты персональных данных, обрабатываемых автоматизированным способом в корпоративной сети предприятия.

Актуальность разработки системы защиты персональных данных, обрабатываемых автоматизированным способом в корпоративной сети предприятия обусловлена многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации и постоянным развитием и усложнением оборудования и приложений, используемых в корпоративной сети повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности.

Ключевые слова: персональные данные (ПДн), информационная система персональных данных (ИСПДн), несанкционированный доступ, средства защиты информации (СЗИ), корпоративная сеть.

Для достижения требуемого уровня информационной безопасности корпоративных сетей предприятий требуется построить комплексную систему обеспечения информационной безопасности с применением сертифицированных средств защиты информации, стандартов, протоколов.

Построение комплексной системы обеспечения информационной безопасности ПДн состоит из следующих этапов:

- анализ нормативно-правовой базы в области защиты ПДн;
- определение перечня ПДн, подлежащих защите;
- классификация ИСПДн, обрабатывающих ПДН;
- построение частной модели угроз информационной безопасности;
- проектирование решений по защите ИСПДн;
- внедрение системы защиты ПДн;
- тестирование системы защиты ПДн;
- дополнительные меры защиты.

В систему защиты передаваемых в корпоративных сетях персональных данных входят следующие подсистемы и меры защиты:

– подсистема идентификации и аутентификации;
– подсистема управления доступом субъектов доступа к объектам доступа;
– подсистема регистрации событий безопасности;
– подсистема антивирусной защиты;
– подсистема обнаружения вторжений;
– подсистема контроля защищенности персональных данных;
– обеспечение целостности информационной системы и персональных данных;
– обеспечение безопасного межсетевого взаимодействия;

Средства защиты от НСД реализуют:

– идентификацию и аутентификацию субъектов доступа и объектов доступа;
– управление доступом субъектов доступа к объектам доступа;
– ограничение программной среды;
– обеспечение целостности информационной системы и персональных данных;

Существуют следующие СЗИ от НСД, сертифицированные ФСТЭК:

– продукты линейки СЗИ от НСД «Secret Net», «Secret Net Studio» и ПАК «Соболь» («Код Безопасности»);
– продукты линейки СЗИ (СЗИ от НСД, МЭ, СОВ, СКН, СДЗ) «Dallas Lock» («Конфидент»);
– продукты линейки СЗИ от НСД «Аккорд» (ОКБ САПР);
– СЗИ от НСД «Блокхост-сеть К» и «Блокхост-АМДЗ 2.0» («Газинформсервис»);
– продукты СЗИ от НСД «ПАНЦИРЬ» («НПП «Безопасные информационные технологии»).

Для реализации антивирусной защиты используются антивирусные программы.

Существуют следующие антивирусные программы, сертифицированные ФСТЭК:

– «Kaspersky Endpoint Security»;
– «Dr.Web Enterprise Security Suite»;
– «Eset NOD32 ESET NOD32 SECURE ENTERPRISE».

Безопасность межсетевого взаимодействия и обнаружение (предотвращение) вторжений обеспечивают межсетевые экраны. Существуют следующие межсетевые экраны, сертифицированные ФСТЭК:

– «VipNetCustom»;
– АПКШ «Континент»;
– «Континент-АП»;
– «VipNet Personal Firewall».

Контроль (анализ) защищенности персональных данных осуществляется сканерами уязвимостей.

Существуют следующие сканеры уязвимостей, сертифицированные ФСТЭК:

- «XSpider»;
- «Ревизор сети 2.0»;
- «Сканер-ВС».

Литература

1. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14.05.2013 N 28375).
2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных».
3. Шаньгин В.Ф Комплексная защита информации в корпоративных системах: Инфра-М, 2010. 594 с.
4. Материалы сайта https://www.securitylab.ru.
5. Материалы сайта https://www.altx-soft.ru.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Д. С. Лебедев
руководитель – преподаватель ***Д. П. Киселев***
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье рассмотрены средства защиты информации для построения системы защиты персональных данных, обрабатываемых автоматизированным способом в корпоративной сети предприятия.

Актуальность разработки системы защиты персональных данных, обрабатываемых автоматизированным способом в корпоративной сети предприятия обусловлена многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации и постоянным развитием и усложнением оборудования и приложений, используемых в корпоративной сети повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности.

Ключевые слова: персональные данные (ПДн), информационная система персональных данных (ИСПДн), несанкционированный доступ, средства защиты информации (СЗИ), корпоративная сеть.

Средства защиты информации необходимы для обеспечения требуемого уровня информационной безопасности персональных данных, обрабатываемых в корпоративной сети предприятия.

СЗИ от НСД выполняют следующие функции:

- идентификация и аутентификация пользователей и устройств;
- регистрация запуска (завершения) программ и процессов;
- реализация необходимых методов и правил разграничения доступа;
- управление информационными потоками между устройствами;
- учет носителей информации.

Оцениваются следующие средства защиты информации от НСД:

- Dallas Lock;
- Secret Net;
- Страж NT.

Для оценки вводятся числовые значения критериев оценки.

Значения критериев представлены в табл. 1.

Таблица 1

Оценка критериев

Качественная оценка		Количественная оценка
Отсутствует	Нет	0
Присутствует	Да	1

Оценка СЗИ от НСД представлена в табл. 2.

Таблица 2

Оценка СЗИ от НСД

Критерий/СЗИ	Dallas Lock	Secret Net	Страж NT
1	2	3	4
Наличие сертификата ФСТЭК	1	1	1
Наличие сертификата ФСБ	1	1	0
Дискреционная и мандатная модели разграничения доступа	1	1	1
Доверенная загрузка ОС	1	0	0
Контроль целостности программной среды и файловой системы	1	0	1
Криптографическая защита	1	0	1
Контроль работы внешних носителей	1	0	0
Уничтожение удаляемой информации	1	1	1
Журналирование (регистрация) событий	1	1	1
Самодиагностика	1	0	1
Совместимость с аппаратными средствами защиты информации	1	1	1
Наличие демонстрационных версий ПО	1	1	1
Поддержка ОС семейства Windows	1	1	1
Итого:	17	12	13
Контроль НДВ	2	4	4
Класс защищенности	2	3	3
Цена, руб.:	8 000	7 000	7 500

СЗИ от НСД Dallas Lock имеет наивысшую количественную оценку по показателям, а также наивысший уровень контроля НДВ и класса защищённости.

Проведем количественную оценку средств антивирусной защиты, все показатели, кроме класса защищенности, уровня НДВ и цены, имеют одно из трех значений высокий (2), средний (1), низкий (0).

Выбор средств антивирусной защиты по следующим показателям:

- эффективность работы (качество проверки);
- функциональность;
- скорость работы;
- требования к ресурсам;
- надежность работы;
- интерфейс и настройки.
- класс защищенности;
- контроль НДВ;
- цена.

Сравнительная характеристика антивирусного ПО приведена в табл. 3.

Таблица 3

Сравнительная характеристика антивирусного ПО

Критерий/ПО	Касперский	Dr.Web	ESET 32
Эффективность работы	2	2	1
Функциональность	1	2	1
Скорость работы	2	2	2
Требования к ресурсам	2	1	1
Надежность работы	2	1	1
Интерфейс и настройки	2	2	1
Итог:	11	10	7
Класс защищенности	1	2	1
Контроль НДВ	2	3	3
Цена, руб. в год	1 990	1090	1 750

По количественной оценке, самым лучшим антивирусным ПО является Kaspersky Internet Security, также это ПО имеет наивысший контроль НДВ и класс защищенности.

Литература

1. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14.05.2013 N 28375).

2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных».

3. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Инфра-М, 2010. 594 с.

4. Материалы сайта https://www.securitylab.ru.

5. Материалы сайта https://www.altx-soft.ru.

АНАЛИЗ ОСНОВНЫХ УЯЗВИМОСТЕЙ СИСТЕМЫ СПУТНИКОВОЙ СВЯЗИ И МЕТОДОВ ИХ УСТРАНЕНИЯ

Н. Д. Лобжанидзе, А. В. Степаненко, Д. А. Мирошников, Н. Н. Медведенко
руководитель – д-р техн. наук, профессор ***И. А. Калмыков***
Северо-Кавказский федеральный университет, г. Ставрополь

Проанализированы основные уязвимости систем спутниковой связи и выявлены методы их устранения.

Ключевые слова: системы спутниковой связи, несанкционированный доступ, системы радиоэлектронной борьбы, уязвимости.

Современные информационные системы (ИС), к которым относятся системы спутниковой связи, являются одним из краеугольных камней, на основе которых строят бизнес-процессы компании и предприятия различных форм и назначений. Однако всем ИС присущи «слабые места» с точки зрения обеспечения защиты информации от НСД, в качестве которых выступают уязвимости этих систем. Реализация любой атаки злоумышленника достигается путём активизации той или иной уязвимости, которая присутствует в системе передачи данных. Это в свою очередь создаёт условия для успешного проведения информационных атак на ИС.

Под уязвимостью системы спутниковой связи будем понимать недостатки технологии процесса передачи данных, мер и средств обеспечения информационной безопасности ССС, позволяющие нарушителю совершать действия, приводящие к реализации той или иной угрозы.

Обеспечение информационной безопасности в системах спутниковой связи на основе рационального применения разнообразных технических средств является сложной научно-технической задачей. Чтобы создать и реализовать эффективные механизмы защиты информации от НСД в ССС от различных угроз безопасности необходимо выявить такие элементы системы, которые уязвимы в наибольшей степени.

Проведенные исследования показали, что дестабилизирующие действия на систему спутниковой связи можно разделить на две группы. В основу первой группы будут входить методы радиоэлектронного подавления сигнала. Во вторую группу методов можно отнести те методы, которые базируются на и навязывании ложного базиса сигнала противнику.

Целью радиоэлектронного подавления сигнала КА на низких околоземных орбитах является блокирование передачи сигнала, в результате которого ЦПО утрачивает возможность правильно принимать решение по выбору управляющего воздействия на удаленный объект [РЭБ].

Для достижения поставленной цели злоумышленник может воспользоваться как пассивными, так и активными помехами. Наиболее простыми

являются пассивные помехи, среди которых можно выделить гармонические непрерывные помехи (ГНП), закон создания приведен в [РЭБ]. Наряду с гармоническими непрерывными помехами широкое распространение получили прицельные и заградительные непрерывные шумовые помехи. Закон создания таких помех определяется выражением

$$U\ \ (t) = U_{mm}(t)\cos\left(\omega_{p1}t + \varphi_{p1}(t)\right), \tag{1}$$

где Umm(t) - закон изменения огибающей помехи;

$\varphi_{p1}(t)$ - закон изменения фазы помехи;

ω_{p1} - средняя частота помехи;

$\omega_{p1} \approx \omega_0; \omega_0 = 2\pi L$;

L - несущая частота сигнала.

Наряду с пассивными помехами злоумышленник может использовать активные помехи (АП). В настоящее время существует множество активных помех. Особое место среди них занимают маскирующие помехи, среди которых можно выделить активные непрерывные шумовые помехи. Амплитудно-модулированные шумовые помехи (АМ ШП) представляют собой незатухающие гармонические колебания, моделированные по данному закону

$$U(t) = U_{П}\left[1 + K_a \Delta U_{МОД}(t)\right], \tag{2}$$

где Ка - крутизна модуляционной характеристики передатчика;

$\Delta U_{МОД}(t)$ - моделирующее направление, поступающее от генератора шума.

Наряду с непрерывными шумовыми помехами в системах РЭБ используют последовательности детерминированных импульсных сигналов [реб]. Если $\{x[k]\}, k = 0, \pm 1, \pm 2, ...$ - последовательность детерминированных импульсных сигналов, то мгновенная мощность такого сигнала равна $\left|x[k]^2\right|$, а полная энергия определяется выражением

$$E_x = \sum_{k=-\infty}^{+\infty} |x[k]|^2 \tag{3}$$

Тогда средняя мощность такой активной помехи - последовательности детерминированных импульсных сигналов $\{x[k]\}$ равна

$$P_x = \left\langle |x[k]|^2 \right\rangle = \lim_{T \to \infty} \frac{1}{2T+1} \sum_{k=-T}^{T} |x[k]|^2 . \tag{4}$$

Если рассматривать активные помехи необходимо отметить также хаотические импульсные помехи. Хаотические помехи представляются в виде последовательности радиоимпульсов с заданным значениями частоты заполнения. При этом значения амплитуды и длительности помехи, а также интервалы между соседними импульсами могут изменяться случайным образом.

$$M_{\tau} = \frac{\pi}{\sqrt{-\rho_o}}\left[1 - \Phi\left(\frac{\gamma}{\sqrt{2}}\right)\right]\exp\left(\frac{\gamma^2}{2}\right), \quad (5)$$

$$M_{\Delta} = \frac{\pi}{\sqrt{-\rho_o}}\left[1 + \Phi\left(\frac{\gamma}{\sqrt{2}}\right)\right]\exp\left(\frac{\gamma^2}{2}\right), \quad (6)$$

где $\rho(\tau)$ - коэффициент корреляции шума генератора;

$\gamma = \frac{U_0}{\sigma_ш}$; $\Phi(\gamma) = \frac{2}{\sqrt{\pi}}\int_0^{\gamma} e^{-x^2} dx$ - интеграл вероятности;

При этом каждый вид активных помех оказывает свое воздействие на канал радиосвязи. Поэтому при выборе необходимой помехи учитываются временные, спектральные, а также статистические характеристики используемого сигнала.

В настоящее время в системах РЭБ также применяются активные имитирующие помехи. Такие помехи используются для навязывания ложной информации, а также для перегрузки каналов обработки информации. Для нарушения процесса работы систем радиосвязи применяются прицельная имитирующая помеха, следящая имитирующая помеха, заградительная имитирующая помеха. Эти помехи относят к «интеллектуальным» помехами, так как они способны подстраиваться под передаваемый сигнал, нарушая тем самым эффективную работу системы радиосвязи.

Наряду с пассивными и активными помехами в системах РЭБ широко используются методы подмена базиса ложными сигналами. Основной целью подмены является искажение значений показателей, позволяющих оценить текущее состояние объекта управления, или навязывание некорректного управляющего воздействия, поступающего из центра поддержки операций. При этом подмена подразумевает создание копии базы сигналов и манипулирование его параметрами.

Очевидно, что в условиях Крайнего Севера, территория которого является труднодоступной и малозаселенной, методы, составляющие первую группу и дестабилизирующие работу системы спутниковой связи, являются малоэффективными. При этом, несмотря на многообразие систем способных поставить различные виды радиопомех, данный подход к нарушению рабо-

ты системы мониторинга, контроля и управления удаленным объектом в арктических условиях требует значительных финансовых затрат.

Следовательно, в условиях размещения оборудования в труднодоступных и малозаселенных районах, основным способом негативного воздействия на систему спутниковой связи являются методы, образующие вторую группу. Поэтому в проекте будут рассмотрены методы противодействия попыткам навязывания ложного образа.

Литература

1. Научно-информационный бюллетень «Проблемы Севера и Арктики Российской Федерации». Выпуск девятый (апрель 2009). М.: Издание Совета Федерации, 2009. 194 с.
2. http://studme.org/175408016521/menedzhment/kontrol#549 (дата обращения 22.05.2016).
3. http://enersys.ru/solution/for-disp-centr/rem-control/ (дата обращения 21.05.2016).
4. Калмыков И. А., Дагаева О. И. Разработка псевдослучайной функции повышенной эффективности // Известия ЮФУ. Технические науки. Таганрог: ТРТУ, 2011. №12. С. 160-169.
5. Калмыков И.А., Дагаева О.И. Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции // Известия ЮФУ. Технические науки. 2012. № 12. С. 218-224.

АНАЛИЗ ТИПОВЫХ НАПАДЕНИЙ НА ЗОНУ ОЗУ КЛИЕНТА ЭЛЕКТРОННОЙ ПОЧТЫ

А. П. Львова, Д. А. Дзюба, Е. С. Пелешенко
Северо-Кавказский федеральный университет, г. Ставрополь

В ходе исследования изучена структура системы электронной почты, проведен анализ типовых нападений на зону оперативной памяти клиента электронной почты. На основе полученных результатов предложены возможные рубежи защиты.

Ключевые слова: электронная почта, информационная безопасность, ОЗУ, клиент, утечка, информация, защита.

Электронная почта (ЭП) занимает существенное место в общем информационном потоке и ввиду разделения обрабатываемых данных по категориям доступа, системы электронной почты нуждаются в защите. Для организации мероприятий по обеспечению информационной безопасности необходимо ясно представлять структуру объекта защиты и характер связей и взаимодействий, составляющих основу электронного документооборота.

Электронная почта – это технологии и службы, в совокупности, осуществляющие передачу информации от отправителя к получателю.

Основными компонентами системы являются: линия вычислительной сети (ЛВС), сервер, клиент.

ЛВС обеспечивают надежную передачу данных от клиента-отправителя к серверу и далее к клиенту-получателю. Задачи доставки и

получения почты независимы друг от друга, что обеспечивает гарантированную передачу сообщений, даже если какой-либо из компонентов системы электронной почты временно недоступен. Сервер занимается направлением писем к получателю или отсылкой обратно отправителю на хранение, если получатель не существует или ввиду каких-либо технических неполадок не может прочитать сообщение.

Клиент – это программное обеспечение, выполняющее функции подготовки электронных сообщений, отправки или получения писем с сервера, хранения и поддержки справочника адресов ЭП, а также занимается выполнением стандартных операций по обработке электронных сообщений.

Согласно статистике центра аналитики информационной безопасности Infowatch. растет доля случайны утечек данных через электронную почту. Первым звеном в обработке информации является клиент.

Память клиента разделяется на долговременную (ДЗУ) и оперативную (ОЗУ).

Типовые нападения на зону ДЗУ – это кража баз данных электронных адресов и писем, которые непосредственно хранятся на компьютере. Что касается зоны ОЗУ клиента, то именно она подвержена атакам, при которых информация может стать доступной злоумышленнику в процессе передачи данных.

На основе анализа структуры клиента электронной почты сделан вывод, что типовыми нападениями на зону ОЗУ клиента ЭП являются:

1) ***Утечка классифицированной информации.*** Данный вид нападения характерен для процесса обработки электронной корреспонденции в ОЗУ клиента. Ошибки программного кода, уязвимости операционной системы (ОС) и программного обеспечения являются факторами, которые предоставляют доступ злоумышленнику к информации.

Причиной является использование стандартных функций из библиотек выполнения программ, которые допускают выход информации электронного сообщения из контекста защиты клиента электронной почты и данные потенциально становятся доступными для злоумышленника.

2) ***Перехват*** электронной почты в ОЗУ. Целью данного нападения является доступ к данным до того, как они будут зашифрованы криптографическими алгоритмами ОС или программного обеспечения. Заблаговременный перехват информации, основанный на уязвимостях системы, намного облегчает процесс получения данных и не требует больших вычислительных мощностей на дешифрование сообщения.

Несовершенство систем передачи данных приводит к хищению информации, однако именно это несовершенство и двигает информационную безопасность, мотивируя создавать более надежные средства защиты. ОЗУ клиента можно защитить установкой следующих рубежей защиты:

1. Криптографические, стеганографические алгоритмы операционной системы.

2. Антивирусное ПО.

3. Использование электронной подписи, которая будет обеспечивать авторство и контроль целостности.

4. Средства фильтрации электронных писем, которые позволяют защитить программное обеспечение от нежелательной или вредоносной почты.

На основе проведенного исследования можно сделать вывод, что каждый элемент системы электронной почты нуждается в надежных средствах защиты.

Литература

1. Информационная безопасность автоматизированных систем // А. Ф. Чипига. М.: «Гелиос АРВ», 2010. 336 с.
2. Физические основы защиты информации / Сагдеев К. М., Петренко В. И., Чипига А. Ф.: учебное пособие. Санкт-Петербург, 2017.
3. Модель трехмерной структуры объектов с матрицей доступа // Чипига А. Ф., Ерещенко А. А., Пелешенко В. С. // Известия ЮФУ. Технические науки. 2009. С. 172-176 с.
4. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / Чипига А. Ф., Пелешенко В. С. // Информационное противодействие угрозам терроризма. 2010. С. 114-118.
5. Объектный подход к модели разграничения доступа в компьютерных системах / Чипига А. Ф., Ерещенко А. А. // Информационное противодействие угрозам терроризма. 2005. С. 122-128.
6. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи / Чипига А. Ф., Марков Д. М., Слюсарев Г. В. // Фундаментальные исследования. 2015. 759 с.

СРАВНЕНИЕ АНТИВИРУСНЫХ ПРОГРАММ И МЕЖСЕТЕВЫХ ЭКРАНОВ

В. О. Макарова

руководитель – канд. физ.-мат. наук, доцент ***Н. В. Кононова***

Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье рассматриваются межсетевые экраны (*брандмауэры*) *и антивирусные программы, проведено их сравнение, а также выявлена наиболее эффективная антивирусная программа.*

Ключевые слова: межсетевой экран, антивирусная программа, угрозы несанкционированного доступа, персональная информация, утилита ping, брандмауэр.

В настоящее время возрастает количество угроз несанкционированного доступа к персональной информации, поэтому необходимо позаботится о собственной информационной безопасности. В данной статье будут рассмотрены различные антивирусные программы и межсетевые экраны.

Межсетевой экран(брандмауэр,фаейрвол: от fire «огонь» + wall «стена») – это программно-аппаратная составляющая компьютерной сети, кон-

тролирующая проходящий через нее сетевой трафик в соответствии с заданными требованиями.

Антивирусная программа – программное обеспечение, направленное на обнаружение вирусов, восстановления зашифрованных данных, а также профилактики – предотвращения заражения устройства.

Целью работы является сравнение эффективности работы различных файрволов и антивирусных программ.

Задачей исследования является выявление наиболее надежного программного межсетевого экрана и антивируса.

В ходе проведения исследования будем использовать следующее ПО: брандмауэр Windows, антивирус «KasperskyInternetSecurity» и антивирус «AvastInternetSecurity».

Перед началом работы установим операционную систему «Windows 7 Максимальная» с заводскими настройками на свой персональный компьютер, который в дальнейшем будем называть ПК1. Затем необходимо открыть «Панель управления», выбрать «Брандмауэр Windows» и проверить настройки экрана, нажав на «обновление параметров брандмауэра», выбираем брандмауэр для рабочей, домашней и общественной сетей. После чего подключаемся к домашней сети и сети Интернет. В данной домашней сети находится другой персональный компьютер – ПК2, для которого в командной строке будем использовать утилиту ping, предназначенную для проверки целостности и качества соединений в сетях на основе TCP/IP, а также обиходное наименование самого запроса. Оправку файлов будем производить также с ПК2, на котором отключены пользовательские настройки безопасности.

В командной строке второго ПК (192.168.0.2) напишем команду «ping192.168.0.1», т. е. проверим ответ первого ПК: «Ответ от 192.168.0.1: Заданный узел недоступен». Теперь попробуем в обратном направлении: «Превышен интервал ожидания для запроса». Затем отключим брандмауэр для домашней сети на ПК1: «Ответ от 192.168.0.2: число байт=32 время=1мс TTL=30. (0% потерь)». Запрос утилиты ping в обоих направлениях прошёл успешно. Таким образом брандмауэр не принимает пакет данных со стороны ПК2, даже не разбирая его содержимого, а также не отправляет за пределы ПК1 аналогичный пакет. С отключенным межсетевым экраном выход в Интернет является абсолютно не безопасным.

Перейдем к рассмотрению антивирусных программ. Установим «KasperskyInternetSecurity 2016» trial-версию на 30 дней. Зайдем в настройки Брандмауэра Windows и увидим следующее уведомление: «Управление этими параметрами осуществляет приложение поставщика «KasperskyInternetSecurity»». В данном случае сетевой экран, веб-антивирус и другие функции включены по умолчанию. При использовании утилиты ping, заметим, что успешно будет получен ответ с обоих ПК. Теперь проверим эффективность продукта Касперского в Интернете.

Для этого будем специально искать и скачивать зараженные файлы. Введем в поисковой строке «ключ на AdobePhotoshopCS6», выберем первую ссылку, и антивирус оповестит нас о том, что предотвратил скачивание вредоносного файла разрешения «.exe», благодаря чему наш ПК будем защищен от вирусной атаки. Перейдем на пятидесятую страницу поиска и нажимем уже на другу ссылку. Антивирусная программа покажет уведомление о том, что отклонил атаку с «exampel.su» и при этом предложит проверить состояние всех файлов на ПК1. Через некоторое время полной проверки файлов антивирус выведет статистику, в которой говорится о том, что файл «trojan-exampel-petya-nesushestvuy.exe» был вылечен. Попробуем продолжить поиск вирусов, найдем установочный файл взломанного «фотошопа» и установим его вместе с браузером «Амиго». В это время на нашем рабочем столе появится огромное количество неизвестных ярлыков, а также работа других приложений будет некорректна. Через несколько минут антивирус оповестит о заражении и необходимости полного сканирования, а также удалении вредоносного ПО. Через достаточно большое количество времени от антивируса будет получен отчет о проделанной работе, в котором говорится, что были удалены следующие файлы: trojan-photoshop.exe, cooki-monster.exe, neponytnue.bin,amigo-vk-mail-your-best-friends.exe и так далее.

Далее установим «Avast Internet Security». И по завершению установки получаем оповещение от данного антивируса, что ПК1 заражен kasperskyinternetsecurity.exe, а от «KasperskyInternetSecurity» о том, что ПК1 заражен avast.exe. В итоге получился конфликт антивирусов. Для решения этой ситуации необходимо отключить оба антивируса, удалить «KasperskyInternetSecurity» и переустановитьAvast. Аналогично с предыдущим повторим проверку настройки защиты и удачно используем утилиту ping для ПК1 и ПК2. Теперь начнем проверку с пятидесятой страницы, ссылки exampel.su. Антивирус Avast сообщит о том, что отразил атаку с этого сайта, и обнаружил файл trojan-exampel-petya-nesushestvuy.exe, но вылечить его не удалось. На этом этапе делаем вывод, что антивирус Avast слабее Kaspersky.

Таким образом, после проведения данного исследования можно сделать вывод, что одного межсетевого экрана недостаточно и необходима комплексная защита данных.

Литература

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. М.: ИД «ФОРУМ»: ИНФРА-М, 2011. 416 с.: ил. (Профессиональное образование).

2. Оглтри Т. Firewalls. Практическое применение межсетевых экранов: Пер. с англ. М.: ДМК Пресс, 2001. 400 с.: ил. (Серия «Защита и администрирование»).

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СЕЛЬСКОМ ХОЗЯЙСТВЕ

А. А. Малыгин
руководитель – магистр направления подготовки
«Информационная безопасность» ***С. М. Полухин***
Северо-Кавказский федеральный университет, г. Ставрополь

В наши дни особенно важной проблемой сельского хозяйства в Российской Федерации является значительное отставание его технологического развития по отношению к ведущим аграрным государствам. По данным, которыми оперируют учёные, исследующие этот вопрос, сельскохозяйственное производство в России сегодня приближено к тому уровню, какой был в СССР в 70-х годах XX века. Данная статистика не может не удручать. Принято считать, что ведущим фактором для повышения эффективности сельского хозяйства служат именно новаторские информационные технологии, однако с этим направлением в Российской Федерации сейчас существуют некоторые трудности.

Ключевые слова: сельское хозяйство, информационные технологии.

В нынешнем состоянии развития АПК одной из существенных задач его быстрого распространения, как по всей территории Российской Федерации, так и её регионов по решению вопросов продовольствия и вынужденного повышения конкурентоспособности, является интенсификация АПК, его автоматизация, современная механизация и развитие информационных технологий, которые позволяют с каждой единицы использующихся ресурсов получить большее количество, разнообразие и разносортность высококачественных продуктов питания – это и есть эффективнейший способ развития агропромышленного комплекса. Инновационное развитие АПК замедляется, в том числе из-за низкого уровня технологической оснащенности, во многом определяемой техническим и технологическим уровнем промышленности и недостаточной квалификацией кадров. В то время как мировой и европейский опыт ведения сельскохозяйственных работ уже напрямую связан с информационными технологиями, в России это направление еще практически не открыто и по многим причинам не получает должного внимания.

Во второй половине прошлого века, когда преуспевала командно-регулируемая экономическая система, главной целью государства было не стремление к высоким показателям при минимальных затратах, то есть как можно более рациональное производство, а обеспечение занятости населения страны. В нынешнем XXI веке же процветает рыночная экономика. Первенство изменилось в сторону повышения эффективности сельскохозяйственного сектора, следует как можно быстрее стремиться к развитию АПК, к революции именно информационных технологий в сельском хозяйстве.

Нужно отдать должное государственной политике, направленной на поддержание сельскохозяйственных предприятий и их субсидирование. Выделяемые федеральным бюджетом деньги идут на качественное улучшение технологического оборудования. Введение современных информационных технологий в производство сельского хозяйства предполагает постоянное обогащение информацией от различных внешних источников из практически любой точки местности в подходящий любому работнику момент времени. Например, перманентное получение данных об определенных прогнозах синоптиков может быть доступно фермерам на протяжении дня. Это позволяет более целесообразно и эффективно применять различные химические средства защиты растений, а также существенно снижает риск загрязнения окружающей среды. Список информационных технологий очень велик: например, существуют такие разработки информационных систем, которые предупреждают фермеров о появлении вредителей и болезней растений.

Однако на этом неоспоримые преимущества информационных технологий не заканчиваются. При рациональном использовании информационного обеспечения на предприятии улучшаются такие значимые характеристики, как результативность, чёткая согласованность действий; ускоряется темп производства, а также увеличивается качество изготовляемой продукции. Информационные технологии позволяют отследить ход выполнения тех или иных операций, своевременно заметить возможные неполадки и устранить их до того момента, пока они усугубят положение дел на производстве.

Внедрение информационных технологий также существенно снижает влияние человеческого фактора, что является положительным моментом для предприятия.

Значительный интерес для государства представляют информационные разработки в животноводческой отрасли. Так миниатюрные датчики, которые могут быть безболезненно помещены под кожу животных и находиться в их теле продолжительное время, не причиняя никакого вреда, позволяют получать наиболее точную информацию о здоровье скота и определять его текущее местоположение. Все эти операции могут быть с легкостью проведены при самом упрощённом знании о работе с технологиями, поэтому развитие в этой отрасли производства особенно актуально для Российской Федерации с учетом ее устремленности на повышение уровня аграрного производства.

Сейчас перспективы развития информационных технологий в сельском хозяйстве очень высоки. В разных субъектах Российской Федерации уже проходят мероприятия, направленные на внедрение в предприятия качественно новых достижений науки и техники и ознакомление с ними специалистов и работодателей с опорой на опыт зарубежных западных стран, которые на данный момент преуспели в АПК. В России также фор-

мируются консультационные, организационные, управленческие центры, готовые всегда помочь тем или иным производствам путем их финансирования и осуществления иных инвестиционных проектов. Наконец, полным ходом развивается и научно-технологическая деятельность в рассматриваемой нами сельскохозяйственной отрасли производства.

Безусловно, приведенные выше действия, направленные на развитие сельского хозяйства, оказывают влияние на фермерские хозяйствующие субъекты, однако для увеличения продуктивности проводимых мер нужно создание своего рода единой информационной базы, иначе говоря, системы доступа, а также внедрение информационных технологий на федеральном и региональном уровнях.

Подводя итог, хотелось бы обобщить все вышесказанное и сделать вывод: сельскому хозяйству нужна стабильная государственная поддержка для привлечения «молодой крови». Создание программ для повышения квалификации кадров, не только обещанные, а уже вполне реальные перспективные цели, которые более чем реально достичь — все это будет продвигать сельскохозяйственные производства вперед, завлекая на предприятия новых специалистов. Четко сформулированные этапы подъема сельского хозяйства, определение конечных результатов и сроков, в какие обязательно надо достичь намеченного распорядка, необыкновенно важны для дальнейшего создания мощной стабильной системы, в которой информатизация наряду с автоматизацией сельскохозяйственных субъектов могли бы стать основной движущей силой АПК.

Литература

1. Информационное обеспечение фермерских хозяйств: состояние, проблемы, направления развития / Ермакова А.Н., Ермаков И.В., Ермакова Н.Ю. / Региональная экономика: теория и практика, 2009.

2. Особенности функционирования крестьянских (фермерских) хозяйств / Ермакова А.Н. / Управление экономическими системами: электронный научный журнал, 2011.

3. Приёмы создания и функционирования информационно-консультативных служб в аграрной сфере / Ермакова А.Н. / Вестник АПК Ставрополья, 2011.

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ И КРИТЕРИЕВ ОЦЕНКИ ЗАЩИТЫ ИНФОРМАЦИИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ НОРМАТИВНЫХ ДОКУМЕНТОВ

А. А. Маногарова, С. А. Степанов, И. Р. Евдокимов
руководитель – преподаватель кафедры ИБАС ***И. В. Анзин***
Северо-Кавказский федеральный университет, г. Ставрополь

Проанализированы существующие нормативные документы в области критериев оценки безопасности информационных систем. Определен подход по формированию критериев оценки защищенности информационных систем на основе наиболее актуальных стандартов безопасности. В работе приведена актуаль-

ность проблемы выбора критериев для оценки защищенности информации в автоматизированных информационных системах. Выполнен анализ нормативной базы в области оценки защиты информации. Предложен подход по формированию критериев оценки защищенности информационных систем на основе наиболее актуальных стандартов безопасности.

Ключевые слова: критерии оценки, защита данных, информационная безопасность.

При проведении оценки защищенности АС основополагающими аспектами являются критерии и методы проведения оценки. В качестве условия оценки выступает некий набор критериев безопасности, описанных на основе нормативных документов разных уровней.

На данный момент нормативная база в области защиты информации основательно проработана и насчитывает большое количество методик и документов, охватывающих различные аспекты защиты информации. Нормативные документы можно разделить в зависимости от области действия на три группы: международные, национальные и нормативные документы РФ.

На данный момент наиболее значимыми международными нормативными документами в области защиты информации являются следующие стандарты: ISO/IEC TR 19791:2010, ISO/IEC 15408, ISO/IEC 27002:2005.

Международной организацией по стандартизации (ISO) в 2006 году был выпущен доклад ISCVIEC TR 19791 «Information technology. Security techniques. Security assessment of operational systems» (Информационные технологии. Методы обеспечения безопасности. Оценка безопасности операционных систем). Данный стандарт принимает во внимание ряд важных аспектов операционных систем, не отраженных в стандарте ISO/IEC 15408 оценки АС. Основой для стандарта 19791 является международный стандарт ISO/IEC 15408, который определяет современный понятийный аппарат и подходы к оценке информационных технологий.

В стандарте ISO 15408 собраны и обобщены национальные подходы к разработке критериев в области защиты информации. Данный стандарт устанавливает параметры для проведения оценки механизмов обеспечения безопасности, в первую очередь на программно-техническом уровне. Стандарт обусловливает требования к качеству реализации механизмов безопасности и требования безопасности. Также он включает в себя реестр профилей защиты, прошедших процедуру регистрации. Профили защиты представляют собой набор требований к функциям и надежности, предъявляемых к объектам оценки, учитывающих назначение объектов, угрозы безопасности и т. д.

Для проведения оценки степени защищенности АИС данный стандарт предоставляет набор параметров с анализом степени воплощенных в ней функций безопасности, а также степень надежности этих функций, хотя

основным направлением стандарта являются механизмы безопасности программно-технического уровня.

Наиболее распространенным в мире стандартом является ISO 27002:2005. Данный стандарт определяет требования к организации режима защиты информации и используется на добровольной основе достаточно большим числом организаций. В данном стандарте указаны критерии оценки механизмов безопасности организационно-административного уровня, а также некоторые механизмы безопасности уровня физической защиты. Стандарт ISO 27002:2005 направлен в первую очередь на создание модели системы управления безопасностью организации. В соответствии с моделью, принятой в данном стандарте, основные моменты создания системы ЗИ сгруппированы в десять уровней, а также средствами контроля для каждого уровня.

Многими государствами разработаны собственные национальные стандарты, в которых отражены требования к обеспечению защиты информации, а также критерии оценки СЗИ. В качестве примера национальных нормативных документов по оценке защищенности можно привести:

– SP800-35 «IT Security Services»;
– SP800-36 «Selecting IT Security Products»;
– PD 3001 – Preparing for BS 7799-2 Certification;
– PD 3002 – Guide to BS 7799 Risk Assessment;
– PD 3004 – Guide to the Implementation and Auditing of BS 7799 Controls.

Для разработки систем защиты информации во многих странах используются собственные национальные стандарты обеспечения безопасности АС, например, [3]:

1. США – DOD 5200.28 – STD «Orange Book»;
2. Великобритания – B S 7799;
3. Германия – BSiUT Baseline Protection: Manual.

Практически все требования безопасности, а также критерии оценки защищенности учтены в международных стандартах ISO/IEC 15408 и ISO/IEC 17799. В РФ существует достаточно большая база нормативных документов, а также государственных стандартов по организации защиты информации, а также оценки защищенности АС, например, [1]:

– Доктрина информационной безопасности Российской Федерации;
– ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
– ФЗ № 152-ФЗ «О персональных данных»;
– ФЗ № 126-ФЗ «О связи»;
– ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации;
– ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;

– ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования;

– ГОСТ Р ИСО/МЭК 18028-1-2008. Информационная технология. Методы и средства обеспечения безопасности;

– ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности;

– ГОСТ Р ИСО/МЭК 27005-2009. Информационная технология. Методы и средства обеспечения безопасности;

– ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;

– ГОСТ Р ИСО/МЭК 15408-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

Стандарты ИСО/МЭК 27002-2012 и ИСО/МЭК 15408-2008 имеют большое значение в проведении оценки защищенности АС. Данные стандарты практически являются переводами стандартов ISO 15408 и ISO 17799.

Государственный стандарт ГОСТ Р ИСО/МЭК 27002-2012 содержит набор правил и мер защиты, разбитый на 10 подразделов:

1. Разработка политики и информационной безопасности организации.
2. Организация мероприятий по защите информации.
3. Мониторинг, классификация и контроль ресурсов в АС.
4. Обеспечение безопасного функционирования персонала.
5. Безопасность АС на физическом уровне.
6. Администрирование АС.
7. Контроль доступа к ресурсам АС.
8. Разработка и сопровождение АС.
9. Организация бесперебойной работы организации.
10. Мониторинг выполнения политики безопасности организации.

В вышеперечисленных подразделах стандарта ГОСТ Р ИСО/МЭК 27002-2012 приведено описание механизмов обеспечения безопасности, а также средств контроля, применяемых во многих организация по всему миру.

Основными средствами контроля безопасности являются:

– нормативный документ, описывающий политику информационной безопасности организации;

– закрепление функций реализации информационной безопасности;

– повышение квалификации персонала организации в области поддержания режима информационной безопасности;

– регистрация случаев нарушения защиты;

– антивирусные средства;

– создание регламента организации бесперебойной работы организации;

– контроль возможности несанкционированного копирования информации;

– обеспечение безопасности информации организации;

– защита данных;

– выполнение мониторинга всех процессов на соответствие политики безопасности.

Одним из важнейших процессов при проведении процесса аудита безопасности АИС является анализ степени соответствия рискам, полноты реализации и качества по всем основным средствам контроля защищенности.

Перевод международного стандарта ISO/IEC 15408 в 2002 году был принят в качестве государственного стандарта: ГОСТ Р ИСО/МЭК 15408. В качестве дополнения к данному стандарту был выпущен Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», а также в 2008 году был выпущен стандарт ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».

В предлагаемом подходе к оценке защищенности выделены два основных критерия безопасности: эффективность и актуальность. Актуальность понимается как актуальная реализация средств и механизмов безопасности АИС, реализуемых в соответствии с разработанной документацией, а также мониторингом и фиксации функционирования средств безопасности. Под эффективностью понимается обеспечение противодействия угрозам безопасности, а также предотвращение неавторизованных действий. Данные критерии должны выполняться на всех этапах жизненного цикла АС.

Также помимо вышеперечисленных госстандартов дополняет нормативную базу в области защиты информации достаточно большое число рабочих документов Государственной технической комиссии Российской Федерации, такие как [6]:

– «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения». Решение председателя Гостехкомиссии России от 30 марта 1992 г.

– «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Решение председателя Гостехкомиссии России от 30 марта 1992 г.

– «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации». Решение председателя Гостехкомиссии России от 25 июля 1997 г.

– «Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Приказ председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

Таким образом, на сегодняшний день многие рабочие документы и приказы Гостехкомиссии России во многом потеряли свою актуальность. Наиболее актуальным на сегодняшний день является стандарт ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», в котором отражены все основные аспекты защиты информации в АИС, но применение данного стандарта не всегда возможно [7], т. к. он направлен на программно-технический уровень функционирования АИС и не учитывает административный и процедурный уровни защиты. Данный стандарт не содержит критериев оценки безопасности. В качестве выбора источника критериев оценки безопасности АИС предлагается выбрать ГОСТ Р ИСО/МЭК ТО 19791-2008.

Выводы: в работе определена актуальность проблемы выбора критериев для оценки защищенности информации в автоматизированных информационных системах. Выполнен анализ нормативной базы в области оценки защиты информации. Предложен подход по формированию критериев оценки защищенности информационных систем на основе наиболее актуальных стандартов безопасности.

Литература

1. http://fstec.ru/ – Федеральная служба по техническому и экспортному контролю.

2. «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения». Решение председателя Гостехкомиссии России от 30 марта 1992 г.

3. «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Решение председателя Гостехкомиссии России от 30 марта 1992 г.

4. «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации». Решение председателя Гостехкомиссии России от 25 июля 1997 г.

5. «Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Приказ председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

6. DOD 5200.28 – STD «Оранжевая книга».

7. Галатенко В. А. Оценка безопасности автоматизированных систем. Обзор и анализ предлагаемого проекта технического доклада ISO/IEC PDTR 19791. Jet Info online! // Информационный бюллетень. 2005. № 7.

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ LINUX ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

А. А. Маногарова, С. А. Степанов, И. Р. Евдокимов
руководитель – преподаватель кафедры ИБАС ***И. В. Анзин***
Северо-Кавказский федеральный университет, г. Ставрополь

Определена операционная система, которая может выполнять поставленные требования по защите информации. Проанализирована документация, выделены требования системы и определены соответствие дистрибутивов требованиям. В работе исследованы две операционные системы Astra Linux Special Edition и ALT Linux. Изучен принцип работы каждой из платформ. Проведен анализ на предмет соответствия требованиям для работы с защищаемой информацией. Представлен сравнительный анализ двух дистрибутивов и сделаны выводы по его результатам. Определено, какой дистрибутив может выполнять поставленные требования.

Ключевые слова: Astra Linux Special Edition, ALT Linux, SELinux, защита информации, информационная безопасность.

Обновление требований ФСТЭК России к операционным системам по безопасности информации показывает необходимость внесения изменений в выбор предприятиями сертифицированных платформ. Можно сказать, что операционная система специального назначения Astra Linux Special Edition относится к «доверенным». Она имеет сертификат соответствия Минобороны России № 1339 от 24 сентября 2010 г. (до 15 сентября 2018 г.), и сертификат соответствия ФСТЭК России № 2557 от 27 января 2012 г. (до 27 января 2021 г.).

Для проведения сравнительного анализа на предмет соответствия требованиям по работе с защищаемой информацией проведен анализ еще одного дистрибутива – ALT Linux. Система имеет сертификат соответствия ФСТЭК России № 2317 от 18 апреля 2011 г. (продлен до 18 апреля 2020 г. в марте 2017 г.).

SELinux – способ реализации системы принудительного контроля доступа, может работать вместе с избирательной системой контроля доступа, которая названа классической.

В SELinux права доступа назначаются самой системой при помощи заранее определенных политик. Политики работают на уровне системных вызовов и применяются самим ядром. SELinux действует после классической модели безопасности Linux. При проведении анализа ALT Linux на предмет соответствия требованиям по работе с защищаемой информацией следует отметить, что, в базовой комплектации, дистрибутив не содержит ни установленных политик SELinux, а также не содержит инструментов, выполняющих конфигурирацию и дальнейшую поддержку SELinux.

При выводе команды управления сразу после установки видна только базовая библиотека libselinux. Сам механизм SELinux выключен. Таким образом, специализированные средства по обеспечению защиты, предоставляют доступ для установки, но, так как они не устанавливаются вместе с системой, необходима их настройка.

При проведении анализа Astra Linux SE на предмет соответствия требованиям для работы с защищаемой информацией выявлено, что в ОС своя подсистема безопасности PARSEC, которая использует модель разграничения доступа (рисунок 1). Изображенная модель относится к классу ДП-моделей, то есть моделей управления доступом и информационными потоками.

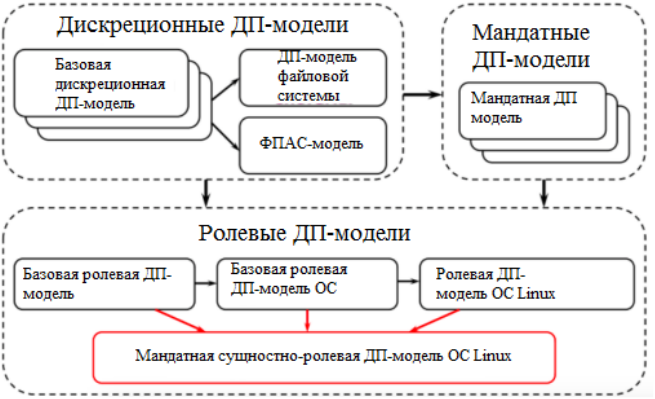


Рисунок 1. ДП модель

Вместо системы принудительного контроля доступа SELinux, в Astra Linux Special Edition используется запатентованная мандатная сущностно-ролевая ДП-модель управления доступом и информационными потокам (МРОСЛ ДП-модель). Она содержит дополнительные способы разграничения доступа. В МРОСЛ модели известно, что к мандатному управлению доступом добавлен мандатный контроль целостности дистрибутива и файловой системы, предусмотрено ролевое управление доступом, наличие иерархии сущностей и применено противодействие запрещённым потокам по памяти и по времени.

Анализ документации, прилагавшейся к официальному дистрибутиву Astra Linux SE 1.4 [1], аналогичной для ALT Linux [4], и Государственного стандарта РФ [2] определил список требований необходимых Astra Linux SE и ALT Linux. Для упрощения проведения сравнительного анализа все требования, объединены в следующие группы:

– требования к средствам вычислительной техники (включает 10 требований);

– защита от несанкционированного доступа (включает 11 требований);

– требования к реализации управления доступом (включает 18 требований).

Таким образом, для ALT Linux:

– полностью удовлетворено требований – 5/38;

– частично удовлетворено требований – 6/38;

– не удовлетворено требований – 27/38.

Система содержит встроенные средства и механизмы:

– полностью выполняющие требования и не требуют затрат на проведение подготовки и конфигурирования;

– требующие больших затрат на проведение подготовки и конфигурирования;

– не выполняющие требования.

Для Astra Linux SE:

– полностью удовлетворено требований – 35/38;

– не удовлетворено требований – 3/38.

Система содержит встроенные средства и механизмы:

– полностью выполняющие большую часть требований и не требуют больших затрат на проведение подготовки и конфигурирования;

не выполняющие приведенные требования. Требования, которые невозможно соблюдать технически и которые выполняются введением административно-организационных мер. Надо обратить внимание, что это усложняет эксплуатацию и сопровождение системы.

В то же время для Astra Linux SE, внесение специализированной документации и привлечение организационных мер для повышения уровня удовлетворения требованиям, дает вероятность в 100 процентов по соответствию необходимым требованиям сертификации.

Выводы: в работе проанализирована документация, выделены требования системы и определено соответствие дистрибутивов требованиям. При проведении сравнительного анализа дистрибутивов ALT Linux и Astra Linux определено, что полностью удовлетворить все требования позволяет только Astra Linux SE, так как из 39 рассматриваемых требований, техническим путем возможно удовлетворить 35 из них, потому что данная система содержит необходимые встроенные средства и механизмы. Следовательно, 4 требования реализуются снабжением СВТ специализированной документацией. В то же время ALT Linux даже при снабжении СВТ специализированной документацией не предполагает полного удовлетворения всем требованиям системы.

Литература

1. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие для вузов П. В. Буренин, П. Н. Девянин, Е. В. Лебеденко, В. Г. Проскурин, А. Н. Цибуля. 2-е издание, стереотипное. М.: Горячая линия – Телеком, 2017. 312 с.: ил.

2. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» // URL: https://www.securitylab.ru/informer/240667.php

3. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. // URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2

4. URL: http://www.altlinux.ru/

БАЙЕСОВСКИЙ КЛАССИФИКАТОР КАК МЕТОД ОБНАРУЖЕНИЯ НЕТИПИЧНЫХ ОБЪЕКТОВ В СИСТЕМАХ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Д. М. Маркарян

Северо-Кавказский федеральный университет, г. Ставрополь

Обнаружение нетипичных объектов является одной из важнейших задач интеллектуального анализа данных, рассматриваемой во многих областях исследования и сферах применения. Необходимость обнаружения аномалий заключается в том, что присутствие аномалий в данных представляет собой важную (или даже критически важную) информацию применительно к широкому ряду областей применения. Байесовский классификатор является одним из фундаментальных подходов к обнаружению аномалий.

Ключевые слова: Интеллектуальный анализ данных, паттерн, нетипичный объект, аномалия, наивный байесовский подход (НБП).

Интеллектуальный анализ данных (Data mining), можно определить как процесс, позволяющий выделить из большого объема данных некоторую новую значимую информацию. Главной задачей интеллектуального анализа данных является выявление скрытых последовательностей, непредвиденных тенденций или других явно невидимых связей в данных – решение которой достигается путем использования методов машинного обучения, статистики и обработки баз данных. На сегодняшний день такое относительно новое направление находит широкий интерес применение в большинстве сфер деятельности человека, таких как экономика, медицина, а также диагностика и контроль технологических процессов. Обнаружение аномалий является одной важнейших задач интеллектуального анализа данных, рассматриваемой во многих областях исследования и сферах применения. Обнаружение аномалий (или детектирование аномалий, поиск аномалий) относится к проблеме нахождения паттернов (шаблонов) данных, не соответствующих ожидаемому поведению. Такие несоответствующие паттерны (шаблоны) в зависимости от прикладной области относят

к аномалиям, выбросам, несогласованным наблюдениям, исключениям, аберрациям, особенностям и загрязнителям. Наиболее часто используемыми и взаимозаменяемыми понятиями в контексте обнаружения аномалий являются «аномалия» и «выброс». В некоторых приложениях аномалии также называют нетипичными объектами или целевыми (особыми) событиями. Обнаружение аномалий нашло широкое применение в таких областях как обнаружение вторжений в компьютерной безопасности, обнаружение мошенничества при проведении банковских транзакций, выявление заболеваний раком, поиск отказов в системе безопасности, слежение за вражеской активностью, контроль движения поездов и многое др. Необходимость обнаружения аномалий заключается в том, что присутствие аномалий в данных представляет собой важную (или даже критически важную) информацию применительно к широкому ряду областей применения. В последнее десятилетие проблема обнаружения аномалий была поднята во множестве книг и статей посвященным различным сферам исследований и прикладным областям. Рассмотрим один из фундаментальных подходов к обнаружению аномалий.

Наивный байесовский подход (НБП) является простым вероятностным классификатором, основанным на применении Теоремы Байеса со строгими предположениями о независимости. Все рассматриваемые переменные исключительно независимы друг от друга, это довольно упрощает процесс вычисления по сравнению с вычислениями при математически зависимых между собой переменных. И хотя это предположение не всегда полностью выполняется, тем не менее на практике данный алгоритм находит широкое применение в разных областях науки.

Обозначим $P\ (c_j)$ как вероятность того, что некоторый объект a_i относится к классу c_j. Пусть объект a_i характеризуется набором независимых переменных $(v_1, v_2 \ldots v_m)$. Событие, соответствующее равенству независимых переменных определенным значениям ($v_1 = v_1^a$ и $v_2 = v_2^b$ и … $v_m = v_m^c$), обозначим как *E,* соответственно, вероятность его наступления будет равна $P(E)$.

Идея алгоритма заключается в расчете условной вероятности принадлежности объекта a_i к c_j при наступлении события E.

Из теории вероятностей известно, что ее можно вычислить по формуле:

$$P(c_j|E) = \frac{P(E|c_j) * P(c_j)}{P(E)}.$$

Априорные вероятности $P(c_j)$ – вероятности того, что произвольно взятый элемент a_i относится к классу c_j – вычисляются на основании информации обучающего множества как отношение числа элементов, принадлежащих данному классу, к общему количеству элементов в нем:

$$P(c_j) = \frac{N}{n_j}.$$

Следующим шагом является вычисление для каждого признака v_i условных вероятностей появления каждого его возможного значения относительно заданных классов. Иными словами, имея множество возможных значений каждого признака $v_1 = \{v_i^1, v_i^2, \dots v_i^a\}$, вычисляют вероятности появления элемента с определенным значением признака $v_1 = v_i^r$ в каждом классе c_j:

$$P(v_i^r | c_j) = \frac{n^{i,r}}{n_j^{i,r}},$$

где $n^{i,r}$ и $n_j^{i,r}$ – общее количество элементов, у которых признак $v_i = v_i^r$ и количество таких элементов, попавших в класс c_j, соответственно.

В результате для каждого класса получим множество (по количеству возможных событий E) записей вида: если $v_1 = v_1^a$ и $v_2 = v_2^b$ и ... и $v_m = v_m^c$, то элемент принадлежит классу c_j с вероятностью $P(c_j|E)$

Максимальное значение вероятности $P_{max} = maxP(c_j|E)$ определяет правило, по которому элемент будет относиться к своему классу.

Несмотря на упрощенные условия, наивные байесовские классификаторы часто работают намного лучше во многих сложных ситуациях.

Одним из немаловажных достоинств наивного байесовского классификатора является малое количество данных для обучения, необходимых для оценки параметров, требуемых для классификации.

Литература

1. Лукацкий А. В. Обнаружение атак. СПб.: БХВ-Петербург. 2003. 608 с.

2. Комашинский Д.В., Котенко И.В. Обнаружение вредоносных документов формата PDF на основе интеллектуального анализа данных // Проблемы информационной безопасности. Компьютерные системы. 2012. № 1. С. 19–35.

СОСТАВЛЕНИЕ СТРУКТУРЫ ЦИФРОВОГО СЛЕДА ДЛЯ МОНИТОРИНГА РАБОТЫ ПОЛЬЗОВАТЕЛЯ

В. И. Мартемьянов

руководитель – канд. техн. наук, доцент ***В. С. Пелешенко***

Северо-Кавказский федеральный университет, г. Ставрополь

Уровень технологий на сегодняшний день позволяет составить подробный портрет человека и узнать о его предпочтениях по посещению различных мест, поисковым запросам, использованию различных программ. Сбор доказательств преступных деяний – заполненный цифровой след, это уже готовая документация, которую можно использовать в случае расследований с компьютерными преступлениями.

Данная тема является актуальной, так как существует мало информации про цифровой след и его анализ. Информационные следы помогают осуществлять сбор доказательств совершения преступных деяний интернет-пользователями в информационных системах или интернет сервисах.

Целью данной статьи является разъяснение информации об информационных отпечатках пользователей и структуризации цифрового следа.

Ключевые слова: цифровой след, цифровой почерк, информационный след, составление цифрового следа, цифровое пространство, анализ цифрового следа, мониторинг работы пользователей, интернет криминалистика, форензика, таргетинг.

Под цифровым следом предложено понимать совокупность информации, содержащейся на материальных накопителях информации в виде файлов-журналов, баз данных, специально сформированных файлах и остальных файлах, в которых содержится информация пригодная для анализа работы пользователя в информационной системе.

Структура цифрового следа пользователя представлена в общем виде на рисунке (рис. 1).

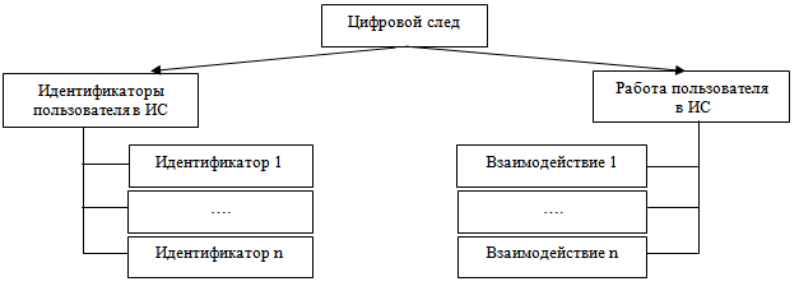


Рисунок 1. Структура цифрового следа

Работа пользователя в ИС, к данной категории относится:

– запуск пользователем процессов и приложений;

– сетевая активность пользователя;

– работа с файловой системой, включая внешние запоминающие устройства на основе ФС, файлы и папки на удаленных компьютерах;

– обращения к программе Windows Installer (стандартная компонента ОС Windows, отвечающая за изменение набора установленных программных средств);

– изменения аппаратной конфигурации, свидетельствующие об установке, удалении или модификации состава технических средств.

Идентификаторы пользователя в ИС:

– логические;

– аппаратные;

– биометрические.

Логические: к данной категории относятся данные содержащие различные данные пользователя – логин пользователя в ос, почтовом клиенте, БД и так далее.

Аппаратные: iButton – в общем виде iButton представляет собой микросхему, вмонтированную в герметичный стальной корпус. В ПЗУ идентификаторов хранится 64-разрядный код - он состоит из 8-разрядного кода типа идентификатора, 48-разрядного уникального серийного номера и 8-разрядной контрольной суммы.

Устройства ввода на базе смарт-карт – основой внутренней организации смарт-карты является так называемая SPOM-архитектура (Self Programming One-chip Memory), предусматривающая наличие центрального процессора (CPU), ОЗУ, ПЗУ и электрически перепрограммируемой постоянной памяти EEPROM. Как правило, в карте также присутствует специализированный сопроцессор.

Процессор обеспечивает разграничение доступа к хранящейся в памяти информации, обработку данных и реализацию криптографических алгоритмов (совместно с сопроцессором). В ПЗУ хранится исполняемый код процессора, оперативная память используется в качестве рабочей, EEPROM необходима для хранения изменяемых данных владельца карты.

Устройства ввода на базе USB-ключей – конструктивно USB-ключи выпускаются в виде брелоков, которые легко размещаются на связке с обычными ключами. Брелоки выпускаются в цветных корпусах и снабжаются световыми индикаторами работы. Каждый идентификатор имеет собственный уникальный серийный номер. Основными компонентами USB-ключей являются встроенные процессор и память. Процессор выполняет функции криптографического преобразования информации и USB-контроллера. Память предназначается для безопасного хранения ключей шифрования, цифровых сертификатов и любой другой важной информации. Поддержка спецификаций PC/SC позволяет без труда переходить от смарт-карт к USB-ключам и встраивать их как в существующие приложения, так и в новые. Основные характеристики USB – ключей представлены в таблице (табл. 1).

Таблица 1

Характеристики USB-ключей

Изделие	**Емкость памяти кб**	**Алгоритм шифрования**
eToken R2	16/32/64	DESX, MD5
eToken Pro(3)	16/32	DES,3DES, AES, RC4
IKey10xx	16/32	DES,3DES, MD5,RC2,RC4,RC5
IKey20xx	8/32	DES,3DES, MD5,RC2,RC4,RC5
ePass1000	8/32	MD5, MD5-HMAC
ePass2000	16/32	RSA,DES,3DES, MD5,SHA-1
Webldenity	16/32	3DES, MD5

Proximity – устройства ввода идентификационных признаков на базе идентификаторов Proximity (от англ. proximity – близость, соседство) или RFID-системы (radio-frequency identification – радиочастотная идентификация) относятся к классу электронных бесконтактных радиочастотных устройств.

Считывающее устройство постоянно излучает радиосигнал. Когда идентификатор оказывается на определенном расстоянии от считывателя, антенна поглощает сигнал и передает его на микросхему. Получив энергию, идентификатор излучает идентификационные данные, принимаемые считывателем. Дистанция считывания в значительной степени зависит от характеристик антенного и приемо-передающего трактов считывателя. Весь процесс занимает несколько десятков микросекунд.

Биометрические: распознавание по форме руки – данный статический метод построен на распознавании геометрии кисти руки, также являющейся уникальной биометрической характеристикой человека. С помощью специального устройства, позволяющего получать трехмерный образ кисти руки (некоторые производители сканируют форму нескольких пальцев), получаются измерения, необходимые для получения уникальной цифровой свертки, идентифицирующей человека.

Распознавание по радужной оболочке глаза – тот метод распознавания основан на уникальности рисунка радужной оболочки глаза. Для реализации метода необходима камера, позволяющая получить изображение глаза человека с достаточным разрешением, и специализированное программное обеспечение, позволяющее выделить из полученного изображения рисунок радужной оболочки глаза, по которому

Распознавание по форме лица – в данном статическом методе идентификации строится двухмерный или трехмерный образ лица человека.

С помощью камеры и специализированного программного обеспечения на изображении или наборе изображений лица выделяются контуры бровей, глаз, носа, губ и т. д., вычисляются расстояния между ними и другие параметры, в зависимости от используемого алгоритма. По этим данным строится образ, выраженный в цифровой форме для сравнения. Причем количество, качество и разнообразие (разные углы поворота головы, изменения нижней части лица при произношении ключевого слова и т. д.) считываемых образов может варьироваться в зависимости от алгоритмов и функций системы, реализующей данный метод. Ведущие производители:

Клавиатурный почерк – поведенческая биометрическая характеристика, которую описывают следующие параметры:

– скорость ввода – количество введенных символов, разделенное на время печатания;

– динамика ввода – характеризуется временем между нажатиями клавиш и временем их удержания;

– частота возникновение ошибок при вводе;

– использование клавиш – например, какие функциональные клавиши нажимаются для ввода заглавных букв.

Клавиатурный почерк является характеристикой, уникальной для каждого человека. Существующие алгоритмы анализа клавиатурного почерка позволяют идентифицировать человека с высокой вероятностью, однако для повышения точности идентификации необходимо использовать дополнительные средства.

Литература

1. Беляков К. Управление и право в период информатизации, 2001.
2. Богуш В. М., Юдин О. К. Информационная безопасность государства, 2003.
3. Словарь по кибернетике. – А – Я / под ред. В. С. Михалевича, 1989. 692с.
4. Широчин В.П., Кулик А.В., Марченко В.В. Динамическая аутентификация на основе анализа клавиатурного почерка, 1999.

МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ ПЛАТЕЖНЫХ СИСТЕМ

С. Л. Матевосян, С. М. Полухин
руководитель – канд. физ.-мат. наук, доцент ***М. А. Лапина***
Северо-Кавказский федеральный университет г. Ставрополь

Мировой рынок банковских переводов имеет большое количество уже сформированных механизмов защиты, но чем сильнее банковские переводы входят в нашу жизнь, тем больше угроз создается для нарушения безопасности пользователей. Системы банковских переводов прочно вошли в нашу жизнь, они имеют большое количество аналогов, но все имеют свои уязвимые места. Данная статья описывает современные средства обеспечения безопасности и поэтому имеет практический интерес.

Ключевые слова: система авторизации граждан, система банковских переводов, защита, аутентификация, банковская карта, безопасные платежи. Клиент, покупатель.

Под платежной системой понимается комплекс правил и средств, позволяющих проводить расчеты между покупателем товара или услуги и торговой или сервисной организацией. Платеж включает совокупность операций по авторизации, взаиморасчетам и передаче платежей, равно как и другой финансовой и нефинансовой информации.

Описывая платежные транзакции и функциональность EMV-карты, мы будем ссылаться на других участников системы. Помимо самой платежной системы в процессе проведения транзакции участвуют:

– банк-эмитент – банк, который выпустил платежную карту, и счет которой находится в этом банке;

– банк-эквайер – банк, который обслуживает терминал платежной точки;

– платежный терминал – устройство, которое обеспечивает работу с платежной картой.

Различают несколько основных видов безналичных платежей

1. С помощью банковской карты и платежного терминала

1.1. Аутентификация происходит посредством магнитного кода или микропроцессора, установленного в карте

1.1.1. Карты, использующие магнитный код считаются устаревшей технологией. Они имели серьезные уязвимости, так как магнитный код можно легко скопировать и банк не может точно определить достоверность и как следует, вероятность мошенничества возрастает.

1.1.2. Для карт(EMV) использующих микропроцессор процедура транзакции начинается в момент установки карты в терминал. Терминал передает карте данные транзакции (сумма, валюта, страна и т.д.). Затем карта и терминал производят взаимную проверку рисков транзакции. Если оба устройства все «устраивает», то карта предоставляет подпись, а терминал пересылает полученные данные в банк-эквайер. Тот, в свою очередь, отправляет сообщение банку-эмитенту. Эмитент, получив данные, проверяет подлинность подписи карты, которая рассчитана на основании динамических данных текущей транзакции, тем самым проверяя подлинность самой карты. Описанный выше процесс является сильно упрощенной моделью EVM-транзакции. Однако он раскрывает главный аспект безопасности EVM-платежей – использование для аутентификации карты динамических данных вместо статических.

1.1.3. Для карт с использованием бесконтактной оплаты, процесс похож на подобный у EMV-карт отличие лишь в том, что нет необходимости вставлять карту в терминал, связь с микропроцессором происходит посредством технологии NFC. Процесс использования средств в данном случае не требует введения, пин-кода и несмотря ни на что считается слабозащищенным, в связи с этим установлено ограничение на объем используемых средств.

2. С помощью банковской карты и персонального кода, указанного на карте

2.1. Основным методом подтверждения подлинности карты в онлайн-транзакциях является аутентификация карты онлайн. В основе данного метода лежит генерация картой криптограммы ARQC (Authorisation Request Cryptogram) для каждой платежной операции. В основе генераций и проверок криптограмм лежит алгоритм 3DES. Эмитент и карта владеют общим секретным ключом MKac (Application Cryptogram Master Key). В начале транзакции карта генерирует на основе MKac сессионный ключ SKac (Application Cryptogram Session Key). Криптограмма ARQC длинной 8 байт генерируется картой с помощью алгоритма MAC, на сессионном ключе SKac с использованием данных транзакции. В процессе транзакции, сгенерированная картой криптограмма ARQC, отправляется в банк-эмитент, Банк

сверит пришедшую ARQC с криптограммой которую, рассчитал самостоятельно. Для этой операции банком генерируется сессионный ключ, затем на основании пришедших данных транзакции, рассчитывается собственный ARQC. Если собственный (сгенерированный эмитентом) ARQC и ARQC карты сходятся – карта подлинная. Далее эмитент по похожему алгоритму на основе динамических данных транзакции и данных ответа генерирует ARPC (Authorisation Response Cryptogram) и отсылает эту криптограмму назад карте. В тот момент, когда карта подтвердит пришедший ARPC, взаимная аутентификация карты и эмитента – выполнена.

3. С помощью электронного счета с авторизацией через интернет-браузер

3.1. Для защиты обслуживания подобных платежных систем использует набор современных инструментов, включая TLS, двухфакторную авторизацию и инструменты, отслеживающие вирусную активность на компьютерах клиентов.

3.1.1. TLS Протокол предназначен для предоставления трёх услуг всем приложениям, работающим над ним, а именно: шифрование, аутентификацию и целостность. Технически, не все три могут использоваться, однако на практике, для обеспечения безопасности, как правило, используются все три:

– шифрование – сокрытие информации, передаваемой от одного компьютера к другому;
– аутентификация – проверка авторства передаваемой информации;
– целостность – обнаружение подмены информации подделкой.

3.1.2. Многофакторная авторизация – механизм защиты при котором, для аутентификации используется несколько различных паролей (устройств). После ввода пары логина и пароля, генерируется одноразовый пароль, присылаемый на мобильный телефон пользователя. На практике, может использоваться не только одноразовый пароль, но и системы биометрической идентификации, и шифрованные ключи на флешках и других носителях.

4. С помощью мобильного банкинга (когда банковский счет привязан к мобильному телефону клиента)

4.1. В данном случае так же используется несколько механизмов для обеспечения безопасной и достоверной аутентификации: использование протоколов TLS, многофакторной аутентификации, антивирусных систем.

5. С помощью мобильного телефона со счета клиента у мобильного оператора

5.1. Аутентификация происходит посредством номера телефона, записанного при регистрации, данной услуги, и одноразового код-пароля, приходящего на указанный номер для подтверждения операции. Но поскольку в таком методе отсутствуют дополнительные методы защиты или

аутентификации банки устанавливают ограничение на максимальную сумму перевода.

Литература

1. https://habr.com/company/payonline/blog/303204/
2. https://habr.com/post/281438/
3. Чипига А. Ф. Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010. 336 с.
4. http://pay2.ru/payment-security/
5. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учеб. пособие / А.А.Афанасьев. М.: Горячая линия – Телеком, 2012. 550 с.
6. Исхаков А. Ю. Система двухфакторной аутентификации на основе QR-кодов // Безопасность информационных технологий. 2014. № 3 С. 97–101.
7. http://pay2.ru/payment-systems/
8. https://habr.com/company/gemaltorussia/blog/307532/

УСТРОЙСТВО ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Н. Н. Медведенко, Н. Д. Лобжанидзе, Д. А. Мирошников
Северо-Кавказский федеральный университет, г. Ставрополь

В настоящее время нефтедобывающие районы Крайнего Севера получили дополнительный стимул своего развития. Это связано с тем, что нефтедобывающая промышленность в РФ является стратегическим направлением развития всего общества страны. Так как необслуживаемые объекты добычи и транспортировки углеводородов находятся в малонаселенных районах, то для их управления создаются комплексы дистанционного мониторинга и контроля, которые для обмена данными используют низкоорбитальные системы спутниковой связи (ССС).

Однако при увеличении числа нефтедобывающих компаний возрастает и количество группировок космических аппаратов (КА). Это может привести к ситуации, когда чужой спутник-нарушитель, оказавшись в зоне видимости станции ССС, расположенной на объекте управления, попытается навязать неправильную команду управления объектом.

Одним из методов, позволяющих устранить данную ситуацию, является использование запросно-ответной системы аутентификации статуса КА [1]. Чтобы повысить имитостойкость такой системы предлагается разработать генератор сеансовых ключей, которые будут периодически меняться. Для этого необходимо использовать псевдослучайную функцию (ПСФ).

Ключевые слова: спутниковая связь, криптография, псевдослучайная функция.

В настоящее время достаточно широкое применение нашли генераторы псевдослучайной последовательности, алгоритм построения которых использует сдвиговые регистры с линейной обратной связью (СРЛОС).

Широкое распространение таких генераторов объясняется достаточно простой схемой построения, которая состоит из следующих подсистем:

- регистра сдвига;
- подсистемы, выполняющей функции обратной связи.

В общем виде схему СРЛОС можно представить следующим образом (рис. 1). Размер сдвигового регистра определяется последовательность битов, то есть степенью порождающего полинома p(x). Если степень порождающего полинома равна n, то регистр называют n–битовым сдвиговым регистром. Для получения, текущего бита выходной ПСП содержимое сдвигового регистра подвергается сдвигу вправо на одну позицию. Очевидно, что новый крайний левый бит b_{n-1} определяется подсистемой, выполняющей функции обратной связи. С выхода регистра сдвига с ОС снимается, как правило, один младший бит, находящийся в регистре генератора ПСП.

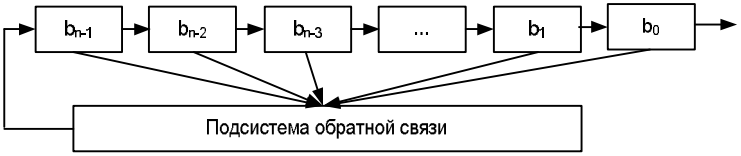


Рисунок 1. Схема генератора на основе регистра сдвига с обратной связью

Широкое распространение генераторов ПСП на основе СРЛОС объясняется тем, что их модно легко получить с помощью цифровой аппаратуры. При этом существует целое множество генераторов псевдослучайной последовательности, которые используют регистры сдвигов с обратной связью [генераторы ПСПС].

Простейшим генератором псевдослучайной последовательности сдвигового регистра с обратной связью является линейный сдвиговый регистр с обратной связью (рис. 2).

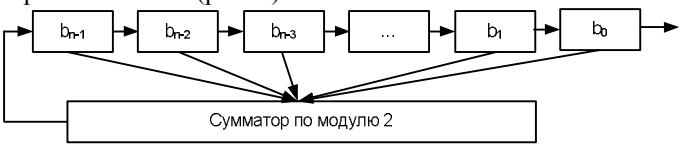


Рисунок 2. Сдвиговый регистр с линейной обратной связью

В качестве подсистемы, реализующей функцию обратной связи, используются сумматор по модулю два, которые реализуют логическую функцию XOR («исключающее или»).

Такие генераторы псевдослучайной последовательности называются генераторами ПСП типа Фибоначчи (рис. 3).

Длина регистра сдвига в генераторе с конфигурацией Фибоначчи определяется степенью порождающего неприводимого полинома.

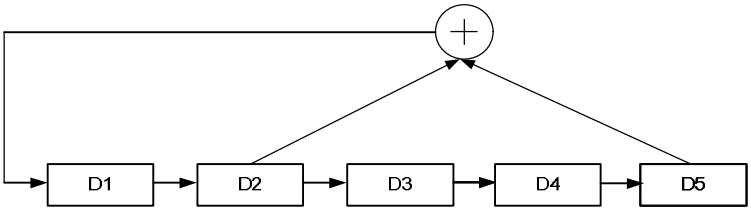


Рисунок 3. Структура генератора ПСП типа Фибоначчи

При этом соотношения, описывающие работу генератора псевдослучайной последовательности, имеют вид

$$\begin{aligned} D_1(nT) &= D_2((n-1)T) \oplus D_5((n-1)T); \\ D_2(nT) &= D_1((n-1)T); \\ D_3(nT) &= D_2((n-1)T); \\ D_4(nT) &= D_3((n-1)T); \\ D_5(nT) &= D_2((n-1)T). \end{aligned} \qquad (1)$$

где $D_j(nT)$ – содержимое j-го D-триггера в момент времени nT; j =1, 2, 3, 4, 5; $D_j((n-1)T)$ - содержимое j-го D-триггера в момент времени (n-1)T.

Данный генератор псевдослучайной последовательности содержит регистр сдвига, состоящий из пяти D-триггеров. При этом обратная связь на сумматор по модулю два поступает с пятого и второго D-триггеров.

Пусть начальное заполнение генератора псевдослучайной последовательности типа Фибоначчи составляет 10101. В табл. 1 показана работа такого генератора ПСП в течение 11 тактов. Значение псевдослучайной последовательности можно снимать с выхода первого D-триггера.

Таблица 1. Работа генератора ПСП типа Фибоначчи

№ такта	D_1	D_2	D_3	D_4	D_5
0	1	0	1	0	1
1	1	1	0	1	0
2	1	1	1	0	1
3	0	1	1	1	0
4	1	0	1	1	1
5	1	1	0	1	1
6	0	1	1	0	1
7	0	0	1	1	0
8	0	0	0	1	1
9	1	0	0	0	1
10	1	1	0	0	0
11	1	1	1	0	0
12	1	1	1	1	0

В рассмотренном примере с выхода первого D-триггера снимается двоичная псевдослучайная последовательность X = 110110001111…. Данную генерируемую псевдослучайную последовательность можно разбить

на числа разрядностью 4 бит. В результате получаем ПСП, состоящую из следующих чисел $X = \{1101\ 1000\ 1111\ldots\}_2 = \{D\ 8\ F\ldots\}_{16}$.

Литература

1. В. П. Пашинцев, М. И. Калмыков, О. В. Вельц. Методы защиты передаваемой информации для системы удаленного контроля и управления высокотехнологическими объектами // Вестник Северо-Кавказского федерального университета, 2014 г. № 4. С. 38-43

2. Шнаер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Издательство ТРИУМФ, 2003. 816 с.

3. Калмыков И. А., Дагаева О. И. Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции // Известия ЮФУ. Технические науки. 2012. № 12. С. 218-224.

РАСЧЁТ ИНДЕКСА ФЛУКТУАЦИИ ФАЗОВОГО ФРОНТА СИГНАЛА ДЛЯ ПРИЁМНИКА NOVATEL GPSTATION-6

Д. М. Марков, А. В. Степаненко
руководитель – канд. техн. наук, профессор ***А. Ф. Чипига***
Северо-Кавказский федеральный университет, г. Ставрополь

Предложена методика вычисления индекса флуктуаций фазового фронта с частотой дискретизации 50Гц для низкочастотных систем спутниковой связи.

Ключевые слова: индекс флуктуации, фазовый фронт, GPStation-6, частота дискретизации, низкочастотные спутниковые системы связи.

Задача разработки методики вычисления индекса флуктуаций фазового фронта с частотой дискретизации 50 Гц декомпозирована на следующие подзадачи:

1. Анализ содержания известных источников и определение исходных данных, необходимых для расчёта значения индекса флуктуации фазового фронта.
2. Анализ документации приёмника Novatel GPStation-6 и определение значений, необходимых для вычисления значения σ_φ с частотой 50 Гц.
3. Разработка методики расчёта индекса флуктуации фазового фронта с частотой 50 Гц.
4. Сравнение результатов расчёта σ_φ, найденного с помощью разработанной методики, и полученного с выхода приёмника Novatel GPStation-6.
5. Сравнение результатов расчётов вероятности ошибочного приёма сигнала, вычисленного с помощью разработанной методики и значений индекса флуктуации фазового фронта, полученного с выхода приёмника Novatel GPStation-6.

В [3-5, 7] приведена формула для расчёта значения флуктуации фазового фронта сигнала:

$$\sigma_{\phi_i} = \sqrt{\langle \varphi_i^2 \rangle - \langle \varphi_i \rangle^2}, \quad (1)$$

где φ_i – значение измерения фазы сигнала для заданной частоты наблюдаемого спутника. В [5, 7] указано, что для вычисления индекса флуктуации фазового фронта требуется получить фазовые измерения с исключённым мгновенным средним значением.

Для расчёта значений индекса флуктуации фазового фронта сигнала требуется использование «сырых» фазовых измерений. Данные измерения могут быть получены путём считывания значений типа ISMDETOBS в бинарном формате, что обеспечивает наилучшую производительность при обработке данных наблюдений с высокой частотой дискретизации [4, 5, 7]. Конечная формула для расчёта значений индекса флуктуаций фазового фронта:

$$\sigma_{\phi_i} = \sqrt{\langle (2\pi\varphi_i)^2 \rangle - \langle (2\pi\varphi_i) \rangle^2}, \quad (2)$$

где φ_i – значение измерения фазы сигнала для *i*-го спутника.

На основе формулы 1 разработана методика расчёта значений индекса флуктуации фазового фронта сигнала с частотой дискретизации 50 Гц, алгоритм реализации которой представлен на рисунке 1.

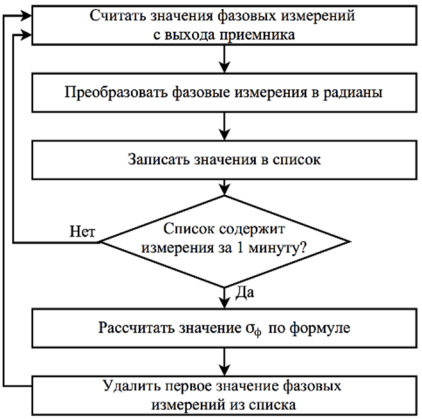


Рисунок 1 – Алгоритм реализации методики расчёта значений индекса флуктуации фазового фронта

Эксперимент показал, что экстремально большие значения связаны со срывом фазы слежения сигнала. Приёмник Novatel GPStation-6 позволяет отслеживать срыв фазы слежения через значение поля locktime измерения типа RANGE. Определено, что минимальное время отслеживания спутника после срыва фазы слежения составляет 120 секунд.

Дополнительные условия, найденные экспериментальным путем, добавлены в методику расчёта индекса флуктуации фазового фронта (рисунок 2).

Особенностью работы Novatel GPStation-6 является то, что значения индекса флуктуации фазового фронта получаются каждые 60 секунд, начиная с 00:00 UTC. Таким образом, визуально будет наблюдаться совпадение или расхождение рассчитанных значений.

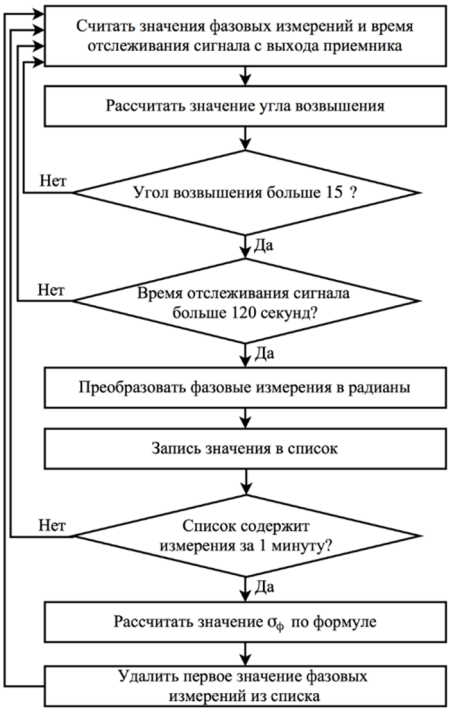


Рисунок 2 – Методика расчёта значений индекса флуктуации фазового фронта с дополнительными ограничениями

Экспериментально получены дополнительные граничные условия, позволившие отфильтровывать неправильные значения, такие как минимальный угол возвышения и минимальное время устойчивого приёма фазы слежения. Введение граничных условий внесло корректировку в методику расчёта σ_ϕ). Сравнение вероятности ошибочного приёма сигнала для индекса флуктуации фазового фронта, полученного с помощью разработанной методики, и значений, полученных с выхода приёмника Novatel GPStation-6, наглядно показало, что значения с низкой частотой дискретизации не способны отразить влияния мелкомасштабных неоднородностей

на принимаемый сигнал, а также может быть пропущена ситуация, при которой значение вероятности ошибочного приёма сигнала превысит пороговое значение.

Литература

1. Марков Д. М. Методика расчета индекса мерцания с высокой частотой дискретизации для приёмника GPStation-6 // Студенческая наука для развития информационного общества: сборник материалов V Всероссийской научно-технической конференции. – Ставрополь: СКФУ, 2016. – 624 с.
2. Марков Д. М., Чипига А. Ф. Анализ скорости обработки сжатых форматов протоколов измерений приемника GPStation-6 // Материалы международной научно-практической конференции Молодежный форум: технические и математические науки. –Воронеж: ВГЛТУ, 2015. – 442 с.
3. Прогнозирование помехоустойчивости спутниковой связи по результатам мониторинга индекса мерцаний ионосферы / В. А. Шевченко, А. Ф. Чипига, В. П. Пашинцев, К. И. Топорков // Инфокоммуникационные технологии. – 2015. – Т. 13, № 4. – с. 365 – 375.
4. Чипига А. Ф. Анализ энергетической скрытности низкочастотных систем спутниковой связи от обнаружения сигналов // Известия ЮФУ. Технические науки. – 2014. – № 2. – с. 209 – 217.
5. Чипига А. Ф., Марков Д. М., Слюсарев Г. В. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи // Фундаментальные исследования. – 2015. – Т. 4, № 11. – с. 759 – 762.
6. GPStation-6™ GNSS Ionospheric Scintillation and TEC Monitor (GISTM) Receiver User Manual. – 2012. – URL: https://www.novatel.com/assets/Documents/Manuals/om-20000132.pdf.
7. Novatel OEM6® Family Firmware Reference Manual. – 2017. – URL: https://www.novatel.com/assets/Documents/Manuals/om-20000129.pdf.

ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ ЗАЩИТЫ КИБЕРПРОСТРАНСТВА В СОЕДИНЕННЫХ ШТАТАХ АМЕРИКИ

Д. О. Мунич, М. М. Савельев
руководитель – канд. техн. наук, доцент ***Т. В. Минкина***
Северо-Кавказский федеральный университет, Ставрополь

В данной статье рассмотрены основные составляющие информационной безопасности в сети. Рассматривается международная стратегия США для киберпространства. Проанализированны основные структуры подразделения отвечающие за решение проблем информационной безопасности. В результате анализа характеристик защиты киберпространства в США определены главные отличительные особенности защиты информации этой страны.

Ключевые слова: международная стратегия, кибербезопасность, информационная безопастность, угроза сети, конфиденциальность, стабильность сети, целостность, государственные ресурсы, США.

Главным элементом борьбы США за безопасное будущее сети остается «Международная стратегия США для киберпространства». Три основных составляющих информационной безопасности:

– Доступность информации – обеспечение готовности системы к обслуживанию поступающих запросов;

– Целостность – обеспечение существования информации в неискаженном виде;

– Конфиденциальность – обеспечение доступа к информации только авторизованному кругу субъектов.

«Стратегия» соответствует основной цели США: «глобальной работе по развитию открытой, легкодоступной, безопасной и надежной ИК-инфраструктуры, которая поддерживала бы международную коммерческую деятельность, обеспечивала бы должный уровень безопасности и поощряла самовыражение и использование новейших технологий».

«Международная стратегия США для киберпространства» полностью соответствует мнению о том, что существующие международные нормы мирного поведения и разрешения конфликтов вполне применимы и в киберпространстве, признавая при этом, что следует поработать для того, чтобы понять, как и в каком виде эти нормы следует применять. Таким образом, эти нормы следует привязать к традиционным принципам поддержки фундаментальных свобод, уважения права частной собственности, права на сохранение тайны личных данных, права на защиту от правонарушителей, а также права на применение средств самозащиты. Именно на этом фундаменте стоят международные нормы:

– глобальная совместимость систем;
– стабильность сети;
– надежный доступ к сетевым ресурсам;
– многостороннее управление;
– обеспечение кибербезопасности усилиями государств.

Во многих отношениях рост угроз стимулирует рост количества инициатив по обеспечению безопасности. В 2012 году США поддержали проекты ООН, усилия ОБСЕ и НАТО, нацеленные на поиски компромиссов в отношении вопросов безопасности.

В феврале 2013 года в Белом доме был издал указ, устанавливающий процедуры повышения защищенности критических объектов инфраструктуры. Данный указ – отлична возможность для сторонних лиц получить представление о комплексном взаимодействии многочисленных федеральных агентств по вопросам кибербезопасности, начиная с Министерства внутренней безопасности, и заканчивая такими органами как Администра-

тивно-бюджетное управление и Федеральное бюро расследований. Данные службы ответственны за налаживание связей со своими зарубежными коллегами и координированием вопросов кибербезопасности.

Основным структурным подразделением, отвечающим за решение проблем информационной безопасности, является один из 22 постоянных комитетов Палаты представителей – Особый комитет по национальной безопасности (Select Committee on Homeland Security). Основным профильным подкомитетом является подкомитет по новым угрозам, кибербезопасности и науке (Subcommittee on Emerging Threats, Cybersecurity, *and Science and Technology*). В эту сферу входят вопросы, связанные с безопасностью компьютерных систем, телекоммуникаций, информационных технологий, систем автоматического управления в промышленности, а также вопросы предотвращения внутренних и внешних атак на правительственные и частные сети, ущерба, нанесенного гражданскому населению вследствие атак на информационные системы.

Также к числу общефедеральных программ относится информационная сеть для предупреждений об угрозах критической инфраструктуре (Critical infrastructure Warning Information Network, CWIN), основной задачей которой является предоставление возможности обмена предупреждениями и передачи сигналов тревоги между правительственными организациями, а также частными компаниями и некоторыми зарубежными партнерами. По замыслу Министерства национальной безопасности, данная сеть должна обеспечить надежную связь с различными субъектами, чье участие принципиально необходимо для восстановления критически важной инфраструктуры в случае происшествий национального масштаба.

Фактически данные документы могут считаться официальной общенациональной политикой США в сфере информационной безопасности, на основе которой строится вся система деятельности государственной власти в этой области и структура государственных органов, обеспечивающих информационную безопасность в стране. В соответствии со стратегией информационной безопасности основными государственными приоритетами в этой области являются:

– становление и развитие национальной системы реагирования на происшествия в сфере информационной безопасности;

– реализация комплексной системы мер по уменьшению угроз информационной безопасности;

– обеспечение подготовки специалистов в сфере компьютерной безопасности и обеспечение ответственного отношения всего населения страны к вопросам защиты информации;

– обеспечение защиты информационных систем, имеющих отношение к государственным органам;

– развитие различных форм кооперации (в том числе и международной) в сфере обеспечения информационной безопасности.

Приоритет 1. Развитие системы реагирования на происшествия в сфере информационной безопасности предполагает, что быстрое обнаружение атак и своевременный обмен информацией о них во многих случаях могут значительно снизить ущерб. Для обеспечения безопасности стратегия предполагает расширение работы «Информационной сети для предупреждений об угрозах критической инфраструктуре» (CWIN) для поддержки роли Министерства национальной безопасности в разрешении кризисов и некоторых других.

Приоритет 2. Реализация программы устранения угроз для информационной безопасности и уязвимостей в информационных системах предполагает, что наличие уязвимостей в различных информационных системах само по себе в определенной мере обуславливает возможность атак на них и, соответственно, является источником опасностей для элементов критически важной инфраструктуры страны. Таким образом, устранение уязвимостей является одним из наиболее важных направлений работы по обеспечению информационной безопасности. Для обеспечения безопасности стратегия предполагает реализацию следующих основных мероприятий:

– расширение возможностей проведения расследований компьютерных преступлений для последующего предотвращения возможных атак;

– повышение безопасности сети Интернет путем совершенствования используемых протоколов и механизмов маршрутизации и некоторых других.

Приоритет 3. Развитие ответственного отношения к вопросам информационной безопасности и подготовка кадров в этой сфере предполагает, что источником многих уязвимостей является недостаточно ответственное отношение некоторых пользователей, системных администраторов и разработчиков информационных систем к вопросам защиты информации, их недостаточная осведомленность и информированность в этой сфере. Для обеспечения безопасности стратегия предполагает реализацию следующих четырех основных мероприятий:

– продвижение многосторонней общенациональной программы по информированию и развитию ответственного отношения граждан страны к обеспечению безопасности тех информационных систем, к которым они имеют какой-либо доступ;

– поощрение создания программ подготовки специалистов, которые обеспечили бы удовлетворение потребности в персонале;

– повышение эффективности существующих программ подготовки специалистов в сфере информационной безопасности;

– поддержание усилий частных компаний по созданию, распространению и обеспечению всеобщего признания сертификационных программ в сфере информационной безопасности.

Приоритет 4. Охрана государственных информационных ресурсов. Для решения задач в этой сфере стратегия предполагает реализацию следующих основных мероприятий:

– обеспечение непрерывного оценивания угроз для государственных информационных систем и существующих в них (системах) уязвимостей;

– обеспечение безопасности локальных правительственных беспроводных сетей;

Приоритет 5. Развитие кооперации между различными ведомствами и компаниями, а также международной кооперации в сфере обеспечения информационной безопасности обусловлено тем, что практически все информационные системы (и в стране, и в мире) являются взаимосвязанными и требуют глобального системного подхода к вопросам защиты информации. Для решения задач в этой сфере стратегия предполагает реализацию следующих основных мероприятий:

– усиление контрразведывательной деятельности в сферах, имеющих отношение к информационным системам и технологиям;

– поощрение присоединения других стран к Конвенции Совета Европы по киберпреступлениям или совершенствования национальных законодательств и некоторых других.

Соединенные Штаты двигаются по нескольким направлениям для усиления собственной защиты, учитывая при этом срочность, которая возникла после повышения частоты атак в мире. Планируется повышение защиты всей онлайн-активности в стране, и распространяться это будет на правительственные организации, частные компании, некоммерческие объединения, сообщества, а также на отдельных граждан. Цель Соединенных Штатов – это будущее поколение, которое хорошо информировано о возможных рисках более тесного взаимодействия с сетью. США активно участвуют во всех возможных начинаниях, относящихся к выстраиванию международной структуры законов и норм, которые помогали бы обитателям киберпространства. И, наконец, США заинтересованы в насаждении культуры открытой и безопасной сети.

Литература

1. Ваганов П. А. Правовая защита киберпространства в США // Правоведение. 2006. № 4.

2. Иванский В. П. Принципы защиты персональных данных в зарубежных государствах // Информационные системы и технологии. 2011. № 4.

3. Стрельников В. Персональным данным - особую защиту // ЭЖ-Юрист. 2013. № 12.

4. Бойченко О. В., Борщ Л. М., Мандрица И. В., Мандрица О. В., Соловьева И. В., Петренко В. И., Матвеев В. В., Титаренко В. Н., Титаренко Д. В., Потанина М. В., Байздренко Е. А., Писарюк С. Н., Шишкин В. М., Воробьев В. И., Евневич Е. Л., Монахова Т. В., Гавриков И. В., Рыбников А. М., Рыбников М. С., Королев О. Л. и др. Информационная безопасность социально-экономических систем // под ред. О. В. Бойченко. Симферополь, 2017. 302 с.

5. Nemkov R., Mezentseva O., Mezentsev D., Brodnikov M. Image recognition by a second-order convolutional neural network with dynamic receptive fields// CEUR Workshop Proceedings 2. Сер. "YSIP2 2017 - Proceedings of the 2nd Young Scientist's International Workshop on Trends in Information Processing" 2017. С. 147-151.

6. Nemkov R.M., Mezentseva O.S., Mezentsev D.Using of a convolutional neural network with changing receptive fields in the tasks of image recognition// Advances in Intelligent Systems and Computing. 2016. Т. 451. С. 15-23.

7. Севастьянов С.А., Гогуля В.А., Палканов И.С. WAN технологии: уникальные возможности использования// Студенческая наука для развития информационного общества сборник материалов VII Всероссийской научно-технической конференции. 2018. С. 282-286. Advances in Intelligent Systems and Computing. 2016. Т. 451. С. 15-23.

СОЗДАНИЕ СЛУЖБЫ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

В. В. Небогатов
руководитель - канд. техн. наук, доцент кафедры ОТЗИ ***В. В. Антонов***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье определена ведущая роль службы безопасности предприятия в предотвращении угроз. Рассмотрен возможный алгоритм построения службы безопасности предприятия. Рассматриваются два взаимосвязанных вопроса. Во-первых, обосновывается необходимость и целесообразность создания на предприятиях службы безопасности. Во-вторых, излагаются основные функции службы безопасности на предприятии, а также структура этой службы.

Развитие нашего государства напрямую зависит от стабильного функционирования предприятий, увеличения их экономического потенциала в условиях рыночных отношений. Опыт свидетельствует, что организация современной предпринимательской деятельности нуждается в создании надежной службы безопасности (СБ) предприятия в условиях существования рисков. В Законе РФ «О безопасности» понятие «безопасность» определяется как состояние защищенности жизненно важных интересов. Однако в сознании большинства граждан все еще сильны стереотипы, согласно которым данная область относится многими к сфере компетенции государства и специальных органов. Защищать свои интересы нужно компании самой, а не надеяться на помощь государства. Одним из инструментов по обеспечению защиты безопасности предприятия может стать создание на его базе собственной службы безопасности.

Ключевые слова: служба безопасности, угрозы, безопасность предприятия, структура службы безопасности.

Прежде всего, охрана предприятия представляет собой систему организационно-правовых мер, направленных на обеспечение нормального функционирования частного предприятия в условиях острой конкурентной борьбы на внутреннем рынке.

Для каждого предприятия разрабатывается свой режим безопасности. Охранная тактика производственных объектов представляет целый комплекс мероприятий, учитывающий все характеристики объекта: его территориальную обособленность, техническую оснащенность, площадь внутренних помещений, прилегающей зоны и многое другое.

Чтобы охрана предприятия была максимально эффективной, сначала необходимо провести анализ исходной ситуации и выработать план по обеспечению безопасности на данном объекте. Чем разностороннее ваша коммерческая деятельность, чем больше сфер а охватывает, тем тщатель-

нее должна быть организована охрана. Причем, не только территориальная, но и индивидуальная: предупреждение физического/ морального ущерба персоналу предприятия также входит в компетенцию сотрудников службы безопасности.

Стоимость услуг по обеспечению безопасности предприятия варьируется.а зависит от комплекса мер, которые будут осуществляться на территории вашего предприятия специалистами охранного агентства. В любом случае, необходимо прислушаться к мнению экспертов, которые разработают оптимальный для объекта режим охраны.

Создание службы безопасности на предприятии начинается с выбора руководителя, которому можно доверить практически всю информацию о предприятии, ее деятельности, сильных и слабых сторонах, возможностях и потенциальных угрозах. Приоритетом стратегии является сосредоточение конфиденциальной информации в узком кругу внутренней службы безопасности в рамках одного предприятия. Возглавлять СБ должен начальник службы в должности заместителя руководителя предприятия по безопасности. При этом руководитель СБ должен обладать максимально возможным кругом полномочий, позволяющим ему влиять на другие подразделения и различные области деятельности предприятия, если этого требуют интересы безопасности.

Единой методики формирования структуры службы безопасности не существует. В одной из публикаций предлагается следующий алгоритм построения СБ (рис. 1.)

Рисунок1. Алгоритм построения службы безопасности

В зависимости от целей обеспечения безопасности могут создаваться различные варианты структуры службы безопасности. Организационно служба безопасности должна состоять из следующих структурных единиц (рис. 2.):

– отдел режима и охраны, в составе сектора режима и сектора охраны;
– отдел защиты информации;
– инженерно-техническая группа;
– группа безопасности внешней деятельности.

Рисунок 2. Возможная структура службы безопасности

Приведенная структура службы безопасности не универсальна и должна корректироваться под определенную организацию. В частности, в нее могут быть введены новые отделы, например, отдел пожарной безопасности, группа управления персоналом или группа сопровождения грузов. Как правило, формирование или реформирование структуры СБ осуществляется по мере понимания задач, которые должны ею решаться на текущий момент. В большинстве случаев это происходит после проведения аналитических исследований степени защищенности объекта.

Служба безопасности предприятия выполняет следующие основные общие функции:

– организует и обеспечивает пропускной и внутри объектовый режим в зданиях и помещениях;

– руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;

– участвует в разработке основополагающих документов с целью закрепления в них требований обеспечение безопасности и защиты коммерческой тайны

– изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов

утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций о деятельности предприятия и его клиентов, партнеров, смежников;

– организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия; поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).

В заключение хочу кратко подвести итоги проделанной работы.

Итак, основной целью службы безопасности является своевременное пресечение противоправных посягательств на экономические интересы и персонал предприятия.

Если говорить о структуре, численности и составе службы безопасности предприятия (фирмы, компании и т.д.), то в первую очередь и определяются реальными потребностями самого предприятия и степенью конфиденциальности ее информации. Поэтому представить универсальную структуру службы безопасности невозможно безопасности.

Литература

1. Василий Петрович Мак-Мак «Служба безопасности предприятия» Бесплатная научная электронная библиотека. http://disus.ru/knigi/365970-4-sluzhba-bezopasnosti-predpriyatiya-avtor-vasiliy-petrovich-mak-mak-soderzhanie-knigi-glava-sistema-bezopasnosti-predpriyatiya.php.

2. КиберЛенинка: https://cyberleninka.ru/article/n/neobhodimost-sozdaniya-i-funktsii-sluzhby-ekonmiches-koy-bezopasnosti-predpriyatiya.

3. Журнал «Директор безопасности»: http://www.sdirector.ru/magazineorder.html?-_openstat=ZGlyZWN0LnlhbmRleC5ydTszNjc2NjA3OzQwODAwNjUzO3d3dy55YW5kZXgucnU6Z3VhcmFudGVl&yclid=1648340630506313146

РАСШИРЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ КОНТРОЛЯ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ ЭВМ

Е. А. Огриско, М. Г. Огур, Н. Ю. Свистунов
руководитель – канд. техн. наук, доцент ***Д. Л. Осипов***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрен способ расширения функциональности программного обеспечения (ПО) для контроля действий пользователей ЭВМ за счёт введения возможности контроля состояния аппаратного и программного обеспечения компьютеров. Определены основные характеристики и события, подлежащие наблюдению. Введение дополнительных направлений контроля позволяет упростить решение таких задач, как обнаружение вредоносного ПО и аппаратных

неисправностей, выработка рекомендаций по рационализации использования ресурсов ЭВМ и обновлению аппаратного обеспечения.

Ключевые слова: контроль действий пользователя, программное обеспечение, аппаратное обеспечение, вычислительные ресурсы, обнаружение неисправностей.

Программные средства, предназначенные для контроля действий пользователя ЭВМ, позволяют обнаруживать несоблюдение распорядка на рабочем месте, нецелевое использование ресурсов ЭВМ и иные нарушения со стороны пользователя. Принципы разработки таких программных средств, а также недостатки ряда существующих решений рассмотрены в работе [1]. Одним из способов расширения функциональности ПО такого типа является внедрение дополнительных направлений контроля, позволяющих помимо действий пользователя также отслеживать состояние программного и аппаратного обеспечения компьютера.

Цель данной работы – определить и классифицировать основные характеристики и события, подлежащие контролю.

Контролируемые события и характеристики могут быть отнесены к трём основным направлениям (рис. 1):

–состояние программного обеспечения ЭВМ;

–состояние аппаратного обеспечения ЭВМ;

–действия пользователя ЭВМ.

К характеристикам состояния аппаратного обеспечения относятся:

–сведения об аппаратной конфигурации ЭВМ;

–сведения о физическом режиме работы компонентов (температура, напряжение питания, рассеиваемая мощность, скорость вращения вентиляторов системы охлаждения и иные доступные показатели);

– использование аппаратных ресурсов (загрузка центрального процессора и графического ускорителя, занятый объём ОЗУ, загруженность дисковой подсистемы, использование пропускной способности сетевых интерфейсов и т.д.);

– состояние накопителей (значения атрибутов S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology – технология самоконтроля, анализа и отчётности), остаток свободного места).

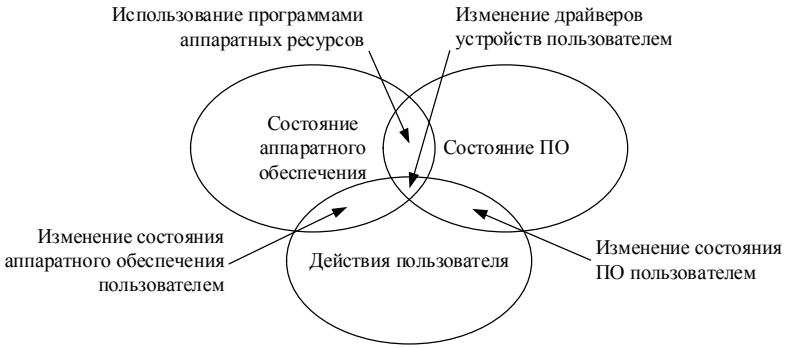


Рисунок 1. Схема классификации направлений контроля ЭВМ

К характеристикам состояния ПО относятся:

–сведения об установленных программах;

–список работающих процессов;

–перечень объектов операционной системы, с которыми работает ПО (файлы, библиотеки, элементы системного реестра и др.);

–сведения о сетевой активности приложений.

На пересечении двух данных категорий находятся такие характеристики, как использование аппаратных ресурсов программным обеспечением.

К характеристикам действий пользователя относятся:

–элементы файловой системы (файлы, каталоги), к которым обращается пользователь;

–сетевые ресурсы, посещаемые пользователем;

–снимки рабочего стола.

Действия пользователя, влияющие на состояние ПО:

–установка, удаление, обновление ПО;

–запуск и остановка процессов.

О внесении пользователем изменений в аппаратную конфигурацию ЭВМ свидетельствуют такие события, как:

–подключение и отключение периферийных устройств;

–изменение набора внутреннего аппаратного обеспечения ЭВМ.

К пересечению трёх категорий можно отнести установку, удаление и изменение пользователем драйверов устройств.

Реализация рассмотренных направлений контроля позволяет упростить решение следующих задач:

1. Обнаружение факта заражения компьютеров вредоносным ПО, признаками работы которого могут являться повышенное или нетипичное использование аппаратных ресурсов, необычная сетевая активность приложений, изменение системных файлов.

2. Профилактика и обнаружение аппаратных неисправностей контролируемых компьютеров на основе таких фактов, как отличающиеся от номинальных напряжения питания, высокие рабочие температуры компонентов, нулевая скорость вращения вентиляторов, ухудшение состояния атрибутов S.M.A.R.T.

3. Более рациональное использование ресурсов ЭВМ. Если большую часть рабочего времени аппаратные ресурсы конкретной ЭВМ простаивают или задействованы слабо, данную машину можно загрузить дополнительными задачами, что, в частности, позволяет повысить экономическую эффективность работы организации [2].

4. Выработка рекомендаций по обновлению аппаратного обеспечения. К примеру, если при выполнении рабочих задач загрузка определённых компонентов ЭВМ (ЦП, ОЗУ, видеоядро и т.п.) близка к максимальной, это может свидетельствовать о необходимости замены данных компонентов на более производительные.

Для реализации предложенного способа расширения функциональных возможностей не требуется значительных изменений архитектуры ПО для контроля действий пользователя [3]. Необходимо оснастить клиентскую часть модулями сбора данных об аппаратном и программном обеспечении, а также сделать возможными обработку и вывод собранной информации серверной частью.

Литература

1. Огриско Е. А., Свистунов Н. Ю., Осипов Д. Л. Принципы разработки программного обеспечения для контроля действий пользователей персональных компьютеров // Студенческая наука для развития информационного общества: сборник материалов V Всероссийской научно-технической конференции: в 2-х частях. Часть 2. Ставрополь: Изд-во СКФУ, 2016. С. 335-337.

2. Мандрица И. В., Мандрица О. В., Соловьева И. В., Петренко В. И. Метод обоснования затрат на информационную безопасность бюджетных организаций // Вестник Северо-Кавказского федерального университета. Ставрополь: Изд-во СКФУ, 2017. № 1 (58). С. 67-71.

3. Огриско Е. А., Осипов Д. Л., Свистунов Н. Ю. Контроль рабочих столов. Свидетельство о государственной регистрации программы для ЭВМ № 2017613700, 24 марта 2017 г.

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

В. Ю. Панин

руководитель – канд. физ.-мат. наук, доцент ***М. А. Лапина***

Северо-Кавказский федеральный университет, г. Ставрополь

При обзоре и анализе методов обнаружения сетевых атак необходимо выделить те способы, алгоритмы и процедуры, которые позволяют обнаружить реализации угроз на информационную систему (ИС). Также необходимо рассмотреть сами сетевые атаки, их способы реализации и классификацию атак воздействующие на информационную систему, определить понятие сетевой атаки, моделей и

методов обнаружения сетевых атак. Разрабатываемые средства обнаружения сетевых атак используют нейронные сети, преимущества которых заключается в обнаружении ранее не известных угроз путем обучения сети.

Ключевые слова: TCP/IP, сетевая атака, алгоритм, нейросеть, обучение, веса, итерация, идентификация, коэффициент, СОА.

Обнаружение сетевых атак обязательно требует выполнение хотя бы одного из двух условий: полное понимание поведения выбранного объекта системы, или знание всех известных атак и их модификаций. В первом случае используется метод обнаружения аномального поведения в сети, а во втором – метод обнаружения направленного нанесения вреда информационной системе или злоупотреблений.

Нейронные сети применяются для различных задач, например: распознавании объектов, теории управления, криптографии, преобразование данных. Нейронные сети обладают способностью обучения по ранее известному примеру, и обобщению из частичных данных. В процессе обучения происходит настройка коэффициентов, группируемые с «синаптическими» весами. На рисунке 1 представлена полная модель искусственного нейрона.

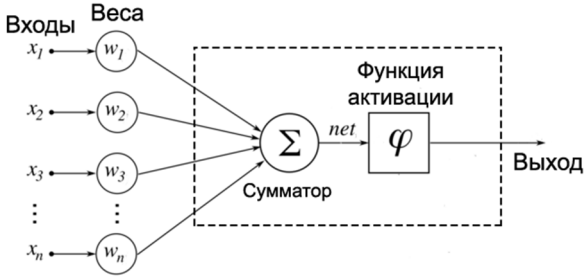


Рисунок 1. Модель искусственного нейрона

где W_i – вес связи, X_n– поступающий входной сигнал. Поступившие на входы сигналы суммируются на свои веса. Сигнал первого входа X_1 суммируется на соответствующий этому входу вес W_1. В итоге ся W_1X_1. И так до *n* входа. В конечном итоге на последнем входе получается W_nX_n.

Способность анализировать заголовки пакета – позволяет обнаруживать сетевые атаки, связанные со значениями заголовков IP пакетов. Приемная сторона попадает в замкнутый цикл, что может вывести из строя сеть.

Сборка пакетов – способность нейронной сети объединять «разбитый» трафик и обнаруживать сетевые атаки, собранный и объединенный в определенном количестве пакетов. Это может вызвать сбой в функционировании сети или всей системы.

Анализ данных пакета – позволяет нейронной сети обнаруживать сетевые атаки, методом сканирования пакета на наличие данных, тем самым обнаружить вредоносные данные путем сканирования целостности пакета.

Необходимо учитывать все детали и реализацию средства обнаружения атак, основанную на следующих параметрах:

– способность средства обнаружения атак определять «IP Dsync» – обнаружение сетевых атак, при которых с целью скрытой маскировки задаются измененные значения номера последовательности и целостности данных;

– возможность средства обнаружения атак обнаруживать распределённые сетевые атаки – выявляются характеристики средства обнаружения атак, используя метод «корреляции», обнаруживать атаки, распределённые во времени или в пространстве;

– возможность записи информации в файл для дальнейшего анализа – характеризует возможности программы сохранять информацию о случаях для дальнейшего анализа;

– система принятия решения – демонстрирует, на каком этапе происходит окончательное решение об обнаружении сетевой атаки;

– пропускная способность – позволяет оценить способность средства обнаружения атак перехватывать пакеты, не вызывая потерю целостности данных;

– влияние средства на производительность системы – тест для оценки влияния работы средства обнаружения атак, на загруженность оборудования, на котором установлено программное обеспечение.

Нейронную сеть обучают правильной идентификации на предварительно подобранной выборке примеров предметной области. Реакция нейронной сети анализируется и система настраивает параметры таким образом, чтобы достичь необходимых результатов. В дополнение к начальному периоду обучения, нейронная сеть набирается опыта с течением времени, по мере того, как она проводит анализ полученных данных, связанных с предметной областью.

Важным достоинством нейронных сетей при обнаружении сетевых атак является их способность обнаруживать ранее неизвестные атаки, это позволяет использовать нейронную сеть преимущественно по сравнению с другими похожими средствами обнаружения атак.

Литература

1. А. Ф. Чипига, В. С. Пелешенко. Формализация процедур обнаружения и предотвращения сетевых атак.

2. Система обнаружения компьютерных угроз: http://www.jetinfo.ru/jetinfo_arhiv/novyj-podkhod-k-zaschite-informatsii-sistemy-obnaruzheniya-kompyuternykh-ugroz/novyj-podkhod-k-zaschite-informatsii-sistemy-obnaruzheniya-kompyuternykh/2007

3. Нейронные сети: https://ru.wikipedia.org/wiki

4. Применение нейронных сетей для обнаружения сетевых атак: https://knowledge.-allbest.ru/programming/3c0b65635a3bd69b5c43b89421316c26_0.html

5.Система обнаружения атак в локальных беспроводных сетях: http://www.ugatu.su/assets/files/documents/dissov/07/2015/SharabyrovIV/diss.pdf

ПРИМЕНЕНИЕ МЕТОДОВ ОБУЧЕНИЯ НЕЙРОННОЙ СЕТИ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

В. Ю. Панин
руководитель – канд. физ.-мат. наук, доцент ***М. А. Лапина***
Северо-Кавказский федеральный университет, г. Ставрополь

При обзоре методов обучения нейронной сети для обнаружения сетевых атак необходимо выделить те способы, технологии и процедуры, которые позволяют обучить нейронную сеть, обнаружить и предотвратить угрозы, воздействующие на информационную систему (ИС). Также необходимо рассмотреть подход обучения нейронной сети, и способы реализации, определить понятие обучения. В настоящее время разрабатываемые методы обучения нейронных сетей достаточно эффективны, хорошо обученная нейронная сеть может обнаруживать ранее не известные сетевые атаки.

Ключевые слова: нейронная сеть, сетевая атака, метод, нейросеть, обучение, веса, итерация, идентификация, коэффициент.

Важнейшим свойством нейронных сетей является их способность обучаться на основе данных окружающей среды и в результате обучения нейронной сети, увеличивать свою производительность. Увеличение производительности происходит со временем в соответствии с соответствующими правилами. Обучение нейронной сети происходит посредством интерактивного процесса корректировки синаптических весов и порогов. В идеале нейронная сеть получает знания об окружающей среде на каждой итерации метода обучения. С понятием обучения ассоциируется огромное количество видов деятельности, поэтому сложно дать этому процессу однозначное определение. Процесс обучения в большинстве зависит от точки зрения на него. С позиций нейронной сети, вероятно, можно использовать следующее определение:

Обучение – это процесс, в котором свободные параметры нейронной сети определяются посредством моделирования среды, в которую эта сеть встроена. Тип обучения определяется способом настройки этих параметров.

Это определение процесса обучения нейронной сети определяет следующую последовательность событий:

1. На вход нейронной сети поступают «стимулы» из внешней среды.
2. В результате первого пункта изменяются «пустые» параметры нейронной сети.
3. После изменения внутренней структуры нейронная сеть отвечает на «возбуждения» уже иначе.

Перечисленный список «четких» правил решения проблемы обучения нейронной сети называется алгоритмом обучения. Нет универсального алгоритма обучения, подходящего для всех известных нейронных сетей. Есть лишь набор средств, представленный разнообразным алгоритмов обучения, каждый из которых имеет свои ряд достоинств.

Существуют два концептуальных метода подхода к обучению нейронных сетей: обучение с учителем и обучение без учителя.

Обучение нейронной сети с учителем предполагает, что для каждого входного вектора из обучающей «выборки» существует необходимое значение выходного вектора, называемого целевым. Эти вектора образуют обучающую пару. Веса сети изменяются до тех пор, пока для каждого входного вектора не будет получен необходимый уровень отклонения выходного вектора.

Обучение нейронной сети без учителя является намного более определенной моделью обучения с точки зрения биологических корней искусственных нейронных сетей. Обучающее множество состоит лишь из входных векторов. Метод обучения нейронной сети «подгоняет» веса сети так, чтобы получались определенные выходные векторы.

Как правило, самым эффективным методом является обучение с учителем. На рис. 1 представлена схема обучения нейронной сети с учителем.

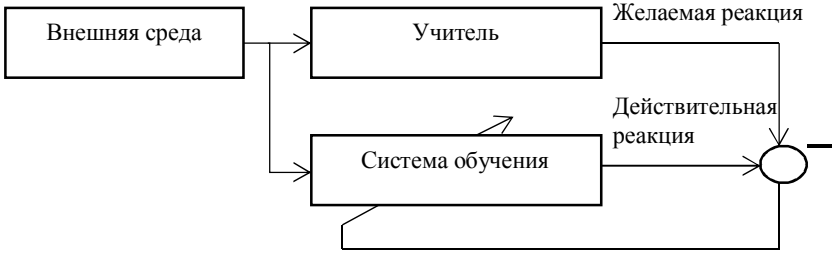


Рисунок 1. Схема обучения сети с учителем

Результат представляет собой общее количество оптимальных действий, которые должна обрабатывать нейронная сеть. Параметры сети определяются с учетом обучающего вектора и сигнала ошибки. Сигнал ошибки – это разность между необходимым сигналом и текущим откликом нейронной сети. Корректировка параметров выполняется поочередно с целью имитации нейронной сетью поведения обучающей «выборки». Таким образом, в процессе метода обучения знания учителя с определенной обучающей выборки подаются в сеть в максимально полном объеме. После окончания обучения учителя можно убрать и позволить обученной нейронной сети работать со средой самостоятельно.

При обучении методом обратного распространения ошибки проводится таким образом, чтобы доля ошибок на выходе при подаче на входы определенных эталонных векторов-примеров которое не превышало заранее определенного заданного значения равного 0.001.

Структура векторов-примеров: $P_i = <X_i, D_i>$, $i = 1 \ldots N$,

где $X_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ – n-мерный вектор входных параметров сигналов,

$D_i = (d_{i1}, d_{i2}, \ldots, d_{im})$ – m-мерный вектор выходных эталонных значений,

N – общее количество обучающих примеров выборки.

Проверка критерия окончания обучения:

$$\frac{\sqrt{\sum_{i=1}^{N}(D_i - Y_i)^2}}{N} \leq \delta,$$

где $(D_i - Y_i)^2 = \sum_{i=1}^{m}\left(d_y - y_y\right)^2 \; i = 1 \ldots N$

Конфигурация обученной нейронной сети сохраняется в отдельный файл, и использовалась для последующего тестирования на подготовленной выборке.

Литература

1. А. Ф. Чипига, В. С. Пелешенко. Формализация процедур обнаружения и предотвращения сетевых атак

2. Нейронные сети: https://ru.wikipedia.org/wiki

3. Применение нейронных сетей для обнаружения сетевых атак: https://knowledge.-allbest.ru/programming/3c0b65635a3bd69b5c43b89421316c26_0.html

4. Система обнаружения компьютерных угроз: http://www.jetinfo.ru/jetinfo_arhiv/novyj-podkhod-k-zaschite-informatsii-sistemy-obnaruzheniya-kompyuternykh-ugroz/novyj-podkhod-k-zaschite-informatsii-sistemy-obnaruzheniya-kompyuternykh/2007

5. Система обнаружения атак в локальных беспроводных сетях: http://www.ugatu.-su/assets/files/documents/dissov/07/2015/SharabyrovIV/diss.pdf

ЗАЩИТА АВТОРСКИХ ПРАВ

Р. Р. Партоян

руководитель – канд. техн. наук, доцент ***В. В. Антонов***

Северо-Кавказский федеральный университет, г. Ставрополь

В статье определена значимость защиты авторских прав в современном мире. Рассмотрены составляющие авторского права и способы защиты авторского права.

Ключевые слова: авторские права, интеллектуальная собственность, безопасность, способы защиты авторских прав.

Авторское право – один из важнейших институтов гражданского права. Без него регулирование правоотношений, связанных с созданием и использованием произведений науки, литературы или искусства не пред-

ставляется возможным. С развитием новых технологий, в конце двадцатого века, объекты интеллектуальной собственности стали весьма ценным ресурсом, используемым не только гражданами, но и юридическими лицами. Следовательно, задача защиты авторских прав становится как никогда актуальной.

По действующему Гражданскому Кодексу РФ авторские права – это интеллектуальные права на произведения науки, литературы и искусства.

Авторские права включают в себя:

1) исключительное право на произведение, являющееся имущественным правом;

2) личные неимущественные права, к которым относятся:

право авторства;

право автора на имя;

право на неприкосновенность произведения;

право на опубликование произведения;

другие права (право на отзыв, право следования, право доступа к произведениям искусства и другие) [2].

Суть авторских прав заключается в возможности автора совершать определенные действия с произведением и запрещать такие действия лицам, не имеющим на это право. Неисполнение запрета повлечёт за собой наказание. Таким образом, можно сделать вывод, что нарушение авторских прав – это действия субъектов права, проявляющиеся в нарушении исключительного права на использование произведения или личных неимущественных прав автора.

Нарушение авторских прав, из приведенного выше определения, можно условно разделить на две категории. Для каждой из которых предусмотрены свои обстоятельства привлечения к ответственности, способы и порядок защиты.

Способы, с помощью которых реализуется защита авторских прав предусмотрены гражданским законодательством. Способом защиты является совокупность требований, которые автор (правообладатель) может предъявить к нарушителю исключительного права или личных неимущественных прав. На основе анализа литературы по данной теме можно выделить наиболее эффективные способы защиты авторских прав:

Установление исключительного права. Применяется в том случае, если оспаривается принадлежность авторских прав определенному лицу. Позволяет установить истинного правообладателя произведения и направлено на устранение разногласий по поводу личных неимущественных прав. Чаще всего с данным требованием обращаются соавторы произведения.

Прекращение действий, нарушающих авторских права или создающих угрозу нарушения. Например, данное требование может быть направлено на запрет распространения нелегальных экземпляров произведения.

Компенсация потерь. Применяется если противоправное использование произведения, без заключения соглашения с правообладателем, привело к материальным убыткам последнего или причинило какой-либо ущерб.

Конфискация нелегальных экземпляров произведений, а также приборов и средств, осуществляющих создание таких экземпляров. Защита авторских прав таким способом позволяет предотвратить будущие нарушения.

Объявление решения суда с указанием настоящего правообладателя.

Взыскание денежных средств за нарушение авторских прав. Наиболее распространённый способ защиты на практике [2].

Таким образом, защита авторских прав является одной из главных задач в современном мире. Каждое произведение должно нести что-то новое и оригинальное. Авторское право должно решать проблему принадлежности авторства и возможности использования результата интеллектуального труда всем обществом.

Литература

1. Мэггс П. Б., Сергеев А.П. Интеллектуальная собственность. М.: Юристъ, 2000. 400 с.
2. Sum IP- Интеллектуальная собственность в России и за рубежом [Электронный ресурс]. Режим доступа: http://sumip.ru/biblioteka/avtorskoye-pravo/zashhita-avtorskix-prav/. Дата обращения: 10.04.2018.
3. Интернет-портал BusinessMan.ru [Электронный ресурс]. - Режим доступа: https://businessman.ru/new-zashhita-avtorskix-prav/. Дата обращения: 10.04.2018.

ИССЛЕДОВАНИЕ ВИРУСА WANNA CRY

В. В. Пасько, С. М. Полухин
Северо-Кавказский федеральный университет, г. Ставрополь

Компьютерные вирусы – вредоносное ПО, разработанное злоумышленником, с целью нанесения вреда компьютеру, дестабилизации всей сети. Вирусы могут нарушать целостность файловой системы, вызывая разного рода искажения на жестком диске, что может полностью уничтожить данные. В статье рассмотрен вирус Wanna Cry, приведены способы лечения, а также необходимые меры защиты.

Ключевые слова: Вирус Wanna Cry, способы защиты.

Давайте поговорим, что такое вирус Wanna Cry. Wanna Cry – это вредоносное ПО, которое является видом трояна и относится к типу «ransomware». Вирусы вида «ransomware» («вымогатели») предназначены для шантажа с целью получения денежных средств у владельцев зараженных компьютеров. Фактически, WannaCry держит ваш компьютер в заложниках и требует выкуп. Если выкуп не будет выплачен – заложник будет убит, т.е. вы потеряете всю информацию, которая хранилась на вашем ПК.

Вирус Wanna Cry был продемонстрирован на весь мир 12 мая, в этот злополучный день о заражении своих сетей заявили ряд медицинских учреждений в Великобритании, Испанская телекоммуникационная компания и МВД России сообщили о отражении хакерской атаки.

Wanna Cry относится к категории вирусов шифрующих данные, которые при внедрении в компьютер зашифровывает файлы криптостойким алгоритмом, после которого – работа с этими файлами просто не возможна.

В настоящее время, известен ряд следующих популярных расширений файлов, которые наиболее часто подвергаются шифрованию Wanna Cry:

– файлы пакета MO (doc, xlsx и др.).

– файлы мультимедиа и различных архивов (iso,zip,rar,mp3, wav,avi, png и др).

WannaCry представляет собой некую программу под названием WanaCrypt0r 2.0, которая атакует ПК на ОС Windows. Программа использует уникальные «дыры» в системе —Microsoft Security Bulletin Ms-17-010, происхождение которой было ранее неизвестно. За деактивацию вируса требуют заплатить денежные средства 300-600 долларов. В настоящее время хакеры заполучили уже более 42 тысяч долларов.

Вирус Wanna Cry распространяется вот таким образом образом: электронную почту клиента приходит письмо с неким интересным файлом – это может быть анимация, мелодия, фильм, но вместо обычного соответствующего расширения для этих объектов, файл будет иметь расширение осуществлённого файла – exe. При воспроизведении данного файла происходит «зараженность» системы и через «дыры» в ОС Windows загружается сам вирус Wanna Cry, который шифрует данные клиента.

Вирусы, которые шифруют данные относятся к разряду самых «злых» вирусов, т.к. в большой вероятности случаев, файлы клиента шифруются 128bit'ным или 256bit'ным ключом. Самое главное здесь то, что в каждом инциденте — ключ уникален и на расшифровку каждого требуются обширные вычислительные мощности, большое количество времени, что делает задачу расширфровки практически невозможным.

Если же вы все-таки пострадали от вируса Wanna Cry, вам необходимо:

1. Обратитесь на сайт поддержки Лаборатории Касперского – https://www.kaspersky.ru/ с описанием проблемы. На сайте работают, как представители компании, так и опытные программисты, активно помогающие в решении подобных проблем.

2. Существенным решением будет – полное удаление ОС Windows с компьютера с дальнейшей «пустой» установкой новой. При таком раскладе – все пользовательские файлы и данные полностью удаляются.

Первым «исцелением» от нового шифрующего вируса нашел иностранный программист, данные которого не распространяется в СМИ. Как говорят, он и его товарищ увидели, что вирус обращается к адресу iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. Эта строка была «огражде-

нием» в сам код вредоносной программы. Регистрация доменного имени с тем же именем помогла на какое-то время остановить действие вируса. При этом о полном «разгроме» врага пока говорить рано, поскольку вредоносные атаки могут возобновиться, если злоумышленник изменит адрес.

Чтобы свести к минимуму риск внедрения вируса Wanna Cry на ПК специалисты «Лаборатории Касперского» советуют установить все новейшие обновления ОС Windows.

Еще, необходимо внимательно просматривать письма, которые приходят на почтовый ящик. Нельзя открывать письма с расширениями .exe, .vbs и .scr. Злоумышленники могут использовать несколько расширений, чтобы скрыть вредоносный файл как видео, фото или документ (например, avi.exe или doc.scr)..

Еще один метод борьбы с вирусом может стать блокировка 445 порта, через которое идет заражение.

Для обнаружения вредоносных файлов, необходимо включить опцию «Показывать расширения файлов» в настройках Windows.

Если же преступнику все-таки удалось «влезть» в ваш компьютер, программисты рекомендуют не платить злоумышленникам. Потому что, вероятнее всего, атака продлится недолго, так как срок хранения Ransomware обычно короткий. По результатам, после выкупа восстанавливаются файлы не во всех случаях, и, даже заплатив деньги, можно лишиться всей важной документации.

Меры по защите от вируса Wanna Cry:

1. Установить патч для Windows Server. Компания Microsoft создала экстренный патч для следующих ОС – Vista, 7, 8.1, 10. Установить данный патч можно просто запустив обновление системы, через службу обновлений Windows.

2. Установка антивирусных программ с актуальными базами данных. Известные компании по созданию антивирусных программ, такие как Касперский, Dr.Web, уже выпустили актуальные обновления для своих продуктов содержащие информацию о Wanna Cry, тем самым обезопасив своих клиентов.

3. Иметь копии важных документов на съемном носителе. Если ваш ПК еще не подвергся атаки злоумышленников, вы можете сохранить наиболее важные документы на отдельный носитель (flash-накопитель, диск). Таким образом, даже став жертвой – вы сможете иметь доступ к своим документам.

Литература

1. www.forum.kaspersky.com
2. https://ru.wikipedia.org/wiki/WannaCry

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ СОВРЕМЕННЫХ ГАДЖЕТОВ

Д. А. Плахутин, О. В. Зименков
руководитель – канд. физ. мат. наук, доцент ***Н. Ю. Братченко***
Северо-Кавказский федеральный университет, г. Ставрополь

Современные смартфоны способны выполнять много различных задач (от общения в социальных сетях, до покупок в интернете, банковских операций). Поэтому на сегодняшний день актуальна проблема защиты информации, которую применяет смартфон. В данной статье описаны способы, с помощью которых возможно защитить информацию пользователя.

Ключевые слова: смартфоны, безопасность смартфонов, персональная информация, датчики, приложения.

На сегодняшний день в современном мире новых технологий гаджеты оснащены достаточно большим количеством датчиков, в том числе такими, о наличии которых мы даже не предполагаем. Так, например, датчики света, давления, температуры.

Поскольку смартфоны прочно вошли в нашу жизнь, они остаются рядом с нами в течение всего дня. Онипозволяют нам решать различные задачи. Но огромное количество персональной информации, которуюиспользуют смартфоны, делает их не безопасными хранителями ее. При этом, возникает возможность различным приложениям получать доступ к персональной информации и распространять ее без ведома пользователя, вести запись с помощью микрофона, отслеживать местоположение телефона, фотографировать, а затем извлекать данные. Таким образом похищенные данные, фотографии и звуковые записи нарушают закон онеприкосновенности личной жизни.Кроме того, данные имеющихся датчиков также могут передавать важную информацию.

Расположение смартфона в пространстве и его динамика позволяют выявить вводимую пользователем информацию или раскрыть его местонахождение. Даже показания барометра, которые меняются с увеличением высоты, также могут определитьместонахождения пользователя.

Вторжение в личную жизнь этими способами возможно еще не происходят в реальной жизни, но заинтересованныеисследователи в научных кругах работают над предотвращением возможных вторжений.

Детекторы движения в смартфонах, такие как акселерометр и гироскоп, могут быть первыми инструментами для тайного сбора данных. Они не защищены правами доступа – пользователю телефона не требуетсяпредоставлять разрешение приложениям для доступа к этим датчикам. Например, прикосновения к различным областям экрана приводит к тому, что телефон наклоняется, и это фиксируетсясоответствующими датчиками движения.

Известно, что ученые из калифорнийского университета разработали приложение TouchLogger, которое собирает данные датчика движения при нажатии на виртуальную клавиатуру смартфона.При этом, в процессе тестирования телефоновHTC, TouchLogger правильно распознал более 70% нажатий.В дальнейшем в подобных приложениях использовался целый набор датчиков смартфонов, в том числе, гироскоп, акселерометр, датчик освещённости, для распознавания нажатий. При тестировании из 50 веденныхPIN кодов приложениеразличает нажатие клавиш с точностью до 97,5 процентов.

Существует и другие способыраспознаваниевведённыхданных– с помощью микрофона. Некоторые вредоносные приложенияимеют возможности записыватьвведённые символы и звуки нажатия, слушать в фоновом режиме, когда пользователь вводит конфиденциальную информацию. При тестированиитаких программ на телефонах Samsung и HTC на *Конференции по безопасности и конфиденциальности в беспроводной и мобильной сетях 2017 года* было представлено, что при вводе 100 четырехзначных PIN-кодов приложение распознает до 94 процентов веденной информации.

Можно отметить и следующее, возможности встроенных датчиков многообразны. Так, датчики движения способны отображать поездки человекана метро или на автобусе. Известно, что исследователи разработали приложение, описанное в 2017 году в *IEEE Transactionson Information Forensicsand Security,* для извлечения данных различных маршрутов метрополитена из показаний акселерометра. Например, в процессе экспериментовс смартфонами Samsung, подобные приложенияопределило, какими станциями метро пользовались пользователи с точностью до 81%. Таким образом, человек становится беззащитен в информационном мире персонализации.

Поэтому проблема безопасности персональной информации пользователей смартфонов и других гаджетов достаточно актуальна. На сегодняшний день разрабатываются прототипы новой системы безопасности, которыепозволятконтролировать активность датчиков и предупреждать владельцев о необычном поведении систем.Однако сейчаспользователю не следует принимать каких-либо трудоёмких и дорогостоящих мер ради повышения безопасности смартфона. Достаточно поставить автоблокировку и быть внимательным при загрузке контента и подключении к Wi-Fi-сетям.Для уверенности в том, что гаджет не подвергнется внешнему влиянию, следуетиспользовать антивирусную защиту.

Литература

1. Безопасность Андроид-устройств [Электронный ресурс]. Режим доступа: http://www.spy-soft.net/bezopasnost-android. (Дата обращения 28.04.18)

2. Как защитить Android [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/blog/android-maximum-security-tips/5938/. (Дата обращения 28.04.18)

3. Приложение TouchLogger [Электронный ресурс]. Режим доступа: https://clck.ru/DKFCb. (Дата обращения 28.04.18)
4. Системе обеспечения безопасностиAndroid [Электронный ресурс]. Режим доступа: ndroidios.org/bezopasnost-android-problemyi-virusyi-i-poleznyie-sovetyi/. (Дата обращения 28.04.18).

АНАЛИЗ РУБЕЖЕЙ ЗАЩИТЫ ЗОНЫ ОЗУ СЕРВЕРА-ПОЛУЧАТЕЛЯ ЭЛЕКТРОННОЙ ПОЧТЫ

Н. А. Попов
Северо-Кавказский федеральный университет, г. Ставрополь

Произведен анализ типовых нападений на оперативное запоминающее устройство сервера-получателя электронной почты.
Ключевые слова: электронная почта, оперативное запоминающее устройство, информационная безопасность.

В связи с развитием электронного документооборота, все больше вытесняющем традиционный бумажный, значительную ценность в конкурентных условиях приобретают электронные сообщения, а как следствие и системы, обеспечивающие прием и отправку электронной почты. Критически важной частью подобных систем является зона оперативного запоминающего устройства сервера-получателя электронной почты.

Перечень функций сервера электронной почты, которые могут быть нарушены вследствие нападения, представлены на рис. 1.

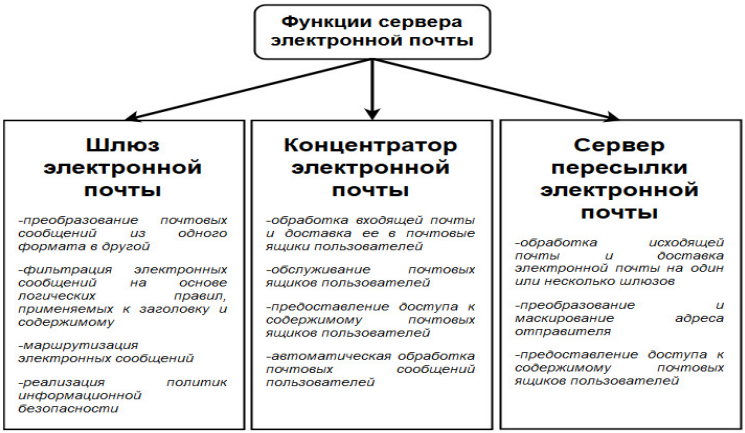


Рисунок 1. Функции сервера электронной почты

ОЗУ сервера занимает положение в системе электронной почты наряду со следующими структурными элементами(рис.2):

- долговременное запоминающее устройство клиента (ДЗУ клиента);
- оперативное запоминающее устройство клиента (ОЗУ клиента);
- оперативное запоминающее устройство сервера (ОЗУ сервера);
- долговременное запоминающее устройство сервера (ДЗУ сервера);
- локальная вычислительная сеть (ЛВС).

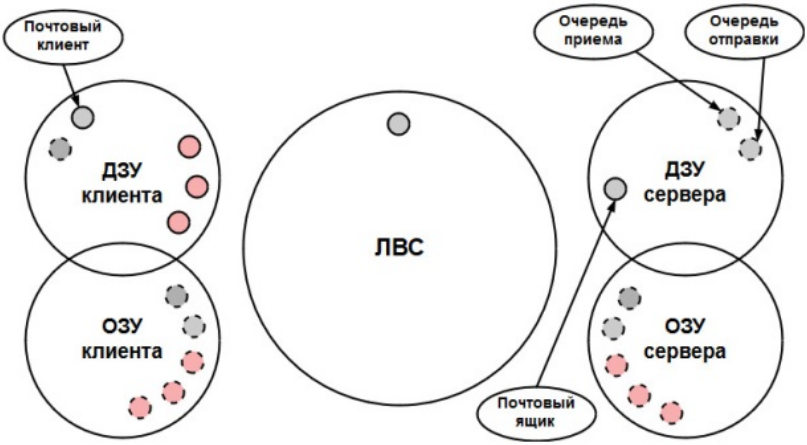


Рисунок 2. Структура объекта защиты и его место в системе электронной почты

В системе электронной почты можно выделить несколько контуров системы защиты. Первый контур защиты соответствует взаимодействию “клиент-сервер”. Второй контур защиты затрагивает взаимодействие “сервер-сервер”.

Против зоны ОЗУ сервера-получателя применяются следующие типовые атаки:

1) Использование служебных функций электронной почты для сбора информации о системе электронной почты, организации атак типа “отказ в обслуживании”, использовании уязвимостей ПО и его конфигурации.

2) Похищение услуг, сервисов электронной почты. Используя изъяны конфигурации программного обеспечения и средств защиты сервера-получателя, вынудить выполнить его дополнительные функции (пересылка, тиражирование почты и т.д.).

3) Обход фильтров электронной почты. С помощью криптографических или специальных преобразований затруднить или сделать полностью неэффективной работу фильтров серверов-получателей, реализующих по-

литику управления информационными потоками или политику информационной безопасности.

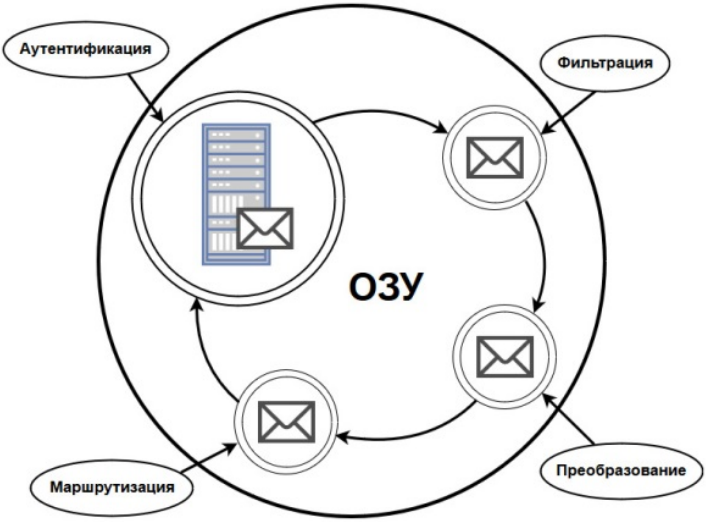


Рисунок 3. Рубежи защиты в зоне ОЗУ сервера-получателя

Функциональное назначение рубежей защиты (рис. 3) для сервера-получателя зеркально-симметрично аналогичным рубежам сервера отправителя.

Основной рубеж образуют встроенные средства системного и прикладного программного обеспечения операционной системы и электронной почты. Важнейшие функции: аутентификация и криптографическая защита канала передачи данных. На основе главного рубежа реализуются **дополнительные рубежи**: фильтрация, преобразование, маршрутизация.

Рубеж фильтрации предназначен для борьбы с навязыванием ложной информации, с распространением вредоносного ПО и нежелательной корреспонденции, он также участвует в реализации политики управления информационными потоками.

Рубеж преобразования на основе системы правил осуществляет модификацию заголовков и содержимого электронного сообщения. Главная задача – скрыть внутреннюю структуру организации, замаскировать каналы обмена информацией, реализовать централизованную криптографическую защиту сообщений электронной почты.

Рубеж маршрутизации выполняет основную работу по управлению информационными потоками. Именно здесь принимаются решения о доставке электронной почты на тот или иной концентратор электронной почты. Дополнительной задачей является реализация отказоустойчивости за счет использования избыточных каналов связи.

Таким образом были выделены возможные типы нападений на зону ОЗУ сервера-получателя электронной почты и проведен анализ рубежей ее защиты.

Литература

1. А. Ф. Чипига. Информационная безопасность автоматизированных систем. Учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем». М., 2010.

2. А. Ф. Чипига, В. С. Ерещенко. Объектный подход к модели разграничения доступа в компьютерных системах. Информационное противодействие угрозам терроризма. 2005. №5. С. 122-128.

РАЗРАБОТКА АЛГОРИТМА К ПОСТРОЕНИЮ ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ СТАВРОПОЛЬСКОГО КРАЯ

П. В. Радайкин

Северо-Кавказский федеральный университет, г. Ставрополь

В Ставропольском крае органы государственной власти используют множество информационных систем, регулятором которых, на региональном уровне, является Закон Ставропольского края от 28.07.2009 № 51-КЗ «О государственных информационных системах Ставропольского края».

Защита от несанкционированного доступа в органах государственной власти Ставропольского края имеет большое значение и влияет на общую репутацию информационной безопасности края.

В органах государственной власти, почти на каждом рабочем месте имеется доступ к определенной государственной информационной системе, поэтому необходимо разработать алгоритм, по которому можно создать типовой решение защиты от несанкционированного доступа.

Задача является актуальной, потому что уровень знаний основных требований по защите информации в Ставропольском крае довольно высок, но реализация данных мер не всегда удовлетворяет требования федеральных законов. Нарушение требований может повлечь за собой серьезный ущерб, не только для конкретной организации, но и для всех пользователей государственных информационных систем, в том числе и оператора. Цель: обеспечить безопасность от несанкционированного доступа государственных информационных систем и рабочих мест, с которых осуществляется подключение к ГИС.

Ключевые слова: органы государственной власти, государственная информационная система, требования к государственной информационной системе, несанкционированный доступ, Ставропольский край, защита информации.

Угрозой информации называется потенциально возможное влияние или воздействие на автоматизированную систему с последующим нанесением убытка чьим-то потребностям или активам.

В данный период существует более ста позиций и разновидностей угроз информационной системе. Проанализировав все риски с помощью разных методик диагностики и проанализировав показатели их детализации, можно грамотно выстроить систему защиты от угроз в информационном пространстве.

Созданная с помощью моделирования логическая цепочка трансформации информации выглядит следующим образом (рис. 1).

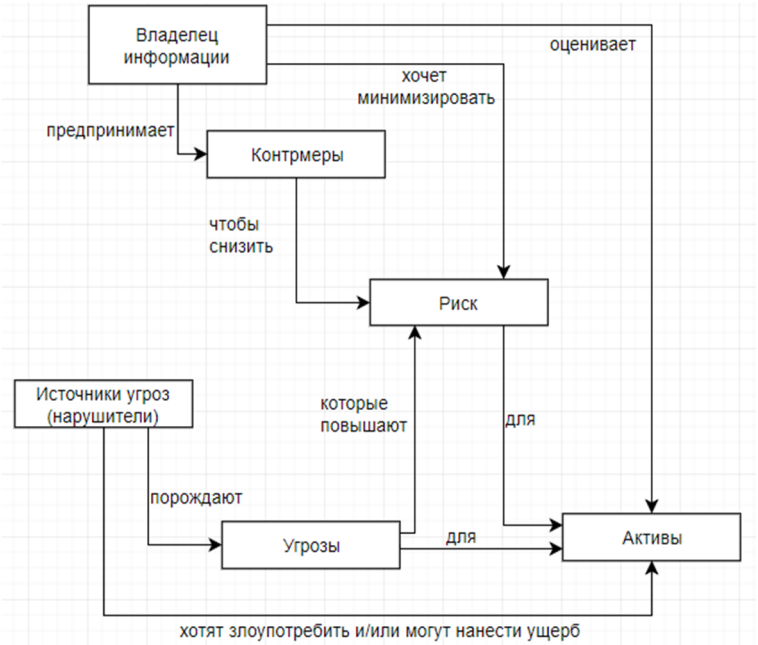


Рисунок1. Цепочка трансформации информации

Угрозы информационной безопасности проявляются не самостоятельно, а через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости. Угроза приводит к нарушению деятельности систем на конкретном объекте-носителе.

Основные уязвимости возникают по причине действия следующих факторов (рис. 2).

Рисунок 2. Источники утечки информации

Чаще всего источники угрозы запускаются с целью получения незаконной выгоды вследствие нанесения ущерба информации. Но возможно и случайное действие угроз из-за недостаточной степени защиты и массового действия угрожающего фактора.

Существует разделение уязвимостей по классам (рис. 3).

Рисунок 3. Разделение уязвимостей по классам

Устранение угроз, как минимум ослабляет влияние уязвимостей, при которых можно избежать полноценной угрозы, направленной на систему хранения информации.

Случайные виды уязвимостей зависят от непредвиденных обстоятельств и особенностей окружения информационной среды. Их практически невозможно предугадать в информационном пространстве, но важно

быть готовым к их быстрому устранению. Устранить такие неполадки можно с помощью проведения инженерно-технического разбирательства и ответного удара, нанесенного угрозе информационной безопасности.

Объективные разновидности уязвимостей напрямую зависят от технического построения оборудования на объекте, требующем защиты, и его характеристик. Полноценное избавление от этих факторов невозможно, но их частичное устранение достигается с помощью инженерно-технических приемов, следующими способами:

Субъективные уязвимости представляют собой результат неправильных действий сотрудников на уровне разработки систем хранения и защиты информации. Поэтому устранение таких факторов возможно при помощи методик с использованием аппаратуры и программного обеспечения:

Ранжирование уязвимостей должно быть учтено и оценено специалистами. Поэтому важно определить критерии оценки опасности возникновения угрозы и вероятности поломки или обхода защиты информации. Показатели подсчитываются с помощью применения ранжирования. Среди всех критериев выделяют три основных:

Чтобы узнать информацию о степени защиты системы точно, нужно привлечь к работе аналитический отдел с экспертами. Они произведут оценку всех уязвимостей и составят информационную карту по пятибалльной системе. Единица соответствует минимальной возможности влияния на защиту информации и ее обход, а пятерка отвечает максимальному уровню влияния и, соответственно, опасности. Результаты всех анализов сводятся в одну таблицу, степень влияния разбивается по классам для удобства подсчета коэффициента уязвимости системы, данный вид анализа (рис. 4).

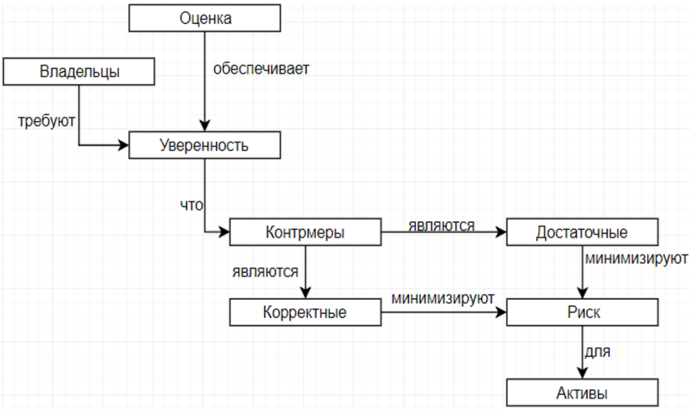


Рисунок 4. Анализ оценки по классам уязвимостей

Способ доступа к основным ресурсам системы. Выделяют следующие угрозы такие как: применение нестандартного канала пути к ресурсам, что

включает в себя несанкционированное использование возможностей операционной системы; использование стандартного канала для открытия доступа к ресурсам.

Способы несанкционированного доступа к информации (рис. 5).

Рисунок 5. Способы несанкционированного доступа к информации

Возможно 3 варианта реализации способов, представленных выше, это: применение, использование и получение. Схема реализации (рис. 6).

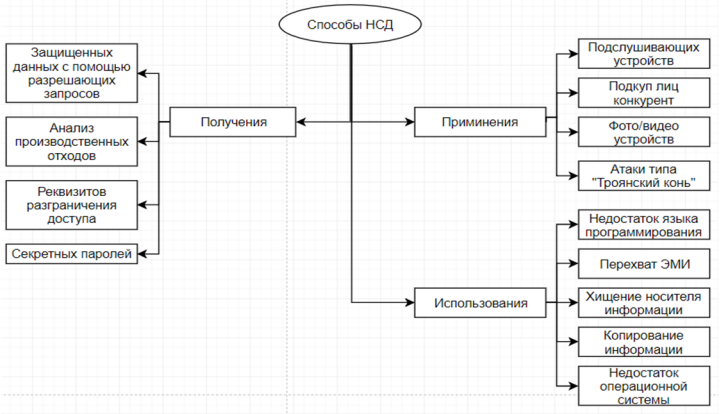


Рисунок 6. Схема реализации способов несанкционированного доступа

Литература

1. Закон Ставропольского края от 28 июля 2009 г. № 51-КЗ «О государственных информационных системах Ставропольского края».

2. Методический документ ФСТЭК «Методика определения угроз безопасности информации в информационных системах».

3. Методический документ ФСТЭК от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».
4. Приказа ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
5. Приказ ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
6. Решение Коллегии Гостехкомиссии России № 7.2/02.03.2001 г. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К).
7. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

ОСНОВНЫЕ МЕТОДЫ АНАЛИЗА РИСКОВ ОСУЩЕСТВЛЕНИЯ УГРОЗ НА ПРЕДПРИЯТИИ

М. М. Савельев, В. Д. Клименко, Т. М. Петрова
руководитель – канд. техн. наук, доцент ***Т. В. Минкина***
Северо-Кавказский федеральный университет, г. Ставрополь

В настоящее время существует множество подходов к моделированию угроз информационной безопасности. В статье определены основные методы анализа рисков и задача управления информационными ресурсами. Сделаны выводы, что необходимо соблюдая баланс между ценой информации и затратами на ее сохранение, предполагается уделять внимание анализу конфигурации и протоколам работы устройств, отвечающих за обмен информацией с внешним миром, для предотвращения угроз ресурсам, хранимых в базе данных внутреннего сервера и на рабочих станциях.

Ключевые слова: информационной системы, угрозы, информационная безопасность, конфиденциальная информация, определение рисков.

На сегодняшний день существует малое количество предприятий, которые в полной мере контролируют защиту конфиденциальной информации. Каждое предприятие обладает ценной информацией, несанкционированный доступ к которой может нанести определенный ущерб.

Наиболее распространенными объектами утечки информации на предприятии являются:

- информация или данные;
- программно-аппаратные средства;
- программное обеспечение;
- персонал;
- телефоны, а также другое оборудование для обеспечения связи;

– имидж компании;
– документы.

Оценить нанесенный ущерб предприятию, возможно разобравшись с методами анализа рисков осуществления угроз на данном предприятии, они позволят оценить, насколько важно необходимо произвести защиту данной информации.

В ходе определения рисков необходимо выполнение следующих шагов:

1) идентифицировать главные ресурсы в информационной системе предприятия;
2) определить важность этих ресурсов для организации;
3) идентифицировать существующие угрозы безопасности и уязвимостей;
4) вычислить риски, связанные с осуществлением угроз безопасности.

В каждой категории ресурсы делятся на классы и подклассы. Необходимо выделить только те ресурсы, которые определяют функциональность ИС и существенны с точки зрения обеспечения безопасности:

1) были раскрыты данные, изменены, удалены или стали недоступны;
2) была повреждена или разрушена аппаратура;
3) нарушена целостность программного обеспечения;
4) локальные и удаленные атаки на ресурсы ИС;
5) стихийные бедствия;
6) ошибки, либо умышленные действия персонала ИС;
7) сбои в работе ИС, вызванные ошибками в программном обеспечении или неисправностями аппаратуры.

Свойства информационных систем, осуществляющих возможность успешного применения угроз безопасности, называются уязвимостями.

На основе вероятности осуществления угрозы, величины уязвимости и стоимости ресурса, может быть определена величина риска по следующей формуле:

$$R = \frac{Cost_{ресурса} \cdot P_{угрозы}}{V_{уязвимости}}, \quad (1)$$

где R – это **р**иск угрозы; Cost – стоимость ресурса; P – вероятность угрозы; V – величина уязвимости.

Практически каждая из систем защиты информации (СЗИ) не всегда может обеспечить стопроцентную надежность, то в меру сильной считают такую систему защиты информации, которая обеспечит ее надежную защиту в течение достаточно долгого периода времени. Проще говоря, СЗИ должна быть такая, чтобы на взлом требовалось времени больше, чем тот

период, за которой информация будет оставаться секретной. По этой причине даже самое незначительное уменьшение вероятности реализации угрозы, свидетельствует о затруднении взлома существующей СЗИ.

К основным методам анализа рисков можно отнести следующее:

1) анализ ресурсов информационной системы, включая людские, технические, информационные ресурсы и программные средства;

2) анализ бизнес процессов и задач, решаемых системой;

3) построение модели ресурсов информационной системой, определяющей взаимосвязи между людскими, программными, информационными и техническими ресурсами, их взаимное расположение и способы взаимодействия;

4) оценка критичности информационных ресурсов, а также программных и технических средств;

5) определение критичности ресурсов с учетом их взаимозависимостей;

6) определение уязвимостей защиты и наиболее вероятных угроз безопасности в отношении ресурсов информационной системы;

7) оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации в случае успешного осуществления угроз;

8) определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость.

Это достаточно общий набор задач, а для решения этих задач могут быть использованы различные методики анализа рисков.

Информационные ресурсы можно определить, как весь имеющийся объем информации в информационной системе. Для предприятия – информационные ресурсы – это информация о поставщиках, клиентах, заказах, сотрудниках организации. Другими словами, информационные ресурсы – это весь объем знаний, зафиксированный на материальных носителях и предназначенный для использования.

ФЗ-149 «Об информации, информационных технологиях и о защите информации» определяет информационные ресурсы как отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информационные ресурсы предприятия формируются из многих источников**.** Любое предприятие существует в некоторой внешней среде. Также, предприятие порождает свою внутреннюю среду. Внутренняя среда формируется совокупностью работающих там людей, структурных подразделений предприятия, технологическими, социальными, экономическими и другими отношениями между ними.

В рамках организации, в зависимости от источника возникновения, имеется внутренняя и внешняя информация, которая составляет ее информационные ресурсы.

Информация внутренней среды наиболее полно отражает финансово-хозяйственное состояние. Обработка такой информации часто осуществляется с помощью стандартных формализованных процедур.

Внутренняя информация для рассматриваемого предприятия – о сотрудниках, ассортименте продукции, технологических процессах, выполненных заказах.

Внешняя среда – это субъекты, которые действуют за пределами предприятия и отношения с ними. К ним относятся отношения предприятия с клиентами, посредниками, поставщиками, конкурентами, государственными органами. Соответственно, к внешней информации можно причислить данные о рынке, конкурентах, тенденциях изменений в деловой среде страны и состоянии международных рынков, покупателях, спросе, требованиях клиентов и конкурентов, изменении законодательства.

Информационными ресурсами, необходимо управлять. Еще не разработана единая методология качественной и количественной оценки информационных ресурсов, а также прогнозирования потребности в них. Тем не менее, на уровне организации следует изучать информационные потребности, управлять информационными ресурсами и осуществлять планирование ресурсов.

Управление информационными ресурсами подразумевает:

1. оценка информационных потребностей;
2. создание системы управления данными;
3. изучение и рационализация документооборота предприятия;
4. типизация информации и данных;
5. преодоление проблемы несовместимости типов данных;
6. стандартизация и унификация типов и форм документов.

Из сказанного можно сделать выводы, что задачи управления информационными ресурсами являются важными факторами, формирующими систему информационной безопасности системы управления предприятием и накладывающим определенные ограничения на всю информационную систему в целом.

Учитывая специфику каждого предприятия, необходимость соблюдать баланс между ценой информации и затратами на ее сохранение, а также то, что ценные данные не покидают пределов локальной вычислительной сети предприятия, наибольшее внимание предполагается уделить анализу конфигурации и протоколам работы устройств, отвечающих за обмен информацией с внешним миром, для предотвращения угроз ресурсам, хранимых в базе данных внутреннего сервера и на рабочих станциях.

Литература

1. Рачков В. Е., Будко П. А. Информационный поток в современной логистической среде // Модели управления производством и совершенствование информационных технологий: сб. тр. VI Междунар. науч.-практ. конф. Ставрополь. 2010. С. 162-163.

2. Соколов А. И., Стадник В. А., Минкина Т. В. Системное описание научной проблемы // Студенческая наука для развития информационного общества: сборник материалов IV Всероссийской научно-технической конференции: в 2х томах, 2016. С. 178-179.
3. Петренко В. И., Мирошников Д. А., Емельянов Е. А. Обзор современных средств сетевой защиты информации//Проблемы автоматизации. Региональное управление. Связь и автоматика («ПАРУСА-2015»), Материалы IV Всероссийской научной конференции молодых ученых, аспирантов и студентов, Геленджик, 2015.
4. Забокрицкий Е.И., Заводнов В.С., Минкина Т.В. Предпосылки угроз информационной безопасности объекта // Материалы III Всероссийской научно-технической конференции «Студенческая наука для развития информационного общества». СКФУ(Ставрополь), 2015 г. С.181-182.
5. Домашенко А.А., Беспутнев В.В., Минкина Т.В. Актуальность защиты информации в сети интернет // Материалы III Всероссийской научно-технической конференции «Студенческая наука для развития информационного общества». СКФУ(Ставрополь), 2015 г. С.174-176.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ СРЕДСТВ НЕСАНКЦИОНИРОВАННОГО СЪЁМА ИНФОРМАЦИИ, ИСПОЛЬЗУЮЩИХ В КАЧЕСТВЕ КАНАЛА УТЕЧКИ ОГРАЖДАЮЩИЕ КОНСТРУКЦИИ ПОМЕЩЕНИЯ

А. В. Свирь, А. Р. Джадтоева, М. А. Мороз, М. Г. Огур
руководитель – канд. техн. наук, доцент кафедры прикладной математики и компьютерной безопасности ***Л. Л. Гусева***
Северо-Кавказский федеральный университет, г. Ставрополь

В этой статье речь пойдёт об обеспечении безопасности помещения от утечки информации по акустическим каналам. Будут рассмотрены каналы утечки информации. Так же, будут рассмотрены средства противодействия несанкционированному доступу, такие как: генераторы шума, блокираторы сотовых телефонов, подавители диктофонов, генераторы вибро и аудио-излучения. Будут приведены цены наиболее дешёвых и актуальных средств защиты. Так же будет приведено сравнение функций и стоимости стационарных и переносных комплексов защиты помещения от несанкционированной утечки информации через ограждающие конструкции помещения, сотовые телефоны и диктофоны.

Ключевые слова: защита информации, защита помещений, средства защиты, экономия, акустические каналы течки информации, стационарные комплексы, переносные комплексы.

Эта статья посвящена проблеме защиты помещения от средств несанкционированного съёма информации по акустическим каналам. Обеспечение безопасности информации от несанкционированного доступа – это всегда актуальная, приоритетная и сложная задача, требующая больших финансовых затрат. Для защиты информации от средств несанкционированного доступа, которые используют в качестве канала утечки

ограждающие конструкции помещения, используется большой спектр средств противодействия. Средствами, использующими акустические каналы утечки информации, могут являться:

1. Акустические и электронные стетоскопы – могут применяться для прослушивания через стены, потолок или пол.

2. Проводные, или радиомикрофоны – могут быть установлены на ограждающие конструкции, либо трубопроводы (водопроводные или отопительные).

3. Микроволновые, или лазерные системы съёма информации через оконные проёмы помещений.

Для комплексной защиты помещения от вышеперечисленных средств несанкционированного доступа используются такие устройства, как: генераторы шума, блокираторы сотовых телефонов, подавители диктофонов, генераторы вибро и аудио-излучения.

Для комплексной защиты помещения от утечки информации следует скомбинировать средства защиты для разных каналов. Так же, стоит обратить внимание на то, что средства защиты бывают, условно, стационарными и портативными. Условно, потому что по отделтности все эти устройства защиты относительно компактны, но портативные комплексы более универсальны. Портативные устройства стоят дороже, но обладают рядом преимуществ пред стационарными.

Приведём цены актуальных стационарных устройств для комбинированной защиты от утечки информации по акустическим каналам в (табл. 1):

Таблица 1

Общая стоимость оборудования: 119900 рублей

Название прибора	Назначение прибора	Цена
Подавитель диктофонов «Канонир К 7»	защищает от прослушивания через: беспроводные и проводные микрофоны (на всех частотах), диктофоны; мобильные телефоны и смартфоны; лазерные звукосниматели (при подключении колонок); другие подслушивающие устройства со встроенным микрофоном.	39900 руб.
Виброакустический генератор для защиты окон, стен и потолков «ANG-2»	Генератор акустического шума предназначен для создания заградительной помехи в оконных проемах и препятствованию утечки конфиденциальной информации через устройства съема информации, установленные под подвесным потолком и в воздуховодах.	45000 руб.
Прокруст - 2000	Антипрослушка для защиты одной аналоговой телефонной линии.	35000 руб.

Стационарные средства защиты информации хорошо подходят для обеспечения безопасности помещения на постоянной основе, но, бывают случаи, когда оборудовать помещение не представляется возможным, в таком случае, можно использовать портативные комплексы защиты:

1. Подавитель диктофонов UltraSonic-Кейс – портативное устройство, для создания ультразвуковой и акустической помехи. на расстоянии до 9 метров подавляется ориентировочно 70% звукозаписывающих устройств, преимущественно, запись на большинство смартфонов, IPhone, диктофоны. Глушатся прослушивающие проводные и радио микрофоны – «жучки». Стоимость прибора – 69900 руб.

2. Акустический подавитель диктофонов «Факир-М» – генератор формирует речеподобную помеху сложного спектра, что необходимо для нарушения нормальной работы всех устройств несанкционированного съёма информации. Благодаря малому размеру и универсальному питанию, может применяться в машине. Цена – 10900 руб. [1, 2].

Портативные устройства хоть и обладают большей универсальностью, не могут обеспечить безопасность по всем каналам утечки информации. Стационарные обеспечивают защиту по всем каналам утечки, но обходятся дороже, и их сложно переносить из одного помещения в другое.

Литература

1. http://www.spydetect.ru/index.php?categoryID=67&sort=Price&direction=ASC
2. http://www.detsys.ru/article/zaschita-ot-proslushivaniya

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКИХ СИСТЕМ

В. Н. Сенченко
руководитель – канд. техн. наук, доцент ***В. В. Антонов***
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье рассматривается информационная безопасность банковских систем. Были представлены внутренние и внешние угрозы банковских систем, а также основные меры по защите данных. Выявлен ряд основных принципов, согласно которым осуществляется обеспечение информационной безопасности банка.

Ключевые слова: банковская система, информационная безопасность, внутренние угрозы, внешние угрозы, электронная цифровая подпись.

В наше время хранение банковской информации, ее значимость и стоимость заметно возросли, что не могло не привлечь рост преступного интереса к ней.

Банковская система является совокупностью различных видов национальных банков и кредитных учреждений, включающих в себя центральный банк, сеть коммерческих банков и других кредитно – расчетных центров. Они занимаются обработкой, хранением и передачей информации требующей соответствующего уровня защищенности [2].

Необходимость обеспечивать достаточную безопасность хранения данных, регулярная проверка и смена паролей, и контроль возможности утечки информации стали неотъемлемой частью работы службы безопасности банка [1].

Банковские информационные системы и базы данных содержат конфиденциальную информацию о клиентах банка, состоянии их счетов и проведении различных финансовых операций. Необходимость сохранности этих сведений очевидна, но без быстрого и своевременного обмена и обработки информации банковская система даст сбой. Поэтому необходим целый комплекс мер, который сможет обеспечить защиту банковской системы и конфиденциальность данных содержащихся в клиентской базе. Следовательно, необходимы глубокие знания угроз, которым подвергаются информационные банковские системы.

В результате исследования были выявлены внутренние и внешние угрозы [2].

Внутренними угрозами являются:

1. Непосредственные операторы и пользователи информационной системы.
2. Администраторы системы информационной безопасности и вычислительных сетей.
3. Прикладные и системные программисты.
4. Сотрудники службы безопасности организации.
5. Технический персонал по обслуживанию зданий и вычислительной техники.
6. Вспомогательный персонал и временные работники, осуществляющие деятельность, как вне контролируемой зоны, так и в ее пределах.

Внешними угрозами являются:

1. Приглашенные посетител.
2. Клиенты.
3. Представители конкурирующих организаций.
4. Сотрудники ведомственного надзора и управления.
5. Наблюдатели за пределами охраняемой территории.
6. Нарушители пропускного режима.

Данные представленные на рисунке 1, показывают, что человеческий фактор является главной угрозой информационной безопасности, в первую очередь зависящей от человеческих отношений. Большая часть утечки информации объясняется халатностью и недостаточной компетентностью персонала банка [4].

Основные меры по защите данных можно представить таким образом:

1. Оценка и разработка конфиденциальной информации.
2. Оборудование объекта для осуществления защиты.
3. Грамотный набор персонала.
4. Контроль проведенных мероприятий по защите информации.

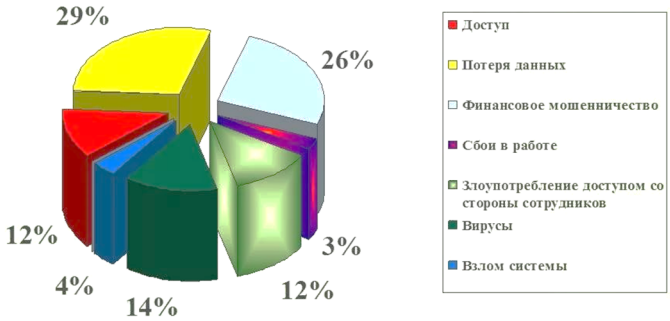


Рисунок 1. Уязвимость банковских информационных систем

Несмотря на множество возможностей взлома, кражи и утечки информации, обеспечение безопасности банковских данных и их конфиденциальности является вполне выполнимой задачей.

Современные методы защиты информации позволили сделать более совершенной систему криптографии, а также реализовать такую меру, как электронная цифровая подпись (ЭЦП). Она служит аналогом собственноручной подписи и имеет непосредственную привязку к электронному ключу, который хранится у владельца подписи.

Проведя анализ существующих сведений, о защите банковских систем, выделяется ряд основных принципов, согласно которым осуществляется эффективное обеспечение информационной безопасности банка [3]:

1. Своевременное установление и обнаружение проблем.
2. Актуальность и эффективность проведенных мероприятий по защите информации.
3. Возможность прогнозирования развития проблем.

Можно сделать вывод, что информация, находящаяся в базе данных банков, представляет собой действительно важную ценность, а значит требования к хранению, передаче и обработке данных всегда будут повышены, так же как и к подбору персонала.

Специфика и особенности системы обеспечения безопасности индивидуальны для каждого банка, поэтому профессиональное и комплексное предоставление систем защиты является важным и необходимым условием работы всей банковской системы.

Литература

1. Вихорев С. В. Информационная безопасность предприятий. М., 2006.
2. Гайкович В., Першин А. Безопасность электронных банковских систем – Издательство Компании «Единая Европа». М., 1994.
3. Демин В.С. и др. Автоматизированные банковские системы. М.: Менетемп – Информ, 1997.
4. Николаева Т. П. Финансы и кредит: Учебно-методический комплекс. М: Изд. Центр ЕАОИ, 2008. 371 с.

ПОИСК УЯЗВИМОСТИ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ. МЕТОД ФАЗЗИНГА

А. О. Скрынник, М. Г. Огур, Б. Н. Батыров
руководитель – канд. техн. наук, доцент ***Л. Л. Гусева***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрен способ поиска уязвимости в программном обеспечении (ПО) методом фаззинга. Определены основные достоинства и недостатки метода. Использование фаззинга позволяет найти некоторые из наиболее распространенных уязвимостей, а его применение на этапе разработки помогает избежать убытков в будущем.

Ключевые слова: Метод фаззинга, фаззер, уязвимости в программном обеспечении, мутационные фаззеры, порождающие фаззеры.

Недостатки современных приложений заключаются в том, что за счет частого выпуска новых версий, они не всегда полностью доработаны с точки зрения безопасности. Самые распространённые уязвимости это: возможность переполнения буфера, недостаточно устойчивое шифрование, утечка памяти, недостаточное внимание к вопросам контроля входных данных, SQL-инъекции и прочее.

Недостаточное внимание к вводу входных данных, их типу и размерности делает программу уязвимой для фаззинга.

Фаззинг – это процесс отсылки намеренно некорректных данных в исследуемый объект с целью вызвать ситуацию сбоя или ошибку [5].

Фаззер – приложение или фреймворк, дающие возможность проводить автоматизированный фаззинг приложений, кода, файлов и т.п. [4].

В отличие от большинства инструментов тестирования безопасности для динамических приложений, фаззеры не ищут определенных сигнатур атак и не пытаются найти известные уязвимости в продуктах, а предоставляют максимально широкий диапазон неожиданных входных данных для выявления новых и неизвестных уязвимостей в сетевых продуктах.

Чаще всего фаззинг используется либо во время процесса разработки программного продукта, чтобы автоматически обнаруживать дыры в системе безопасности. Это позволяет разработчику устранять уязвимости перед выпуском программы на рынок, что позволяет избегать затрат на исправление ошибок в дальнейшем. Также фаззинг может использоваться хакерами для выявления уязвимостей и дальнейшего написания эксплойтов для данной программы.

Одной из наиболее распространенных проблем на современном рынке программного обеспечения являются многочисленные попытки хакеров взломать защиту приложений. Каждый день обнаруживаются и публикуются новые уязвимости. Это причиняет колоссальный ущерб, включающий в себя финансовые потери, связанные с затратой времени и средств на ис-

правление проблемы, вред имиджу компании разработчика и ущерб третьей стороны, конфиденциальная информация которых, хранится в приложении.

Рисунок 1. Принцип работы фаззера

Фаззинг тестирование может включать в себя комбинации атак на числа, символы, метаданные и двоичные последовательности. Могут охватываться любые операции ввода-вывода, включая пользовательский интерфейс, параметры командной строки, импорт/экспорт и любые URL-адреса, формы, пользовательский контент, запросы и т.д.

Все фаззеры делятся на две категории: мутационные, которые изменяют существующие образцы данных и создают условия для тестирования, и порождающие, которые создают условия для тестирования с чистого листа, моделируя необходимый протокол или формат файла [5].

Так же фаззеры можно разделить на умные и глупые. Глупые фаззеры ничего не знают о структуре входного файла. Глупые фаззеры используют принцип мутации входных данных, изменяя определенное количество байт в исходном пакете, что не всегда приводит к удачному результату фаззинга.

Умные фаззеры имеют некоторое представление о структуре данных. Учитывая известный формат входных данных, они способны передавать заведомо некорректные значения. Умные фаззеры используют принцип генерации данных, что делает их наиболее эффективными.

Преимущества и недостатки фаззинга.

Преимущества:

−Фаззинг тестирование повышает безопасность программного обеспечения;

−Ошибки, обнаруженные с помощью фаззинга, часто бывают серьезными и могут включать дефекты, используемые хакерами, такие как необработанные исключения, сбои, ошибки и утечки памяти и т. д.;

−Ошибки, обнаруженные с помощью фаззинга, часто попадают в области, которые не просматриваются тестерами или в области, которые не указаны из-за ограничений времени и ресурсов.

Недостатки:

−Обычно обнаруживает очень простые ошибки;

−Данные от фаззинга могут быть трудно интерпретируемы;

−Может потребоваться значительное время и усилия для эффективного тестирования программного продукта.

Хотя фаззинг и не охватывает все ошибки безопасности в приложениях, это хороший способ найти некоторые из наиболее распространенных уязвимостей. Использование фаззинга на этапе разработки позволит избежать убытков в будущем и повысить экономическую эффективность [3].

Литература

1. Fuzzing and fuzzers: on using black box, security testing tools [Электронный ресурс]. URL: https://www.beyondsecurity.com/fuzzer_bestorm_whitepaper.html (Дата обращения: 30.04.2018).

2. Security Testing: Web Application Fuzz Testing – Coveros [Электронный ресурс]. URL: https://www.coveros.com/our-blogs/ (Дата обращения: 01.05.2018);

3. Мандрица И. В., Мандрица О. В., Соловьева И. В., Петренко В. И. Метод обоснования затрат на информационную безопасность бюджетных организаций // Вестник Северо-Кавказского федерального университета. – Ставрополь: Изд-во СКФУ, 2017. № 1 (58). С. 67-71.

4. Национальная библиотека им. Н. Э. Баумана [Электронный ресурс]. URL: https://ru.bmstu.wiki/Фаззинг (Дата обращения: 29.04.2018).

5. Саттон М., Грин А., Амини П. Fuzzing: исследование уязвимостей методом грубой силы. Пер. с англ. СПб.: Символ-Плюс, 2009. 560 с.

ЗАКОНОДАТЕЛЬСТВО О ПЕРСОНАЛЬНЫХ ДАННЫХ

Д. А. Солдаткин
руководитель – канд. техн. наук, доцент ***В. В. Антонов***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрены законодательства о персональных данных. Проведён обзор основных статей и федеральных законов, а также технологий и обработки персональных данных.

Ключевые слова: данные, оператор, федеральные законы, технологии обработки, субъект.

Персональные данные – это сведенье, подходящие прямо или косвенно определяемому физическому лицу (субъекту персональных данных);

Законодательство ужесточает хранение, передачу и распространение персональных данных, тем самым улучшает информационный поток данных и конфиденциальной информации;

Лицо, которое обрабатывает персональные данные, называется оператором, им может быть, как физическое лицо, так и муниципальный орган, либо учреждение.

Система, которая хранит в себе персональные данные, базы данных, совокупность определенных данных и сведений называется – информационная система персональных данных;

Обработка персональных данных при помощи компьютера или компьютерного комплекса называется – автоматизированная обработка персональных данных;

Раскрытие персональных данных на всеобщее обозрение или же в открытый доступ называется – распространение персональных данных;

Передача данных определенному лицу или кругу лиц называется – предоставление персональных данных;

Временное прекращение обработки персональных данных (в случае, когда это необходимо и никак не нарушает Федеральный закон) называется – блокирование персональных данных;

Операция, вследствие, которой происходит полное стирание, без возможности восстановление называется – уничтожение персональных данных.

Операция, в результате которой невозможно определить к какому субъекту принадлежат персональные данные без дополнительной информации называется – обезличивание персональных данных;

Информационная система персональных данных – это сочетание имеющихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Передача персональных данных иностранному лицу или компании называется – трансграничная передача персональных данных и осуществляется по средствам Федерального закона.

Функцией Федерального закона заключается в осуществлении и обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих фактов и особенности обработки персональных данных федеральных законов.

Особенности обработки персональных – это данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и другими нормативными правовыми актами Российской Федерации с соблюдением положений настоящего Федерального закона.

В процессах, связанных с иностранными лицами или организациями и компаниями осуществляется другое законодательство, непосредственно связанное с Федеральным законом «О персональных данных».

Персональные данные должны храниться на цифровых носителях, базах данных, быть полностью автоматизированы и иметь несколько копий во избежание утерь или кражи.

Лица обрабатывающие персональные данные могут поручить обрабатывать данные другому лицу, только в случае если это не нарушает конфиденциальности и регламентируется законом, так же должен быть заключен акт.

Операторы и иные лица, получившие доступ к персональным данным, не должны раскрывать информацию посторонним или людям, не допущенным к персональным данным, во избежание различного рода преступлений, связанных с персональными данными.

Сведенья о субъекте персональных данных при первой необходимости или же по решению суда должны быть ликвидированы с открытых информационных порталах, либо баз данных.

Таким образом, можно утверждать, что персональные данные очень важны для государства и данный закон регламентирует и решает множества проблем, связанных с персональными данными и их следует защищать, и предотвращать случаи их кражи или распространения в всеобщее пользование.

Литература

1. Положение о порядке хранения и защиты персональных данных пользователей - Электронный ресурс URL: http://enco72.ru/polozhenie-o-personalnyh-dannyh/

2. Статья 3. Закон о персональных данных № 152-ФЗ от 27.07.2006 – Электронный ресурс URL: https://www.zakonrf.info/zakon-o-personalnyh-dannyh/3/

3. Положение о персональных данных – Электронный ресурс URL: http://www.bionorica.ru/polozhenie-o-personalnykh-dannykh

Обработка персональных данных – Электронный ресурс URL: https://newcontact.su/?id=10

ЦЕЛЕСООБРАЗНОСТЬ ИСПОЛЬЗОВАНИЯ В СОВРЕМЕННОМ МИРЕ ТЕХНОЛОГИИ WiMAX

Н. Э. Степанян
руководитель – канд. техн. наук, доцент ***Т. В. Минкина***
Северо-Кавказский федеральный университет, Ставрополь

В данной статье будут рассмотрены особенности и задачи технологии Wi-MAX, как целесообразной к использованию в реалиях современного мира. Будут изучены отличие данной технологии от Wi-Fi и LTE. А также будут рассмотрены преимущества технологии WiMAX.

Ключевые слова: технологияWiMAX, Wi-Fi, стандарт связи IEEE 802.16, LTE, сети, система, локальные сети, телекоммуникации, передача данных.

Для начала нужно понять, что же такое технология WiMAX. Данная технология была разработана в 2003 году (однако задатки для её появления были ещё в 2001 году). Главной целью данной технологии является предоставление беспроводной связи для широкого спектра устройств – от рабочих станций до устройств, которые можно носить с собой (мобильные телефоны, планшет и т.п.). [1]

Данная технология основывается на стандарте связи IEEE 802.16. Название технологии берёт своё начало с WiMAX Forum, который был создан для продвижения и развития данного вида связи.

WiMAX направлен на решения целого ряда определённых задач, в который входят: соединение точек доступа Wi-Fi; обеспечение мониторинга системами (подобно тому как это реализовано в SCADA); создание новых точек доступа, которые не привязаны к вашему местоположению; предоставление широкополосного доступа, который обладает высокой скоростью.

На сегодняшний день перед связистами всего мира стоит проблема, так называемой, последней мили (канал, который соединяет клиентское оборудование с узлом доступа провайдера). Есть множество технологий, которые позволяют решить данную проблему, в их число входит и WiMAX [5; с. 5].

Существуют два частных вида технологии, каждый из них направлен на свою сферу пользования: стандарт 802.16 – 2004 и стандарт 802.16 – 2005, утверждённые в 2004 и 2005 году соответственно. Первый предназначен для статичных пользователей, а второй для поддержки мобильных пользователей [7; с. 223].

Оборудование для WiMAX устанавливают и на улицах, и в помещениях. Устройства, устанавливаемые в помещениях, могут работать лишь на малых расстояниях от базовой станции, поэтому им требуются крупные инвестиции.

В сетях 802.16 MAC используется алгоритм планирования. Работает это так: пользователь подключается к точке доступа, для которой будет создан отдельный слот, к которому другие пользователи не имеют доступ, а это означает, что перебои в связи полностью исключены [8; с. 22].

Что касается архитектуры, она довольно специфична. Она не привязана к какой-либо конфигурации, что позволяет добиться высокой гибкости и масштабируемости. Рассмотреть архитектуру технологии WiMAX можно на рус. 1.

Многие компании делают уклон именно в сторону WiMAX, и этому есть несколько причин. Технологии 802.16 позволяют развернуть сеть в труднодоступных местах и расширить её. Сама технология довольно проста в использовании, что характерно для всех беспроводных технологий. Как отмечалось выше, технология обладает высокой гибкостью и легко масштабируется, что позволяет развернуть сеть на нужной территории в

самые короткие сроки. Это позволяет снизить затраты на предоставление доступа с сети [3; с. 3].

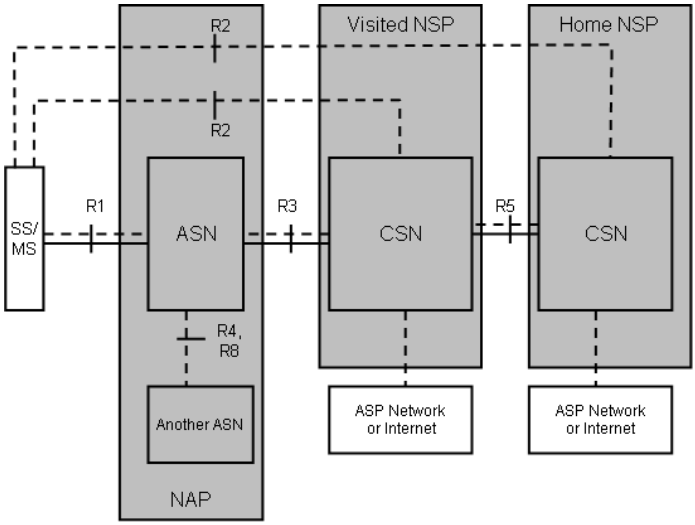


Рисунок 4. WiMAX Архитектура

Оборудование для подключения к сети можно приобретать и у сторонних производителей, что, безусловно, удобно для обычных пользователей. Также установка самого оборудования довольно проста и не предполагает владением специфичных навыков [4].

Теперь стоит перейти к сравнению рассматриваемой нами технологии с технологиями схожими по принципу действия.

Чаще всего технологию WiMAX сравнивают с Wi-Fi. Связано это с тем, что их названия похожи, как и названия стандартов, на которых они основаны. Однако обе технологии имеют различия, также они направлены на решение разных задач.

WiMAX имеет довольно широкую зону действия. При работе используются лицензированные частоты. Технология имеет виды доступа, распространяющиеся от мобильных видов, до связанных с вашим местоположением [6; с. 19].

Wi-Fi же имеет малую зону действия в отличии от WiMAX. В работе используются нелицензированные спектры частот. Зачастую используется для создания автономной локальной сети. Из-за своей дешевизны чаще используется в местах публичного пребывания. Приведённая ниже таблица позволяет сравнить две технологии, исходя из их спецификации.

Таблица 1

Сравнительная таблица стандартов беспроводной связи

Технология	Стандарт	Использование	Пропускная способность	Радиус действия	Частоты
Wi-Fi	802.11ac	WLAN	до 1 Гбит/с	до 300 метров	5 ГГц
Wi-Fi	802.11g	WLAN	до 54 Мбит/с	до 300 метров	2,4 ГГц
Wi-Fi	802.11n	WLAN	до 300 Мбит/с (в теории до 600 Мбит/с)	до 300 метров	2,4-2,5 (5,0) ГГц
WiMAX	802.16d	WMAN	до 75 Мбит/с	25-80 км	1,5-11 ГГц
WiMAX	802.16e	Mobile WMAN	до 40 Мбит/с	1-5 км	2,3-13,6 ГГц
WiMAX 2	802.16m	WMAN, Mobile WMAN	до 1 Гбит/с (WMAN), до 100 Мбит/с (Mobile WMAN)	120-150 км	До 11 ГГц

Технология LTE, как и WiMAX способен предоставить доступ к сети Интернет, при этом обладая большой скоростью. Именно LTE в основном используется для перехода к сетям 4G [1; с. 472].

Однако, несмотря на несомненное первенство LTE, WiMAX всё также продолжает развиваться. Обе технологии отличаются лишь стоимостью тарифов и скоростью передачи данных.

Из-за бурного развития LTE, появление WiMAX в населённых пунктах с относительно малым числом жителей движется очень медленно.

Технология WiMAX обладает рядом преимуществ, вот некоторые из них: большая скорость и зона действия (до 50 км). Как уже упоминалось ранее, оборудование можно приобретать у разных поставщиков, что приводит к низкой стоимости услуг; отсутствует прямая видимость между абонентом и базовой сетью; высокое качество передачи аудиозаписей и фотоизображений; содержит в себе протокол IP, что позволяет с лёгкостью преобразовывать её в.

Хотя и у WiMAX есть свои небольшие недостатки, но при этом она обладает рядом преимуществ, которые могут сделать её самой передовой на рынке локальные сети беспроводных телекоммуникационных технологий.

Литература

1. http://proremontpk.ru/technology/wimax/chto-takoe-wimax.html
2. https://ru.wikipedia.org/wiki/WiMAX
3. В. Вишневский, С. Портной, И. Шахнович – Энциклопедия WiMax. Путь 4G. М.: Техносфера, 2009. С. 472.
4. Стандарт IEEE 802.16-2001

5. Мезенцева О. С., Трофимова М. В. Интеллектуальные системы и технологии/ Рецензенты: профессор В. И. Дроздова, профессор Н. В. Кандаурова. Ставрополь, 2013.

6. Nemkov R. M., Mezentseva O. S., Mezentsev D. Using of a convolutional neural network with changing receptive fields in the tasks of image recognition// Advances in Intelligent Systems and Computing. 2016. Т. 451. С. 15-23.

7. Шевченко Д.А., Минкина Т.В. Угрозы безопасности информации в автоматизированных системах //сб. Культура и общество: история и современность материалы IV Всероссийской научно-практической конференции. Российский государственный социальный университет, 2015. С. 221-223.

8. Петренко В. И., Мирошников Д. А., Емельянов Е. А. Обзор современных средств сетевой защиты информации//Проблемы автоматизации. Региональное управление. Связь и автоматика («ПАРУСА-2015»), Материалы IV Всероссийской научной конференции молодых ученых, аспирантов и студентов. Геленджик, 2015.

СИСТЕМНАЯ ОЦЕНКА ТИПОВЫХ НАПАДЕНИЙ НА ЗОНУ ДЗУ СЕРВЕРА-ПОЛУЧАТЕЛЯ ЭЛЕКТРОННОЙ ПОЧТЫ

В. А. Стратьев
руководитель – канд. техн. наук, профессор ***А. Ф. Чипига***
Северо-Кавказский федеральный университет, г. Ставрополь

Произведена системная оценка типовых нападений на долговременное запоминающее устройство сервера-получателя электронной почты.

Ключевые слова: электронная почта, долговременное запоминающее устройство, нападение, информационная безопасность.

В связи с постепенным уходом от бумажного документооборота во многих организациях, а также развитием информационных технологий с их интеграцией во все сферы общества, все большую стратегическую ценность в конкурентных условиях приобретают электронные сообщения и, соответственно, системы, обеспечивающие прием и отправку электронной почты [1]. Частью такой системы является зона долговременного запоминающего устройства сервера-получателя электронной почты [2].

Структура защищаемого объекта (зона ДЗУ сервера) состоит из следующих компонентов (рис. 1) [3]:

- очереди приема;
- очереди отправки;
- почтового ящика.

ДЗУ сервера занимает место в системе электронной почты на ряду со следующими структурными элементами (рис. 1):

- долговременное запоминающее устройство клиента (ДЗУ клиента);
- оперативное запоминающее устройство клиента (ОЗУ клиента);
- оперативное запоминающее устройство сервера (ОЗУ сервера);
- локальное вычислительное устройство (ЛВС).

Понять важность сервера электронной почты можно исходя из перечня функций (рис. 2), выполнение которых сервером может быть нарушено при нападениях.

Выделяются следующие типы нападений, которые могут осуществляться на зону ДЗУ сервера [4]:

1) перехват электронной почты в очереди на отправку;
2) навязывание электронной почты в очередь на отправку.

Приведенные типы нападений соответствуют нападениям, осуществляемым на зону ОЗУ сервера, однако их реализация происходит внутри ресурсов файловой системы сервера. Защита реализуется средствами контроля целостности операционной системы и прикладного программного обеспечения электронной почты [5].

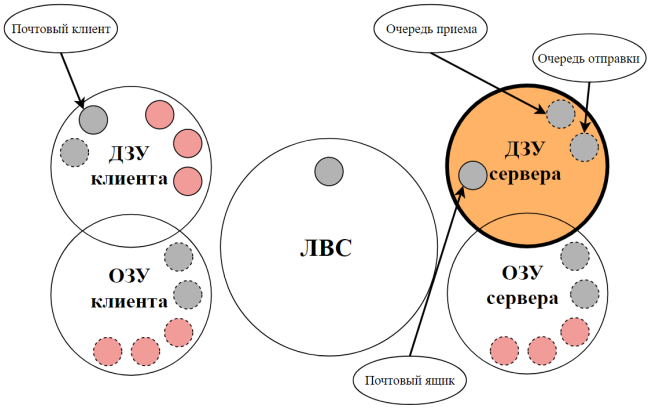


Рисунок 1. Структура защищаемого объекта и занимаемое им место в системе электронной почты

Для системной оценки нападений выделены соответствующие им показатели уязвимости информации:

1) вероятность того, что злоумышленнику удастся модифицировать информацию при сохранении синтаксических характеристик:

2) вероятность того, что злоумышленнику удастся получить (похитить) защищаемую информацию.

Кроме того, согласно общей модели злоумышленных действий в АСОД несанкционированное воздействие на информацию возможно только при наступлении определенных событий [6]. Для системной оценки нападений были выделены показатели уязвимости информации на основе этих событий:

– вероятность получения нарушителем доступа в соответствующую зону АСОД, причем, зона ДЗУ сервера электронной почты относится к зоне баз данных (рис. 3);

– вероятность проявления в зоне АСОД канала несанкционированного получения информации (КНПИ) во время нахождения в этой зоне.

Рисунок 2. Функции сервера электронной почты

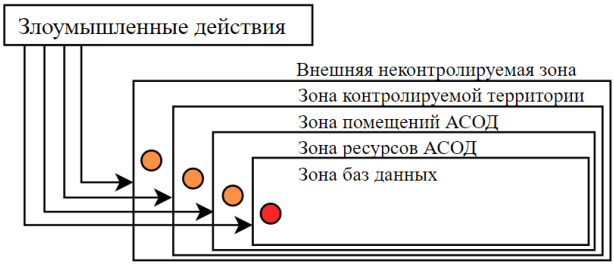


Рисунок 3. Общая модель злоумышленных действий в АСОД

Таким образом, были выделены возможные типы нападений и проведена системная оценка типовых нападений на зону ДЗУ сервера-получателя электронной почты.

Литература

1. А. Ф. Чипига. Информационная безопасность автоматизированных систем. – Учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем». М., 2010.

2. К. М. Сагдеев, В.И. Петренко, А.Ф. Чипига. Физические основы защиты информации. – Учебное пособие. Санкт-Петербург, 2017. (2-е издание, исправленное и дополненное).

3. А. Ф. Чипига, В. С. Пелешенко. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей. – Информационное противодействие угрозам терроризма. 2010 № 15. С. 114-118.

4. А. Ф. Чипига, А. А. Ерещенко, Пелешенко В. С. Модель трехмерной структуры объектов с матрицей доступа. Известия ЮФУ. Технические Науки. 2009. № 11 (100). С. 172-176.

5. А. Ф. Чипига, А. А. Ерещенко. Объектный подход к модели разграничения доступа в компьютерных системах. – Информационное противодействие угрозам терроризма. 2005. № 5. С. 122-128.

6. А. Ф. Чипига, Д. М. Марков, Г. В. Слюсарев. Влияние упакованных форматов протоколов измерений на скорость обработки данных в адаптивных системах спутниковой связи. – Фундаментальные исследования. 2015. № 11. С. 759.

СТРУКТУРА ПРОГРАММНОГО ПРОДУКТА ДЛЯ НАХОЖДЕНИЯ ЗАПРЕЩЕННОГО ТЕКСТОВОГО КОНТЕНТА НА ЛОКАЛЬНЫХ КОМПЬЮТЕРАХ

А. В. Суслов
руководитель – д-р техн. наук, доцент ***И. М. Ажмухамедов***
Астраханский государственный университет, г. Астрахань

Статья посвящена анализу методов и программных средств для обнаружения запрещенного текстового контента на локальном компьютере на основе рассмотрения полной карты заданной директории. Результат исследования наиболее распространенных решений, основной задачей которых является текстовый поиск, показал, что основным недостатком является невозможность комплексного поиска требуемой информации. Это снижает успешность нахождения запрещенного контента.

В работе предложен способ повышения эффективности поиска текстового контента путем разработки программного обеспечения, осуществляющего поиск запрещенного текстового контента на локальном компьютере, основывающийся на анализе полной карты заданной директории.

Ключевые слова: текстовый поиск, программирование, запрещенный контент, программное обеспечение, разработка ПО, методики поиска, анализ директорий.

Развитие компьютерных технологий открыло для человечества небывалые возможности для автоматизации умственной работы и привело к созданию большого числа различных информационных систем, а также появлению принципиально новых технологий. Требование обеспечить высокий уровня информационной безопасности (ИБ) в этих технологиях является одной из приоритетных задач, решаемых как коммерческими организациями, так и государственными учреждениями [5].

Одной из значительных проблем, возникших в связи с развитием информационных технологий, является неконтролируемое распространение

разрушительного и запрещенного контента в информационном пространстве Российской Федерации (РФ).

Согласно статье 29 пункту 4 Конституции РФ: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом» [2]. Однако некоторые виды информации, направленные на разжигание межнациональной, религиозной, межрасовой розни, содержащие призывы к «подрыву» авторитета государственной, законно-выбранной власти, также имеющие суицидальную направленность и т.п., запрещены к распространению в РФ [4]. При рассмотрении таких фактов в контексте проведения оперативно-розыскных и следственных мероприятий, возникает необходимость в изучении машинных носителей с целью установления наличия деструктивной и запрещенной информации.

В связи с тем, что объем информации, хранящейся на локальном компьютере, очень велик и может доходить до десятков и сотен терабайт, ручной поиск становится практически невозможным. Поэтому весьма актуальной является разработка инструментария, позволяющего автоматизировать процесс поиска запрещенной информации на компьютере. Использование существующих программ контекстного поиска, в большинстве случаев нецелесообразно, поскольку условия поиска в этих программах необходимо вводить вручную.

Структуру хранения данных на машинном носителе можно представить в виде разветвленного графа, а значит, для сканирования данной структуры используется алгоритм поиска на графе. В связи с тем, что, для правильной работы программного обеспечения для поиска информации, проверять необходимо все файлы, алгоритм поиска должен являться неинформированным. Неинформированный поиск - поиск, в котором дополнительная информация о состояниях, отличных от того, которое будет частью задачи, не используется.

На рис. 1 представлена структура разработанного программного обеспечения, в свою очередь, на рис. 2 приведена диаграмма потоков данных.

Для корректной обработки различных типов файлов были подключены следующие сторонние модули:

- обработчик Microsoft Office Word;
- обработчик Microsoft Office PowerPoint;
- обработчик Microsoft Office Excel;
- просмотр и анализ CSV файлов;
- просмотр и анализ архивов;
- подбор простых паролей для зашифрованных архивов;

Рисунок 1. Общая структура программного обеспечения

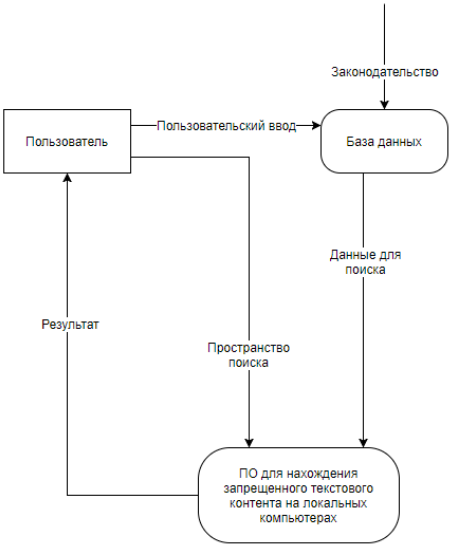


Рисунок 2. Диаграмма потоков данных

- анализ изображений, содержащих текстовую информацию;
- просмотр и анализ шестнадцатеричного кода файлов;
- преобразователь бинарных изображений в текстовые файлы;
- модуль подключения и обновления внешней базы данных.

Внешняя база данных создается на основе списка ключевых слов, полученных во время автоматического анализа запрещенного контента. Сгенерированный список может использоваться для поиска и идентификации документов, содержимое которых аналогично тем, чье распространение

запрещено. База содержит в себе список слов с вариантами склонений и опечаток.

Для выявления сильных и слабых сторон существующих решений поиска информации было проведено сравнение по основным характеристикам. Результаты сравнения программ, осуществляющих поиск деструктивной и запрещенной информации представлены в табл. 1.

Таблица 1

Сравнение с аналогами

	dtSearch Desktop	Ищейка Проф Deluxe	Copernic Desktop Search	ISYS Desktop	SearchInform	Терьер	Созданное ПО
Индексация	+	+	+	+	+	+	+
Русификация	-	+	-	+	+	+	+
Морфологический поиск	+	-	-	-	+	+	+
Поиск по звучанию	+	-	-	-	-	-	-
Поиск с коррекцией ошибок	+	-	-	-	-	-	+
Поиск синонимов	+		-	-	-	-	-
Поиск фраз	+	-	+	+	+	+	+
Поиск по атрибутам	+	+	-	-	-	-	+
Выбор расширений	+	-	+	+	+	+	+
Поддержка поиска содержимого на русском	+	+	-	+	+	+	+
Поиск коллекции значений	+	-	-	+	-	+	+
Анализ изображений и PDF-файлов	-	-	-	-	-	-	+

Результаты тестирования (табл. 2) и сравнения свидетельствуют о том, что разработанное ПО имеет ряд преимуществ перед существующими продуктами, а именно:

- высокая скорость работы;
- меньший размер файла индекса;
- поиск с коррекцией ошибок;
- поиск по атрибутам;
- анализ изображений и PDF-файлов.

Таблица 2

Экспериментальная проверка

	dtSearch Desktop	Ищейка Проф Deluxe	Copernic Desktop Search	ISYS Desktop	SearchInform	Терьер	Созданное ПО
Время индексации 20 Гб данных	6ч. 13м.	38ч. 46м.	10ч. 51м.	6ч. 13м.	3ч. 17м.	3ч. 14м.	2ч. 58м.
Размер файла индекса	7,9 Гб	19 Гб	6,7 Гб	7,9 Гб	4,4 Гб	4,2 Гб	4 Гб

Используя современные методы разработки, было создано программное обеспечение, которое позволяет, благодаря большому количеству успешно обрабатываемых форматов, захватывать больший объем данных и, в отличие от существующих аналогов, использовать внешнее хранилище данных правил поиска. Эти преимущества делают программу конкурентоспособной продукцией, направленной на поиск разрушительной и запрещенной информации.

Литература

1. Информационная безопасность предприятия – SearchInform [Электронный ресурс]. URL: https://searchinform.ru/ (дата обращения: 25.03.2018).
2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ).
3. ООО "Центр безопасности информации" [Электронный ресурс]. URL: http://www.cbi-info.ru (дата обращения: 25.03.2018).
4. Статья 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 19.02.2018).
5. Суслов А.В., Сологубова Е.М «Структура программного обеспечения для нахождения запрещенного текстового контента на локальных компьютерах» // Проблемы информационной безопасности: Материалы VII Всероссийской заочной Интернет-конференции 20 – 21 февраля 2018 года - Ростов-н/Д, Издательство ООО «АзовПринт», 2018. С. 129-132.
6. DtSearch – Text Retrieval / Full Text Search Engine [Электронный ресурс]. URL: http://www.dtsearch.com/ (дата обращения: 25.03.2018).
7. ISYS Search Software [Электронный ресурс]. URL: http://www.isysdemo.com (дата обращения: 25.03.2018).
8. Search Technology to instantly find files, emails, documents & much more! [Электронный ресурс]. URL: http://www.copernic.com (дата обращения: 25.03.2018).

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕТЯХ

Э. А. Титов
руководитель – канд. физ.-мат. наук, доцент ***М. А. Лапина***
Северо-Кавказский федеральный университет, г. Ставрополь

Почему беспроводные сети считаются более уязвимыми, чем кабельные? В проводных сетях данные могут быть перехвачены только в том случае, если злоумышленник получит физический доступ к среде передачи. Злоумышленнику даже не обязательно пребывать на территории компании, достаточно попасть в зону распространения радиосигнала.

Ключевые слова: безопасность сети, беспроводная сеть, Wi-Fi, WEP, WPA2.

При создании беспроводной сети подразумевается ряд действий, направленных на обеспечение безопасности получаемой инфраструктуры. Зачастую из этого списка действий не выполняется вообще ничего. Широкое распространение беспроводных технологий привело к возникновению большего количества злоумышленников, иногда стандартные средства защиты не обеспечивают нужный уровень безопасности. Изначальная уязвимость беспроводной сети состоит в том, что её могут «прощупать» не только из Интернета, но и любой, кто находится в непосредственной близости к точке доступа, что может привести ко вторжению или отказу работы, в публичных сетях злоумышленник может осуществлять перехват трафика пользователей и другую деятельность. Готовясь к обеспечению безопасности беспроводных сетей, прежде всего необходимо установить, что может им угрожать.

Пассивная атака – перехват сигналов беспроводной сети аналогичен прослушиванию радиопередачи. Достаточно иметь ноутбук и анализатор беспроводных протоколов. Можно уменьшить вероятность несанкционированного подключения к сети путём уменьшения мощности сигнала, но не следует оставлять без внимания возможность «прослушивания» трафика, поэтому для безопасной работы в беспроводных сетях необходимо шифровать передаваемую информацию.

Активная атака – небезопасно оставлять точку доступа открытой, подсоединенной к локальной сети, так как это является «открытой дверью» для злоумышленника и чревато утечкой конфиденциальных данных. Незащищенные беспроводные сети позволяют обойти межсетевые экраны и настройки безопасности.

Необходимо следить за несанкционированными точками доступа, которые могут установить сами сотрудники. Такая точка вполне может служить целям злоумышленника. Целью атаки так же могут быть сотрудники, работающие дистанционно через компьютеры с сетевыми картами, настроенными по умолчанию и подключенными напрямую к сети рабоче-

го места, так как любой находящийся рядом злоумышленник может перехватить трафик.

Отказ в обслуживании – целью злоумышленника является вывод сети из строя. Такая атака может быть достигнута несколькими способами:

1. Рассылка ARP ответов, с целью нарушения маршрутизации.
2. Внедрение несанкционированного DHCP сервера.
3. Отключение пользователей от сети.

Методы защиты беспроводной сети

Разграничение доступа по MAC-адресам, фильтрацию можно осуществлять тремя способами:

1. Точка доступа позволяет получить доступ станциям с любым MAC-адресом;
2. Точка доступа позволяет получить доступ только станциям, чьи MAC-адреса находятся в доверительном списке;
3. Точка доступа запрещает доступ станциям с MAC-адресами в «черном списке».
4. Сокрытие SSID, идентификатор сети может быть скрытым, тогда подключаясь, клиенту придется вручную прописать его, эта мера не делает сеть более надежной так как значение SSID можно подслушать через Probe response, но понижает её гибкость и может вызвать проблемы у клиентов.

Методы аутентификации

Открытая аутентификация – в запросе аутентификации есть только MAC-адрес клиента, точка доступа отвечает подтверждением, либо отказом. По сути этот способ является защитой на основе MAC, что небезопасно.

Аутентификация с общим ключом, например, с помощью алгоритма WEP (Wired Equivalent Privacy). Клиент запрашивает у точки аутентификацию, получает подтверждение, содержащее 128 байт случайной информации. Клиент шифрует эту информацию алгоритмом WEP и отправляет точке с запросом на ассоциацию, затем точка расшифровывает этот текст и сравнивает с исходными данными. При совпадении, клиент подключается к сети. Эта схема уязвима к атаке «человек посередине». Протоколы аутентификации:

WPA (Wi-Fi Protected Access) – этот вариант является улучшенной версией WPE, включает два варианта аутентификации: с помощью RADIUS-сервера и с помощью предустановленного ключа.

WPA2 – финальный вариант стандарта безопасности беспроводных сетей, в основе лежит блочный шифр AES. По сравнению с WPA система аутентификации почти не отличается.

CCKM (Cisco Centralized Key Managment) – вариант от фирмы CISCO, поддерживается роуминг между точками доступа после аутентификации на RADIUS-сервере.

Таким образом, при правильном построении радиосети наиболее вероятную угрозу безопасности представляет нарушение физической целостности, нехарактерное для проводных сетей. Поэтому необходимо учитывать все варианты атак и следить за пользователями в сети, которые могут стать объектом атак, либо перейти к незащищенному соединению из корпоративной сети. Наличие современного оборудования и многоуровневой безопасности, которая включает использование современных методов шифрования и аутентификации может свести угрозы сети практически к нулю.

Литература

1. Stewart S. Miller, Wi-fi Security, 2003.

2. Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. Л., Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005.

3. Гордейчик С. В., Дубровин В. В., Безопасность беспроводных сетей. Горячая линия - Телеком, 2008.

АНАЛИЗ МЕТОДОВ ШИФРОВАНИЯ БЕСПРОВОДНЫХ СЕТЕЙ WI-FI

Н. Ю. Унтевский

руководитель – канд. техн. наук, доцент ***Т. В. Минкина***

Северо-Кавказский федеральный университет, Ставрополь

В данной статье подробно представлена процедура шифрования данных, а также рассмотрены различные методы шифрования беспроводных сетей. Также проведен анализ, соизмеримы между собой и выявлены наиболее подходящие способы шифрования, в зависимости от целей эксплуатации.

Ключевые слова: Wi-Fi, WEP, WPS, WPA/WPA2, шифрование, передача данных, роутер, конфиденциальность, тип шифрования.

Для начала разберем, что же такое шифрование и в чем заключается основная цель данного метода. Шифрование – преобразование информации основной задачей которого является ограничение неавторизованных пользователей от данных и в это же время предоставление авторизованным пользователям доступ к ним. В первую очередь шифрование отвечает за конфиденциальность передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма. Пользователи являются авторизованными, если они обладают определённым аутентичным (аутентификация – процедура проверки подлинности) ключом. Вся сложность и, собственно, задача шифрования состоит в том, как именно реализован этот процесс. В целом, шифрование состоит из двух составляющих – зашифровывание и расшифровывание. и выглядит эта процедура следующим образом:

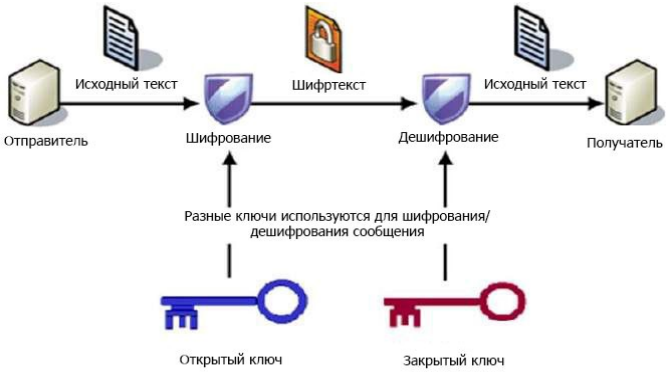


Рисунок 1. Процесс шифрования и дешифрования

Сейчас речь пойдет о различных методах шифрования беспроводных сетей Wi-Fi.

WEP шифрование – тип шифрования WEP появился ещё в 90-х и являлся первой вариацией защиты Wi-Fi сетей: выступал он как аналог шифрования в проводных сетях и применял шифр RC4. На тот момент передаваемые данные можно было зашифровать только тремя распространенными алгоритмами – Neesus, Apple и MD5 – но ни один из них не обеспечивал необходимый уровень безопасности. В 2004 году в IEEE данный стандарт был признан устаревшим так как он окончательно перестал обеспечивать безопасное подключение к сети. Во многих современных роутерах этот тип шифрования вовсе исключен из списка возможных для выбора:

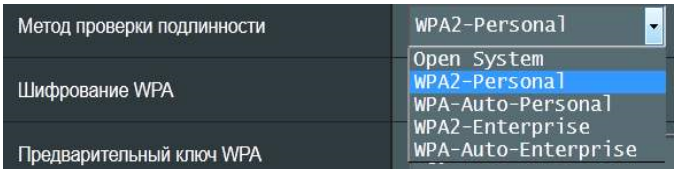


Рисунок 2. Список доступных типов шифрования

На сегодняшний WEP шифрование не стоит использовать, т.к. этот метод не является криптостойким.

Wi-Fi шифрование WPS, он же QSS – это стандарт, при котором можно обойтись без использования пароля для подключения к беспроводной сети. Данная технология позволяет пользователю быстро, просто и безопасно настроить беспроводную сеть, не вникая в тонкости работы Wi-Fi и протоколов шифрования. По факту это «легальный» метод обхода защиты по паролю вообще, но интереснее всего то, что широкую популярность он обрел благодаря очень серьёзному просчёту в самой системе допуска – это

спустя годы после печального опыта с WEP**.** В данном случае необходимо лишь нажать на кнопку с надписью WPS на роутере. Эта технология позволяет подключиться к точке доступа по восьмизначному коду, но зачастую достаточно лишь четырех. Этим фактом с удовольствием пользуются многочисленные хакеры, которые достаточно быстро (за 3 – 15 часов) взламывают сети wifi при помощи различных утилитов, в связи с этим данное соединение также не рекомендуется использовать.

Тип шифрования WPA/WPA2. Куда благоприятнее обстоят дела с шифрованием WPA. Вместо уязвимого шифра RC4 используется шифрование AES, длина пароля в котором варьируется (8 – 63 бита). Этот тип шифрования обеспечивает средний уровень безопасности, и вполне подходит для простых wifi маршрутизаторов. При этом существует две его разновидности.

Тип PSK (Pre-Shared Key) – к точке подключаются при помощи заранее заданного пароля.

Enterprise – пароль автоматически генерируется для каждого узла при этом проходя проверку на серверах RADIUS.

Тип шифрования WPA2 является улучшенной версией WPA. В данном протоколе используется RSN, в основе которого лежит шифрование AES. Тип шифрования WPA2, как и немного уступающий ему аналог WPA, имеет два режима работы: PSK и Enterprise. Абсолютно все Wi-Fi оборудование поддерживает WPA2 еще с 2006 года, соответственное его можно выбрать для любого маршрутизатора.

Преимущества шифрования WPA2 перед WPA:

1) Вместо статических ключей шифрования они генерируются в процессе подключения к роутеру.

2) Использование алгоритма Michael для контроля целостности передаваемых сообщений.

3) Существенно увеличена длина вектора инициализации.

Теперь сравним все эти типы шифрования между собой, чтобы наглядно убедиться в преимуществе одних над другими: (WPS не участвует в данном сравнении т.к. основной целью его создания было все же упрощение процесса настройки беспроводной сети, а не предоставление защиты).

Кроме того, тип шифрования Wi-Fi выбирать стоит в зависимости от того, где используется ваш роутер:

1) Шифрование WEP, TKIP и CKIP вообще не стоит использовать, ибо на наши дни он невероятно устарел и в связи с этим легко поддается взлому;

2) Для домашней точки доступа подойдет WPS, так как он невероятно удобен в использовании, но при этом он не обеспечит должный уровень защиты, о чем тоже не стоит забывать.

Рисунок 3. Таблица сравнения WEP vs WPA vs WPA2

3) Также для домашней точки доступа вполне подойдет WPA/WPA2 PSK ведь он обеспечивает достаточный уровень защиты и не вызывает особых сложностей при использовании;

4) Для корпоративной сети стоит выбрать WPA/WPA2 Enterprise, ведь он отлично защитит вашу сеть от неавторизированных пользователей.

Литература

1. Авдошин С. М. Дискретная математика. Модулярная алгебра, криптография, кодирование. ДМК-Пресс, 2017. 352 с.

2. Адаменко, М.В. Основы классической криптологии. Секреты шифров и кодов. ДМК-Пресс, 2012. 256 с.

3. https://ru.wikipedia.org/wiki/Шифрование

4. Лапина М. А., Лапин В. Г. MICROSOFT OFFICE: EXCEL, POWERPOINT/ Практикум / Ставрополь, 2009. Том Часть 2.

5. Петренко В. И., Мирошников Д. А., Емельянов Е. А. Обзор современных средств сетевой защиты информации//Проблемы автоматизации. Региональное управление. Связь и автоматика («ПАРУСА-2015»), Материалы IV Всероссийской научной конференции молодых ученых, аспирантов и студентов, Геленджик, 2015.

6. Домашенко А. А., Беспутнев В. В., Минкина Т. В. Актуальность защиты информации в сети интернет //Материалы III Всероссийской научно-технической конференции «Студенческая наука для развития информационного общества». СКФУ(Ставрополь), 2015. С.174-176.

МЕТОДЫ БОРЬБЫ С ФИШИНГОВЫМИ АТАКАМИ

А. Н. Урывский
руководитель – канд. техн. наук, доцент ***В. В. Антонов***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрена проблема защиты от фишинговых атак. Проведён обзор основных рисков и угроз, а также технологий и методов защиты от них.

Ключевые слова: Фишинг, phishing, угрозы, технологии защиты, спам, антивирус, электронная почта, безопасность.

Фишинг – это один из видов сетевых преступлений, заключающийся в получении от людей конфиденциальных, идентификационных или секретных данных. Средства массовой информации постоянно публикуют списки организаций, чьи клиенты, или даже сотрудники, подверглись фишинговым атакам. Несмотря на то, что жертвы таких атак пытаются обезопасить себя всеми возможными методами и средствами, угроза фишинга постоянно растет. [1] Разработка новых приемов атак ведется ежедневно, однако организации так же предпринимают активные меры борьбы с таким видом преступлений, вводя строгие правила в фильтрации спама.

Сам фишинг основан на изучении всех факторов и человеческих слабостей, которые определяют склонность людей «клевать на удочку». Совершенствуя технологии защиты и обучения пользователей, можно пресечь попытки мошенничества. Для борьбы с фишингом необходимо объединить усилия специалистов по защите информации, правоохранительных органов и, конечно же, обычных пользователей.

Цель такого вида сетевой атаки состоит в том, чтобы побудить человека перейти на какой-нибудь сторонний сайт, ответить на письмо, или даже позвонить по определенному номеру и выдать мошенникам свои персональные данные или конфиденциальную информацию. Порой достаточно перейти по ссылке или открыть прикрепленный к письму файл, чтобы компьютер оказался заражен вредоносной программой, которая позволит фишеру (phisher, искаженный вариант английского слова fisher – «рыбак») извлекать нужную информацию или управлять самим компьютером жертвы для дальших атак. Хотя у каждой фишинговой атаки есть свои особенности, результат обычно один и тот же – беспечные жертвы предоставляют мошенникам секретную и конфиденциальную информацию.

Фишинг атаки являются результатом объединения методов технического обмана и факторов социальной инженерии. В большинстве случаев фишер убеждает жертву намеренно выполнить ряд действий, которые впоследствии могут обеспечить доступ к конфиденциальной информации. Мошенник должен представляться официальным или доверенным источником, тем самым внушая доверие жертве.

Существует так же онлайн фишинг, под которым подразумевается, что злоумышленник копирует какие-либо известные сайты, использует похожие доменные имена и практически идентичный дизайн страниц, а потом завлекает на него потенциальных жертв, которым позже предлагают произвести некоторые операции. Как правило, используются методы психологического воздействия, и жертва до последнего момента может не понять, что ее обманули. [3]

Однако, многочисленные предупреждения, практически ежедневно появляющиеся в сети Интернет, делают подобные методы мошенничества все менее эффективными.

На данный момент существует несколько «традиционных» методов противодействия фишинговым атакам. Ниже приведены некоторые из них [1]:

1. Одноразовые пароли. Классические пароли являются многоразовыми, т.е. пользователь вводит один и тот же пароль каждый раз при прохождении процедуры аутентификации. Однако такие пароли могут быть перехвачены злоумышленниками, а позже неоднократно использоваться без ведома жертвы. Одноразовый пароль, в свою очередь, используется только один раз, и при каждом запросе на предоставление доступа, пользователь вводит новый пароль. Однако этот метод не защищен от атаки под названием «человек посередине» (англ. Man in the middle). Суть заключается в том, что во время информационного обмена между пользователем и сервером, злоумышленник может представиться сервером, тем самым являясь как бы посредником, без ведома жертвы.
2. На практике, метод защиты с помощью одноразовых паролей используется не так часто. Для повышения безопасности применяется установленное защищенное соединение еще до аутентификации, например, при использовании протокола SSL.
3. Уникальный дизайн сайта. Суть этого метода следующая: например, клиент банка при заключении договора выбирает одно из предложенных изображений, которое в дальнейшем будет показываться при входе на сайт этого банка. В том случае, если пользователь увидит другое изображение, или вовсе не увидит, он должен покинуть «поддельный» сайт и сообщить об этом службе безопасности банка. На практике этот способ практически не используется, так как пользователь должен сначала идентифицироваться на сайте, введя логин, и только потом получить свою картинку. Злоумышленник, в свою очередь, может подготовить поддельный сайт и таким образом узнать эту информацию.
4. Односторонняя аутентификация. Как говорилось ранее, такой метод борьбы с фишинговыми атаки является одним из лучших. Использование протокола безопасных соединений SSL (Secure Sockets Layer) обеспечивает защищенный обмен данными между сервером и пользователем. Протокол позволяет аутентифицировать не только сервер, но и пользователя, однако на практике почти всегда применяется только односторонняя

аутентификация. Для установления SSL-соединения необходимо, чтобы сервер имел цифровой сертификат, который обычно выдается и заверяется третьей доверенной стороной, в роли которой выступают удостоверяющие центры. Список таких центров обычно хранится в реестре операционной системы или в настройках браузера, и именно эти списки подвергаются атакам со стороны злоумышленников. Мошенники, выдавая фишинговому сайту сертификат от поддельного удостоверяющего центра и добавляя этот центр в доверенные, могут успешно осуществить атаку, не вызывая никаких подозрений у своих жертв.

5. URL-фильтрация. В корпоративных сетях фильтрация сайтов применяется не только для ограничения нецелевого использования сети Интернет сотрудниками, но и как защита от фишинговых атак. Во многих антивирусных средствах защиты данный способ борьбы с поддельными сайтами является единственным. Выявлением фишинговых сайтов и внесением их в черные листы занимаются многие компании - от производителей антивирусных программ и правоохранительных органов, до банков и платежных систем. Совместные мероприятия заинтересованных сторон и сотрудничество хостинговыми компаниями позволяют оперативно закрывать поддельные сайты. Совместные усилия направлены на максимально быстрое обновление черных списков и блокирование работы сайтов злоумышленников.

Постоянное совершенствование антифишинговых фильтров и осведомление пользователей о новых типах фишинговых атак поможет сократить число жертв фишинга. Помимо этого, может помочь координация международных усилий правоохранительных органов и поиск способов сделать фишинг менее прибыльным. Тем не менее, борьба с этим видом сетевых преступлений остается чем-то похожим на гонку вооружений, и полностью победить его нельзя, поэтому пользователям нужны все возможные виды защиты, а также их собственная бдительность.

Литература

1. Обзор методов борьбы с фишинговыми атаками – Электронный ресурс URL: http://www.itsec.ru/articles2/focus/obzor-metodov-bor-s-fishingov-atakami-chast-1

2. Что тако фишинг и методы борьбы с ним - Электронный ресурс URL: https://barbadosmaney.ru/fishing-i-kak-ot-nego-zashhititsya.

3. Фишинг – Электронная публикация со свободной энциклопедии Wikipedia.org – URL: https://ru.wikipedia.org/wikiФишинг

4. Фишинг – Защита от фишинга – Электронный ресурс URL: https://ru.norton.com/security_response/phishing.jsp

БЕЗОПАСНОСТЬ WI-FI СЕТЕЙ

Н. М. Хабалонов
Северо-Кавказский федеральный университет г. Ставрополь

Пароль и фильтрация по MAC-адресу должны защитить вас от взлома. На самом деле безопасность в большей степени зависит от вашей осмотрительности. Неподходящие методы защиты, незамысловатый пароль и легкомысленное отношение к посторонним пользователям в домашней сети дают злоумышленникам дополнительные возможности для атаки. Из этой статьи вы узнаете, как можно взломать WEP-пароль, почему следует отказаться от фильтров и как со всех сторон обезопасить свою беспроводную сеть.

Ключевые слова: Надежность ключей безопасности, WPA2.

Ваша сеть не защищена, следовательно, рано или поздно к вашей беспроводной сети подсоединится посторонний пользователь — возможно даже не специально, ведь смартфоны и планшеты способны автоматически подключаться к незащищенным сетям. Если он просто откроет несколько сайтов, то, скорее всего, не случиться ничего страшного кроме расхода трафика. Ситуация осложнится, если через ваше интернет-подключение гость начнет загружать нелегальный контент.

Если в вашей беспроводной сети используется незащищенное соединение, следует быть особенно осторожным с контентом, который расположен в папках с общим доступом, так как в отсутствие защиты он находится в полном распоряжении остальных пользователей. Отсутствие должной защиты в беспроводной сети является источником и других опасностей, так как хакеры могут с помощью специальных программ (снифферов) выявлять все незащищенные соединения. Таким образом, взломщикам будет несложно перехватить ваши идентификационные данные от различных сервисов.

Наилучшую защиту обеспечивает технология WPA2, которая применяется производителями компьютерной техники еще с 2004 года. Большинство устройств поддерживают этот тип шифрования. Но, как и другие технологии, WPA2 тоже имеет свое слабое место: с помощью атаки по словарю или метода bruteforce («грубая сила») хакеры могут взламывать пароли – правда, лишь в случае их ненадежности. Словари просто перебирают заложенные в их базах данных ключи – как правило, все возможные комбинации чисел и имен. Пароли наподобие «1234» или «name» угадываются настолько быстро, что компьютер взломщика даже не успевает нагреться.

Метод bruteforce предполагает не использование готовой базы данных, а, напротив, подбор пароля путем перечисления всех возможных комбинаций символов. Таким способом взломщик может вычислить любой ключ – вопрос только в том, сколько времени ему на это потребуется.

В инструкциях по безопасности рекомендуется пароль минимум из восьми символов, а лучше – из шестнадцати. Прежде всего важно, чтобы он состоял из строчных и прописных букв, цифр и специальных символов. Чтобы взломать такой пароль, злоумышленнику потребуются десятилетия.

Пока еще ваша сеть защищена не до конца, так как все пользователи внутри нее имеют доступ к вашему маршрутизатору и могут производить изменения в его настройках. Некоторые устройства предоставляют дополнительные функции защиты, которыми также следует воспользоваться.

Как и любая программа, прошивка роутера несовершенна — небольшие недоработки или критические дыры в системе безопасности не исключены. Обычно информация об этом мгновенно распространяется по Сети. Регулярно проверяйте наличие новых прошивок для вашего роутера (у некоторых моделей есть даже функция автоматического обновления). Еще один плюс перепрошивок в том, что они могут добавить в устройство новые функции.

Периодический анализ сетевого трафика помогает распознать присутствие незваных гостей. В интерфейсе управления роутером можно найти информацию о том, какие устройства и когда подключались к вашей сети. Сложнее выяснить, какой объем данных загрузил тот или иной пользователь.

Надежность ключей безопасности

– WEP (WIRED EQUIVALENT PRIVACY). Использует генератор псевдослучайных чисел (алгоритм RC4) для получения ключа, а также векторы инициализации. Так как последний компонент не зашифрован, возможно вмешательство третьих лиц и воссоздание WEP-ключа.

– WPA (WI-FI PROTECTED ACCESS) Основывается на механизме WEP, но для расширенной защиты предлагает динамический ключ. Ключи, сгенерированные с помощью алгоритма TKIP, могут быть взломаны посредством атаки Бека-Тевса или Охигаши-Мории. Для этого отдельные пакеты расшифровываются, подвергаются манипуляциям и снова отсылаются в сеть.

– WPA2 (WI-FI PROTECTED ACCESS 2) Задействует для шифрования надежный алгоритм AES (Advanced Encryption Standard). Наряду с TKIP добавился протокол CCMP (Counter-Mode/CBC-MAC Protocol), который также базируется на алгоритме AES. Защищенную по этой технологии сеть до настоящего момента взломать не удавалось. Единственной возможностью для хакеров является атака по словарю или «метод грубой силы», когда ключ угадывается путем подбора, но при сложном пароле подобрать его невозможно.

Литература

1. https://ru.wikipedia.org/wiki/
2. https://habr.com/

СИСТЕМНАЯ ОЦЕНКА ТИПОВЫХ НАПАДЕНИЙ НА ЗОНУ ОЗУ СЕРВЕРА РЕЗЕРВНОГО КОПИРОВАНИЯ

Т. А. Хахалев
Северо-Кавказский федеральный университет, г. Ставрополь

Произведена системная оценка типовых нападений на зону ОЗУ сервера резервного копирования.
Ключевые слова: системная оценка, типовые нападения, сервер резервного копирования, информационная безопасность.

Зоне оперативной памяти сервера резервного копирования могут угрожать следующие типовые нападения:

1) Восстановление на фиктивный сервер: задачей данного нападения является похищение сообщений электронной почты путем подлога сбоя на санкционированном сервере почты и последующего перехвата сеанса восстановления данных из резервной копии с подавлением легитимного сервера электронной почты;

2) Изъяны системы резервного копирования: цель этого нападения состоит в получении контроля над сервером резервного копирования, в следствие воздействия на ошибки ПО и уязвимостей настроек;

3) Резервное копирование с ложного сервера: в этом случае, целью является резервное копирование мнимой информации на сервер, с последующим ложным срабатыванием сбойной ситуации и восстановления с подложной резервной копии. Такое нападение происходит при подавлении средства резервного копирования санкционированного сервера;

4) Перехват электронных сообщений в ОЗУ: здесь целью нападения является получение доступа к электронным сообщениям в ОЗУ сервера резервного копирования с помощью программной закладки, на этапе подготовки к сохранению на резервном сервере.

Для защиты от этих нападений в зоне ОЗУ сервера резервного копирования используются рубежи защиты. В создании рубежа защиты сервера резервного копирования участвуют встроенные средства защиты операционной системы и ПО системы резервного копирования.

Для системной оценки этих нападений будет использоваться Общая система оценки уязвимостей. Она состоит из трех частей: базовая, временная и контекстная метрики. Каждая часть – это число от 0 до 10 и вектор.

Далее, подробно будет разобрана первая уязвимость, для остальных будут представлены лишь оценка и вектор.

Для примера будет использовано первое типовое нападение: «Использование уязвимостей системы резервного копирования»:

Базовые метрики:

Способ получения доступа (AV). Отображает, как эксплуатируется уязвимость: Сетевой (N);

Сложность получения доступа (AC). Сложность эксплуатации, если злоумышленник получил доступ к целевой системе: Высокая (H);

Аутентификация (Au). Количество этапов аутентификации, которые злоумышленник должен пройти в целевой системе, чтобы эксплуатировать уязвимость: Множественная (M);

Влияние на конфиденциальность (C): Полное (C);

Влияние на целостность (I): Частичное (P);

Влияние на доступность (A): Частичное (P);

Временные метрики:

Возможность использования (E): Функциональная (F);

Уровень исправления (RL): Официальное (OF);

Степень достоверности отчета (RC): Подтверждена (C);

Контекстные метрики

Вероятность нанесения косвенного ущерба (CDP). Средняя, повышенная (MH);

Плотность целей (TD): Высокая (H);

Требования к безопасности (CR, IR, AR): Высокие (H).

Таким образом, вектор данной угрозы – (AV:N/AC:H/Au:M/C:C/I:C/A:P/E:F/RL:OF/RC:C/CDP:MH/TD:H/CR:H/IR:H/AR:H);

Базовая оценка (BS): 6.4;

Временная оценка (TS): 5.3;

Контекстная оценка (ES): 7.4;

Для угрозы «Резервное копирование с ложного сервера»:

Вектор:

(AV:N/AC:H/Au:M/C:C/I:C/A:N/E:F/RL:OF/RC:C/CDP:H/TD:H/CR:H/IR:H/AR:H);

Базовая оценка (BS): 6.2;

Временная оценка (TS): 5.1;

Контекстная оценка (ES): 7.8;

Для угрозы «Восстановление на ложный сервер»:

Вектор:

(AV:N/AC:H/Au:M/C:C/I:C/A:P/E:F/RL:OF/RC:C/CDP:H/TD:H/CR:H/IR:H/AR:H);

Базовая оценка (BS): 6.4;

Временная оценка (TS): 5.3;

Контекстная оценка (ES): 7.8;

Для угрозы «Перехват электронных сообщений в оперативной памяти»:

Вектор:

(AV:L/AC:H/Au:N/C:C/I:C/A:P/E:F/RL:OF/RC:C/CDP:MH/TD:H/CR:H/IR:H/AR:H);

Базовая оценка (BS): 5.9;

Временная оценка (TS): 4.9;

Контекстная оценка (ES): 7.1;

Литература

1. Чипига А. Ф. Информационная безопасность автоматизированных систем. М: «Гелиос АРВ», 2010. 336 с.

2. Чипига А. Ф. Методология обнаружения и предотвращения угроз и компьютерных атак на информационные системы и психику людей / А. Ф. Чипига, В. С. Пелешенко// Информационное противодействие угрозам терроризма, 2010. С. 114-118.

3. Чипига А. Ф. Модель трехмерной структуры объектов с матрицей доступа / А. Ф. Чипига, А. А. Ерещенко, Пелешенко В.С. //Известия ЮФУ. Технические науки. 2009. С. 172-176.

2. Чипига А. Ф. Объектный подход к модели разграничения доступа в компьютерных системах / А. Ф. Чипига, А. А. Ерещенко // Информационное противодействие угрозам терроризма, 2005. С. 122-128.

ВОПРОСЫ, ВОЗНИКАЮЩИЕ ПРИ ВЫБОРЕ МЕЖСЕТЕВЫХ ЭКРАНОВ ПРИ ОРГАНИЗАЦИИ КОМПЛЕКСНОЙ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ

В. А. Ходакова
руководитель – канд. физ.-мат. наук, доцент ***М. А. Лапина***
Северо-Кавказский федеральный университет, г. Ставрополь

При защите локальной вычислительной сети может существенно помочь технология межсетевого экранирования, внедрение которой может вызвать множество вопросов у сотрудников системы безопасности и IT-отдела. В данной статье описывается, зачем необходимы межсетевые экраны в компании, принципы их выбора и разделения полномочий между различными подразделениями, из чего складывается стоимость компонентов.

Ключевые слова: межсетевой экран, комплексная защита, информационная безопасность, безопасность сети.

Межсетевой экран является методом сохранения безопасности сети больших компаний и различных предприятий, который содержит в себе целый пакет технологий контроля и отслеживания трафика, исключения возможности проникновения и утечки информации, инспектирования данных приложений и четкой координации работ на базе политик.

Когда организация рассматривает возможности потенциального внедрения межсетевых экранов, вопросы появляются как при разработке и конструировании комплексной системы защиты локальной вычислительной сети, так и при попытке обосновать, зачем тратить финансовые средства для покупки каких-либо средств защиты информации и программно-аппаратных комплексов [1, с. 213]. Кроме того, проблемы могут возникнуть и в процессе интеграции и начальной эксплуатации определенного способа защиты, включающего межсетевой экран.

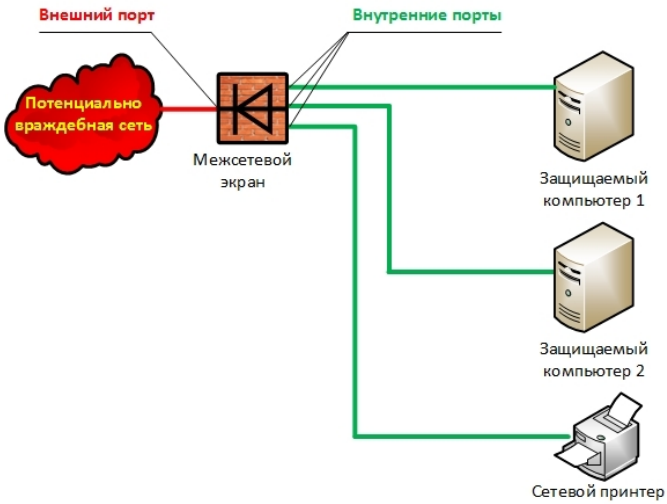


Рисунок 1. Структура системы информационной безопасности, использующая межсетевой экран

Следовательно, в любом предприятии в первую очередь нужно определить, в чем же состоит обязательность внедрения межсетевых экранов. А нужно это с целью разграничения и управляемого контроля доступа к важнейшим составляющим инфраструктуры организации (серверному сегменту, различным службам и сервисам и др.). Также существует необходимость обеспечения регистрации действий пользователей и реализации разрешительной системы допуска к конфиденциальной информации. Конечно, одной из главных задач межсетевого экрана будет являться предотвращение проникновений злоумышленников в объекты защиты ЛВС с целью хищения, модификации, уничтожения информации и вмешательства в функционирование автоматизированных систем.

Учитывая то, что на рынке представлено большое множество отечественных и иностранных межсетевых экранов, подобрать нужный не так легко. Каждая компания, выбирая межсетевой экран для корпоративной сети, учитывает собственные критерии. Некоторые руководители руководствуются лишь стоимостью – чем меньше, тем лучше. Другие смотрят на объем удачных внедрений за определенный промежуток времени или на мнения о производительности и эффективности работы межсетевого экрана. Третьи в первую очередь будут учитывать набор обязательных требований, обозначенных в техническом задании или озвученных руководителем проекта или компании еще до начала выбора устройств.

Но наиболее действенным решением является создание пилотных проектов, способных показать характерные свойства и отличительные чер-

ты определенного межсетевого экрана при его внедрении в инфраструктуру данной компании. В этом случае будет проведена проверка результативности и эффективности выбранного решения и целесообразности его введения в корпоративную сеть ЛВС.

Следующим вопросом, который может возникнуть при выборе межсетевого экрана, является его стоимость и от чего она зависит [2, с. 167]. На данную характеристику могут влиять комплект необходимых опций, подбор совместимой программно-аппаратной платформы, активация лицензии на составляющие и работы, которые нужно провести при интеграции межсетевого экрана в инфраструктуру организации.

Т.к. почти в каждой компании бюджет, направленный на совершенствование информационной безопасности, ограничен, именно вопрос общей стоимости межсетевых экранов становится камнем преткновения. Иногда определенный межсетевой экран покупается именно исходя из небольшой стоимости, хотя его функциональность в компании может оставлять желать лучшего. После покупки возникает необходимость обучения персонала управлению выбранным экраном, происходит перестройка инфраструктуры, определенным образом меняются технологические операции, проводится нормативное документирование процессов [3]. Но спустя какое-то время организация может наткнуться на ограниченность применения: отсутствие незанятых физических портов, наличие «узких» мест в сети, ограниченность параллельно установленных соединений и т.д. Это не дает компании возможность реализации стратегии по своему усовершенствованию без замены данного межсетевого экрана на экран с большими возможностями и более широким спектром опций и функций. Интеграция же другого опять требует вложения денежных средств, коих у компании может не быть, т.к. стоимость нового экрана будет больше предыдущего.

С одной стороны тактика последовательного вложения в совершенствование информационной безопасности более целесообразна. Но она не берет в расчет дополнительные расходы и расходы на интеграцию и обновление составляющих. Вследствие этого, выбирая межсетевой экран, есть смысл выдвигать повышенные требования по эффективности и опциональности. Не стоит гнаться лишь за маленькой ценой.

Порой возникает вопрос о том, кто должен обеспечивать функциональность и возможность успешной эксплуатации межсетевого экрана: подразделения организации, отвечающие за техническое сопровождение или за информационную безопасность. За контроль действий персонала без сомнений несет ответственность администратор информационной безопасности. Но, к примеру, маршрутизация данных внутри ЛВС между различными подразделениями или же доступ в Интернет осуществляется сотрудниками IT-отдела. В этом случае только руководитель организации может решать, в какой отдел отдавать межсетевой экран на сопровождение.

Кроме того, есть и еще один вариант – аутсорсинг межсетевых экранов. Данное решение применяется, если в организации не хватает своих средств для управления и администрирования межсетевого экрана. Но в этом случае наносится вред гибкости и более высокой адаптации при настройке устройств; запросы на передачу доступа требуют больше времени; контроль информационных процессов в режиме онлайн невозможен, т.к. работоспособность межсетевого экрана является ответственностью другой стороны.

Создатели межсетевых экранов утверждают, что их продукты универсальны при обеспечении информационной безопасности корпоративных сетей [4]. Но при этом нужно осознавать, что межсетевой экран в первую очередь фильтрует трафик и контролирует установление рабочей сессии и соединений. Кроме опасностей, существующих на сетевом уровне, есть и другие, предотвращение которых лежит за границами функционирования межсетевого экранирования. К таким опасностям относятся несанкционированный доступ злоумышленников к конфиденциальной информации, возможность нарушения контроля доступа в распределенной локальной вычислительной сети, утечки информации при передаче данных по не зашифрованным или открытым каналам связи и т.д. При всем этом нужно осознавать межсетевой экран является лишь одной из составляющих комплексной системы информационной безопасности, которая требует сложного совокупного подхода [4].

Когда клиенты начинают закупать межсетевые экраны, то они могут столкнуться со множеством пунктов, специально раньше не указанных в документации, чтобы минимизировать общую стоимость. Часто эти в начале не известные требования добавляют немалое количество денежных средств к начальной цене. Но при этом функциональность межсетевого экрана может быть снижена. Следовательно, рассчитывая общую стоимость есть смысл добавлять стоимость таких «латентных» компонентов [5, с.315]. Также стоит учитывать регулярное продление лицензии и функции, за которые нужно платить. Большая часть отечественного рынка производителей межсетевых экранов требует систематично продлевать лицензию на свои продукты. Их стоимость складывается из процента от начальной цены межсетевого экрана и процента от стоимости специально купленных дополнительных функций. Эта цена включает пакет услуг по техподдержке, который определяет производитель, и предоставление обновлений составляющих межсетевых экранов.

Литература

1. Лапонина О. Р. Межсетевое экранирование. Бином, 2014. 343 с.

2. Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. МГТУ им. Н. Э. Баумана, 2002. 306 с.

3. Мэйволд Э. Лекция 10 «Межсетевые экраны» // Безопасность сетей: Информация. – ИНТУИТ, 2006.

4. Фаронов А. Е. Основы информационной безопасности при работе на компьютере. ИНТУИТ, 2016.
5. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – ИНФРА-М, 2011. 416 с.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

Е. В. Черкашин
руководитель – канд. техн. наук, доцент ***В. В. Антонов***
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье рассматривается проблема организации защиты персональных данных на предприятии, актуальность защиты персональных данных, приведён вариант организационных мероприятий по защите информации.
Ключевые слова: персональные данные, информация, оператор, организация, защита информации.

На сегодняшний день организация защиты персональных данных актуальна на любом коммерческом или же государственном предприятии. Обеспечение безопасности информации в любой компании является одной из главных задач в информационной сфере и взаимоотношениях государства, юридических и физических лиц. Необходимо обеспечивать защиту персональных данных в каждой организации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) [4].

Информация является одним из наиболее ценных ресурсов любой компании, поэтому обеспечение защиты информации считается одной из важнейших и приоритетных задач. Для того, чтобы обеспечить целостность и конфиденциальность персональных данных необходимо обеспечить защиту информации как от несанкционированного доступа к ней, так и от случайного уничтожения [1].

Персональные данные каждого работника организации, а также данные граждан относятся к особо защищаемой законом РФ информации. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и осуществляющее обработку персональных данных. Таким образом, при обработке персональных данных оператор обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных. Оператором персональных данных может быть, как один человек, так и

целый отдел или даже организация. Все они занесены в специально созданный реестр операторов персональных данных. Сейчас таких операторов более 230 тысяч.

Ответственность за сбор, обработку, хранение и защиту персональных данных работников организации и клиентов, лежит целиком на работодателе. Поэтому на любом предприятии должен быть установлен порядок работы с персональными данными, а также разработаны документы и мероприятия по организации защиты данных. Для этого на предприятии должно быть разработано и утверждено в соответствии с законодательством «Положение», которое устанавливает порядок обработки и защиты персональных данных [2].

Обеспечение защиты информации, а именно данных сотрудников должно быть направлено, прежде всего, на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности. Любая утечка информации может привести к серьезным проблемам для компании – от значительных финансовых убытков до полной ликвидации. Проблема утечек появилась ещё до появления персонального компьютера (ПК), промышленный шпионаж и переманивание квалифицированных специалистов существовали еще и до эпохи компьютеризации. Так с появлением ПК и интернета возникли новые приемы незаконного получения информации. Если раньше для этого необходимо было украсть и вынести из фирмы целые связки бумажных документов, то сейчас огромные объемы сведений можно запросто записать на флеш-накопителе, помещающемся в кармане. Также сведения можно отправить по сети, прибегнув к использованию семейства руткитов, троянов, бэкдоров, кейлоггеров и ботнетов, либо просто уничтожить посредством вирусов, устроив диверсию.

Таким образом, необходимо решить проблему с защитой персональных данных в организации при помощи организационных мероприятий. В первую очередь необходимо назначить ответственных за обеспечение безопасности персональных данных в организации. Особое внимание следует уделить так называемым специальным категориям персональных данных.

Далее следует провести обследование информационных систем персональных данных организации. Главным смыслом обследования будет, принятие решения о том, является ли организация оператором персональных данных или нет

После этого необходимо определиться с целями обработки каждого вида персональных данных. Целями могут быть:

- обеспечение трудовых взаимоотношений
- обеспечение медицинской деятельности
- исполнение федеральных законов.

Для обработки персональных данных в организации требуется согласие субъекта персональных данных. Таким образом, производится разработка и утверждение документов под названием: «Согласие на обработку персональных данных».

Далее необходимо провести внедрение системы защиты персональных данных.

И наконец, необходимо определиться с техническими средствами защиты персональных данных, они бывают:

- несанкционированного доступа;
- антивирусные средства;
- криптографические средства.

Все применяемые средства должны быть сертифицированы. Далее, после выбора, приобретения, установки средства его необходимо правильно настроить [3].

Таким образом, защита персональных данных, является одной из главных задач как в информационной сфере, так и во взаимоотношениях государства, юридических и физических лиц. Для надежной защиты персональных данных в организации, используется большое количество организационных мероприятий, выполнение которых позволит повысить безопасность персональных данных на предприятии. На данный момент существует огромное количество способов хищения информации, поэтому угрозы персональным данных всегда останутся, таким образом, необходимо использовать всевозможные организационные мероприятия.

Литература

1. Статья по теме «Защита персональных данных в организации» //Сайт [[rstnw.ru]]. URL: http://www.rstnw.ru/7step.html.

2. Статья по теме «Организация защиты персональный данных в организации по ФЗ № 152-ФЗ» // Сайт [[hr-elearning.ru]]. URL: http://hr-elearning.ru/organizaciya-zashhity-personalnyy-dannyx-organizacii/.

3. Статья по теме «Руководство по организации защиты персональных данных» // Сайт [[russianit.ru]]. URL: http://russianit.ru/informationsecurity/4/memo/.

4. Статья по теме «О ЗАКОНЕ» // Сайт [[pointlane.ru]]. URL: http://www.pointlane.ru/-personal/

САБОТАЖ В КОРПОРАТИВНОЙ СРЕДЕ

В. А. Черненко
руководитель – магистр направления подготовки
«Информационная безопасность» ***С. М. Полухин***
Северо-Кавказский федеральный университет, г.Ставрополь

В наши дни актуальной проблемой является саботаж в корпоративной среде в области информационной безопасности. Сегодня специалисты должны пони-

мать, на что готов классический саботажник. В большинстве случаев саботажником оказывается мужчина. И большая часть из них занимает инженерные должности. Чтобы бороться с корпоративными диверсантами начальству следует овладеть рядом приемов борьбы с ними. Иначе результат саботажа станет неконтролируемым. Из-за этого продуктивность компании может оказаться под вопросом. Все эти проблемы будут рассматриваться в данной статье.

Ключевые слова: корпоративный саботаж, информационный саботаж, корпоративная диверсия.

Корпоративный саботаж – это вредоносные поступки, направленные на причинение вреда компании, совершаемые злоумышленниками чтобы поквитаться, в порыве гнева или просто недобросовестным выполнением своих прямых обязанностей. Так же своими действиями саботажники могут выражать свое несогласие с курсом компании.

Стоит отметить, что от саботажников страдают компании, которые работают в сфере ИТ и телекоммуникаций.

Диверсии часто совершаются из-за эмоциональных, иногда бессмысленных оснований. Инсайдера не волнует финансовый вопрос, его основная цель не заработок. Отметим, что под словом «инсайдер» рассматриваются бывшие и настоящие служащие компании.

Итогом диверсии единично бывают материальные убытки, но в то же время новые исследования не подтверждают данную точку зрения. Тем не менее, по сравнению с другими угрозами, суммарные материальный ущерб компании в результате действий инсайдеров на фоне убыток от иных угроз кажутся не такими огромными.

Тем не менее, при толковании этих сведений нужно быть осторожным. Саботаж можно приравнять к скрытым правонарушениям. Руководители нехотя рассказывают, что в их предприятии произошла диверсия, потому что ее часто связывают с неосторожностью сотрудников.

Если отвлечься от финансовых моментов, угроза саботажа заключается в огромных потерях, которые несут предприятия, окажись в числе ее сотрудников личность со слабой психикой. В отдельных случаях это может нести угрозу защищенности страны, но в сфере бизнеса, за вычетом материального ущерба, обнаруживается ряд неблагоприятных последствий: это ухудшение имиджа компании и ущерб, который наносится другим сотрудникам, работающим в компании. Таким образом, саботаж может нанести приличные финансовый ущерб компании и вредит имиджу. По этим причинам с саботажем нужно вести борьбу.

Акт саботажа зачастую ведет к тому, что злоумышленник шантажирует начальство или своих коллег. Иногда он даже рассказывает свой план кому-то из служащих компании.

Действенный метод – семинары и тренинги, на которых до сотрудников доводят сведения об угрозах информационной безопасности и саботаже. При этом подходе руководство делает ставку на тех, кто взаимодей-

ствует с инсайдером в офисе, видят его странное поведение, получают угрозы в свой адрес и т. п. Все эти служащие должны знать, что о подобные инциденты нельзя скрывать и сразу же извещать начальство.

Следующий метод четкого разделения обязанностей. Очевидно, что административных полномочий у обычных служащих не должно быть. Также понятно, что сотрудник, отвечающий за резервное копирование, не должен иметь возможности удалить оригинальные данные. Этому служащему следует поручить информирование начальства в случае, если на резервные копии покусится кто-то другой. Так как в компании не так много по-настоящему ценных данных, создание нескольких резервных копий является разумным решением.

Так же важен момент эффективного управления учетными записями. Система информационной безопасности, разрешающая удаленный доступ уже уволенным сотрудникам, никуда не годится. Администраторы должны внимательно следить за правами доступа сотрудника, покидающего компанию. Соответствующие учетные записи следует удалять сразу же.

Лучшей профилактической мерой можно назвать мониторинг. Нанести реальный ущерб компании может только топ-менеджер, поскольку у остальных служащих, которые имеют доступ к цифровым активам компании, просто не будет прав на удаление важной информации.

Чтобы смягчить удар от действий злоумышленника, защищать важные сведения и части информационной инфраструктуры, а также систематически выполнять резервное копирование данных.

Таким образом, в распоряжении современных компаний есть целый ряд приемов, позволяющий минимизировать ущерб информационного саботажа.

Литература

1. http://ej.kubagro.ru/2014/01/pdf/69.pdf, 0,75 у.п.л.

2. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. Издательство: Питер, 2008, 321 с., ил.

3. http://ej.kubagro.ru/2014/10/pdf/116.pdf, 1,375 у.п.л.

РАЗРАБОТКА СНИФФЕРА ДЛЯ НЕЙРОННОЙ СЕТИ C++

Н. К. Чистоусов

руководитель – старший преподаватель ***Д. В. Соломонов***

Северо-Кавказский федеральный университет, г. Ставрополь

В современном мире наиболее актуальны вопросы информационной безопасности в компьютерных системах. Основными способами защиты от несанкционированного доступа на данных момент является антивирусное ПО и межсетевые экраны или файрволы (firewalls). Однако такое ПО действует по строго

определенным алгоритмам, из-за чего они не способны распознавать угрозы новых типов. Искусственные нейронные сети, напротив, после обучения способны адаптироваться под новые типы угроз, распознавая их, ни разу с ними до этого не сталкиваясь. Данная особенность позволяет системе защиты стать более гибкой и независимой.

Ключевые слова: сетевой трафик, сниффер, нейронная сеть, caffe, C++, uml, WinPcap, Qt.

Нейронная сеть – это громадный распределенный параллельный процессор, состоящий из элементарных единиц обработки информации, накапливающих экспериментальные знания и предоставляющих их для последующей обработки.

В основе разработки снифера положена статья [1]. В качестве графического интерфейса использована библиотека Qt – это сильно интегрировало разрабатываемые классы, но значительно облегчило процесс разработки, а в качестве библиотеки для захвата трафика использована библотека WinPcap.

Activity diagram представлена на рисунке 1:

1. В графический интерфейс вводятся данные;
2. После нажатия на кнопку «Запустить» идет проверка введенных данных;
3. Далее параллельно обрабатываются 2 процесса: получение IP адресов процессов по PID и сбор сетевого трафика в количестве равному $100 * \text{количество batcheй}$;
4. Когда оба процесса завершились, то происходит маркировка трафика в соответствии с полученными IP;
5. Далее идет сохранение каждого batch в файл с расширением h5.

Получение списка интерфейсов выполняется следующим образом с помощью библиотеки WinPcap:

```
static QList<network_interface> getAllAdapters(){
pcap_if_t *alldevs, *d;
char errbuf[PCAP_ERRBUF_SIZE];
QList<network_interface> interfaces;
if (pcap_findalldevs_ex(PCAP_SRC_IF_STRING, &alldevs, errbuf) == -1)
throw ExceptionAll(errbuf);
for(d=alldevs;d;d=d->next){
network_interface buffer;
buffer.description=QString(d->description);
buffer.name=QString(d->name);
buffer.addresses = *(d->addresses);
interfaces<<buffer;
}
pcap_freealldevs(alldevs);
return interfaces;
}
```

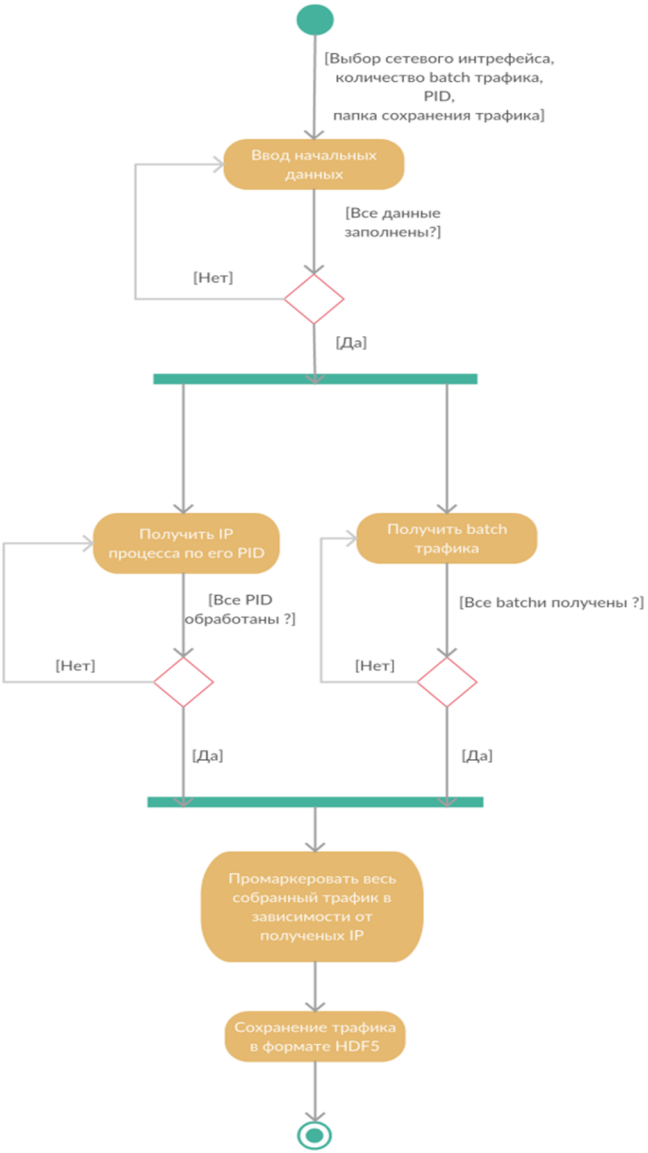


Рисунок 1. Activity diagram

Обработка трафика происходит так

```
while((res = pcap_next_ex( adhandle, &header, &pkt_data)) >= 0)
{
if (res == 0)
continue;
```

```
Traffic traffic(pkt_data,header->caplen);
buffer.push_back(traffic);
if(buffer.size()==batch_size){
BatchTraffic batchTraffic(buffer);
batchs.push_back(batchTraffic);
buffer.clear();
}
if(batchs.size()==batch_amount)
break;
}
```

Важно отметить, как происходит сохранение трафика с сетевой карты в класс Traffic:

```
Traffic(const u  char *pkt  data_ref,const int & len_ref):len(len_ref),flag(false){
pkt  data=new u  char[len];
for (int i = 0; i < len; i++)
pkt_data[i] = pkt_data_ref[i];
}
```

Получение IP по PID происходит с помощью встроенной программы *netstat* с флагом *-ano*.

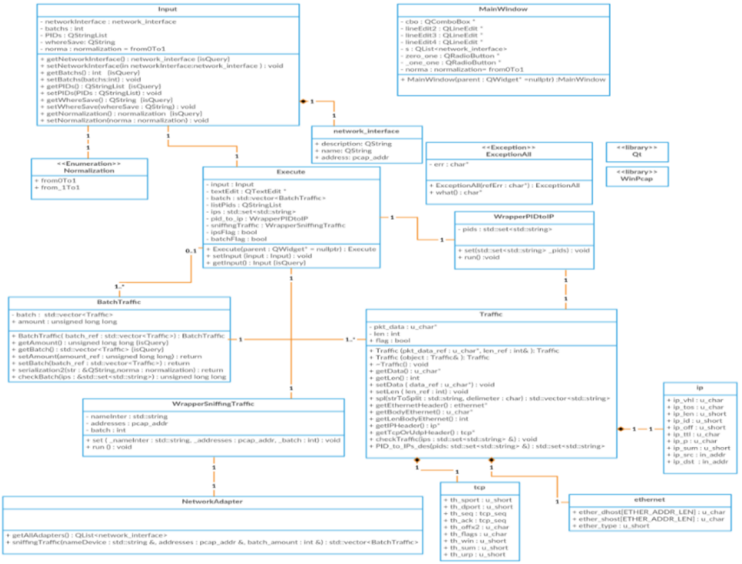


Рисунок 2. Class diagram

Class diagram показана на рис. 2. Исходный код можно модифицировать для сохранения любого специфичного трафика.

Вывод: использование нейронных сетей в разработке ПО для безопасности набирает популярность. В частности, развивается направление,

где нейронную сеть используют для обнаружения враждебного по отношению к организации трафика. Данный сниффер способен собрать обучающий материал для любой такой нейронной сети.

Литература

1. Студенческая наука для развития информационного общества: сборник материалов VII Всероссийской научно-технической конференции. Ставрополь: Изд-во СКФУ, 2018. 544 с. Чистоусов Н. К. Разработка модели системы обнаружения трафика, у которого адрес назначения заранее не известен, программного обеспечения с применением нейронной сети.
2. Официальный сайт WinPcap [Электронный ресурс]: – Режим доступа: https://www.winpcap.org/
3. Официальный сайт HDF5 [Электронный ресурс]: – Режим доступа: https://www.hdfgroup.org/
4. Последняя спецификация по UML [Электронный ресурс]: – Режим доступа: https://www.omg.org/spec/UML

Официальный сайт Qt [Электронный ресурс]: – Режим доступа: https://www.qt.io/

СИСТЕМНЫЙ АНАЛИЗ ТИПОВЫХ НАПАДЕНИЙ НА ЗОНУ ЛВС, СВЯЗЫВАЮЩУЮ КЛИЕНТА, СЕРВЕР ЭЛЕКТРОННОЙ ПОЧТЫ И СЕРВЕР РЕЗЕРВНОГО КОПИРОВАНИЯ

М. В. Шевцова, И. Р. Евдокимов

Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассматриваются типовые угрозы на зону ЛВС, связывающую клиента, сервер электронной почты и сервер резервного копирования. Приведены и рассмотрены 3 типовых нападения на зону ЛВС, к некоторым из них представлены изображения.

Ключевые слова: почтовый сервер, электронная почта, спам, вредоносное ПО, социальная инженерия.

В данной статье будут рассмотрены нападения связывающую клиента, сервер электронной почты и сервер резервного копирования, которые должны знать как сетевые инженеры, так и системные администраторы.

В зависимости от цели атаки, киберпреступникможет реализовать множество различных угроз. В статье рассматриваются такие угрозы,как:

- перехват электронной почты;
- распространение вредоносного программного обеспечения;
- распространение нежелательной корреспонденции.

Перехват электронной почты является, пожалуй, одним из самых простых способов получения информации у организации незаконным путем. Перехват почтового трафика осуществляется такими способам, как:

– внедрение в программное обеспечение почтового сервера контролирующего модуля, который позволяет гарантированно проверять

все письма, проходящие через сервер, а также заблокировать либо задержать отсылку письма;

– автономный (пассивный) мониторинг почтового трафика, в котором контролируется абсолютно весь почтовый трафик, в том числе и письма, отправленные на чужие почтовые серверы.

Данные способы атаки на сервер электронной почты представляют собой атаку «человек по середине», где злоумышленник пропускает трафик, в данном случае электронной почты, через себя.В то время пока жертва считает, что работает напрямую с почтовым сервером в своей организации, трафик проходит через промежуточный узел злоумышленника, который таким образом получает все отправляемые пользователем данные.

Довольно распространенным способом атаки на клиента и сервер электронной почты является распространение вредоносного программного обеспечения, таких как вирусы, трояны, черви и т.д.

Принцип работы данной атаки заключается в том, что злоумышленник путем социальной инженерии пытается обмануть пользователя и заставить его открыть зараженное письмо. Как правило, злоумышленник внедряет вредоносный код в письма, которые часто встречающиеся в обычной почте:

– письма от друзей с текстом или картинкой;

– письма от почтового сервера, о том, что какое-то из сообщений не может быть доставлено;

– письма от провайдера с информацией об изменениях в составе услуг;

– письма от производителей защитных программ с информацией о новых угрозах и способах защиты от них и т.д.

На рис. 1 представлен пример вредоносного письма, в котором злоумышленник, подделав заголовок письма и внедрив туда вредоносный код, обращается к жертве от имени Федеральной Налоговой службы.

Открыв зараженное письмо, на компьютере пользователя запускается «тихая установка» вредоносного приложения или в компьютер пользователя внедряется вредоносный код. После внедрения вредоносного ПО, злоумышленник полностью контролирует компьютер жертвы.

Широкое распространение сетевых средств обмена информацией привело к возникновению явления массовой несанкционированной рассылки сообщений рекламного или вредоносного характера, которое получило название «Спам».

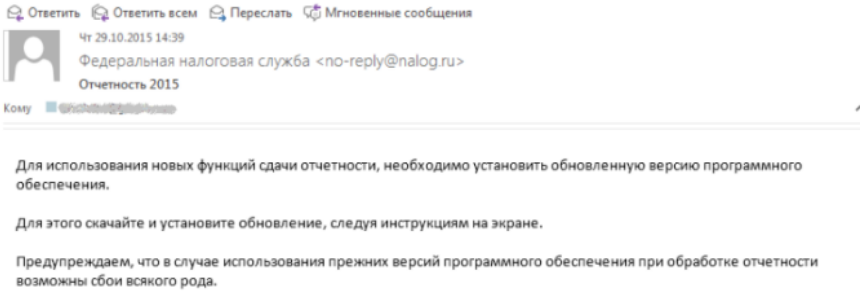


Рисунок 1. Пример вредоносного письма, в котором злоумышленник, подделав заголовок письма и внедрив туда вредоносный того код, обращается пока к жертве от имени вред Федеральной вред Налоговой службы

Для рассылки нежелательной почтовой корреспонденции злоумышленники используют специальные программы, работающие с базами данных различных адресов. Источники пополнения базы адресов различны: сбор адресов в открытых источниках (анализ web-страниц), перебор коротких имен, кража и скупка личных данных пользователей. Для того чтобы спам доходил до адресатов, злоумышленники применяют сложные методы маскировки содержимого писем: искажение написания, вставка объявления в невидимый текст как иллюстрации, выполнение рассылки через посредников (в основном зараженные машины) и т.п.

Данный тип атаки схож с атакой «отказ в обслуживании», где спам сообщения забивают буфер и память почтового сервера или почтовый ящик клиента, в результате чего почта перестает функционировать. Также данный вид атаки может нанести вред получателю, так как в таких письмах, как правило, могут содержаться вирусы и другие вредоносные ПО.

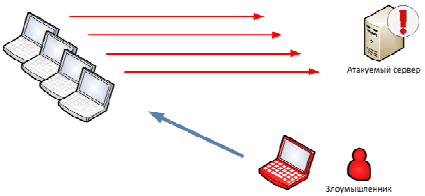


Рисунок 2. Спам сообщения забивают буфер и память почтового сервера или почтовый ящик клиента, в результате чего почта спам перестает пока функционировать

Таким образом, из всего написанного следует, что электронная почта организаций может быть подвержена различным рискам, которые могут привести к потере эффективности работы, снижению качества услуг информационных систем и разглашению конфиденциальной информации.

Литература

1. Информационная безопасность автоматизированных систем: учеб. пособие для студентов вузов,обучащихся по специальностям в обл.информ.безопасности. / А.Ф.Чипига. М.: Гелиос АРВ, 2010. 336 с., ил.

2. Информационное противодействие угрозам терроризма / Чипига А. Ф., Пелешенко В. С., 2010.

3. Известия ЮФУ. Технические науки / Чипига А. Ф., Ерещенко А. А., Пелешенко В. С., 2010.

4. Информационное противодействие угрозам терроризма / Чипига А. Ф., Ерещенко А. А., 2005.

5. Фундаментальные исследования / Чипига А. Ф., Марков Д. М., Слюсарев Г. В., 2009.

РАЗДЕЛ 5
РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ

СОЗДАНИЕ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ ДЛЯ АНТРОПОМОРФНОГО РОБОТА

З. Д. Алиев, А. А. Гусейнов, Д. А. Бондаренко, К. Ганьшин
руководитель – канд. техн. наук, доцент ***Е. И. Николаев***
Северо-Кавказский федеральный университет, г. Ставрополь

Настоящее исследование направлено на решение задач компьютерного зрения в приложении к различным роботизированным антропоморфным устройствам. Задача разработки системы распознавания лиц в настоящее время затрагивает многие стороны жизни человека и находит применение в различных ее областях: создание систем безопасности, систем контроля доступа, развлекательных систем.

Ключевые слова: распознавание образов, распознавание лиц, компьютерное зрение, нейронная сеть.

Разработанная информационная система имеет модульную архитектуру и реализует функции добавления, удаления, изменения компонентов системы независимо друг от друга.

Система состоит из четырех основных модулей:

1) Модуль обнаружения лиц в кадре. Модуль был реализован как с использованием метода Виолы-Джонса, так и методом Гистограммы направленных градиентов (Histogram of Oriented Gradients, HOG).

Версия модуля, реализующая метод Виолы-Джонса, была разработана на основе библиотеки OpenCV. Для реализации метода HOG использовалась библиотека dlib. Итоговое решение было построено на основе метода HOG, т.к. проигрывая в скорости работы, метод продемонстрировал более высокую точность, то есть не имел ложных срабатываний на тестовых кадрах.

2) Модуль выделения признаков лица. Модуль построен на основе предварительно обученной глубокой сверточной нейронной сети (ГСНС) ResNet [6,7]. Для решения задачи внедрения ГСНС была использована библиотека машинного обучения dlib, которая использует модифицированный вариант сети ResNet34 [5] (рис. 1).

layer name	output size	18-layer	34-layer	50-layer	101-layer	152-layer
conv1	112×112	7×7, 64, stride 2				
		3×3 max pool, stride 2				
conv2_x	56×56	[3×3, 64; 3×3, 64] ×2	[3×3, 64; 3×3, 64] ×3	[1×1, 64; 3×3, 64; 1×1, 256] ×3	[1×1, 64; 3×3, 64; 1×1, 256] ×3	[1×1, 64; 3×3, 64; 1×1, 256] ×3
conv3_x	28×28	[3×3, 128; 3×3, 128] ×2	[3×3, 128; 3×3, 128] ×4	[1×1, 128; 3×3, 128; 1×1, 512] ×4	[1×1, 128; 3×3, 128; 1×1, 512] ×4	[1×1, 128; 3×3, 128; 1×1, 512] ×8
conv4_x	14×14	[3×3, 256; 3×3, 256] ×2	[3×3, 256; 3×3, 256] ×6	[1×1, 256; 3×3, 256; 1×1, 1024] ×6	[1×1, 256; 3×3, 256; 1×1, 1024] ×23	[1×1, 256; 3×3, 256; 1×1, 1024] ×36
conv5_x	7×7	[3×3, 512; 3×3, 512] ×2	[3×3, 512; 3×3, 512] ×3	[1×1, 512; 3×3, 512; 1×1, 2048] ×3	[1×1, 512; 3×3, 512; 1×1, 2048] ×3	[1×1, 512; 3×3, 512; 1×1, 2048] ×3
	1×1	average pool, 1000-d fc, softmax				
FLOPs		1.8×10^9	3.6×10^9	3.8×10^9	7.6×10^9	11.3×10^9

Рисунок 1. Полное описание архитектуры ГСНС ResNet

На входе модуль получает изображение лица, найденного детектором лиц. Результат работы – 128 числовых параметров, описывающих лицо [2, 3, 4] (рис. 2).

Рисунок 2. Пример выходных данных модуля

3) Модуль идентификации лица по признакам. В ходе разработки модуля проводились эксперименты с тремя методами классификации:

– метод опорных векторов (SVM) (точность ~60%);

– дерево принятия решений (точность ~60%)»

– метод k-ближайших соседей (точность ~97%).

По итогам проведенных экспериментов принято решение о включение в основу данного модуля метода “k-ближайших соседей”. Скорость обучения классификатора 3-5 секунд.

Результатом работы данного модуля является строка с именем распознанного человека, которой подписывается найденное в кадре лицо (рис. 3).

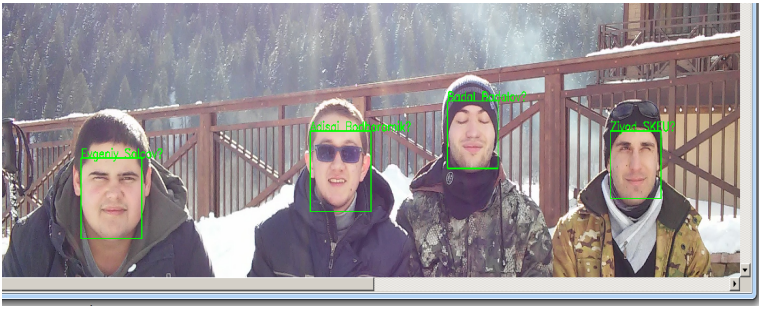


Рисунок 3. Распознавание нескольких лиц в одном кадре

4) Модуль создания базы признаков. Дополнительный компонент системы, необходимый для подготовки обучающей выборки для тренировки автоматического классификатора. На входе полный путь к папке, содержащей необходимые изображения. Выход – файл с расширением «*.data», хранящий 128 числовых параметров для каждого человека из выборки.

Преимуществами разработанного программного продукта являются модульная архитектура, позволяющая наращивать состав функциональных модулей; открытый исходных код и высокая скорость обучения классификатора, которая позволяет быстро расширить базу известных системе лиц.

Литература

1. Ю. К. Гаврилей, А. И. Самарин, М. А. Шевченко. Активный анализ изображений в системах с фовеальным восприятием. – Нейрокомпьютеры в системах обработки изображений, №7-8, 2002. С.34-46.
2. https://www.cv-foundation.org/openaccess/content_cvpr_2015/app/1A_089.pdf - the computer vision foundation.
3. Koch C., Mathur B. Neuromorphic vision chips // IEEE Spectrum, 33 (5), 1996, pp.38–46.
4. https://algotravelling.com-Algo Travelling .
5. https://www.asozykin.ru/deep_learning/2017/08/11/foto-verification-with-dlib
6. Самарин А.И. Нейросетевые модели в задачах управления поведением робота, «НЕЙРОИНФОРМАТИКА-2001».
7. Н. А. Лагунов, О. С. Мезенцева Влияние предобработки изображений на качество обучения нейронной сети // Вестник Северо-Кавказского федерального университета. 2015. № 1 (46). С. 51-58.

СХЕМА ПЛАНИРОВАНИЯ ОПТИМАЛЬНОЙ ТРАЕКТОРИИ ДВИЖЕНИЯ ТРЕХЗВЕННОГО АНТРОПОМОРФНОГО МАНИПУЛЯТОРА В РАБОЧЕЙ ЗОНЕ С ПРЕПЯТСТВИЕМ

В. О. Антонов
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрена обобщенная схема и дополнена до схемы планирования оптимальной траектории движения трехзвенного антропоморфного манипулятора в рабочей зоне с препятствием. Предлагаемый подход обеспечит высокую точность и энергоэффективность при выполнении целевых операций в объемном пространстве с препятствием в режиме реального времени.

Ключевые слова: антропоморфный манипулятор, схема планирования оптимальной траектории движения, формирование траектории движения.

Предлагаемый комплексный подход для решения задачи увеличения продолжительности работы автономных мобильных манипуляционных роботов заключается в разработке нового метода планирования траектории движения антропоморфных манипуляторов на основе итерационной кусочно-линейной генерации траектории движения точки в пространстве с препятствием и решения обратной задачи кинематики постановкой представлением Денавита-Хартенберга и постановкой задачи нелинейной оптимизации с 6 переменными.

Проведем обобщение и модификацию обобщенной схемы методов планирования траектории движения трехзвенного антропоморфного манипулятора для решения задачи минимизации энергопотребления при перемещении.

Приведем обобщенную схему планирования траектории движения трехзвенного антропоморфного манипулятора в объемном пространстве с препятствием (рис. 1).

Обобщенная схема состоит из 5 внутренних блоков [1]. Ввод данных начального и конечного положения манипулятора регулирует задает начальные параметры для решения задачи планирования. Если работа совершается в сложном пространстве, то необходимы данные об окружающей среде. Блок синтеза траектории движения включает в себя математический аппарат для расчета траектории движения и последующего вывода расчетных данных.

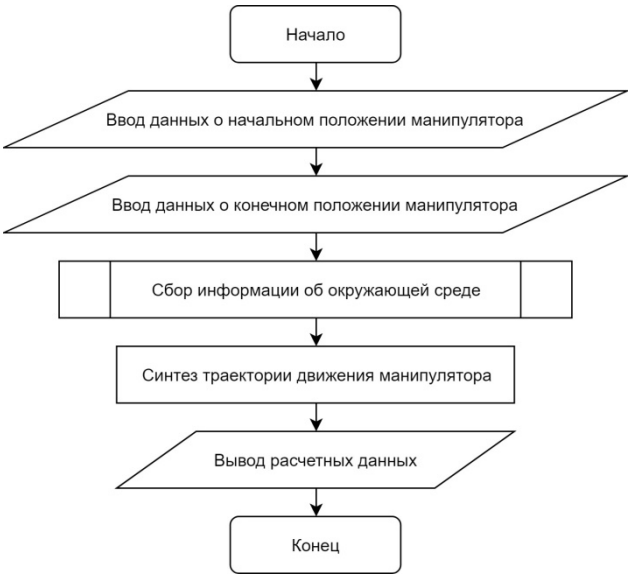


Рисунок 1. Обобщенная схема планирования траектории движения трехзвенного антропоморфного манипулятора в объемном пространстве с препятствием

Схема планирования оптимальной траектории движения трехзвенного антропоморфного манипулятора в объемном пространстве с препятствием представлена на рис. 2. В данной работе производится модификация двух блоков данной схемы – блока «Формирования двухточечной траектории движения манипулятора», а также блока «Формирования сложной траектории обхода препятствия».

Для блока «Формирования двухточечной траектории движения манипулятора» входными данными являются конструктивные параметры манипулятора, значения присоединенных координат в исходном состоянии, координаты положения начала манипулятора в пространстве – $A = (x_A; y_A; z_A)$, в также целевая точка, в которой должен оказаться эффектор манипулятора по окончанию движения – $D = (x_D; y_D; z_D)$ [2].

Задачей данного блока является решение обратной задачи кинематики, заключающейся в поиске такого значения присоединенных координат $\alpha_A, \beta_A, \gamma_A, \alpha_B, \alpha_C, \beta_C, \gamma_C$, при котором эффектор манипулятора окажется в целевой точке D [3]. Схема планирования оптимальной траектории движения трехзвенного антропоморфного манипулятора в объемном пространстве с препятствием опирается на метод итерационной кусочно-линейной генерации траектории движения трехзвенного антропоморфного манипулятора, приведенного ниже.

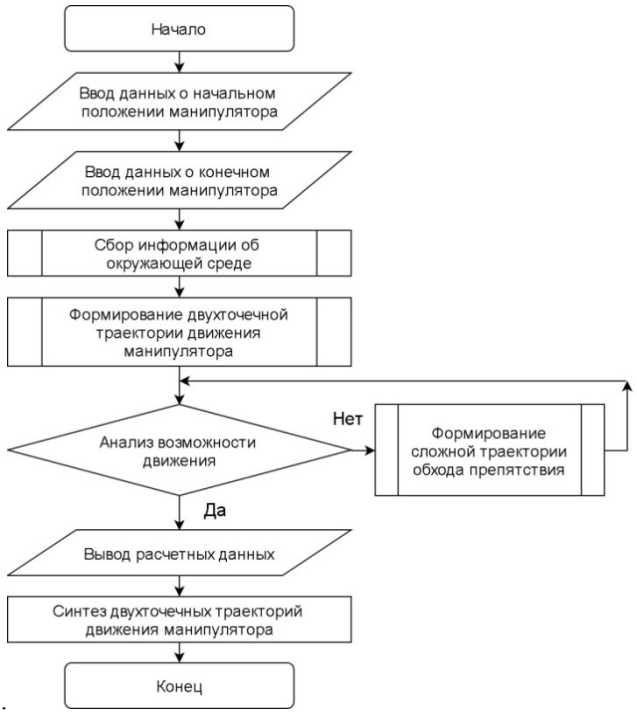


Рисунок 2.Схема планирования оптимальной траектории движения трехзвенного антропоморфного манипулятора в объемном пространстве с препятствием

Литература

1. Антонов В. О., Гурчинский М. М., Петренко В. И., Тебуева Ф. Б. Метод планирования траектории движения точки в пространстве с препятствием на основе итеративной кусочно-линейной аппроксимации // Системы управления, связи и безопасности. 2018. № 1. С. 168-182. URL: http://sccs.intelgr.com/archive/2018-01/09-Antonov.pdf

2. Петренко В. И., Тебуева Ф. Б., Антонов В. О., Гурчинский М. М. Математическая модель поиска оптимальных углов Эйлера для двигателей трехзвенного манипулятора // Современная наука: Актуальные проблемы теории и практики. Естественные и технические науки. 2018. №3. С. 67-74.

3. Петренко В. И., Тебуева Ф. Б., Антонов В. О., Гурчинский М. М. Метод планирования оптимальной траектории движения трехзвенного манипулятора в объемном пространстве с препятствием // Вестник Дагестанского государственного технического университета. 2018. №1. Том 45. С. 67-84.

ПЕРСПЕКТИВНЫЕ МЕТОДЫ ТРЕХМЕРНОЙ ИНТЕГРАЦИИ ИЗДЕЛИЙ МИКРОЭЛЕКТРОНИКИ

А. И. Артемова, В. Е. Вилков
руководитель – научный сотрудник ***А. В. Суханов***
НПК «Технологический центр», г. Зеленоград

Новые технологии миниатюризации электронных приборов находят обширное применение при проектировании для любых отраслей, будь это гражданская электроника или техника, предназначенная для работы в жестких условиях. В докладе представлен обзор перспективных технологий трехмерной интеграции на уровне подложек для применения в области силовой электроники. В обзоре описаны основные принципы технологий трехмерной интеграции, их применимость для изготовления изделий электронной техники, основные преимущества и недостатки.

Ключевые слова: трехмерная интеграция, 3D-MID, LTCC, гибкие печатные платы, технология встроенного кристалла, BGA.

Миниатюризация электронных устройств является одним из основных аспектов технологического прогресса [1]. На сегодняшний день стандартная технология монтажа дискретных элементов на печатные платы не способна обеспечить требуемые габаритные характеристики электронных изделий. В связи с этим активно развиваются технологии трехмерной интеграции. Они позволяют не только уменьшить размеры устройства или его элементов, но и повысить ключевые характеристики, такие как скорость работы, функциональность, надежность, защиту от внешних воздействий и др. В данной статье проводится обзор и сравнение основных технологий трехмерной интеграции на уровне подложек, которые нашли применение при производстве устройств в реальных секторах экономики, в частности при производстве силовой электроники.

Одна из перспективных технологий миниатюризации электроники – это технология 3D-SiP (Three-dimensional System-In-A-Package). Эта технология заключается в упаковке нескольких электронных подсистем (ячеек либо блоков) в одну функциональную высокоинтегрированную систему на уровне кристаллов. Данная система содержит 2 или более уровней. В роли таких уровней выступают технологические подложки, на которые монтируются различные компоненты, либо кристаллы. В данной технологии для соединения подсистем как правило используется шариковый припой, или BGA (англ. Ball grid array – массив шариков) монтаж, то есть выводы представляют собой шарики припоя. Кроме этого возможно применение таких методов межсоединения как термокомпрессионная микросварка (Wire Bond), присоединение перевернутого кристалла (Flip Chip), присоединение кристалла к выводам ленточного кристалла (TAB – Tape Automated Bonding), использование underfill материалов и т.д. Пример многокристальной упаковки по технологии 3D-SiP показана на рис. 1.

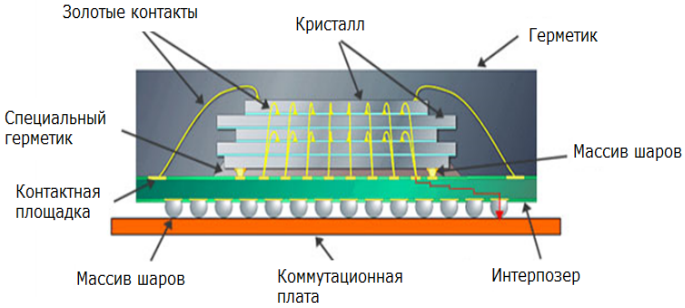


Рисунок 1. Пример многокристальной упаковки

На уровне микросборок перспективной является технология 3D-MID. 3D-MID технология основана на использовании высокотемпературного пластика и его структурированной металлизации для интеграции электронных, механических и оптических функциональных компонентов, создавая трехмерные системы на базе самого пластика без использования специальных плат и технологических подложек. Данная технология имеет ряд преимуществ. За счёт высокой гибкости проектирования возможно создать изделие любой формы и размеров. Использование меньшего количества компонентов обуславливает более короткий и простой технологический процесс производства, повышает надёжность устройства, снижает расход материалов и материальных затрат.

В LDS технологии (Laser Direct Structuring – прямое лазерное структурирование) применяется легированный соединением металл-органический комплекс термопласт (рис. 2) [2]. Первоначально заготовка отливается из термопласта. Затем согласно топологии проводящей металлизации дорожки, на поверхности изделия облучаются лазером (активируются), за счёт чего происходит абляция пластмассовой и органической составляющей. На поверхности образуются шероховатости, обеспечивающие достаточную адгезию для последующего нанесения металлического проводника. Нанесение проводится химическим и гальваническим методом, металл осаждается только в обработанных лазером областях.

У LDS технологии есть недостатки: ограничение на некоторые геометрические формы, которые препятствуют активации поверхности лазером, большое количество операций. В 2S (Two-shot molding – 2S) технологии лазер не используется, поэтому ограничений по форме изделия нет (рисунок 3). Идея процесса заключается в проведении двух заливочных операций: сначала формируется основа из уже активированного термопласта, затем поверх наносится слой неактивного термопласта, заполняющий полости. Далее, как и в LDS технологии, осаждается металл. Финишной

операцией после образования металлизации в обоих технологиях является стандартный монтаж компонентов [3].

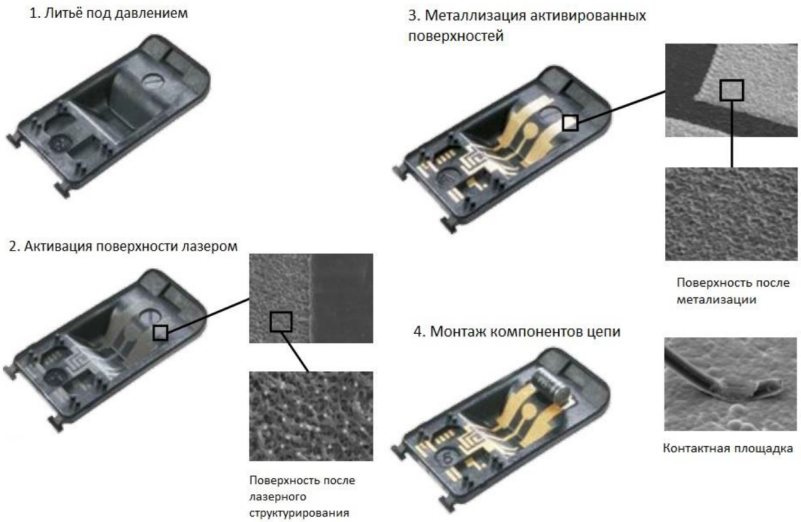


Рисунок 2. Последовательность технологических операций в технологии LDS

Рисунок 3. Последовательность технологических операций в технологии 2S

Одна из самых быстроразвивающихся и популярных технологий на сегодняшний момент является технология низкотемпературной керамики

LTCC (Low Temperature Cofired Ceramics – низкотемпературная совместно-обжигаемая керамика) [4]. Она успешно применяется для различных целей – телерадиовещания, телекоммуникаций, мобильной связи, портативных компьютеров, производства ВЧ- и СВЧ-микросхем низкой и средней степени интеграции и др. Так же LTCC-технология оказалась востребована в сфере силовой электроники. В первую очередь это связано с ее предельными рабочими параметрами и характеристиками. Керамика обладает рядом преимуществ на фоне традиционных материалов, используемых в нашей стране. К ним можно отнести следующие показатели: очень хорошие электрические характеристики, превосходная механическая стабильность и сохранение линейных размеров, низкий КТР, хорошая теплопроводность, возможность 3D интеграции, герметичность и возможность высокотемпературной пайки [5].

Производство керамики начинается с подготовки и отливки специальной суспензии в формы. Суспензия, как правило, изготавливается смешиванием керамического порошка, органических связующих, растворителей и модифицирующих добавок. После процесса отливки формируются керамические листы, которые затем нарезаются под необходимый размер. Далее выполняется формирование переходных отверстий, их заполнение проводящей пастой и создание с помощью специальных проводящих и резистивных паст необходимой топологии (трафаретная печать). Готовые листы совмещаются в сборку, которая затем ламинируется и проходит обжиг при температуре 850°С. Такой технологический процесс гарантирует стабильность структуры керамики в широком диапазоне температур. Конечным этапом производства становится монтаж электронных элементов в стек. Стоит отметить, что температура отжига такова, что позволяет использовать металлы с низким удельным сопротивлением (золото, серебро).

Следует выделить следующие преимущества технологии LTCC:

1 Плотная структура LTCC керамики не пропускает влагу, поэтому корпуса из нее могут быть использованы в высоко влажной атмосфере без дополнительной защиты;

2 Низкий КТР, близкий к такому коэффициенту большинства основных полупроводниковых материалов электроники (Si, GaAs, InP). Это позволяет монтировать полупроводниковые кристаллы непосредственно на основание платы;

3 Хорошая теплопроводность, составляющая 2–4 Вт/мК, что гораздо выше, чем у печатных плат на основе органических материалов (0,1–0,5 Вт/мК). Теплопроводность LTCC также может быть повышена до 20 Вт/мК за счет создания с помощью металлизации тепловых стоков.

В свою очередь недостатками являются:

1 Проблемы получения качественной керамической суспензии, параметры которой могут варьироваться от партии к партии.

2 Проблемы усадки керамики после отжига, на борьбу с которой нацелены ряд последних исследований.

3 Ограниченная возможность интеграции электронных компонентов. Пока что успешно интегрировать внутрь керамической структуры удается только пассивные электронные компоненты, такие как резисторы, катушки индуктивности, созданные за счет нанесения на поверхность керамического листа специализированных паст. Все остальные компоненты устанавливаются стандартными методами монтажа уже на поверхность готовой керамической структуры.

4 Стоимость исходных материалов и затраты на весь производственный цикл. Как правило, каждая LTCC система представляет собой уникальное решение, поэтому замена отдельных компонентов невозможна. В случае появления необходимости доработки того или иного компонента керамической структуры, весь производственный цикл приходится начинать сначала. Для формирования металлизации применяются специализированные пасты на основе драгоценных металлов Au, Ag и Pt.

Принимая во внимание все перечисленные особенности реализации технологии LTCC керамики, становится ясно, почему на сегодняшний момент основной областью ее применения является военно-промышленный комплекс, и особо распространения данная технология на сегодняшний момент не получила.

Технологии трехмерной интеграции активно развиваются и находят все более обширное применение. Данные нововведения не вытесняют стандартные технологии, так как их использование для проектирования устройства целиком нецелесообразно с точки зрения финансовых и временных затрат. Однако использование технологий интеграции для отдельных элементов, а также совмещение различных подходов в одном изделии позволяют добиться существенного выигрыша по габаритам и ключевым характеристикам конечного изделия.

Работа выполнена при финансовой поддержке Минобрнауки России в рамках государственного контракта № 14.577.21.0225 (уникальный идентификатор прикладных научных исследований RFMEFI57716X0225) с использованием оборудования ЦКП «Функциональный контроль и диагностика микро- и наносистемной техники» на базе НПК «Технологический центр».

Литература

1 Sukhanov A. V., Artemova A. I., Litvinenko R. S. Review of modern three-dimensional integration technologies and analysis of prospects of their use for high power micro-assemblies. Indonesian Journal of Electrical Engineering and Computer Science. 2018 . vol. 9(1), pp. 198-203.

2 Что такое трехмерные схемы на пластиках // ЗАО предприятие Остек URL:http://www.3dmid.ru/ (дата обращения 18.03.2018) 4. Сомонов В. В., Туричин Г. А., Земляков Е. В., Бабкин К. Д., Климова- Корсмик О. Г. Прямое лазерное выращивание изделий из порошковых материалов: принцип, оборудование и материалы // Технические науки в России и за рубежом: материалы VI Междунар. науч. конф. (г. Москва, ноябрь 2016 г.). М.: Буки-Веди, 2016. С. 34-38. URL: https://moluch.ru/conf/tech/archive/228/10881/ (дата обращения: 20.03.2018).

3 И.Волков Технология 3D-MID Новые возможности прототипирования изделий, печатный монтаж, №2, 2013, с. 170-174.

4 Р.Кондратюк, LTCC – Промышленные нанотехнологии: Низкотемпературная совместно обжигаемая керамика, Наноиндустрия научно-технический журнал, №2, 2011. С. 26-30.

5 С. Чигиринский, Особенности и преимущества производства многослойных структур на основе керамики (LTCC, HTCC, MLCC), КОМПОНЕНТЫ И ТЕХНОЛОГИИ, № 11, 2009. С. 130-131.

ОБЗОР ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ РЕЧИ

Л. Ш. Багдасарян
руководитель – канд. физ.-мат. наук, доцент ***О. С. Мезенцева***
Северо-Кавказский федеральный университет, г. Ставрополь

Вопрос распознавания речи исследуется и развивается в науке в течение последних 60 лет ввиду необходимости разработки голосового человеко-машинного интерфейса, что особенно актуально в настоящее время в связи с широким распространением робототехнических систем. В данной статье осуществлен обзор технологий автоматического распознавания речи; представлен процесс предварительной обработки звукового сигнала; методы, применяемые для извлечения информационных признаков сигнала речи, а также технологии получения акустической модели речевого сигнала. Также в статье затрагивается вопрос о выборе базовой лексической единицы речи.

Ключевые слова: автоматическое распознавание речи, технологии распознавания речи, акустическая модель речи, нейронные сети.

Создание систем распознавания речи, имеющих реальное практическое приложение, – чрезвычайно сложная задача, требующая скоординированной работы специалистов в области лингвистики, акустики, математики, программирования и др. Кроме того, несмотря на увеличение вычислительных мощностей современных компьютерных систем, их не всегда достаточно для реализации сложных алгоритмов распознавания. К техническим характеристикам компьютеров предъявляются определенные требования также в связи со сложностью структуры речи и выбранной языковой модели. В ходе анализа речи в качестве базовой лексической единицы могут выступать предложения, словосочетания, отдельные слова, слоги, такие части слов как фонемы, аллофоны (конкретная реализация фонемы), трифоны, дифоны, а также одновременно могут анализироваться несколько структурных уровней. Выбор языковой модели зависит от решаемых системой распознавания задач (распознавание изолированных слов, ключевых слов в речевом потоке, связанной речи (с паузами между словами), слитной речи) и определяет сложность и модель словаря распознаваемых элементов.

Задача распознавания заключается в выделении, классификации и определенной реакции на человеческую речь. Процесс автоматического распознавания речи может быть разделен на несколько этапов. На первом

этапе осуществляется выделение речи из непрерывного аудио потока, удаление шумов посредством применения специальных методов фильтрации и др. Затем выполняется предварительная обработка, в результате которой производится оцифровка сигнала. Далее производится сегментация непрерывного сигнала в зависимости от выбранной структурной единицы. Сегментация осуществляется посредством методов «оконного» анализа, например, функции Хэмминга. Предполагается, что признаки сигнала остаются постоянными на протяжении отдельно взятых фреймов, соответствующих базовой единице речи.

На втором этапе распознавания предварительно подготовленные фреймы анализируются как независимые структуры. Не вдаваясь в подробности строения слуховой системы человека, а также в психоакустические особенности восприятия звука (громкости, высоты) человеком, скажем, что не все признаки речи являются значимыми для распознавания. Цель этапа – получение для каждого фрейма набора числовых параметров в виде отдельного вектора информационных признаков. Для извлечения значимых признаков могут быть использованы такие методы цифровой обработки сигналов как спектральный анализ Фурье (FT), коэффициенты линейного предсказания (LPC), перцепционные коэффициенты линейного предсказания (PLP), вейвлет-преобразования, мел-частотные кепстральные коэффициенты (MFCC) и др. Самые современные методы определения информационных признаков являются гибридными, а также могут включать использование нейронных сетей. Одним из наиболее успешных (особенно в ситуации отсутствия фонового шума) является вычисление мел-частотных кепстральных коэффициентов. MFCC применяется как в коммерческих приложениях, так и в системах с открытым кодом, например, в таких как CMU Sphinx, Kaldi, Julius, Microsoft CNTK, Hidden Markov Model Toolkit (HTK) и др.

На третьем этапе автоматического распознавания работа состоит в получении акустической модели сигнала, посредством классификации полученных на предыдущем этапе векторов-признаков. Задача распознавания решается различными методами: метод динамического программирования (DTW), скрытые марковские модели (HMM), неоднородные марковские модели (CD HMM) и др. Одним из перспективных методов является использование искусственных нейросетей как универсального средства классификации объектов. Сети характеризуются «биологичностью», т.к. функционирование нейросетей с послойным обучением напоминает деятельность слухового аппарата человека [7, с. 36]. Для задачи распознавания используют многослойные нейронные сети (DNN) различных топологий.

Описанные методы и технологии автоматического распознавания речи обобщенно представлены в табл. 1.

Таблица 1

Методы и технологии распознавания речи

Этапы процесса распознавания речи	1. Предварительная обработка речевого сигнала	2. Извлечение информационных признаков сигнала	3. Получение акустической модели сигнала
Используемые методы и технологии	Фильтрация Оцифровка Сегментация «Оконный» анализ	Спектральный анализ Фурье Коэффициенты линейного предсказания, Перцепционные коэффициенты линейного предсказания Вейвлет-преобразования, Нейронные сети Мел-частотные кепстральные коэффициенты	Метод динамического программирования Скрытые марковские модели Неоднородные марковские модели Нейронные сети

Основные сложности автоматического распознавания связаны с распознаванием дикторонезависимой слитной речи; с распознаванием в ситуации, когда дикторы говорят одновременно; а также с распознаванием речи, сопровождающейся большим количеством шумов; и др. Однако, разрабатываемые в науке методы и алгоритмы распознавания, а также увеличивающиеся мощности компьютеров позволяют достигать высоких результатов в качестве работы систем распознавания речи. Перспективным в плане развития и совершенствования голосового интерфейса является применение нейронных сетей, которые превосходят другие технологии распознавания по показателям точности и скорости распознавания.

Литература

1. https://www.speechpro.ru

2. Magnuson, James S.; Mirman, Daniel; Luthra, Sahil; и др. Interaction in Spoken Word Recognition Models: Feedback Helps / Frontiers in Psychology. 2018. Т. 9. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00369/full

3. Odell J.J., «The Use of Context in Large Vocabulary Speech Recognition», Dissertation, 1995.

4. Основы построения интеллектуальных систем: учеб. пособ. / Г. В. Рыбина. М.: Финансы и статистика; ИНФРА-М, 2010. 432 с.

5. Системы искусственного интеллекта. Практический курс: учебное пособие / В. А. Чулюков, И. Ф. Астахова, А. С. Потапов и др.; под ред. И.Ф. Астаховой. М.: БИНОМ. Лаборатория знаний, 2008. 292 с.

6. Тампель И.Б. Автоматическое распознавание речи – основные этапы за 50 лет // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 6. С. 957–968.

7. Тампель И.Б., Карпов А.А. Автоматическое распознавание речи. Учебное пособие. СПб.: Университет ИТМО, 2016. 138 с.

РАЗРАБОТКА СИСТЕМЫ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО РЕЧЕВОМУ СИГНАЛУ ДЛЯ АНТРОПОМОРФНОГО РОБОТА

Б. М. Бадалов, А. А. Гусейнов
руководитель – старший преподаватель
межинститутской базовой кафедры ***А. М. Исаев***
Северо-Кавказский федеральный университет, г. Ставрополь

Настоящее исследование направлено на решение задач идентификации личности по голосовым признакам в приложении к различным роботизированным антропоморфным устройствам. Решение этой задачи может найти применение в робототехнике, криминалистике, обеспечении безопасности доступа к физическим объектам, информационным и финансовым ресурсам.

Ключевые слова: идентификация личности по голосу, робототехника.

Задача идентификации по голосу состоит в том, что наблюдатель должен определить принадлежность некоторого сегмента речи (объекта) тому или иному классу из множества известных пользователей, основываясь на векторе значений признаков, вычисленных по данному речевому сигналу.

При решении задачи идентификации диктора по голосу можно выделить следующие этапы:

– получение образца речевого сигнала;

– кластеризация и выделение признаков;

– проверка качества (которой система может отклонить данный образец как непригодный для сравнения и потребовать повторное получение образца);

– сравнение с эталонами базы данных, определяющее степень схожести для каждого сравнения;

– принятие решения об идентичности полученного образца и эталона, основанное на том, превышает ли порог принятия решений и (или) находится среди первых значений степеней схожести;

– получение результата идентификации на основе принятия решения об идентичности образца и эталона.

Архитектура системы идентификации диктора по голосу представлена на рис. 1.

В исследовании были проанализированы и опробованы три метода идентификации личности по голосу. Для оценки эффективности работы алгоритмов применялся набор фонем, произнесенных пользователем. Для этого был создан словарь эталонов ЭРЕ по 10-ти названиям числительных русского языка. Все полученные фонемы числительных были занесены в фонетическую базу данных.

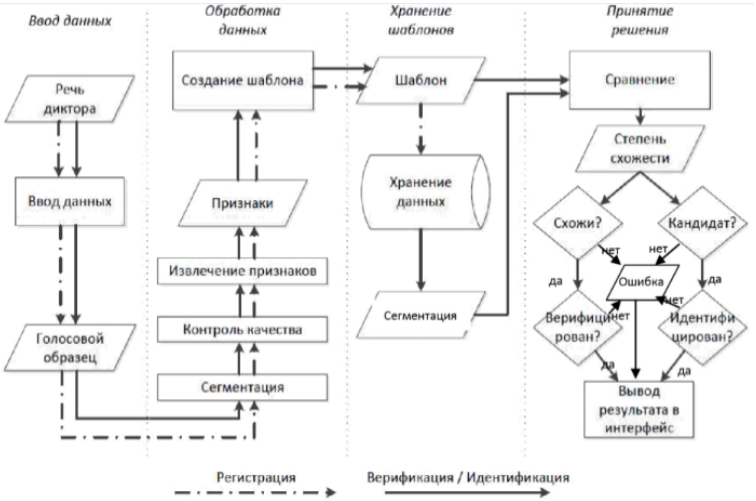


Рисунок 1. Архитектура системы идентификации диктора по голосу

Метод кластеризации элементарных речевых единиц.

Речь можно разбить на элементарные речевые единицы (ЭРЕ) имеющие различные представления с помощью устойчивых параметров и объединяемые человеком в группы одноименных речевых единиц. Для решения задачи кластеризации требуется набор неклассифицированных объектов и средства измерения подобия объектов. Целью кластеризации является организация объектов в классы, удовлетворяющие некоторому стандарту качества, например, на основе максимального сходства объектов каждого класса.

Метод формирования голосовых эталонов на основе элементарных речевых единиц.

Этот подход заключается в нахождение информационного центра по множеству различных реализаций одной фонемы. По найденной реализации максимально приближенной к информационному центру вычисляются параметры ЭРЕ. Внутри каждого такого класса информационный центр определяется аналогично поиску центра масс для множества точечных элементов. Реализацию расположенную максимально близко к такому центру масс считают эталонной, и ее образ и будем считать образом всего класса.

Метод статистического анализа фонем и принцип накопления информации.

Принцип накопления полезной информации строится по результатам сравнения двух образцов: тестируемого и эталонного на множестве их ЭРЕ. Указанный метод широко применяется во многих ИС при обработке информации на фоне помех. Основываясь на данном методе, был разрабо-

тан новый алгоритм принятия решений и статистического анализа фонем пользователя для решения задачи идентификации по голосу. Этот метод позволяет снизить количество ошибок идентификации пользователей по голосу не менее чем в 4,5 раза по сравнению с существующими методами. Вероятности ошибок 1ого и 2-ого рода составили 0,025 и 0,005, что позволяет эффективно противодействовать различным атакам на процесс идентификации.

Сравнение показателей программно-аппаратных комплексов идентификации по голосу российских производителей (рис. 2).

Система идентификации **Параметры проверки системы**	**«ИКАР Лаб»**	**«ИС ИДГ»**	**«Voice Key»**	**«GTS-ID»**
1	2	3	4	5
EER (Equal Error Rate) - вероятность ошибок биометрической системы доступа, при котором FAR и FRR равны	1-3%	1%	2–3%	4%
Отказ в регистрации	1%	2%	4%	~0%
FRR (False Rejection Rate) – вероятность ложного отклонения. Вероятность отклонения «своего» пользователя, приняв его за «чужого» (ошибка первого рода)	0,001	0,025	0,01	0,04
FAR (False Acceptance Rate) – вероятность ложного принятия. Вероятность принятия «чужого» пользователя за «своего» (ошибка второго рода)	0,012	0,005	0,025	0,004
Стоимость системы	Очень высокая	Низкая	Высокая	Высокая

Рисунок 2. Сравнение систем идентификации диктора по голосу

Достигнутые характеристики систем идентификации диктора могут удовлетворять требованиям практической применимости в условиях малой вероятности вторжения самозванца, малой стоимости ошибки, или в случаях, когда окончательное решение принимается экспертом.

Литература

1. Горшков Ю. Г. Новые решения речевых технологий безопасности. // Специальная техника. №4, 2006.

2. Савченко В. В. Автоматическая обработка речи по критерию минимума информационного рассогласования на основе метода обеляющего фильтра // Радиотехника и электроника. 2005. Т50. №3. С.309-314.

3. Центр речевых технологий [Электронный ресурс]: официальный сайт компании «Центр речевых технологий». URL: http://www.speechpro.ru (дата обращения: 23.10.2015).

РАЗРАБОТКА КОНСТРУКЦИИ, СИСТЕМЫ ВЕБ-КОНТРОЛЯ И МОНИТОРИНГА РОБОТА ТЕЛЕПРИСУТСТВИЯ

Д. А. Бондаренко, К. Ю. Ганьшин, Д. И. Степанов, Е. И. Голимблевская
руководитель – канд. физ.-мат. наук, профессор кафедры информационных систем и технологий ***О. С. Мезенцева***
Северо-Кавказский федеральный университет, г. Ставрополь

Телеприсутствие – это область робототехники, которая занимается изучением и разработкой дистанционно-управляемых роботов, главным образом используя беспроводные соединения, ориентированные на обеспечение связи между людьми. Данная статья является кратким обзором магистерской диссертации и работы студентов СКФУ. В статье обозревается ход разработки мобильной платформы, системы для контроля и мониторинга робота, которая обеспечит простоту использования, будучи интуитивно понятной, эргономичной, доступной, переносимой и масштабируемой. Существующие на данный момент приложения для контроля робота телеприсутствия основываются на установке программного обеспечения непосредственно на ПК. Управление исследуемым роботом включает в себя простоту веб-интерфейса для подключения и удобного управления.

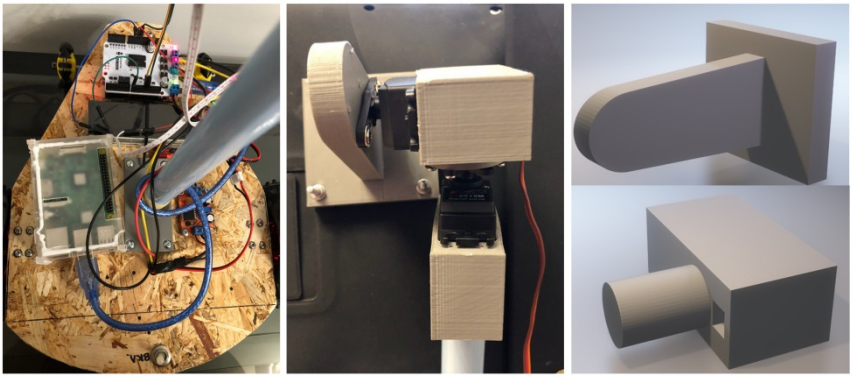
Ключевые слова: Arduino, Raspberry Pi, web, робототехника, робот телеприсутствия, разработка механической платформы, создание веб-интерфейса.

Роботы телеприсутствия – это сложная форма телеоперации, имеющая основные компоненты контроля, реализованные в визуальном и управляющем приложении. Удаленная камера обеспечивает оператору визуальную связь с людьми, находящимися в другой локации. Камера должна определенным образом предоставлять информацию для интуитивного управления роботом. Удобство контроля напрямую зависит от временной задержки, разрешения потокового видео и требуемой полосы пропускания сети. В свое время с данной проблемой столкнулись специалисты наземного управления космическими роботами, где эффекты временных задержек и ограничений пропускной способности чрезвычайно значительны. С целью ограничения большой передачи данных через WLAN соединение за один сеанс, было принято решение разделить потоковую передачу избыточного видео и данных по управлению платформой на несколько устройств, что позволило оптимизировать процесс использования робота в удаленном режиме, в зависимости от доступной скорости беспроводной передачи данных.

При создании робота соблюдались следующие критерии: обеспечение низкой стоимости разработки, ориентированность на максимальную пригодность для реализации иных робототехнических задач, возможность усовершенствования платформы.

Конструкция робота спроектирована для удобного размещения электронных компонентов и ориентирована на дальнейшее расширение воз-

можностей посредствам установки дополнительных датчиков. Основой платформы является лист ДСП с двумя установленными моторами постоянного вращения, включающие понижающий редуктор и энкодер для считывания оборотов. На платформе (рис. 1а) размещены: плата с микроконтроллером Arduino UNO, плата расширения с драйверами двигателей L298P для управления моторами, одноплатный компьютер Raspberry Pi 3, литий-ионный аккумулятор на 12В, стабилизатор напряжения и другая периферия. Верхняя часть робота состоит из механического кронштейна на сервомоторах для установки планшета и управления его поворотом (рис. 1б). Все крепления были смоделированы в САПР и распечатаны на 3D принтере (рис. 1в).



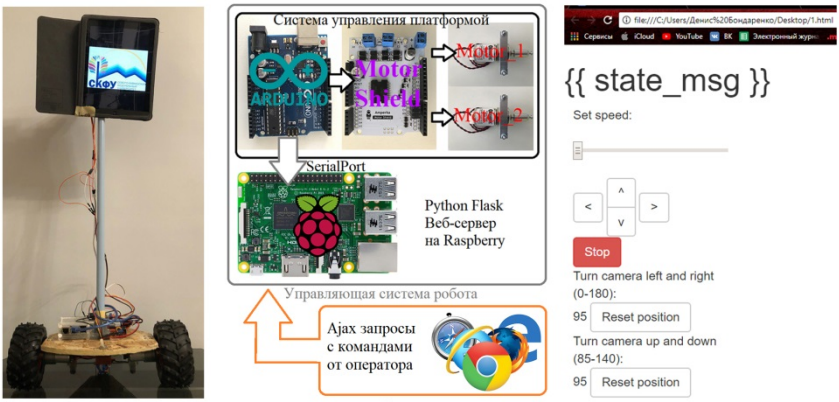
а б в

Рисунок 1. Конструкция роботизированной платформы

Готовая платформа приняла вид, представленный на рисунке 2а.

Первым шагом, при программировании робота телеприсутствия, стало написание в среде программирования Arduino IDE кода для управления моторами, который позволил изменять скорость и направление движения. Плата Arduino Uno не имеет встроенного модуля беспроводной связи, поэтому было целесообразно запрограммировать её на прием команд по последовательному порту (SerialPort) от миникомпьютера Raspberry Pi, который в свою очередь подключается к WiFi сети и управляется по VNC [2]. Вторым шагом стало программирование одноплатного компьютера Risp-berry Pi на языке Python, а именно разработка веб-приложения на фреймворке Flask [1]. Данный веб-сервер получает запросы по адресам и вызывает методы сервера, которые посылаются на плату Arduino по последовательному порту. Третьим шагом стала разработка страницы HTML с панелью управления роботом (рис. 2в). Страница робота включает несколько кнопок управления для движения в разные стороны и регулятор скорости,

эти элементы управления, после обработки JavaScript, создают AJAX запросы на веб-сервер Raspberry Pi 3. Схема подключения представлена на рис. 2б.



а б в

Рисунок 2. Робот телеприсутствия, схема подключения и программа управления

В ходе исследования потребовалось изучить работу платформы с применением нескольких вариантов управления, чтобы выполнять простые функции, такие как: вперед, назад, влево, вправо и остановка. Разработанный робот телеприсутствия управляется с помощью веб-интерфейса и передачи потокового видео. Были проанализированы различные веб-интерфейсы пользователя и выбран наилучший веб-сервер для управления. В результате выполненных исследований была решена задача, актуальная для каждой теле-роботизированной системы - создание пользовательского интерфейса, который будет одновременно эргономичным и простым в использовании.

Литература

1. Build a Python Web Server with Flask [Электронный ресурс]. – Режим доступа: https://projects.raspberrypi.org/en/projects/python-web-server-with-flask. – (18.02.2018).

2. VNC (VIRTUAL NETWORK COMPUTING) [Электронный ресурс]. – Режим доступа: https://www.raspberrypi.org/documentation/remote-access/vnc/. – (21.10.2017).

ПРОБЛЕМЫ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РОЕВОГО УПРАВЛЕНИЯ БПЛА

К. Ю. Ганьшин, Д. А. Бондаренко, Ф. В. Самойлов
руководитель – старший преподаватель
межинститутской базовой кафедры ***А. М. Исаев***
Северо-Кавказский федеральный университет, г. Ставрополь

Роевое управление беспилотными летательными аппаратами – одна из свежих задач в дисциплине конструирования передвижных робототехнических систем, развивающаяся благодаря доступности и дешевизне как компонентов, составляющих цельную конструкцию, так и технологий её моделирования и проектирования. Разрабатываемое ПО подразумевает универсальность в применяемых БПЛА, однако на данном этапе ориентировано на мультироторную систему «Альбатрос». Проблема заключается в невозможности выполнять расчёты курса непосредственно на БПЛА, а использование мобильных компьютерных систем для данной задачи вместе с управляющим ПО может породить замирания и задержки в общей цепи выполнения управления. Конечной целью является создание ПО, контролирующего ход выполнения команд множеством БПЛА, получающим обработанные данные из удалённого дата-центра.

Ключевые слова: БПЛА, квадрокоптер, роевое управление, проблемы навигации.

Программное обеспечение, разрабатываемое для роевого управления мультироторными системами, на данном этапе являет собой координирующий центр: модемы БПЛА подключаются к одному переносному ПК с работающим ПО. Пользователь видит базовую информацию о состоянии каждой подключённой системы: текущее местоположение в пространстве, скорость перемещения, магнитный курс, статусы работы систем навигации, ошибки датчиков и т.п. Также пользователю доступны базовые настройки и команды управления: настройка количества БПЛА в рое, привязка физических интерфейсов модемов к визуальным блокам управления, команды взлёта/посадки, перемещения и приостановки выполнения курсирования.

Разработка ведётся с использованием технологии Qt [1]. Данная технология выбрана в связи с её кроссплатформенностью и удобной надстройкой над языком C++ в виде фреймворка. Программный код пишется на языке C++ соответственно, визульная составляющая (GUI) построена с использованием QtDesigner.

Мультироторная система «Альбатрос» является транспортируемой и быстросборной, её время нахождения в воздухе от полного заряда аккумуляторов до разряда составляет 25 минут [2], что оказывается достаточным для выполнения исследовательских задач. Обмен данными между БПЛА и наземной станцией выполняется по беспроводному шифрованному каналу, модем наземной системы использует протокол последовательного порта, реализуемый через шину USB, для обмена данными с компьютером. Та-

ким образом, управление БПЛА представляет собой коммуникацию с использованием пакетов байтов фиксированной длины. Для задач роевого управления применим пакет, позволяющий перемещать квадрокоптер в относительной системе координат. Пакет позволяет совершать управляемой машине простые перемещения и вращения на малые дистанции: перемещения в горизонтальной плоскости в четырёх направлениях относительно носовой части БПЛА, повороты по часовой и против часовой стрелки, перемещение вверх и вниз (изменение высоты). В одном пакете данного типа возможно задать смещение лишь по одной из степеней свобод с указанием масштаба смещения. Однако, данный подход не подразумевает прецизиозности, отчего маневрирование на малых дистанциях (около 2-3 метров) оказывается затруднительным. Другая проблема, возникающая при использовании управления данным пакетом байтов, – перемещения в виде рывков. В случае использования абсолютной навигации, БПЛА совершит перемещение в указанную точку плавно, т.к. наземной станции не приходится вносить корректировок по пути следования, а также не возникает потребности в длительной передаче управляющих пакетов. Однако, абсолютное динамическое управление технически не реализуемо в данной конфигурации.

На данном этапе исследования и разработки, из наземной части системы убран удалённый дата-центр. В виду того, что пока не используются сложные математические вычисления, требующие быстрой обработки поступающих пакетных данных, обработка выполняется в координирующем ПО. Под сложными математическими вычислениями подразумевается вычисление обходных траекторий при маневрировании и задач быстрого изменения строя в пространстве. Простые задачи, решаемые силами координирующей части: вычисление линейных траекторий для получения плоского строя, линейное перемещение всего строя по определённым координатам.

Как указано выше, невозможность указывать координаты в виде широты и долготы вынуждает перемещать БПЛА на дискретные отрезки до достижения конечной точки. В данном случае возникает проблема высокой погрешности. БПЛА использует навигацию на основе систем GPS и ГЛОНАСС. Как известно, среднеквадратичное значение погрешности навигации системы GPS с использованием приёмников общего назначения, находящих применение в смартфонах, составляет 4,9 м [4]; погрешность ГЛОНАСС оказывается на уровне 7 м [5]. Текущее ПО вычисляет дистанцию между точкой, в которой находится БПЛА, и точкой назначения. Для данного вычисления используется функция на основе синуса-версуса [3] (1):

$$d = 2r\ arcsin(\sqrt{hav(\varphi_1 - \varphi_2) + cos(\varphi_1)\,cos(\varphi_2)\,hav(\lambda_2 - \lambda_1)}) \quad (1)$$

В выражении (1) φ_1и φ_2– широты начальной и конечной точек в радианах, λ_1 и λ_2 – долготы начальной и конечной точек в радианах. Основ-

ная проблема заключается в параметре r, который выражает радиус, в данном случае – радиус Земли. Как известно, радиус планеты не является константой, поэтому при использовании среднего значения (6,371.0088 км) и модели сферы появляется навигационная ошибка, составляющая до 0.3%, что эквивалентно 19 км. Несмотря на существование более точных методов расчётов, выражение (1) вычисляется за небольшой промежуток времени (до 2 мкс с использованием процессоров i5 первого поколения). Возможно внедрение коррекции в параметр r в виде вычисленного радиуса от центра до поверхности Земли в точке нахождения БПЛА.

Помимо вычисления дистанции, необходимо получать и пеленг, т.к. носовая часть БПЛА должна быть повёрнута в направлении конечной точки перед началом совершения линейного перемещения. В данном случае используется выражение (2):

$$\theta = arctan2(\, sin(\Delta\lambda)cos(\varphi 2), cos(\varphi 1)sin(\varphi 2) - sin(\varphi 1)cos(\varphi 2)\, cos(\Delta\lambda)\,) \quad (2)$$

В выражении (2) φ_1и φ_2– широты начальной и конечной точек в радианах, $\Delta\lambda$ – разность долгот начальной и конечной точек в радианах.

Другая часть проблем, возникающих в использовании полной системы из вычислительных станций и БПЛА, связана с каналами связи. Часть данных последовательного порта может не достигать БПЛА, возможны потери части пакетов на стороне наземных машин. Ввиду этого, следует вводить защитные интервалы как по времени, так и по вычисляемым отрезкам, на которые следует переместиться конкретному БПЛА. Данные подходы снижают вероятность возникновения ошибок, но увеличивают время на выполнение задач перемещений.

Литература

1. About Qt http://wiki.qt.io/About_Qt
2. Комплекс с БЛА «Альбатрос» https://stilsoft.ru/catalog/Albatros
3. What is the best way to calculate the distance between 2 points? https://www.movable-type.co.uk/scripts/gis-faq-5.1.html
4. GPS Accuracy https://www.gps.gov/systems/gps/performance/accuracy/
5. Точность измерений псевдодальностей ГЛОНАСС http://www.sdcm.ru/smglo/errs?-version=rus&repdate&site=extern

МИКРОКОНТРОЛЛЕРЫ В СОВРЕМЕННОЙ РОБОТОТЕХНИКЕ

А. А. Гусейнов, Д. В. Иванников
руководитель – старший преподаватель
межинститутской базовой кафедры ***А. М. Исаев***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрены возможности и особенности микроконтроллеров, используемых в современной робототехнике, а также семейства чипов и разработанные на их базе устройства. Представлены некоторые аспекты программирования, приведены рекомендации для начинающих программистов микроконтроллеров.

Ключевые слова: микроконтроллер, arduino, микроконтроллер AVR, программирование микроконтроллеров, регистровая память.

Микроконтроллерами называют особый вид микросхем, используемый для управления различными электронными устройствами. Обычно в микроконтроллерах есть функции процессора, периферийных устройств, а также имеется оперативная память и / или постоянное запоминающее устройство (ПЗУ) [4].

Микроконтроллеры широко используются в вычислительной технике, бытовой электронике, промышленности, робототехнике и т. д.

Существует несколько семейств микроконтроллеров. Чаще всего используются микроконтроллеры следующих семейств:

- MSP430 (TI);
- ARM (ARM Limited);
- MCS 51 (INTEL);
- STMB (STMicroelectronics);
- PIC (Microchip);
- AVR (Atmel);
- RL78 (Renesas Electronics).

Одной из популярных в электронной промышленности является продукция компании Atmel, построенная на базе RISC-ядра. В линейке устройств Arduino в основном применяются микроконтроллеры семейства Atmel AVR [6].

Arduino – платформа для разработки различного рода электронных устройств и автоматических систем. На данной платформе возможно создать умный дом с множествами функция, таких как автоматической подачи еды для домашнего питомца, полив растений, идентификация человека по голосу, отпечаткам пальца и т. д.

Микроконтроллеры AVR оснащены Гарвардской архитектурой. Каждая из областей памяти располагаются в своем адресном пространстве. Память данных в контроллерах осуществляется посредством регистровой, энергонезависимой и оперативной памяти.

Регистровая память предусматривает наличие 32 регистров общего назначения, которые объединены в файл, а также служебные регистры для ввода и вывода. Оба регистра располагаются в пространстве ОЗУ, однако не являются его частью.

В области PBB (регистров ввода и вывода) находятся различные служебные регистры – состояния, управления микроконтроллером и т. д., а также регистры, которые отвечают за управление периферийных устройств, являющихся частью микроконтроллера. По сути, управление данными регистрами и является методом управления микроконтроллером.

Микроконтроллеры AVR являются простыми в использовании, имеют низкую потребляемую мощность и высокий уровень интеграции.

Обычно, такие микроконтроллеры могут использоваться на самых разных устройствах, в том числе системах общего назначения, системах оповещения, для ЖК-дисплеев, плат с ограниченным пространством.

Кроме того, они используются для измерителей уровня заряда аккумулятора, аутентификации, в автомобильной электронике, для защиты от короткого замыкания и перегрева и т. д. Кроме промышленных целей, микроконтроллеры могут использоваться (и чаще всего используются новичками) для создания следующих устройств:

- регистратор температуры на Atmega168;
- кухонный таймер на Attiny2313;
- термометр;
- измеритель частоты промышленной сети на 50 Гц;
- контроллер светодиодного стоп-сигнала на Attiny2313;
- светодиодные лампы и светильники, реагирующие на температуру или звук;
- электронные или сенсорные выключатели.

Стоит отметить, что для разных устройств используются разные модели микроконтроллеров. Так, 32-разрядные микроконтроллеры AVR UC3 (а также XMEGA, megaAVR, tinyAVR и т. д.) подойдут для систем общего назначения с технологиями picoPower, QTouch, EEPROM, системами обработки событий и самопрограммированием [1 – 3].

Если вы собираетесь программировать микроконтроллеры, такие как Ардуино, например, а также собирать устройства, которые предусматривают их наличие в схеме, необходимо учитывать некоторые правила и рекомендации:

- Перед решением любых задач следует делить их на более мелкие, вплоть до базовых действий.
- Не следует пользоваться кодогенераторами и прочими «упрощающими» материалами, хотя бы на начальных этапах.
- Рекомендуется изучить язык С и Ассемблер – это упростит понимание принципа работы микроконтроллеров и программ.

По своей структуре языки программирования микроконтроллеров мало отличаются от тех, что используются для персональных компьютеров. Среди них выделяют группы низкого и высокого уровня. Современные программисты в основном используют C/C++ и Ассемблер. Между приверженцами этих языков ведутся бесконечные споры о том, какой из них лучше.

Так как Ассемблер использует прямые инструкции, которые обращаются непосредственно к самому чипу это требует от программиста безукоризненное знание системных команд процессора. Потому Ассемблер в последнее время используется все реже, несмотря на то что главным преимуществом языка является высокая скорость исполнения готовой программы.

На самом деле, можно использовать практически любые языки программирования микроконтроллеров. Но популярнее всех C/C++. Это язык высокого уровня, позволяющий работать с максимальным комфортом. Более того, в разработке архитектуры AVR принимали участие создатели Си. Поэтому микросхемы производства «Atmel» адаптированы именно к этому языку.

C/C++ – это гармоничное сочетание низкоуровневых и высокоуровневых возможностей. Поэтому в код можно внедрить вставки на Ассемблере. Готовый программный продукт легко читается и модифицируется. Скорость разработки достаточно высокая. При этом досконально изучение архитектуры МК и системы команд ЦП не требуется. Компиляторы Си снабжаются библиотеками внушительного размера, что облегчает работу программиста.

Выбор оптимального языка программирования зависит также от аппаратного обеспечения. При малом количестве оперативной памяти использовать высокоуровневый Си нецелесообразно. В данном случае больше подойдет Ассемблер. Он обеспечивает максимальное быстродействие за счет короткого кода программы. Универсальной среды программирования не существует, но в большинстве бесплатных и коммерческих приложений можно использовать как Ассемблер, так и C/C++ [5].

Литература

1. Баранов В. Н. Применение микроконтроллеров AVR: схемы, программы и алгоритмы. М.: Издательский дом «Додэка-XXI», 2006. 288 с.

2. Мортон Дж. Микроконтроллеры AVR: вводный курс. М.: Издательский дом «Додэка-XXI», 2008. 271 с.

3. Прокопенко В.С. Программирование микроконтроллеров ATMEL на языке С. М.: МК-Пресс, 2012. 394 с.

4. Микроконтроллеры: что это такое и зачем нужны [Электронный ресурс]. – URL: https://arduinoplus.ru/mikrokontrollery-chto-eto-takoe/#i-5 (Дата обращения: 26.04.2018).

5. Программирование микроконтроллеров для начинающих [Электронный ресурс]. – URL: https://arduinoplus.ru/programmirovanie-mikrokontrollerov-dlya-nachinayuschih/#i-3 (Дата обращения: 26.04.2018).

6. Самые популярные микроконтроллеры и платы Atmel [Электронный ресурс]. URL: https://arduinoplus.ru/mikrokontrollery-atmel/ (Дата обращения: 26.04.2018).

ИССЛЕДОВАНИЕ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА СИСТЕМЫ УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫМИ СИСТЕМАМИ

Н. В. Ледовская, А. В. Шевченко, Д. Б. Таникеев
руководитель – старший преподаватель межинститутской базовой кафедры ***А. В. Шипулин***
Северо-Кавказский федеральный университет, г. Ставрополь

Графический интерфейс является наиболее популярным видом пользовательских интерфейсов, с его помощью происходит взаимодействие пользователя с информационной системой. В данной работе проанализированы направления развития интерфейсов информационных систем, описан разработанный графический интерфейс системы управления роботизированной системой, были рассмотрены основные элементы главного окна, выявлены основные черты интерфейса.

Ключевые слова: информационная система, роботизированная система, пользовательский интерфейс, графический интерфейс, программный пакет WinForms, платформа .NET Framework.

Роль информационных технологии в жизни людей увеличивается с каждым годом. Практически каждое современное предприятие имеет свою собственную информационную систему, которая позволяет сохранить все необходимые для предприятия данные, чем самым поддерживать его деятельность.

Информационной системой называют взаимосвязанную совокупность средств, а также методов и персонала, которые используются для хранения, обработки и выдачи информации необходимой для достижения поставленных целей [4].

В информационных технологиях конечного пользователя большую роль играет пользовательский интерфейс, с его помощью реализуется работа пользователя ПК посредством элементов взаимодействия [2, с. 563]. Существует общепринятая классификация интерфейсов, согласно которой они подразделяются на следующие виды:

- Текстовый пользовательский интерфейс (TUI);
- Интерфейс командной строки (CLI);
- Графический пользовательский интерфейс (GUI);
- Голосовой пользовательский интерфейс (VUI);
- Натуральный пользовательский интерфейс (NUI);
- Перцептивный пользовательский интерфейс (PUI);
- Интерфейсы мозг-компьютер (ИМК) [1, с. 21].

Более подробно рассмотрим графический пользовательский интерфейс информационной системы (ИС) управления роботизированными системами. Графический пользовательский интерфейс обеспечивает взаимодействие пользователя с программой с помощью мыши и клавиатуры или использованием пунктов меню в окне программы.

Графический пользовательский интерфейс разработанной ИС управления роботизированными системами создан с помощью средств стандартного пакета WinForms для C# на платформе .NET Framework [3, с. 144]. Выбор данного программного пакета позволил добиться снижения уровня возникновения программных ошибок, а также более быстрой и упрощенной работы.

Главное окно ИС управления роботизированными системами (рис. 1) поделено на 5 основных частей:

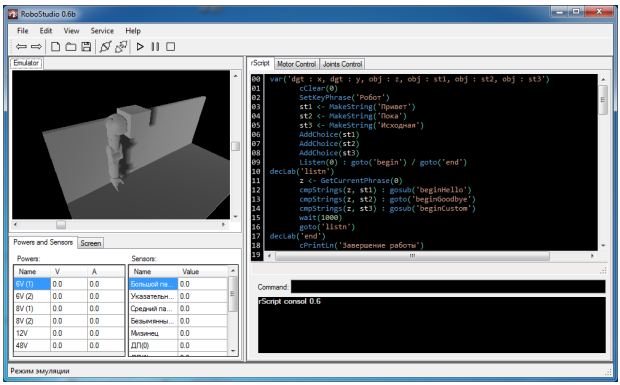


Рисунок 1. Интерфейс главного окна ИС управления роботизированными системами

Главное окно системы поделено на 5 основных областей:

– Панель управления (рис. 2) состоит из следующих элементов:

Рисунок 2. Панель управления ИС

– кнопка отмены – данную кнопку можно использовать для отмены последнего выполненного действия;

– кнопка повтора ввода – данная кнопка позволяет вернуть последнее действие;

– кнопка создания нового проекта – данная кнопка производит инициализацию создания нового проекта;

– кнопка открытия проекта – данная кнопка выводит окно необходимое для загрузки проекта из файла;

– кнопка сохранения проекта – данная кнопка позволяет сохранить проект в файл.

– Панель 3-мерной визуализации (рис. 3) выводит на экран трех мерную модель выбранной для роботы робототехнической системы, с по-

мощью данной панели существует возможность удаленного контроля за выполнением сценария роботизированной системы, в результате принятия позы подключенного физического оборудования.

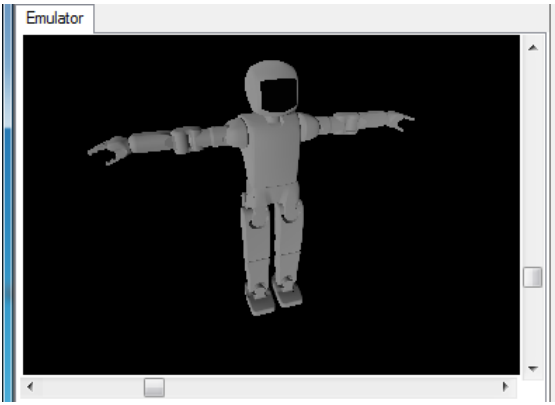


Рисунок 3. Панель з-х мерной визуализации ИС

– Текстовый редактор среды разработки (рис. 4) данное поле служит для введения сценариев работы роботизированной системы управления.

Рисунок 4. Текстовое поле ИС

– Панель мониторинга оборудования (рис. 5) данная панель позволяет в конкретный момент времени отследить за показаниями всевозможных датчиков и сенсоров, а также получить информацию о потребляемом токе и подающемся напряжении.

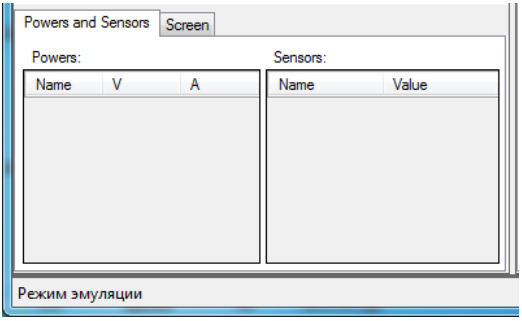


Рисунок 5. Панель мониторинга оборудования ИС

– Программная консоль (рис. 6) текстовое поле, предназначенное для вывода на экран системных и программных сообщений.

Рисунок 6. Программная консоль интерпретатора

Разбиение главного окна на области удалось выполнить благодаря использованию стандартного класса .NET SplitContainer. Данный класс также дает возможность в рассматриваемом интерфейсе изменять размеры панелей, их положение и ряд других параметров отображения.

Таким образом, можно сделать вывод, что графический интерфейс данной ИС обладает гибкой настройкой, благодаря использованию специального класса, задачами которого являются: изменение положения элементов, окон и панелей, добавление элементов управления, сохранение настроек с возможностью их дальнейшего запуска из конфигуратора.

Литература

1. Ледовская Н. В., Маркарян Д. М., Основные типы и характеристики пользовательских интерфейсов. 2018. № 1. С. 21-22.

2. Мезенцева О. С., Бадалов Б. М., Ганьшин К. Ю., Попова Н. В., Разработка системы голосового управления робототехническими системами. В сборнике: Студенческая наука для развития информационного общества Сборник материалов V Всероссийской научно-технической конференции. 2016. С. 563-567.

3. Мезенцева О. С., Бадалов Б. М, Разработка программы визуализации данных для системы «Синергет». В сборнике: Студенческая наука для развития информационного общества, Сборник материалов I Всероссийской научно-технической конференции. 2015. С. 143-145.

4. Мезенцева О. С., Трофимова М. В., Интеллектуальные системы и технологии. Рецензенты: профессор В. И. Дроздова, профессор Н. В. Кандаурова. Ставрополь, 2013.

РАЗРАБОТКА ВЫСОКОТЕМПЕРАТУРНОГО ПРЕОБРАЗОВАТЕЛЯ ДАВЛЕНИЯ ДЛЯ СПЕЦИАЛИЗИРОВАННЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ

В. М. Матвеев
руководитель – канд. техн. наук,
старший научный сотрудник ***И. В. Годовицын***
НПК «Технологический центр», г. Зеленоград

В статье рассматривается разработка преобразователя давления для автономных робототехнических систем. Описана структура "кремний-на-изоляторе", которая позволяет реализовывать преобразователи давления с расширенным температурным диапазоном, высокими измерительными характеристиками, малыми размерами и весом и низкой себестоимостью. Рассмотрена конструкция чувствительного элемента (ЧЭ) *давления, особенности конструкции кристалла мембраны, имеющего сложную профилированную форму, которая образуется в результате глубокого анизотропного жидкостного травления кремния. Описаны основные этапы технологического маршрута кристалла мембраны на КНИ-структуре незначительно отличаются от таковых при изготовлении кристалла мембраны на обычной пластине, используемой в серийном ЧЭ. Проводится обсуждение полученных результатов.*

Ключевые слова: высокотемпературный кремниевый преобразователь давления, КНИ-структура, датчик давления, робототехническая система.

Высокотемпературные преобразователи давления незаменимы в применениях, требующих измерение давления при высокой температуре и жестких условиях окружающей среды. В настоящее время в специальных робототехнических системах существует потребность в измерении давления при высокой температуре с минимальной абсолютной погрешностью. Данная задача чаще всего решается при помощи импортных дорогих высокотемпературных кремниевых преобразователей давления. В настоящее время в НПК «Технологический Центр» разработана серия отечественных высокотемпературных преобразователей давления, которая может использоваться в робототехнических системах.

Структура «кремний-на-изоляторе» (КНИ) обладает целым рядом важных достоинств, позволяющих решать наиболее сложную задачу – разработку и изготовление высокотемпературного ЧЭ. КНИ-структуры формируются с помощью спекания двух окисленных кремниевых пластин и шлифовки одной из них до требуемой толщины (bonded SOI), и широко используются как исходный материал для формирования МЭМС-приборов [1-3] и, в частности, преобразователей давления.

В данной работе проведена разработка конструкции ЧЭ высокотемпературного преобразователи давления на основе КНИ-структуры для температурного диапазона от -45 °С до +220 °С. При разработке конструкции использован многолетний опыт НПК "Технологический центр" в об-

ласти создания кремниевых преобразователей давления. Эскиз конструкции ЧЭ высокотемпературного преобразователя давления приведен на рисунке 1. В качестве основы использована конструкция ЧЭ, используемого в датчиках давления серии ИПД5. ЧЭ состоит из 3х частей: основания, прокладки и кристалла мембраны. Кристалл мембраны формируется из КНИ-пластины. Основание обеспечивает крепление кристалла мембраны к корпусу. Прокладка соединяет основание и кристалл мембраны. Тензорезисторы расположены в местах концентрации механических напряжений на кристалле мембраны. Кристалл мембраны непосредственно осуществляет преобразование давления в выходное напряжение. Части кристалла преобразователя соединены между собой легкоплавким стеклом.

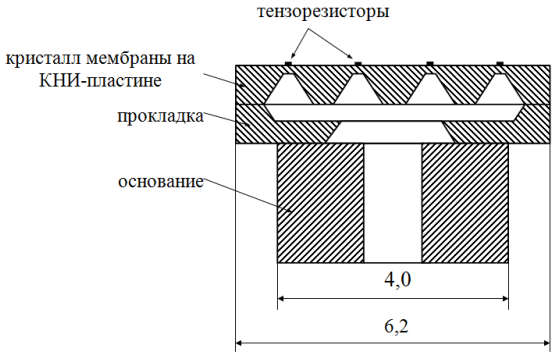


Рисунок 1. Эскиз конструкции ЧЭ высокотемпературного преобразователя давления

Предложенная конструкция ЧЭ высокотемпературного преобразователя давления имеет ряд характерных особенностей. В частности, кристалл мембраны имеет сложно-профилированную форму, которая образуется в результате глубокого анизотропного жидкостного травления кремния. Сформированные пирамидки из монокристаллического кремния обеспечивают достижение максимального уровня механических напряжений в заданных точках мембраны. Основные этапы технологического маршрута изготовления кристалла мембраны с использованием КНИ-структуры незначительно отличаются от таковых при изготовлении кристалла мембраны с диффузионными тензорезисторами, используемого в серийном ЧЭ. Схожесть основных этапов изготовления позволяет использовать набор одинаковых процессов, что существенно облегчает реализацию этапов разработки и исследования. Кроме того, одинаковые технологические маршруты позволяет проводить обоснованную оценку качественных характеристик преобразователя.

На первом этапе (рис. 2а) на пластину наносятся защитные диэлектрические слои, играющие роль защитной маски при травлении, на обрат-

ной стороне выполняется фотолитография, вскрываются окна к кремнию и проводится глубокое травление кремния с помощью концентрированного раствора КОН. В результате формируются выступы из монокристаллического кремния, имеющие форму правильной пирамидки с квадратным основанием – жесткие центры (рис. 2б). Они расположены на мембране симметрично относительно центра и обеспечивают максимальную величину механических напряжений на участках мембраны, расположенных между ними. Далее защитные слои удаляются, и с лицевой стороны пластины проводится фотолитография тензорезисторов и плазмохимическое травление монокристаллического кремния. В результате формируется мостовая схема ЧЭ преобразователя. Тензорезисторы и шины разводки легируются бором. Доза легирования шин разводки выбирается исходя из необходимости снижения паразитного сопротивления, то есть достижения концентрации $(5\text{-}8)\cdot 10^{19}$ см$^{-3}$. Полученная структура из монокристаллического кремния окисляется до толщины окисла 0,1-0,2 мкм. В окисле формируются контактные окна и контактные площадки из металла, стойкого к высокой температуре, например, золота или платины. Далее кристалл мембраны соединяется с другими деталями ЧЭ с помощью легкоплавкого стекла (рис. 2в).

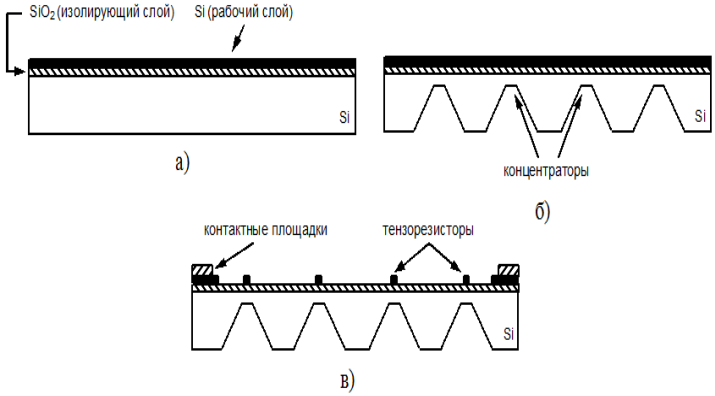


Рисунок 2. Основные технологические этапы изготовления кристалла мембраны

Сформированный ЧЭ размещается в корпусе, который должен удовлетворять требованиям стойкости к высокой температуре (более 150 °С). В наибольшей степени для этого подходят металлостеклянные цилиндрические корпуса типа ТО-5, которые позволяют легко интегрировать в конструкцию штуцера для подачи давления, как со стороны основания, так и со стороны крышки. Это позволяет варьировать конструкцию преобразователя путем изменения стороны мембраны, на которую подается давление. В России большой ассортимент корпусов ТО-5 производится на заводе «Марс» (г. Торжок). Данные корпуса выдерживают температуру более 300 °С.

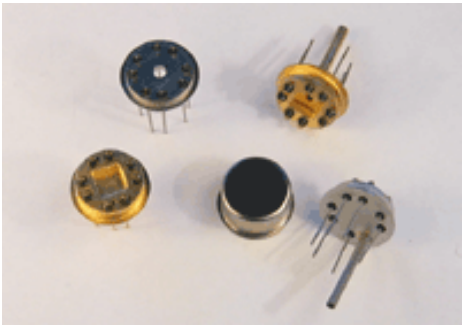


Рисунок 3. Корпуса ТО-5 производства завода «Марс» (г. Торжок)

Монтаж ЧЭ в корпус типа ТО-5 может осуществляться несколькими способами. В качестве одного из них может быть названа пайка на эвтектический припой. Эвтектическая пайка обебспечивает прочное соединение ЧЭ с корпусом, которое одновременно обладает высокой теплопроводностью, что позволяет эффективно отводить тепло от ЧЭ. В то же время высокая жесткость соединения через эвтектическую пайку может внести дополнительные механические напряжения в ЧЭ при изменении температуры и тем самым ухудшить характеристики преобразователя. Наиболее приемлемым подходом для решения проблемы посадки ЧЭ в корпус представляется использование высокотемпературных силиконовых герметиков, таких как "Эласил" или "Эластосил". Данные герметики благодаря своему составу обладают свойством не только выдерживать достаточно высокую температуру (до 250 °С), но и сохраняют при повышенной температуре свои упругие свойства. Кроме того, технология посадки ЧЭ в корпус при использовании силиконового герметика существенно упрощается и удешевляется. В то же время выбор конкретной технологии посадки ЧЭ в корпус определяется разработчиком исходя из совокупности всех требований к конструкции и условий использования преобразователя.

Электрическое соединение ЧЭ с корпусом представляется другим важным технологическим узлом изготовления высокотемпературного преобразователя давления. Электрическое соединение должно обеспечивать не только контакт с минимальным сопротивлением, но и надежное механическое соединение во всем диапазоне рабочих температур. Кроме того, при разработке конструкции и технологии электрического соединения необходимо учитывать, что высокая температура приводит к ускорению электрохимических и эвтектических процессов в контактных соединениях, что через определенное время может привести к драматическому изменению их свойств [4-5]. В наибольшей степени для обеспечения электрического соединения в высокотемпературном датчике давления подходит металлургическая система «золото-золото». Использование золота для контактных площадок и электродных выводов традиционно для технологии

интегральных микросхем. Металлургическая система «золото-золото» обладает наивысшей надежностью среди применяемых. Благодаря применению металла одного типа при воздействии повышенной температуры не образуется интерметаллических соединений, не происходит межкомпонентной коррозии и других процессов, ведущих к ухудшению контакта. При повышенной температуре и с течением времени прочность соединения металлургической системы "золото-золото" только увеличивается, поэтому даже недостаточно качественная сварка не приводит к выходу изделия из строя [6].

Работы выполнены при финансовой поддержке Министерства образования и науки Российской Федерации (Соглашение № 14.577.21.0245, уникальный идентификатор ПРИЭР RFMEFI57717X0245). В работе использовалось оборудование ЦКП «Функциональный контроль и диагностика микро- и наносистемной техники» (ЦКП НПК «Технологический центр»).

Литература

1 Maszara W. P., SOI by Wafer Bonding: A Review // International Symposium on SOI Technology and Devices, Montreal, 1990.

2 Auberton-Herve A.J., SOI: materials to systems, Proc. of International Electron Devices Meeting, 1996. IEDM '96, pp.3-10.

3 Gan C.L., Hashim U., Evolutions of bonding wires used in semiconductor electronics: perspective over 25 years // Journal of Materials Science: Materials in Electronics July 2015, Volume 26, Issue 7, pp. 4412–4424.

4 Breach C.D., What is the future of bonding wire? Will copper entirely replace gold? // Gold Bulletin, Volume 43 No 3 2010, pp.150-167.

5 Levine L., Wire Bonding // Electronic Device Failure Analysis, Volume 18, 2016, No. 1, pp.22-28.

6 http://eesemi.com/wirebond-metallurgies.htm (дата обращения 31.01.2018).

АНАЛИЗ МЕТОДОВ ПЛАНИРОВАНИЯ И ОПТИМИЗАЦИИ ПУТИ НА ОСНОВЕ СИНТЕЗА СИСТЕМЫ ГЛОБАЛЬНОГО ПОЗИЦИОНИРОВАНИЯ И АЛГОРИТМОВ ПРОГНОЗИРОВАНИЯ ТРАЕКТОРИИ

А. С. Павлов, Д. А. Щербаков
руководитель – д-р физ.-мат. наук, доцент ***Ф. Б. Тебуева***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье приведен анализ методов планирования и оптимизации пути на основе синтеза системы глобального позиционирования и алгоритмов прогнозирования траектории. Представлена классификация используемых методов для прогнозирования пути, исследованы достоинства и недостатки каждого из них.

Ключевые слова: беспилотный автомобиль, мультиагентная система, планирование пути, прогнозирование траектории, децентрализованное управление, система глобального позиционирования.

Прогнозирование информации движения транспортных средств является актуальной задачей для разработки как системы управления беспилотным автомобилем, так и усовершенствованной системы помощи водителю и предотвращения столкновений в интеллектуальной транспортной системе. На практике проблема локализации транспортного средства становится еще более сложной, особенно в таких условиях, где сигналы GPS слабы или отсутствует вовсе [1]. В процессе формирования траектории GPS является наиболее широко используемым методом позиционирования транспортного средства, поскольку она может обеспечить точную и надежную локализацию и навигацию автомобиля в наружной среде. Однако ухудшение точности GPS неизбежно из-за блокировки спутниковых сигналов и эффекта многолучевого распространения в плотной городской среде. Чтобы решить эту проблему, в работах [2] предложен многопользовательский метод слияния данных. Так, комбинированная инерциальная навигационная система GPS (INS), стала одной из наиболее перспективных технологий, поскольку INS в состоянии внести поправки в GPS-ошибку в сложной городской среде [3]. Для борьбы с гетерогенным синтезом информации в интеграции GPS/INS фильтр Калмана является классическим методом определения местоположения транспортного средства и траектории [4]. Однако он не может решить нелинейные/негауссовые задачи, что приводит к неточному моделированию траектории и усложнению вычислений. Фильтр частиц считается эталоном метода фильтрации для прогнозирования положения транспортного средства [5]. Недостаток этого метода заключается в том, что требует большого количества частиц и, следовательно, приводит к трудоемкому вычислительному алгоритму [6]. В последние годы широко изучены методы машинного обучения, такие как искусственная нейронная сеть (ANN), нейронные сети обратного распространения (BPNN), случайная регрессия (RFR), регрессия Гаусса (GPR) [7] благодаря их способностям решать проблему нелинейности и неопределенности при планировании пути. Хотя эти методы хорошо работают в позиционировании на основе GPS/INS, они не могут работать в режиме реального времени и высокой точности, которые обязательны для беспилотных транспортных средств. В дополнение к методу слияния данных в позиционировании транспортного средства внешний Инерциальный измерительный блок (ИИБ) является наиболее широко используемым оборудованием для внедрения INS в GPS-позиционировании на основе интеграции GPS/INS и построения траектории, например, смартфонов, встроенных в GPS-приемник и ИИБ датчики могут быть использованы для формирования траекторий транспортных средств [8]. Тем не менее, этот метод является немасштабируемым. Основная причина заключается в том, что данные траектории транспортного средства являются неполными и прерывистыми, поскольку навигационная система смартфонов не будет использоваться во время вождения. Более того, большинству водителей не

нужна навигация смартфонов, так как они знакомы с маршрутом для их часто посещаемых мест в своем городском вождении. Бортовая навигационная система предлагает альтернативное решение для отслеживания транспортных средств и может использоваться для сбора траектории. Однако, несмотря на то, что трассировка транспортного средства может отображаться на экране консоли, данные бортовой навигации представлены в машинном формате, что ограничивает возможность использования необработанных данных траектории без предварительной обработки.

В работе [9] представлен разработанный подход на основе взаимодействующих множественных моделей (IMM) и расширенного фильтра Калмана (EKF) для отслеживания траектории динамических целей, состояние моделей которых измеряется в режиме реального времени. Несмотря на преимущества IMM для решения задач отслеживания объектов с сильной нелинейной динамикой, EKF делает общий метод расходящимся, поскольку последний чувствителен к ошибкам линеаризации, что приводит к худшей оценке точности, особенно в периоды отключения GPS [10]. С другой стороны, для успешной работы прогнозирования, основанной на интеграции GPS / INS, в литературе также широко используется интеллектуальная адаптивная система прогнозирования нейро-нечеткой логики (ANFIS). Более высокая эффективность ANFIS с точки зрения точности предсказания в отношении других интеллектуальных методов в основном связана с комбинацией системы нейронной сети (NN) и нечеткой логики (FL) [11]. Однако основные недостатки связаны с подготовкой и обновлением параметров ANFIS и плохой динамической адаптацией, а также большим количеством вычислений. Поэтому, для решения проблем оптимизации параметров были представлены различные методы, такие как оптимизация роя частиц (PSO) [12] и генетический алгоритм (GA) [14]. PSO является одним из наиболее эффективных методов эволюционной оптимизации [15, 16], которые могут достичь быстрой конвергенции, в то время как склонны к попаданию в локальный минимум. Байесовская оптимизация широко применяется для настройки параметров машинного обучения алгоритмы [17, 18]. Хотя этот метод демонстрирует хорошую сходимость, скорость работы алгоритма слишком медленная для функционирования в режиме реального времени. С решения этой проблемы в работе [21] предложен модифицированный алгоритм оптимизации роя (LS-PSO), позволяющий корректировать параметры глобального и локального поиска, что позволяет получить оптимальные параметры прогноза положения транспортного средства. В работе [12] предложен ANFIS на основе PSO для интеграции систем GPS и INS с целью обеспечения надежного навигационного решения в разные периоды отключения GPS. Хотя предлагаемый метод обеспечивает хорошую производительность при коротких и длительных отключениях GPS, этот метод не тестировался в других условиях сигнала GPS, например, во время частичных отключений GPS. В работе [19]

был предложен вероятностный подход, названный байесовским разреженным случайным гауссовым предсказанием (B-SRGP), для решения проблемы прогнозирования траектории движения транспортного средства во время отключений GPS. Несмотря на то, что предлагаемый метод прогнозирования обеспечивает лучшую производительность по сравнению с существующими методами прогнозирования, он также имеет определенные недостатки, связанные с требованием очень высокой вычислительной мощности из-за плохого управления параметрами измерительной матрицы, главным образом, когда количество транспортных средств группы увеличивается. В работе [20] предложен метод гибридного прогнозирования, основанный на модели GPS / INS, которая обеспечивает лучшую точность позиционирования транспортного средства даже во время полных и частичных отключений GPS. Предлагаемый подход объединяет преимущества как системы нечеткого вывода (FIS), так и разреженных случайных гауссовских (SRG) моделей, следовательно, названных FIS-SRG, что приводит к существенному снижению ошибки прогнозирования местоположения транспортного средства. Вышеупомянутые отключения определяются путем корректировки массы распространения GPS, контролируемой гауссовой моделью и обновленной системой нечеткой логики. Сильные стороны FIS полагаются на то, что они способны не только обрабатывать лингвистические концепции, но и выполнять нелинейные сопоставления между входами и выходами. Успех этого подхода также обусловлен тем, что он смог обрабатывать модель измерения на основе модели интеграции GPS / INS с использованием разреженной случайной гауссовой (SRG) методики. Чтобы справиться с проблемой оптимизации, связанной с разрешающей матрицей, используется метод наименьшей абсолютной усадки и выбора (LASSO). Метод выбора (LASSO) является одним из подходящих оценок, широко используемых для обработки проблемы выбора переменных. С другой стороны, с целью управления потоком данных, генерируемым как INS, так и GPS, а затем получение приемлемой точности предсказания во время частичных периодов отключения GPS, размер скользящего окна используется, как предложено в [13].

Литература

1. C. Boucher, J.C. Noyer, A hybrid particle approach for GNSS applications with partial GPS outages, IEEE Trans. Instrum. Meas. 59 (3) (2010) 498–505.

2. B. Khaleghi, A. Khamis, F. O. Karray, and S. N. Razavi, «Multisensor data fusion: A review of the state-of-the-art, » Information Fusion, vol. 14, no. 1, pp. 28–44, 2013.

3. X. Li and Q. Xu, «A reliable fusion positioning strategy for land vehicles in gps-denied environments based on low-cost sensors,» IEEE Transactions on Industrial Electronics, vol. 64, no. 4, pp. 3205–3215, 2017.

4. V. Havyarimana, D. Hanyurwimfura, P. Nsengiyumva, and X. Zhu, «A novel hybrid approach based-SRG model for vehicle position prediction in multi-GPS outage conditions, » Information Fusion, vol. 41, pp. 1–8, 2018.

5. C. Barrios and Y. Motai, «Improving estimation of vehicle's trajectory using the latest Global Positioning System with Kalman Filtering, » IEEE Transactions on Instrumentation and Measurement, vol. 60, no. 12, pp. 3747–3755, 2011.

6. D. Bhatt, P. Aggarwal, V. Devabhaktuni, and P. Bhattacharya, «A novel hybrid fusion algorithm to bridge the period of GPS outages using lowcost INS,» Expert Systems with Applications, vol. 41, no. 5, pp. 2166– 2173, 2014.

7. P. Aggarwal, Z. Syed, and N. El-Sheimy, «Hybrid Extended Particle Filter (HEPF) for integrated civilian navigation system, » in Position, Location and Navigation Symposium, IEEE/ION, Monterey, CA, USA, 2008, pp. 984–992.

8. N. El-Sheimy, K. W. Chiang, and A. Noureldin, "The utilization of Arti- ficial Neural Networks for multisensor system integration in navigation and positioning instruments, » IEEE Transactions on Instrumentation and Measurement, vol. 55, no. 5, pp. 1606–1615, 2006.

9. R. Toledo-Moreo, M.A. Zamora-Izquierdo, B. Ubeda-Minarro, A.F. Gomez-Skarmeta, High-Integrity IMM-EKF-based road vehicle navigation with low-cost GPS/SBAS/INS, IEEE Trans. Intell. Transp. 8 (3) (2007) 491–511.

10. A. Lahrech, Boucher C, J.C. Noyer, Fusion of GPS and odometer measurements for map-based vehicle navigation, in: Proceedings of IEEE International Conference on Industrial Technology (ICIT'04), 2004, pp. 944–949.

11. W. Navneet, S. Harsukhpreet, S. Anurag, ANFIS: adaptive neuro-fuzzy inference system- a survey, Int. J. Comp. Applic. 123 (13) (2015) 32–38.

12. A.M. Hasan, K. Samsudin, A.R. Ramli, Optimizing of ANFIS for estimating INS error during GPS outages, J. Chin. Instit. Eng. 34 (7) (2011) 967–982.

13. G. Thomaidis, M. Tsogas, P. Lytrivis, G. Karaseitanidis, A. Amditis, Multiple hypothesis tracking for data association in vehicular networks, Inform. Fusion 14 (4) (2013) 374–383.

14. A.M. Hasan, K. Samsudin, A.R. Ramli, A novel intelligent predictor for low-rate global positioning system (GPS) system, Sci. Res. Essays 6 (11) (2011) 2348–2359.

15. Y. Bazi and F. Melgani, «Semisupervised PSO-SVM regression for biophysical parameter estimation, » IEEE Transactions on Geoscience and Remote Sensing, vol. 45, no. 6, pp. 1887–1895, 2007.

16. S. Chen, X. Hong, and C. J. Harris, «Particle Swarm Optimization aided orthogonal forward regression for unified datamodeling, » IEEE Transactions on Evolutionary Computation, vol. 14, no. 4, pp. 477–499, 2010.

17. T. T. Joy, S. Rana, S. Gupta, and S. Venkatesh, "Hyperparameter tuning for big data using Bayesian optimisation, » in International Conference on Pattern Recognition, Cancun, Mexico, 2016, pp. 2574–2579.

18. J. Snoek, H. Larochelle, and R. P. Adams, «Practical Bayesian optimization of Machine Learning algorithms," Computer Science, vol. 4, pp. 2951–2959, 2012.

19. 2V. Havyarimana, Z. Xiao, D. Wang, A novel probabilistic approach for vehicle position prediction in free, partial, and complete GPS outages, Math. Prob. Eng. 2015 (2015) 1–13.

20. V. Havyarimana, D. Hanyurwimfura, P. Nsengiyumva, Z. Xiao. A novel hybrid approach based-SRG model for vehicle position prediction in multi-GPS outage conditions. Information Fusion, Elsevier, May 2018. http://dx.doi.org/10.1016/j.inffus.2017.07.002.

21. GOI: A Novel Design for Vehicle Positioning and Trajectory Prediction under Urban Environments Zhu Xiao, Member, IEEE, Pingting Li, Vincent Havyarimana, Hassana Maigary Georges, Dong Wang, Member, IEEE, and Keqin Li, Fellow, IEEE. DOI 10.1109/JSEN.2018.2826000.

МЕТОДЫ ОПТИМИЗАЦИИ ТРАЕКТОРИИ ДВИЖЕНИЯ ГРУППЫ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ НА ОСНОВЕ МУЛЬТИАГЕНТНЫХ ТЕХНОЛОГИЙ

А. С. Павлов, М. Г. Огур
руководитель – д-р физ.-мат. наук, доцент ***Ф. Б. Тебуева***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье представлен обзор методов оптимизации траектории движения группы беспилотных транспортных средств на основе мультиагентных технологий. Приведены достоинства и недостатки централизованного и децентрализованного подходов оптимизации. Проанализированы известные методы на основе консенсуса и декомпозиции задач.

Ключевые слова: беспилотный автомобиль, мультиагентная система, планирование пути, прогнозирование траектории, децентрализованное управление.

За последнее десятилетие в использовании беспилотных систем наблюдается заметный рост. Эти технологии находят применение в военных разведывательных операциях, миссиях пограничного патрулирования, обнаружения лесных пожаров и т.д. С развитием новых алгоритмов, которые обеспечивают более высокий уровень автономии, тип миссий, выполняемых этими системами становится все более сложным: простые приложения с одним транспортным средством превратились в сложную мультиагентную систему. Поэтому можно утверждать, что следующим шагом станет использование гетерогенной группы беспилотного транспорта, работающие в сотрудничестве для достижения общих целей, при этом они могут безопасно работать и выполнять скоординированные задачи в крайне неопределенной среде [16]. Растущая сложность планируемых сценариев миссий создает несколько новых проблем для проектирования и интеграции беспилотных средств, особенно с точки зрения автономии и кооперации.

Ключевым элементом для успешной реализации подобных задач является наличие архитектуры мультиагентной системы, концептуальная структура которой показана на рис. 1. Представленная архитектура предлагает решение проблемы совместного управления несколькими гетерогенными группами, которые должны действовать в строгих пространственных и временных ограничениях, обеспечивая при этом бесконфликтные маневры. Теоретическая основа принята заимствованиями из разных дисциплин и объединяет алгоритмы генерации траектории, последующие пути, критическая координация времени и предотвращение столкновений. Вместе, эти методы дают архитектуру управления, которая позволяет удовлетворять строгим требованиям к производительности в наличие сложной динамики транспортного средства, ограничения связи и частичные отказы транспортных средств. Успешный результаты, скоординированные по времени, как теоретические, так и экспериментальные, приведены в работах [17, 19], в то время как подходящие алгоритмы предотвращения столкновений представлены в работах [18, 20].

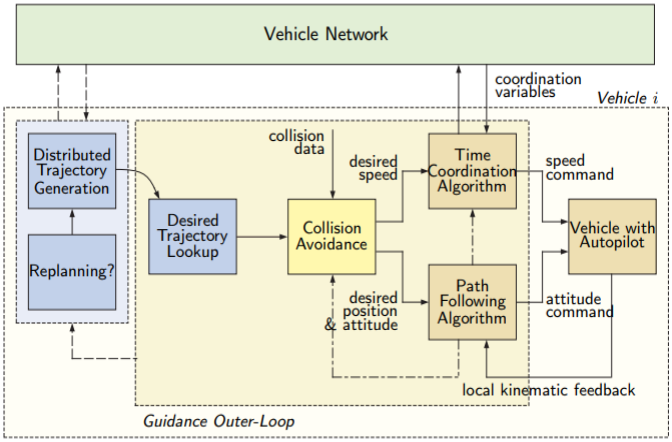


Рисунок 1. Архитектура управления гетерогенными группами беспилотного транспорта

Большинство существующих алгоритмов планирования пути для группы динамических объектов выполняются централизованно. Данный подход эффективен для одиночных объектов, когда транспортное средство не требует информации, которая не доступна на местном уровне. В таком случае задача оптимизации траектории движения представляет собой простую задачу с несколькими ограничениями. Однако, при использовании нескольких транспортных средств, централизованный подход к планированию траектории имеет несколько серьезных недостатков. Во-первых, транспортное средство, которому поручено генерировать траектории, становится единственной точкой отказа в рамках совместной генерации траекторий. В случае потери связи или выхода из строя этого транспортного средства, должна быть выполнена сложная процедура переопределения лидера. Во-вторых, при централизованном подходе транспортное средство, планирующее траектории, должно иметь доступ к информация всех транспортных средств в сети, что создает большую нагрузку на канал связи. И, в-третьих, вычислительная нагрузка распределяется неравномерно по количеству транспортных средств, причем одно транспортное средство выполняет основную массу вычислений. Следовательно, для крупномасштабных миссий с несколькими транспортными средствами, распределенная кооперативная структура генерации траектории не только желательна, но и на самом деле необходима.

Поскольку каждая задача генерации траектории приводит к проблеме оптимизации, решением этой проблемы выступает распределенная мультиагентная оптимизация траекторий движения. Это подтверждают исследования, проведенные в работах [1-15]. В общем случае, глобальная целевая функция представляет собой совокупность локальных целевых функ-

ций агентов системы. Соответственно, каждый агент в задаче формирования траектории опирается на собственную цель, а также ограничения, полученные от других агентов по каналам связи. Авторы работы [10] предлагают простой децентрализованный алгоритм для проблемы оптимизации, основанный на методе двойной декомпозиции. В этом алгоритме задаются переменные глобальной функции, с помощью которых затем задача формулируется путем декомпозиции всех ограничений, кроме динамических ограничений. Таким образом, глобальная задача может быть заменена последовательностью меньших задач, которые могут быть решены локально каждым агентом. Аналогичный подход представлен в работе [14], для работы алгоритма которого необходим доступ ко всем переменным системы.

Распределенный алгоритм на основе консенсуса предложен в работах [7, 8]. Алгоритм предназначен для решения задачи оптимизации, когда глобальная целевая функция представляет собой сумму локальных целевых функций, которые являются выпуклыми, но не обязательно гладкие. Алгоритм использует градиент, поскольку целевые функции не обязательно дифференцируемы. Результаты решения задачи оптимизации приведены в работе [9], где локальные переменные предполагается лежащими в замкнутых множествах. Подобная проблема оптимизации, но с учетом помех в каналах связи, рассматривается в работе [12]. Также интересные решения для оптимизации min-max задачи представлены в работах [11, 13]. Однако, помимо оптимизации на основе консенсуса, предлагается и другая распространенная стратегия, которая описана в работе [15]. Предполагается, что локальные целевые функции в этом подходе могут быть дважды непрерывно дифференцируемым. В отличие от консенсусных подходов, в этой работе используются стандартные алгоритмы нелинейного программирования для решения задач оптимизации распределенным способом и, следовательно, применим к широкому классу задач оптимизации.

Литература

1. I. Matei and J. S. Baras, A performance comparison between two consensus-based distributed optimization algorithms, Tech. Rep. 2012-05, The Institute for Systems Research, College Park, MD, May 2012. http://hdl.handle.net/1903/12480.

2. Distributed algorithms for optimization problems with equality constraints, Florence, Italy, December 2013, pp. 2352–2357.

3. Distributed algorithms for optimization problems with equality constraints, Tech. Rep. 2013-05, The Institute for Systems Research, College Park, MD, February 2013. http://drum.lib.umd.edu/ handle/1903/13693.

4. Distributed nonlinear programming methods for optimization problems with inequality constraints, Osaka, Japan, December 2015, pp. 2649–2654.

5. Nonlinear programming methods for distributed optimization, Tech. Rep. 2015-01, The Institute for Systems Research, College Park, MD, January 2015. http://hdl.handle.net/1903/16055.

6. I. Matei, J. S. Baras, M. Nabi, and T. Kurtoglu. An extension of the method of multipliers for distributed nonlinear programming, Los Angeles, CA, December 2014, pp. 6951–6956.

7. A. Nedić and A. Ozdaglar, On the rate of convergence of distributed subgradient methods for multi-agent optimization, New Orleans, LA, December 2007, pp. 4711–4716.

8. Distributed subgradient methods for multi-agent optimization, IEEE Transactions on Automatic Control, 54 (2009), pp. 48–61.

9. A. Nedić, A. Ozdaglar, and P. A. Parrilo, Constrained consensus and optimization in multi-agent networks, IEEE Transactions on Automatic Control, 55 (2010), pp. 922–938.

10. R. L. Raffard, C. J. Tomlin, and S. P. Boyd, Distributed optimization for cooperative agents: Application to formation flight, Atlantis, Paradise Island, Bahamas, December 2004, pp. 2453–2459.

11. K. Srivastava, A. Nedić, and D. Stipanović, Distributed Bregman-distance algorithms for minmax optimization, in Agent-Based Optimization, I. Czarnowski, P. Jędrzejowicz, and J. Kacprzyk, eds., vol. 456 of Studies in Computational Intelligence, Springer-Verlag Berlin Heidelberg, 2013, pp. 143–174.

12. K. Srivastava, A. Nedić, and D. M. Stipanović, Distributed constrained optimization over noisy networks, Atlanta, GA, December 2010, pp. 1945–1950.

13. Distributed min-max optimization in networks, Corfu, Greece, July 2011.

14. H. Terelius, U. Topcu, and R. M. Murray, Decentralized multi-agent optimization via dual decomposition, vol. 44, Milan, Italy, August-September 2011, pp. 11245–11254.

15. D. Varagnolo, F. Zanella, A. Cenedese, G. Pillonetto, and L. Schenato, Newton-Raphson consensus for distributed convex optimization, IEEE Transactions on Automatic Control, 61 (2016), pp. 994–1009.

16. Concept of operations for the Next Generation Air Transportation System. Joint Planning and Development Office, Version 3.2, September 2010. Available at www.dtic.mil/dtic/tr/fulltext/u2/ a535795.pdf.

17. V. Cichella, R. Choe, S. B. Mehdi, E. Xargay, N. Hovakimyan, V. Dobrokhodov, I. Kaminer, A. M. Pascoal, and A. P. Aguiar, Safe coordinated maneuvering of teams of multirotor unmanned aerial vehicles: A cooperative control framework for multi-vehicle, time-critical missions, IEEE Control Systems Magazine, 36 (2016), pp. 59–82.

18. V. Cichella, I. Kaminer, E. Xargay, V. Dobrokhodov, N. Hovakimyan, A. P. Aguiar, and A. M. Pascoal, A Lyapunov-based approach for time-coordinated 3D path-following of multiple quadrotors, in IEEE Conference on Decision and Control, Maui, HI, December 2012, pp. 1776–1781.

19. E. Xargay, Time-Critical Cooperative Path-Following Control of Multiple Unmanned Aerial Vehicles, PhD thesis, University of Illinois at Urbana-Champaign, Urbana, IL, United States, May 2013.

20. S. B. Mehdi, R. Choe, V. Cichella, and N. Hovakimyan, Collision avoidance through path replanning using Bézier curves, in AIAA Guidance, Navigation and Control Conference, Kissimmee, FL, January 2015. AIAA 2015-0598.

ПОДХОДЫ К ФОРМИРОВАНИЮ ОПТИМАЛЬНОЙ ТРАЕКТОРИИ ДВИЖЕНИЯ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

А. С. Павлов, С. С. Рябцев

руководитель – д-р. физ.-мат. наук, доцент ***Ф. Б. Тебуева***

Северо-Кавказский федеральный университет, г. Ставрополь

В работе проведен обзор подходов к формированию оптимальной траектории движения беспилотных транспортных средств. Рассмотрены существующие методы планирования пути.

Ключевые слова: беспилотные транспортные средства, мультиагентная система, планирование пути, прогнозирование траектории, теория оптимального управления.

Методы теории оптимального управления имеют преимущество в обработке входных данных, на основе которых минимизируется заданная функция, при этом учитываются динамические ограничения транспортных средств. Многие популярные подходы дискретизируют многомерную задачу, чтобы получить конечномерную задачу, которая может быть решена с использованием различных методов оптимизации. Например, особый интерес представляет работа, в которой использована псевдоспектральная теория оптимального управления, которая была успешно применена для решения задач оптимизации траектории и маневрирования [4-6, 11, 12]. Так, на основе этого метода удалось добиться выполнения маневра с нулевым пропеллентом для переориентации Международной космической станции на 90 градусов в ноябре 2006 года [1, 13].

По мере увеличения количества транспортных средств в группе или продолжительности миссии задача оптимизации траектории усложняется, что, в конечном счете, приводит к тому, что формирование полных траекторий от начальных до конечных точек становится трудной и вычислительно дорогостоящей процедурой. Модель прогнозного управления (МПУ) направлена на решение этой задачи путем вычисления частичных траекторий в течение ограниченного интервала времени, и поэтому траектории генерируются итеративно по мере движения. В работе [17] представлен метод на основе МПУ для генерации траекторий, которые позволяют избежать столкновения при наличии статических и динамических препятствий. Для реализации в реальном масштабе времени используется последовательный решатель квадратичного программирования. Генерация траектории для многоцелевых совместных миссий, основанная на МПУ, представлена в работе [16]. В зависимости от рассматриваемых ограничений движения [7, 18], предлагается использование целочисленного линейного программирования для решения задачи оптимизации. Наконец, интересной разработкой в этой области является работа [14], где представлен алгоритм распределенного взаимодействия для задач с внешними возмущениями и связанными ограничениями жесткого состояния, которые являются невыпуклыми.

В дополнение к оптимальным стратегиям управления представлены геометрически-динамические формулировки. В общем, чисто геометрический подход к проблеме генерации траектории является вычислительно эффективным и требует минимальной вычислительной мощности. Однако оптимальные траектории могут нарушать динамические ограничения транспортного средства, поскольку они не учитываются на этапе планирования. Расширением этого класса методов являются геометрически-динамические формулировки, которые обрабатывают динамические ограничения транспортных средств. В работе [9] траектории описываются кривыми Безье, а динамические ограничения накладываются ограничивающими дифференциальными геометрическими свойствами пути, такими как

кривизна и поворот. Вместе с тем, этот подход не подходит для создания трехмерных траекторий. Другой существующий подход – использование дифференциального свойства плоскостности системы для вычисления и проверки обратной динамики транспортного средства по заданной траектории [1]. Аналогичный подход представлен в работе [2], где рассматривается проблема генерации траектории для очень гибких мультитрон. Считается, что дискретизированная кинематическая модель транспортных средств проверяет ускорение и угловую скорость движения по сгенерированным траекториям. Авторы используют последовательное выпуклое программирование, которое аппроксимирует невыпуклые ограничения выпуклыми аналогами. Однако эти аппроксимации могут привести к последовательности чрезмерно ограниченных задач оптимизации, и алгоритмы могут не найти приемлемого решения. Для решения этой проблемы авторы работы [8] вводят инкрементный последовательный алгоритм с выпуклым программированием, где ограничения добавляются итеративно.

Методы поиска на основе перебора, использующие алгоритмы быстрорастущих случайных деревьев, были представлены в работе [15] и активно исследуются в последние годы. Эти планировщики движения, описанные, например, в работе [10], способны быстро разрастаться множеством возможных путей между вершинами, которые отбираются из всей среды.

Литература

1. N. Akhtar, J. F. Whidborne, and A. K. Cooke, Real-time trajectory generation technique for dynamic soaring UAVs, in UKACC International Conference on Control, Manchester, UK, September 2008.
2. F. Augugliaro, A. Schoellig, and R. D'Andrea, Generation of collision-free trajectories for a quadrocopter fleet: A sequential convex programming approach, in 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Vilamoura, Portugal, October 2012, pp. 1917– 1922.
3. N. Bedrossian, S. Bhatt, M. Lammers, L. Nguyen, and Y. Zhang, First ever flight demonstration of Zero Propellant ManeuverTM attitude control concept, in AIAA Guidance, Navigation and Control Conference, Hilton Head, SC, August 2007. AIAA-2007-6734.
4. N. S. Bedrossian, S. Bhatt, W. Kang, and I. M. Ross, Zero-propellant maneuver guidance, IEEE Control Systems Magazine, 29 (2009), pp. 53–73.
5. K. P. Bollino and L. R. Lewis, Collision-free multi-UAV optimal path planning and cooperative control for tactical applications, in AIAA Guidance, Navigation and Control Conference, Honolulu, HI, August 2008. AIAA 2008-7134.
6. K. P. Bollino, L. R. Lewis, P. Sekhavat, and I. M. Ross, Pseudospectral optimal control: A clear road for autonomous intelligent path planning, in AIAA Infotech@Aerospace, Rohnert Park, CA, May 2007. AIAA 2007-2831.
7. F. Borrelli, D. Subramanian, A. U. Raghunathan, and L. T. Biegler, MILP and NLP techniques for centralized trajectory planning of multiple unmanned air vehicles, in American Control Conference, Minneapolis, MN, June 2006, pp. 5763–5768.
8. Y. Chen, M. Cutler, and J. P. How, Decoupled multiagent path planning via incremental sequential convex programming, in 2015 IEEE International Conference on Robotics and Automation (ICRA), Seattle, WA, May 2015, pp. 5954–5961.

9. R. Choe, V. Cichella, E. Xargay, N. Hovakimyan, A. C. Trujillo, and I. Kaminer, A trajectory-generation framework for time-critical cooperative missions, in AIAA Infotech@Aerospace Conference, Boston, MA, August 2013. AIAA 2013-4582.

10. V. R. Desaraju and J. P. How, Decentralized path planning for multi-agent teams with complex constraints, Autonomous Robots, 32 (2012), pp. 385–403.

11. F. Fahroo and I. M. Ross, On discrete-time optimality conditions for pseudospectral methods, in AIAA/AAS Astrodynamics Specialist Conference, Keystone, CO, August 2006. AIAA 2006-6304.

12. Q. Gong, L. R. Lewis, and I. M. Ross, Pseudospectral motion planning for autonomous vehicles, Journal of Guidance, Control and Dynamics, 32 (2009), pp. 1039–1045.

13. M. Karpenko and I. M. Ross, A review of pseudospectral optimal control: From theory to flight, Annual Reviews in Control, 36 (2012), pp. 182–197.

14. Y. Kuwata and J. P. How, Cooperative distributed robust trajectory optimization using receding horizon MILP, IEEE Transactions on Control System Technology, 19 (2011), pp. 423–431.

15. S. M. LaValle, Planning Algorithms, Cambridge University Press, Cambridge, UK, 2006, ch. 5: Sampling-Based Motion Planning.

16. J. Ousingsawat and M. E. Campbell, Optimal cooperative reconnaissance using multiple vehicles, Journal of Guidance, Control and Dynamics, 30 (2007), pp. 122–132.

17. E. Scholte and M. E. Campbell, Robust nonlinear model predictive control with partial state information, IEEE Transactions on Control System Technology, 16 (2008), pp. 636–651.

18. T. Schouwenaars, J. P. How, and E. Feron, Decentralized cooperative trajectory planning of multiple aircraft with hard safety guarantees, in AIAA Guidance, Navigation and Control Conference, Providence, RI, August 2004. AIAA 2004-5141.

ОБЗОР МЕТОДОВ УПРАВЛЕНИЯ ГРУППОЙ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ НА ОСНОВЕ ВИРТУАЛЬНОГО ЛИДЕРА

А. С. Павлов
руководитель – д-р физ.-мат. наук, доцент ***Ф. Б. Тебуева***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье приведен обзор методов управления группой беспилотных транспортных средств на основе виртуального лидера. Исследованы особенности формирования конфигурации строя группы, достоинства и недостатки. Исследован процесс движения группы автономных транспортных средств по заданной траектории в среде с препятствиями.

Ключевые слова: беспилотный автомобиль, мультиагентная система, групповое управление, виртуальный лидер, децентрализованное управление.

В подходе лидер-ведомый один автомобиль группы назначается лидером, получая полный доступ к общей навигационной информации в целях формирования управляющего сигнала для каждого члена группы. Достоинством этого подхода является то, что в случаях, когда критическая надежность системы имеет решающее значение, виртуальному лидеру можно назначить замену в группе [1]. Остальные участники группы рассматриваются как ведомые. Ведомые работают под руководством лидера,

основной целью которого является сохранение топологической формы конфигурации, поддерживая желаемое расстояние между автомобилями при движении и маневрировании. На рис. 1 показаны возможные сценарии управления группой беспилотных транспортных средств: a) формирование строя; b) движение по заданной траектории; c) объезд препятствий.

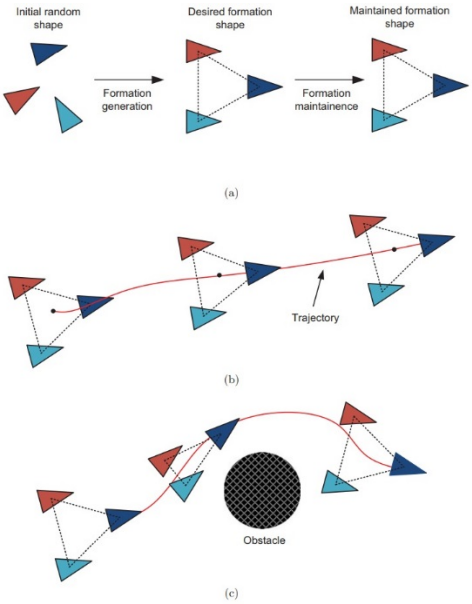


Рисунок 1. Управление группой беспилотных автомобилей на основе метода виртуального лидера

В работе [2] представлена схема формации лидер-ведомый, представленная на рисунке 2. l_{ij} и φ_{ij} – фактическое расстояние и угол между ведущим и ведомым транспортными средствами, а l_{ij}^{d} и φ_{ij}^{d} – желаемое расстояние и угол. Задача управления состоит в том, чтобы определить линейную и угловую скорости для ведомых, чтобы исключить значение ошибки расстояния и угла между лидером и ведомым, так что:

$$\lim_{t\to inf}\left(l_{ij}-l_{ij}^{d}\right)=0 \quad (1)$$

$$\lim_{t\to inf}\left(\varphi_{ij}-\varphi_{ij}^{d}\right)=0 \quad (2)$$

Обычно для разработки закона управления используются два типа контроллеров: $l-l$ контроллер (1) и $l-\varphi$ контроллер (2). Первый контроллер фокусируется на относительных положениях между каждым транспортным средством в группе; в то время как второй относится к рас-

стоянию и углу между лидером и ведомым [3, 4]. Подход лидер-ведомый, описанный в этой работе, возможен только для управления формацией в открытом пространстве, поскольку он только обеспечивает решение проблем 1 и 2 типов. Авторы работы [5] улучшили подход лидер-ведомый, добавив возможность предотвращения столкновений для повышения устойчивости конфигурации группы. Препятствие было устранено, позволяя автомобилю поддерживать новое желаемое расстояние, которое является расстоянием между транспортным средством и препятствием. При объезде препятствия конфигурация строя могла быть адаптивно изменена, как показано на рис. 3, и возвращена к заданной топологии после избежания столкновения. Работа [6] стала стандартным подходом, основанный на виртуальном лидере, которая применяется к группе беспилотных транспортных средств.

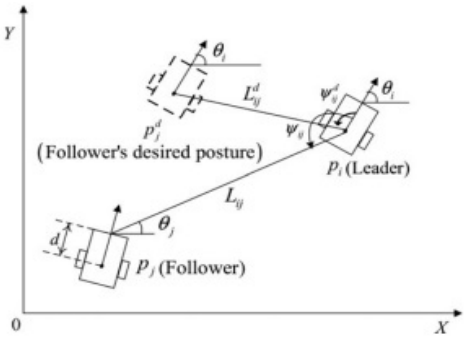


Рисунок 2. Схема формирования конфигурации на основе подхода лидер-ведомый

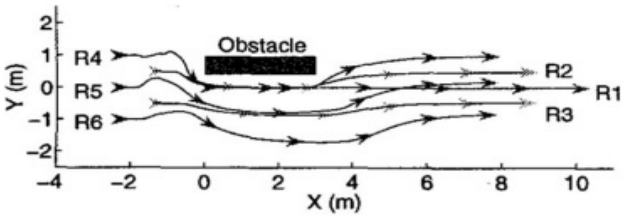


Рисунок 3. Пример работы адаптивной конфигурации строя при объезде препятствий

Однако, одной из проблем реализации управления на основе виртуального лидера является ограничение выработки управляющих сигналов. При объезде препятствия конфигурация строя может значительно измениться, что повлечет за собой увеличение вычислительной сложности управления для возвращения в первоначальной формации. Так, в работе [7] для решения этой проблемы предложено преобразование физических

ограничений скорости в геометрическое представление. Как показано на рисунке 4, траектория движения, представленная точкой, была заменена на дугу, что позволило повысить устойчивость системы.

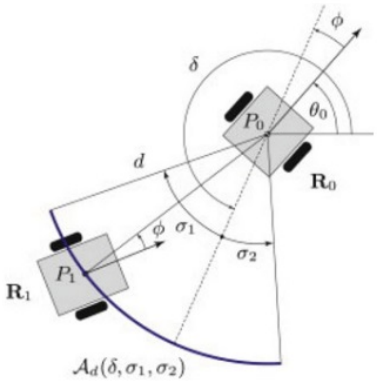


Рисунок 4. Геометрическое представление формации группы беспилотных транспортных средств

Еще одной важной проблемой при управлении группой беспилотных автомобилей на основе метода виртуального лидера является канал связи. Транспортное средство, обозначенное как лидер, должно обеспечить надежную связь со всей группой, чтобы лидер и ведомые могли точно обмениваться информацией о своем местоположении. В работе [8] была исследована проблема неисправности, вызванная потерей связи. Была предложена система монокулярного зрения для расчета относительного движения между лидером и ведомыми. В работе [9] приведены исследования неопределенностей, связанных с морскими наземными транспортными средствами, такими как немодулированная гидродинамика и динамические изменения среды. Авторами работы был разработан адаптивный закон регулирования, основанный на нейронных сетях и методах обратной регрессии, который использовался для обучения сети в режиме реального времени.

Литература

1. Y. Q. Chen and Z. Wang, «Formation Control: A Review and A New Consideration, » Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, IEEE (2005) pp. 3181–3186.

2. P. K. C. Wang, «Navigation strategies for multiple autonomous mobile robots moving in formation, » J. Robot. Syst. 8(2), 177–195 (1991).

3. T. Yang, Z. Liu, H. Chen and R. Pei, «Formation control of mobile robots: State and open problems, » Zhineng Xitong Xuebao (CAAI Trans. Intell. Syst.) 2(4), 21–27 (2007).

4. Z. Peng, G. Wen, A. Rahmani and Y. Yu, «Leader–follower formation control of nonholonomic mobile robots based on a bioinspired neurodynamic based approach, » Robot. Auton. Syst. 61(9), 988–996 (2013).

5. J. P. Desai, J. Ostrowski and V. Kumar, «Controlling Formations of Multiple Mobile Robots, » Proceedings of the IEEE International Conference on Robotics and Automation, volume 4, IEEE (1998) pp. 2864–2869.

6. L. Consolini, F. Morbidi, D. Prattichizzo and M. Tosques, «Leader–follower formation control of nonholonomic mobile robots with input constraints," Automatica 44(5), 1343–1349 (2008).

7. D. B. Edwards, T. A. Bean, D. L. Odell and M. J. Anderson, «A leader-follower algorithm for multiple AUV formations, » IEEE/OES Autonomous Underwater Vehicles (IEEE Cat. No.04CH37578), 2004, pp. 40–46.

8. O. A. A. Orqueda, X. T. Zhang and R. Fierro, «An output feedback nonlinear decentralized controller for unmanned vehicle co-ordination, » Int. J. Robust Nonlinear Control 17(12), 1106–1128 (2007).

9. Z. Peng, D. Wang, W. Lan and G. Sun, «Robust leader-follower formation tracking control of multiple underactuated surface vessels, » China Ocean Eng. 26, 521–534 (2012).

СОЗДАНИЕ СИСТЕМЫ ДИСТАНЦИОННОГО КОНТРОЛЯ ДЛЯ АНТРОПОМОРФНОГО РОБОТА

Д. И. Степанов, Д. А. Бондаренко, З. Д. Алиев, Д. А. Шихмурзаев
руководитель – доцент ***Р. М. Немков***
Северо-Кавказский федеральный университет, г. Ставрополь

Работа посвящена решению задачи установления связи между устройствами с разными операционными системами и обмена командными сообщениями между ними для дальнейшей возможности дистанционного контроля различных антропоморфных устройств. Задача разработки системы дистанционного контроля в настоящее время затрагивает многие стороны жизни человека и находит применение в различных ее областях. Например, создание систем удалённого мониторинга данных, систем беспроводного доступа к управлению, военных систем и т.д. [2].

Разработанная информационная система разделена на подпрограммы для успешной работы на каждом устройстве в общей схеме. Каждая подпрограмма может быть добавлена в общую схему, удалена или изменена независимо от остальных подпрограмм.

Для дистанционного контроля антропоморфным устройством достаточно две основные подпрограммы:

1. Windows подпрограмма.

Данная подсистема позволяет создать и запустить Web-Socket сервер для локальной сети на устройстве с предустановленной операционной системой Windows [1]. После запуска сервера, к данному устройству смогут подключиться другие устройства с предустановленными подпрограммами разработанной информационной системы [3].

Помимо создания и запуска сервера, устройство посредством подпрограммы способно отправлять данные на другие устройства, подключенные к серверу, а также принимать и интерпретировать команды с них.

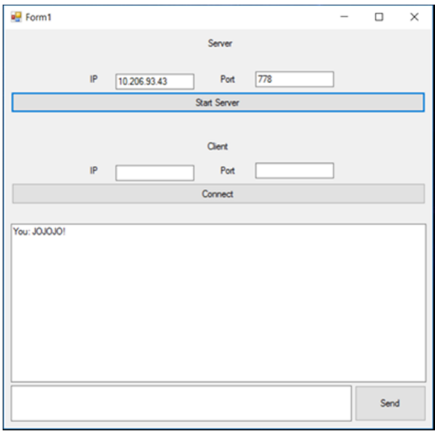


Рисунок 1. Оконный вариант подпрограммы для Windows

2. Android подпрограмма

Настоящая подпрограмма разработана для осуществления возможности подключения к серверу, запущенному на устройстве с предустановленной подпрограммой из первого пункта, с мобильных устройств на операционной системе Android. Функционал приложения позволяет мобильному устройству отправлять текстовые сообщения с командами серверу [4].

Так же разработанное приложение способно принимать мониторинговые данные, собранные, подготовленные и отправленные устройством с запущенным сервером.

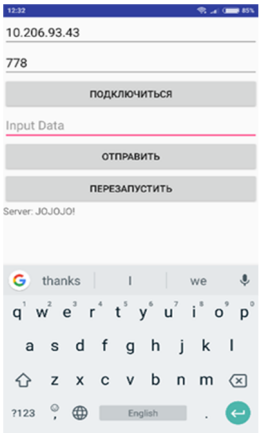


Рисунок 2. Подпрограмма для мобильного устройства на Android

Для полнофункциональной работы системы требуется выполнение ряда условий:

– управляющее устройство должно быть подключено к той же локальной сети, что и запущенный сервер на управляемом устройстве;

– после запуска сервера, на управляющем устройстве необходимо ввести IP адрес и Port управляемого устройства для его идентификации в сети;

– перед запуском системы, требуется задать список команд, на которые будут реагировать устройства с установленными подпрограммами.

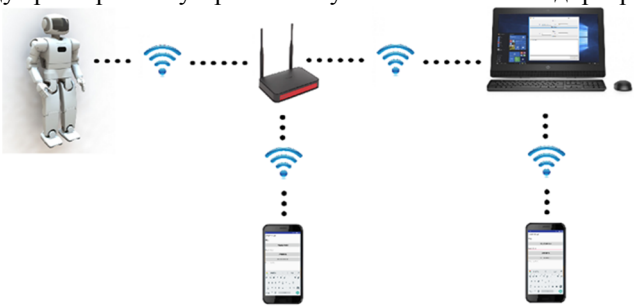


Рисунок 3. Пример схемы размещения устройств в сети

Преимуществами разработанного программного продукта являются разделённая структура, позволяющая наращивать список устройств, имеющих доступ к общей системе; открытый исходных код и высокая скорость обмена данными между устройствами; отсутствие возможности несанкционированного доступа к управляемому устройству, в связи с невозможностью подключения к серверу из сети интернет.

Литература

1. Шестаков В. С., Сагидуллин А. С./Применение технологии Websocket в Web-приложениях технологического назначения. // ж-л Приборостроение апрель 2015

2. Вильямс Д. Программируемый робот, управляемый с КПК. 2006

3. Lubbers P., Greco F. HTML5 Web Sockets: A Quantum Leap in Scalability for the Web. / Peter Lubbers, Frank Greco. // WebSocket.org, 2011.

4. Fette I., Melnikov A. The WebSocket Protocol. // The Internet Engineering Task Force (IETF), December 2011. P. 70.

РАЗДЕЛ 6
ИННОВАЦИОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС ШКОЛЫ

Д. О. Аликберова
руководитель – канд. пед. наук, доцент ***Г. И. Шевченко***
Северо-Кавказский федеральный университет, г. Ставрополь

В российской концепции модернизации образования до 2020 года поставлена задача: подготовить обучающихся к существованию в стремительно развивающемся информационном обществе, в мире, где ускоряется процесс возникновения новых знаний, потребность в развитии новых профессий, в условиях постоянного совершенствования профессиональных навыков. Эта задача, взятая из Концепции, определяет актуальность работы: основную роль в этой задаче играет освоение современных ИКТ на высоком уровне.

Ключевые слова: аспект, образовательные средства, информационные и коммуникационные технологии в образовательном процессе школы.

Общеизвестно, что применение информационных и коммуникационных технологий (ИКТ) в образовательном процессе российской школы изменяет преподавание традиционных школьных предметов, происходит оптимизация процессов восприятия и запоминания учебного материала, возрастает мотивация обучающихся к учебе, творчеству, даже у самых пассивных и незаинтересованных учеников.

Как показывает практика, внедрение ИКТ в образовательный процесс школы способствует:

– индивидуализации образовательного процесса с учетом уровня подготовленности, способностей, индивидуально-типологических особенностей усвоения программного материала, интересов и потребностей обучаемых;

– изменению направления познавательной деятельности обучающихся в сторону большей самостоятельности и работы поискового характера;

– стимулированию стремления обучающихся к постоянному улучшению результатов деятельности и готовности к самостоятельному переобучению;

– усилению междисциплинарных связей в обучении, всестороннему изучению событий и явлений;

– повышению гибкости, мобильности учебного процесса в школе, его постоянному динамичному изменению;

– преобразованию форм и методов организации учебной деятельности школьков и организации их досуга.

В арсенале современного учителя имеется множество средств ИКТ, которые можно успешно использовать как на уроке, так и во внеурочной деятельности: сеть Интернет и ее сервисы (чаты, форумы, блоги, электронная почта, телеконференции, образовательные сайты, вебинары, электронные учебники, справочники, словари энциклопедии, презентации, видеоуроки, сайты для самостоятельной подготовки к выпускным экзаменам, платформы для самостоятельного обучения). Благодаря этим средствам изменяется содержание обучения, происходит обмен информацией между учащимися и учителями. При этом педагог не просто обучает, воспитывает и развивает своего ученика, но и сам получает мощный стимул для дальнейшего самообразования, профессионального роста и творческого развитиях [4].

Помимо этого педагог, используя ИКТ в обучении, способен решать такие дидактические задачи, как:

– сформировать более устойчивую мотивацию;

– активизировать мыслительные и творческие способности обучающихся;

– привлечь к работе пассивных учеников;

– повысить интенсивность учебного процесса;

– обеспечить в ходе учебного процесса современный урок современными материалами;

– приучить учащихся к самостоятельной работе с разнообразными источниками информации;

– реализовать личностно-ориентированный дифференцированный подход к обучению;

– стимулировать процесс обучения,появляется возможность привлечь учащихся к исследовательской и проектной деятельности;

– обеспечить гибкость и динамичное изменение учебного процесса.

По мнению Е.И. Машбиц, к набору существенных достоинств использования компьютеров в образовательном процессе перед традиционными средствами обучения, следует отнести:

– возможность предъявления учебной информации, поскольку использование компьютерной графики, аудиофайлов, видеотехнологий позволяет воссоздавать реальную обстановку деятельности;

– качественное повышение мотивации обучающихся, которая растет за счет применения своевременного поощрения правильных решений поставленных на уроке задач;

– вовлечение обучающихся в учебный процесс, способствует наиболее широкому раскрытию всех их способностей, активизации его умственной деятельности;

– возможности постановки учебных задач и управления учебным процессом их решения. Компьютеры позволяют построить и проанализировать модели различных предметов, ситуаций, явлений. Возможен обмен решениями между учащимися для поиска оптимального решения для поставленной проблемы;

– возможность качественно изменять контроль за деятельностью учащихся, обеспечивая при этом гибкость и плавность управления учебным процессом;

– возможность формирования у обучающихся самостоятельной рефлексии. Обучающая программа дает возможность обучающимся наглядно представить результат своих учебных действий, определить этап в решении задачи, на котором произошла ошибка и исправить ее по ходу самостоятельной работы [2].

Как недостатки использования ИКТ в образовательном процессе школы можно рассматривать:

– недостаточную компьютерную грамотность учителя;

– отсутствие контакта и работы с учителем информатики;

– в рабочем графике учителей не отведено время для изучения возможностей сети интернет.

– отсутствие демонстрационного центра для учителей;

– сложность интеграции компьютера в поурочную структуру учебного плана;

– недостаточное количество компьютерных классов и учебного времени на всех;

– в школьном расписании не предусмотрено время для самостоятельного использования компьютера на уроках;

– вероятность того, что увлекшись применением ИКТ на уроках учитель перейдет от развивающего обучения к наглядно-иллюстративным методам.

Внедрение средств ИКТ в образовательный процесс школы непременно меняет характер работы между учителем и учениками на уроке, мотивируя последнего на активное самостоятельное получение дополнительных знаний с помощью доступных информационно-коммуникативных технологий. Работа педагога в этом случае направлена не на монотонное воспроизводство информации, а на оказание необходимой поддержки и помощи, информационного сопровождения учащегося в образовательном процессе [1].

Применение любого вида ИКТ зависит, в первую очередь, от целей и задач конкретного урока. Диапазон использования компьютера и новых

средств обучения достаточно широк. Информационные и коммуникационные технологии являются отличным средством повышения эффективности обучения и помогают существенно изменить контроль за деятельностью учащихся, гарантируя при этом необходимую гибкость управления учебным процессом в школе.

Внедрение ИКТ способствует практическому осуществлению личностно-ориентированного подхода к субъекту учебного процесса. Современный урок уже не может быть составлен без вспомогательных средств современных информационных технологий, так как меняются не только требования к уроку, но и способности учеников при усваении учебных дисциплин. Ученику легче запомнить материал, представленный с использованием информационных технологий, но необходимо тапк же развивать на уроке другие учебные навыки, поэтому использование ИКТ на уроке должно быть не единственным способом обучения.

Литература

1. Информационные технологии в образовании и науке: Материалы Международной научно-практической конференции «Информационные технологии в образовании и науке «ИТО – Самара – 2014». Самара; М.: Самарский филиал МГПУ, 2014. 494 с.

2. Ксензова Г. Ю. Перспективные школьные технологии: Учебно-методическое пособие. М.: Педагогическое общество России, 2015. 224 с.

3. Ксензова Г. Ю. Инновационные технологии обучения и воспитания школьников. Издательство «Педагогическое общество России», 2015. 144 с.

4. Шевченко Г. И. Образовательная электронная среда: сущность, назначение // Информационные технологии в науке и образовании Материалы Международной научно-практической интернет-конференции и V Всероссийского семинара «Применение MOODLE в сетевом обучении». Под редакцией А.Э. Попова. 2012. С. 72-74.

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ МЛАДШИХ ШКОЛЬНИКОВ

Л. А. Алпеева
руководитель – канд. пед. наук, доцент ***О. П. Панкратова***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье представлены преимущества использования информационных технологий в обучении перед традиционными методами обучения, проведен обзор инновационных средств обучения в начальной школе. Приведены примеры применения интерактивной доски и документ-камеры на различных этапах урока, рассмотрены типы тренировочных программ, а также возможности использование ЛЕГО-конструирования и робототехники во внеурочной и проектной деятельности учащихся.

Ключевые слова: информационные технологии, начальная школа, интерактивная доска, документ-камера, тренировочные программы, ЛЕГО-конструирование, робототехника.

Важнейшей составляющей ФГОС является информатизация образовательного пространства школ, включающая в себя информационно-коммуникационные технологии (ИКТ) обучения, то есть разнообразные программно-технические средства, которые предназначены для решения определенных педагогических задач, имеют предметное содержание и ориентированы на взаимодействие с обучающимися.

Применение информационных технологий в начальной школе позволяет не только модернизировать учебный процесс, повысить его эффективность, мотивировать учащихся, но и дифференцировать процесс с учётом индивидуальных особенностей каждого ученика.

Существенными преимуществами использования информационных технологий в обучении перед традиционными занятиями являются:

1. Значительное расширение возможностей представления учебной информации.

2. Значительное повышение мотивации школьников к обучению.

3. Вовлечение учащихся в учебный процесс, более широкое раскрытие их способностей и активизация умственной деятельности.

4. Увеличение возможностей постановки учебной задачи и управления процессом их решения.

5. Качественное изменение контроля деятельности учащихся.

6. Формирование у учащихся рефлексии.

Чтобы применять информационные технологии на практике, педагогу необходимо изучить и проанализировать возможности, методы, формы и средства обучения, характерные для информационной образовательной среды (ИОС). Поэтому без проектирования урока в современной ИОС педагогу не обойтись. Вследствие этого учителем должна быть разработана технологическая карта конструирования урока, учитывающая проектирование урока по этапам и позволяющая построить урок согласно требованиям ФГОС [5].

Федеральные образовательные стандарты начального общего образования (ФГОС НОО) требуют от учителя внедрения форм организации учебного процесса, отличных от традиционных и основанных, например, на использовании электронного учебника (ЭУ) или сенсорной интерактивной доски, которая может применяться на разных этапах комбинированного урока [2].

На этапе постановки целей и задач урока на экран можно вывести тему и цель.

В ходе проверки домашней работы на интерактивной доске можно показать вопросы для самоконтроля или домашнее задание, выполненное одним учеником для сверки с заданиями остальных детей.

На этапе первичного усвоения новых знаний на экране можно показать список вопросов (для устного опроса), а также творческие задания, рисунки, диаграммы, схемы и т.д. (для самоконтроля или письменной проверки).

В процессе первичной проверки понимания на интерактивной доске можно продемонстрировать план знакомства с новым материалом, а также необходимые иллюстрации (рисунки, таблицы, схемы, графики).

При первичном закреплении нового материала на интерактивной доске можно представить задания на выявление понимания изученного материала, вопросы или тестовые задания (на заполнение пропусков, установление соответствий и др.).

Подводя итоги урока, на экран интерактивной доски можно вывести небольшой текст или схему, раскрывающие основные положения новой темы.

Одним из современных технических устройств является документ-камера – универсальное техническое средство обучения (ТСО), заменяющее графопроектор, эпипроектор, сканер, цифровую фото/видеокамеру, web-камеру.

При обучении, например, русскому языку у учителя появляется возможность демонстрировать правила работы в прописях или дополнительный печатный материал. Работа осуществляется в реальном времени, классу демонстрируется образец, что предостерегает от возможных ошибок.

На уроках математики, положив учебник или рабочую тетрадь с заданиями под объектив камеры, можно научить учеников при помощи палетки измерять площади геометрических фигур. Документ-камера может служить дополнительным инструментом проверки выполнения индивидуальной или фронтальной работы. Для этого ученику необходимо положить свою тетрадь под объектив и продемонстрировать классу на экране решение задачи или уравнения.

На уроках технологии, изобразительной деятельности и окружающего мира документ-камера значительно упрощает объяснение и позволяет сохранить устойчивый интерес учащихся к учебному материалу [1].

Целесообразно использование в начальной школе трех типов тренировочных программ: с простым, составным и неизбирательным типом ответов [3].

Программа с *простым* типом ответов дает задание и программирует ответ по одному основанию, т.е. она характеризуется одной целевой установкой.

Программа с *составным* типом ответов дает задание, программирует ответ по двум (реже – трем) основаниям, т.е. она имеет две или более целевых установки.

Программа с *неизбирательным* типом ответов отличается от предыдущих тем, что ученик не выбирает ответ, а конструирует его самостоятельно.

К современным средствам обучения и формирования ИКТ-компетентности можно отнести ЛЕГО-конструирование и робототехнику, которые широко используются в проектной и внеурочной деятельности

младших школьников [4]. Робототехника – это первый шаг к алгоритмированию и программированию.

Опытно-экспериментальная проверка эффективности внедрения информационных технологий в обучение младших школьников показала, что применение информационных технологий на уроках в начальной школе способствует активизации познавательной деятельности младшего школьника, формированию устойчивых качеств личности, отражающих потребность, желание и внутреннюю убеждённость учащегося в необходимости творческого познания реальной действительности, способности формулирования познавательных задач и поиска их решения.

Литература

1. Балыкина И. И. Возможности применения документ - камеры в начальной школе // Начальная школа. 2014. №2. С. 53-56.
2. Зайналова Л. А., Казакаева М. М. Применение интерактивной доски // Начальная школа. 2016. №3. С. 34-36.
3. Колычева Г. Ю. Формирование информационной компетентности на уроках русского языка // Начальная школа. 2014. - №1. С. 80-82.
4. Кудакова Н. С. Робототехника и компетентность в области компьютерных технологий // Начальная школа. 2016. №12. С. 19-23.
5. Чернобай Е. В. Технология подготовки урока в современной информационной образовательной среде. М., 2012.

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В НЕФОРМАЛЬНОМ ОБРАЗОВАНИИ

Т. В. Бортова
руководитель – канд. пед. наук, доцент ***А. А. Рыбакова***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрена проблема организации и сущность неформального образования, освещены вопросы реализации политики информатизации и модернизации системы образования на основе механизмов интеграции информационных и коммуникационных технологий (*ИКТ*) *в организацию образовательного процесса, проанализированы возможности и преимущества использования ИКТ в неформальном образовании.*

Ключевые слова: информатизация и модернизация системы образования, образовательный процесс, неформальное образование, ИКТ, применение ИКТ в неформальном образовании.

Традиционная модель образования, нацеленная на установку получить «образование на всю жизнь», сегодня стала мало результативной в силу несоответствия социальной динамике и предъявляемым требованиям

к личности в части мобильности, освоения необходимых навыков, актуальных направлений деятельности [3].

В качестве одного из главных компонентов модели социального развития выступает модель непрерывного образования с установкой «образование через всю жизнь» в том числе таких форм, как информальное и неформальное образование [3].

Неформальное образование состоит в сборе образовательных практик, которые не включены в официальную систему образования. Эта отрасль образования способствует неформальному обучению. Согласно словарям, «не» - это приставка, которая означает «нет; отсутствие; обратное», другими словами противоположность чего-то. Но неформальное образование не является противоположностью формального образования. Неформальное образование можно рассматривать как образовательный подход, который может дополнять формальную систему образования. Методы, используемые в неформальном образовании, очень разнообразны и главным образом, основаны на создании здоровой среды доверия и обмена опытом. Этот вид образования обеспечивает дополнительную ценность для молодежи, экономики и общества в плане создания потенциала организаций, систем и учреждений. Это образование имеет место в самых различных областях и адресовано конкретным целевым группам и предметам, что облегчает включение молодежи с меньшими возможностями.

Реализация принципов современного образования происходит в процессе внедрения в него информационных и коммуникационных технологий (ИКТ), благодаря чему складывается принципиально новая образовательная парадигма, в которой преодолеваются ограничения традиционной системы образования. Современные ИКТ позволяют любому человеку в любом месте и в любое время получить необходимую ему информацию.

Информация – это в основном данные, с добавлением которых обучения становятся знанием. Другими словами, обучение, основывается на способности находить, применять и преобразовывать информацию в новые знания. Важные компетенции, которые требуются учащимся, чтобы совершить это преобразование, являются компетенциями в области информационной грамотности и потребность в информации, способность критически анализировать информацию и оценить ее полезность и, в конечном счете, иметь возможность применять информацию, превращая ее в знания.

Коммуникация заключается в простом диалоге между народами и культурой, которые приобретают новое измерение в сочетании с «информацией», и «технологией».

Технология не ограничивается только Интернетом и включает в себя более простые части, такие как CD-ROM, видео, телевидение и т.д., хотя термин «информационные и коммуникационные технологии» подразумевает использование Интернета и телекоммуникационных сетей. В образовательной практике ИКТ разделяют на две части:

– компьютерные технологии, к которым относятся компьютерные курсы, компьютеризированные тесты, текстовые процессоры, графическое программное обеспечение, электронные таблицы, базы данных и презентационное программное обеспечение;

– телекоммуникационное программное обеспечение, которое предлагает дистанционные курсы, распределенные образовательные ресурсы, электронную почту, видеоконференции, рекламные щиты, доски и чаты.

Применение ИКТ может принимать различные формы. Одновременное использование мультимедиа и компьютеров позволяет создавать новые педагогические подходы к активному и интерактивному обучению с использованием компьютера основанные на знаниях, на проблемах обучения, на проектах обучения, онлайн, видеоконференции, спутниковые каналы.

Неформальное образование с применением информационных и коммуникационных технологий позволяет расширить профессиональные компетенции будущего специалиста и реализовать важнейшую потребность человека в личном становлении и развитии, в результате профессионального роста. А в профессии педагога, сама личность является важной предпосылкой успешной профессиональной деятельности.

Реализация политики информатизации и модернизации систем образования на основе механизмов интеграции ИКТ в организацию учебного процесса обуславливает изменения приемов восприятия и способов получения знаний. В связи с этим появляется необходимость модернизации существующей системы образования для достижения максимально возможной эффективности.

Неформальное образование может принимать различные формы, включая корпоративное обучение (самостоятельное и / или работодателя) и непрерывное образование. ИКТ также влияет на эти области. Использование Интернета само по себе уже является неформальным опытом обучения. Такое образование может быть полезно на следующих уровнях: 1) корпоративном, 2) образовательном, 3) индивидуальном. В первом случае – это повышение квалификации и обучение сотрудников (в т.ч. самообразование). Во-втором – это государственные и/или негосударственные (коммерческие) учебные заведения, которые могут оказывать образовательные услуги. В третьем – индивидуальные пользователи, прежде всего пользователи интернета, образовательных порталов, вики-ресурсов и других образовательных услуг в сети. Потребители данного контента читают электронные лекции, смотрят видеоматериалы, посещают вебинары и т.д., причем такая форма обучения доступна для многих направлений дистанционно [1]. Распространение и доступность мобильных устройств стали причиной развития нового направления электронного обучения – Mobile Learning, который изначально подразумевает использование в процессе обучения мобильных средств связи, то есть весь образовательный контент загружается в мобильное устройство и тем самым процесс получения знаний не огра-

ничен местом и временем. Можно читать лекции, изучать материалы, выполнять задания, проходить тестирование, при необходимости общаться с преподавателями и получать оценку своих знаний в режиме реального времени в любом месте [2].

Литература

1. Anohina A. Analysis of the terminology used in the field of virtual learning/ Educational Technology & Society, 8(3), 2005. P.91-102.
2. UNESCO Recommendations adult learning and education (13 November 2015), UNESCO [Electronic resource]. – Available at: http://uil.unesco.org/adult-education/unesco-recommendation/unesco-recommendation-adult-learning-and-education-2015.
3. Дубовик И. М. Становление и развитие неформального образования за рубежом / Педагогические науки №30-1, 10.01.2015 URL: http://novainfo.ru (дата обращения: 27.04.2018).

ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ИНКЛЮЗИВНОМ ОБРАЗОВАНИИ

Ю. А. Дулина
руководитель – канд. пед. наук, доцент ***А. А. Рыбакова***
Северо-Кавказский федеральный университет, г. Ставрополь

Статья посвящена актуализации внедрения информационных технологий, в учебный процесс, удовлетворяя конкретные образовательные потребности детей, обучающихся в системе инклюзивного образования.

Ключевые слова: информационные технологии, инклюзивное образование, образовательные потребности, учебный процесс.

Ускоренное внедрение информационных и коммуникационных технологий в обучение представляется главным аспектом для системы образования, согласующимся со всеми правилами развивающегося информационного общества и процессом модернизации устоявшейся системы образования. В современном развивающемся информационном обществе информационные и коммуникационные технологии имеют важное место в обеспечении взаимодействия между людьми, а также практически во всех системах формирования, передачи и распространения информации.

Информационные и коммуникационные технологии (ИКТ) определяют как совокупность методов и средств, используемых для сбора, хранения, обработки и распространения информации. Этот термин уже стал известным для всех словом, которое хорошо обрисовывает жизнь и потребности современного общества[6].

В нынешнее время жизнь человека очень сильно зависит от технологий, поэтому именно в руках представителей молодого поколения находится будущее развитие, от них зависит то, какими способами человече-

ство будет передавать и получать информацию. Но для начала необходимо обучить будущих специалистов.

Опыт других стран показывает, что наиболее эффективным способом решения этой задачи является использование ИКТ в образовательном процессе в качестве дидактического инструмента. Это содействует улучшению подходов к учебно-методическому процессу и подталкивает к появлению новых методов, форм и средств обучения, контроля и проверки приобретенных знаний, дает возможность привести к минимальному различию между учащимися и позволяет применять современные педагогические приемы, направленные на развитие взаимодействия обучающихся друг с другом и с педагогами. Кроме того, использование ИКТ позволяет реализовать обучения детей с ограниченными возможностями некоторых категорий [3].

Для особых детей интернет-технологии имеют очевидные преимущества. Они позволяют учителю самостоятельно создавать учебный материал для ребенка с учетом его характеристик и потребностей, а также делать необходимые изменения чрезвычайно быстро и гибко.

Но образовательные потребности учеников, с определенными отклонениями, очень различны. С одной стороны, все имеют одинаковые потребности в получении знаний, необходимых для жизни в современном им обществе. С другой стороны, существуют те потребности, которые связаны с функциональными ограничениями, которые препятствуют использованию обычных образовательных методов, форм и средств обучения в учебном процессе, и мешают прогрессу в получении знаний. В этом контексте, использование ИКТ играет важную роль в обеспечении высокого качества образования для людей с ограниченными возможностями. С их помощью можно удовлетворить конкретные образовательные потребности различных групп учащихся. Именно поэтому современные ИКТ, интерактивные и дистанционные технологии обучения, позволяют внедрять инклюзивное образование в полном объеме [4].

В современной России начинают развиваться региональные модели практики такого образования, при которой дети с ограниченными возможностями включаются в образовательный процесс.

В систему инклюзивного образования входят образовательные учреждения среднего, профессионального и высшего образования. Его задача заключается в создании безбарьерной среды в обучении и профессиональной подготовке людей с ограниченными возможностями. Этот комплекс мер включает как техническое оснащение учебных центров, так и разработку дополнительных учебных курсов для педагогов и других учащихся, направленных на развитие их взаимодействия с людьми с ограниченными возможностями. Кроме того, разрабатываются специальные программы, направленные на облегчение процесса адаптации детей с ограниченными возможностями в общеобразовательном учреждении [6].

В связи с этим разработана «интернет-система» дистанционного асинхронного обучения для детей, которые физически не могут заниматься более трёх часов в день; имеют ограничения в пространстве – дети ограничены в движении, обучаются по сетевым технологиям (через интернет) или кейс-технологиям (почтовые пересылки). Асинхронность (обучение по индивидуальной траектории усвоения знаний, в удобное время в удобном месте) принципиально необходима для лиц с ограничениями, которые не всегда хорошо себя чувствуют в режиме группового обучения в условиях определенного графика занятий. Ученики занимаются в реабилитационных центрах или дома используя различные технологии: сетевые технологии, кейс-технологии или смешанные технологии. При этом технологические особенности обучения реализуются в полном соответствии с Государственными образовательными стандартами Российской Федерации, они утверждаются в существующей нормативно-правовой области дистанционного обучения и полностью соответствуют требованиям лицензирования и аккредитации школы [2].

Инклюзивное образование является одним из важнейших процессов преобразования общего образования, основанного на понимании того, что инвалиды в современном обществе могут участвовать в жизни общества. Эта трансформация направлена на создание условий доступности образования для всех, включая обеспечение доступа к образованию для детей с инвалидностью, потому что половина всех, живущих на территории России людей с ограниченными возможностями трудоспособного возраста не работают. Основой является недостаточное обеспечения государством, отсутствие возможности получить интересную и высокооплачиваемую работу. Проблема поиска работы связана с несколькими факторами: отсутствием у людей необходимых знаний, умений и навыков, нежеланием работодателей сотрудничать с людьми с ограниченными возможностями. Экономисты считают, что государству и социальным структурам гораздо выгоднее предоставить инвалидам возможность получить соответствующие профессиональные знания, найти достойную работу, а не проводить политику поддержания особого нравственного и морального настроя. Сегодня, из ста, получить высшее образование могут только два человека с ограниченными возможностями. Многие отечественные университеты и школы отказываются сотрудничать с инвалидами из-за неприспособленности программ и несоответствия условий обучения особым требованиям для конкретных потребностей людей с ограниченными возможностями, поэтому для некоторых детей, технологические решения будут единственным способом обеспечить реализацию своих потребностей в дальнейшей жизни [1].

Для учеников с ограниченными возможностями жизненно необходим доступ к ИКТ. Внедрение информационных технологии в инклюзивное образование немаловажно, поскольку оно решает проблемы, связанные с рядом потенциальных потребностей людей в обществе.

Литература

1. ICTs in Education for People with Special Needs. Specialized Course.// UNESCO Institute for Information Technologies in Education.
2. Алехина С. В., Зарецкий В. К. Инклюзивный подход в образовании в контексте проектной инициативы «Наша новая школа» // Психолого-педагогическое обеспечение национальной образовательной инициативы «Наша новая школа». М., 2015.
3. Дзоз В.А. Организация инклюзии в системе непрерывного образования // Сибирский педагогический журнал, 2013.
4. Назарова Н.М. Интегрированное (инклюзивное) образование: генезис и проблемы внедрения // Научно-методический журнал «Коррекционная педагогика», 2018.
5. Топор А. В., Белая Е., Белая Н. Использование информационно-коммуникационных технологий в образовательном процессе. СПб.: Заневская площадь, 2014.
6. Фролова И. Ю. Инклюзивное образование в России: проблемы и перспективы // Научно-методический журнал «Ученые записки Орловского государственного университета», 2017.

ОЛИМПИАДЫ ПО ИНФОРМАТИКЕ КАК СРЕДСТВО ПРОФОРИЕНТАЦИИ ШКОЛЬНИКА

Н. В. Животова
руководитель – канд. пед. наук, доцент ***Т. А. Куликова***
Северо-Кавказский федеральный университет г. Ставрополь

Статья посвящена проблеме профориентации и популяризации престижности профессии по информационным технологиям, в обобщённом виде представлена структура олимпиады по информатике среди школьников. По мнению автора, олимпиады поддерживают идеи Правительства Российской Федерации по подготовке и обучению грамотных ИТ-специалистов.

Ключевые слова: олимпиада, информатика, информационные технологии, ит-профессии, образование, популяризация, профориентация.

Дефицит кадров в ИТ-отрасли оценивается в 350–400 тыс. специалистов – это число работающих в данной сфере сегодня. Министерство образования и науки Российской Федерации ежегодно увеличивает количество бюджетных мест в ВУЗах (примерно на 30 процентов). Несколько лет назад все вузы в год принимали 25 тысяч человек по ИТ-специальностям, на данный момент это уже 42,5 тысячи человек в год.

– Популяризация ИТ как сферы деятельности сформулирована как задача в следующих документах:

– Стратегия инновационного развития Российской Федерации на период до 2020 года (утв. распоряжением Правительства Российской Федерации от 8 декабря 2011 г. № 2227-р);

– Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года (утв. распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р);

– План мероприятий («дорожная карта») «Развитие отрасли информационных технологий» (утв. распоряжением Правительства Российской Федерации от 30 декабря 2013 г. № 2602-р);

– План деятельности Министерства связи и массовых коммуникаций Российской Федерации на период 2016 – 2021 годов.

По итогам встречи Президента В. В. Путина с участниками Всероссийского молодежного образовательного форума «Территория смыслов на Клязьме», где была обозначена важность популяризации ИТ-направления, был выпущен перечень поручений Президента от 9 августа 2015 г. №Пр-1612, содержащий пункт 2а: «Правительству Российской Федерации: принять меры, направленные на популяризацию профессий в сфере информационных технологий среди молодежи»[2].

Как указано в «Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года», профессии ИТ-отрасли уже к 2018 году должны быть закреплены в числе 4-х популярных в рейтинге профессий среди выпускников средних учебных заведений [3].

Для реализации этой задачи необходимо проводить комплекс мероприятий по популяризации ИТ-направления, формируя у школьников интерес к изучению информационных технологий и повышая привлекательность профессий, связанных с этой областью.

В целях выявления наиболее талантливой творческой молодежи в области информационных технологий, формирования информационной компетентности и развития информационной культуры учащихся, популяризации престижности профессии по информационным технологиям и проведения профориентационной работы среди школьников по направлению информационных технологий проводятся олимпиады.

Для учащихся предметные олимпиады являются одной из наиболее эффективных форм выявления способностей и степени одаренности в предметной области, они развивают умственные и творческие способности, стимулируют самоконтроль результатов обучения. Помимо этого, они выступают как средство профориентации, помогают с выбором специальности при поступлении в вузы и последующей специализации. С другой стороны, для педагогов олимпиады – это средство контроля качества обучения и подтверждения педагогической квалификации, часто олимпиады становятся конкурсом не только самих учащихся, но и их учителей.

По нашему мнению, предметные олимпиады дают возможность учащимся показать уровень предметной подготовки, развития интеллектуальных умений, личностные и морально-волевые качества.

Основными целями и задачами олимпиады являются [4, с. 76]:

1) выявление и формирование у обучающихся творческих способностей и заинтересованности к научно-исследовательской деятельности;

2) создание необходимых условий для поддержки талантливой молодежи;

3) популяризация науки и научных знаний;

4) вовлечение научных работников соответствующих отраслей к работе с молодежью.

Всероссийские олимпиады школьников стали средством, которое обеспечивает эффективное формирование знаний, умений и навыков учащихся, необходимых для их личностного и профессионального самоопределения. Всероссийская олимпиада стимулирует и мотивирует личностное и интеллектуальное развитие учащихся, поддерживает одаренных детей, содействует их самоопределению и продолжению образования, раскрывает связь областей знаний, составляющих содержание олимпийских дисциплин, с другими областями знаний, развивает и поддерживает интерес учащихся к познавательной и научной деятельности.

Всероссийская олимпиада сейчас состоит из четырех этапов – школьного, муниципального, регионального и заключительного. Финал, на который съезжаются лучшие дети из всех регионов России, проходит на высочайшем уровне, финальные задания очень сложные, творческие, многие из них и у взрослых вызывают затруднения.

Региональные команды складываются по результатам третьего (регионального) этапа Всероссийской олимпиады. В последние годы было внесено важное изменение - отменены региональные квоты на участие школьников в финале. Ранее каждый регион посылал команду определенной численности. В некоторых случаях это ограничивало возможности ребят на участие в финале, потому что у жителя крупного региона шансов пробиться в команду фиксированного размера (каким бы он ни был – 5 или 10 человек) было на порядок меньше, чем у жителя региона меньшего. Поэтому в последние годы было установлено правило, которое гарантирует ребятам равные шансы попадания на заключительный этап олимпиады.

Региональный этап проходит по единым задачам по всей стране в один день. После него от каждого региона гарантированно кто-то посылается на заключительный этап. Но основной отбор идет следующим образом – после проверки работ создается единый итоговый список по всей стране, и на финал едут ребята, которые показали лучшие результаты вне зависимости от того, в каком регионе они живут. В один год от региона может поехать 5 человек, в другие – десять, три, два… Это зависит от того, сколько действительно ярких, одаренных ребят в этом регионе, это не завязано на квоты. И если в каком-то регионе идет сильная работа по тому или иному учебному предмету, то эту работу можно смело развивать, не опасаясь, что от региона поедет только 5 человек.

В целях повышения эффективности и результативности профориентационной работы с учащимися учреждений высшего образования следует

проводить мероприятия с применением современных информационно-коммуникационных средств (мультимедийные презентации, видеоролики, он-лайн конференции по профориентации), направленные на обсуждение проблем перспективного развития профессий и рынка труда. Необходимо предоставлять информацию не только о различных профессиях, но и информацию, связанную с такими аспектами, как особенности профессиональной деятельности, содержание профессионально-квалификационных характеристик, условия труда в той или иной профессиональной области, специфика взаимодействия в трудовом коллективе и т. д. [4, с. 105].

Подводя итог вышесказанному, следует сделать вывод, что современное олимпиадное движение – существенно более широкая и разносторонняя область, чем просто испытание знаний и интеллекта. В нем могут найти себя школьники и студенты с самым разным уровнем подготовки, обладатели самых разных наборов интеллектуальных качеств и творческих навыков. Гораздо большее значение имеет готовность одаренного учащегося обновлять знания и видоизменять навыки, не останавливаясь на уже достигнутом и приобретенном опыте. На развитие именно таких качеств следует ориентировать подготовку программистов, такие качества следует учитывать при выявлении и развитии одаренности к этому роду деятельности.

Таким образом, все этапы профориентации и популяризации престижности профессии по информационным технологиям среди учащихся через олимпиады школьников по программированию должны служить одной цели – активизировать учащегося, формировать у него стремление к самостоятельному выбору профессии с учетом полученных знаний о своих способностях, о перспективах своего профессионального пути.

Литература

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ // Информационно-правовой портал Консультант [Электронный ресурс]. Режим доступа: http://www.pravo.gov.ru.

2. Приказ Минобрнауки РФ от 17 мая 2012 г. №413 Об утверждении ФГОС // Информационно-правовой портал Консультант [Электронный ресурс]. Режим доступа: http://www.consultant.ru.

3. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года [Электронный ресурс]: Распоряжение Правительства РФ от 1 ноября 2013 года № 2036-р. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Игнатович Е. С. Система информационно-педагогической поддержки старшеклассников как средство их профессионального самоопределения / Е. С. Игнатович; под ред. О. А.Олекс. Минск: РИВШ, 2009.

ВЛИЯНИЕ ЭКШН-ВИДЕОИГР НА РАБОТОСПОСОБНОСТЬ МОЗГА

Х. Ф. Камолов, А. Ю. Ким
руководитель – канд. техн. наук, доцент ***А. Г. Хныкина***
Северо-Кавказский федеральный университет, г. Ставрополь

Человеческий мозг учится и адаптируется. В многочисленных исследованиях основное внимание уделяется влиянию видеоигр на человеческий мозг, а также измерению когнитивных способностей, таких как восприятие и время реакции. В статье приведены данные психологов о влиянии видеоигр на познание, которые указывают на значительное улучшение когнитивных способностей геймеров.

Ключевые слова: видеоигры, мозг, когнитивные способности, метаанализ, геймер, экшн.

Сегодня компьютер есть практически в каждой семье. ПК используются для выполнения различных операций: набор текста, поиск информации, выполнение различных работ в графических редакторах и т.д. Как правило, дети и используют компьютер для развлекательных целей. В отличии от фильма, книги или представления человек взаимодействует с компьютерной игрой.

Компьютерная игра – это программа, которая служит для организации игрового процесса (геймплея), связи с партнёрами по игре, или сама выступающая в качестве партнера. Компьютерные игры оказывают существенное влияние на общество и в информационных технологиях отмечена устойчивая тенденция к геймификации для не игрового прикладного программного обеспечения. Сегодня, общество привыкло выставлять поклонников компьютерных игр как зависимых и отделенных от внешнего мира людей, доказывая не только умственную, но и психологическую деградацию.

Человеческий мозг податливый – он учится и приспосабливается. В многочисленных исследованиях основное внимание уделяется влиянию видеоигр на мозг путем измерения когнитивных способностей, таких как восприятие, внимание и время реакции. Международной группой психологов, возглавляемых Женевским университетом (UNIGE), были собраны данные за последние пятнадцать лет, чтобы определить, как видеоигры влияют на познание. Проведенное исследование показало, что видеоигры приводят к улучшению когнитивных способностей геймеров [2].

Изучение влияния видеоигр на человеческий мозг началось с конца 80-х годов, когда началось развитие и укоренение Pacman и аркадных игр. В данных исследования был проведен ряд психометрических тестов, в общей сложности 8970 человек в возрасте от 6 до 40 лет с целью оценки их когнитивных способностей. Оценки включали пространственное внимание (например, быстрое обнаружение собаки в стаде животных), а также оценку их навыков при одновременном управлении несколькими задачами и

изменении их планов в соответствии с заранее определенными правилами. Было выявлено, что познание геймеров было вдвое выше стандартного отклонения по сравнению с не-игроками [3].

Однако полученные данные не отвечали на все поставленные вопросы. В связи с этим психологи приступили к анализу интервенционных исследований. Данные исследования проводились на 2883 мужчинах и женщинах, которые играли в течение максимум одного часа в неделю. Сначала на них были опробованы их познавательные способности, а затем случайным образом люди были поделены две группы: одни играли в боевые игры (военные или шутеры), другие – в контрольные игры (SIMS, Головоломка, тетрис). Обе группы играли в течение не менее 8 часов в неделю и до 50 часов в течение 12 недель. По окончании тренинга участники прошли когнитивное тестирование, чтобы измерить любые изменения в их познавательных способностях. Цель данного проекта состояла в том, чтобы выяснить, является ли эффект действия игр на мозг причинным [1, 4, 5].

Проанализировав полученные сведения, можно было сделать вывод, что люди, играющие в видеоигры, увеличили свое познание больше, чем те, кто играл в контрольные игры. Разница в когнитивных способностях между этими двумя экспериментальными группами составила одну треть от стандартного отклонения.

Однако, необходимо отметить, что положительные эффекты наблюдались только в тех исследованиях, в которых люди играли в течение нескольких недель или месяцев. Проведенные исследования помогли улучшить понимание пластичности мозга и потенциально создавать игры, предназначенные для развития внимания или пространственного познания.

Также необходимо обратить внимание, что видеоигры усиливают межнейронные связи и увеличивают определенные области мозга. Структурные изменения наблюдались в волокнах, которые соединяются с визуальной, временной и предлобной корой, а также гиппоталамусом. Помимо положительного влияния видеоигр на человеческий мозг, оказалось, что постоянные геймеры демонстрируют как функциональные, так и структурные изменения в работе системы вознаграждения в мозге. Подобные изменения наблюдались в нервной системе и мозге людей, которые страдают от алкогольной или наркотической, а также зависимости от азартных игр. Данные исследования объясняют тот факт, что многие геймеры часто страдают от зависимости и даже демонстрируют абстинентный синдром.

Таким образом, можно сделать вывод, что видеоигры в жанре экшн развивают зрительное внимание и различные способности мозга, а также по-разному влияют на количество серого вещества в гиппокампе у разных людей, в зависимости от того, к какому типу навигации в пространстве спонтанно склоняется человек.

Литература

1. Anderson CA, Dill KE (2000) Видеоигры и агрессивные мысли, чувства и поведение в лаборатории и жизни. Журнал личности и социальной психологии. С. 772-790.
2. DeLisi M, Vaughn MG, Gentile DA, Anderson CA, Shook JJ (2013) Насильственные видеоигры, преступность и насилие среди молодежи: новые доказательства. Молодежное насилие и правосудие в отношении несовершеннолетних. С. 132-142.
3. Dill KE, Gentile DA, Richter WA, Dill JC (2005) Насилие, пол, возраст и раса в популярных видеоиграх: анализ содержания. В Cole E, Henderson-Daniel J, редакторы. Показывая женщин: феминистские анализы среды. Вашингтон: Американская психологическая ассоциация. С. 115-130.
4. Krahé B, Möller I (2004) Игра в жестокие электронные игры, стиль враждебной атрибуции и нормы агрессии у немецких подростков. Журнал подросткового возраста. С. 53-69.
5. Андерсон К. А., Бушман Б. Ю. (2001) Влияние насильственных видеоигр на агрессивное поведение, агрессивное познание, агрессивный аффект, физиологическое возбуждение и просоциальное поведение: метааналитический обзор научной литературы. Психологическая наука. С. 353-359.

КОМПЬЮТЕРНАЯ ПОДДЕРЖКА ИЗУЧЕНИЯ ПРОПЕДЕВТИЧЕСКОГО КУРСА ГЕОМЕТРИИ В 5–6 КЛАССАХ

А. В. Конкиева
руководитель – доцент ***Р. П. Овчинникова***
Северный арктический федеральный университет, г. Архангельск

Основная цель пропедевтики геометрического материала в 5–6 классах – знакомство с геометрическими фигурами и их свойствами. Роль пропедевтического курса геометрии определяет его содержание, которое включает ряд вопросов, изучаемых в систематическом курсе геометрии. В работе рассматривается компьютерная поддержка изучения пропедевтического курса геометрии в 5–6 классах.

Ключевые слова: компьютерная поддержка, пропедевтический курс, геометрия, геометрические фигуры, планиметрия, обучение школьников.

Целью вводного курса по геометрии в 5–6 классе является ознакомление учащихся с основными фигурами в геометрии и их чертами и качествами. Важно, чтоб дети развивались и интеллектуально, и умственно, получая определенные умения и знания, которые обязательно станут нужны в жизни. Так как во многих ситуациях имеет значение сконцентрироваться, проанализировать, подытожить, существенно развивать мыслительные способности.

В начальных классах дети накапливают и развивают свое понятие о геометрии, благодаря постоянному проведению практических работ, изготовляя модели геометрических фигур, вырезая или начерчивая. Ученики имеют определенную формулировку для себя, но самостоятельно толковать определения им не нужно. Получая четкую базу знаний, уже к 5му классу для школьника важно систематизировать полученные знания и подытожить их.

Для каждого ученика свойственно воспринимать геометрические фигуры, как целую модель или чертеж, которые неподдельны с объектом, который воспринимается. Знакомство с геометрическими фигурами, учениками 5–6-ых классов, происходит сравнениями между ними, которое приводит к понятию в целом. Эти понятия могут отличаться степенью резюмирования. Большинство учеников уже имеют свое мнение, но это еще не понимание [1].

Важность геометрии, её красота и уникальность – это то что нужно донести до школьников в вводном курсе в первую очередь. В данном периоде школьники психологически полностью готовы к правильному восприятию систематического курса геометрии. В период перехода от младшей школы к старшей хорошо развивается образное мышление. Основной целью подготовительного курса геометрии есть: формулировка геометрического склада ума, с помощью приведения примеров. Изучение вводного курса геометрии, возможно, в современных условиях компьютеризации. И такие методы, даже, важно использовать.

Современный подход к проведению занятия – это очень важный момент в условиях развития современных технологий. И это очень важно в геометрии, так как данный предмет влияет на формулировку научного мировоззрения у школьника, дает интеллектуальное развитие и развивает образное мышление. Изначально ученики изучают простейшие фигуры. Позже, изучая планиметрию, знакомятся со свойством фигур и изучают понятие фигуры, которые понятны и легки для них [2].

В наше время для учителей средней школы выносятся требования использовать в учебном процессе: компьютерные технологии, плазменные телевизоры и активные доски, благодаря чему, для учеников легче воспримется свойства в разных пространственных предметов. Естественно преподаватель должен владеть определенными компьютерными программами и иметь представления о новых технологиях, за счет поддержки которых, можно изучить геометрические фигуры.

Главное при изучении пропедевтического курса – это показать красоту геометрии, её уникальность в системе обучения школьников. Систематический курс геометрии начинают изучать в школе позднее психологически благоприятного периода для её изучения. Наглядно-образное мышление и воображение наиболее полно развиваются на стыке старшего дошкольного и младшего школьного возраста. Всестороннее развитие геометрического мышления учащихся 5–6 классов с помощью методов геометрической наглядности является целью изучения пропедевтического курса геометрии [3]. Для решения проблемы развития геометрического мышления необходимо использование в современных условиях компьютерной поддержки изучения пропедевтического курса геометрии.

Геометрия является важной составляющей в школьной программе. При изучении предмета выявляются сложности динамического восприя-

тия. Методы преподавания исчерпали себя в эффективности обучения – это позволило выделить современный метод с помощью инновационных технологий [4]. Компьютер, а точнее, его программы дают возможность наглядно выражать тематические основы каждого раздела геометрии. Тем самым, роль «классной доски» переходит на задний план. Материал излагается в форме иллюстраций, на которых присутствуют картинки, схемы, таблицы. Учащимся это помогает визуализировать данный материал, понять и воспроизвести его через время. Геометрические задачи выводятся на слайды программы Microsoft Power Point и с легкостью решаются. Стоит определиться с целью употребления презентаций на уроке, выделить основную проблему и обосновать важность использования определенного метода. Например, статическую презентацию нет необходимости создавать, так как проблему наглядности может передать обычный плакат. Но если на слайдах присутствуют подвижные эффекты, передающие глубину новых знаний, такие презентации важно показывать для изучения учащимися. В геометрии есть много аспектов, которые передать можно лишь с помощью анимации фигур, пространственных параметров. Тогда педагогу будет удобнее объяснить материал, а он в свое время станет доступным и понятным. Следует учесть факт, что ученики к данному методу обучения проявляют повышенный интерес, и статус учителя становится приоритетным перед детьми.

Презентация на уроке способствует усвоению новой информации быстрее и в короткий срок. Так же, на слайд легко вывести опросники или тесты, что сократит время проведения обычной контрольной работы. При изучении темы всегда есть возможность вернуться на предыдущий слайд и вновь дать информацию, в отличии от школьной доски. С помощью презентаций легче проверять ранее заданное домашнее задание. Ведь проверка ведется всеми учащимися самостоятельно, что облегчает процесс работы преподавателям, повышает у каждого ученика чувство самопроверки и вырабатывает следующие свойства: внимательность, произвольность восприятия, заинтересованность к собственному успеху. После таких условий преподавания ученики проявляют инициативность, желают выступить с собственными докладами и разработками. Поэтому, давать задание становится проще и значительнее для всего класса. Так, инновационные технологии позволяют разобрать каждый курс геометрии поэтапно с существующими механизмами вербально-логического мышления. В изучение входят параметры изображаемого тела, распределение ракурса и проекции. Научить детей строить сечения и проекции на плоскости, а также научить определять на пространственном чертеже ответ к поставленной задаче сложно. Передать это с помощью динамических презентаций намного проще, чем на доске.

Таким образом, компьютерные технологии значительно развивают у учеников различные свойства памяти, мышления. Ученики учатся самоор-

ганизации, моделированию, построению схем, разрабатывают собственные презентации, проекты. Геометрия – наука сложная и для ее понимания, необходимы дополнительные приемы. Именно в наглядности выступает проблема преподнесения основ предмета. А инновационные технологии дают возможность ее решить.

Литература

1. Шарыгин И. Ф., Ерганжиева Л. Н. Математика. Наглядная геометрия. 5-6 классы. Учебник. М.: ДРОФА, 2016. 192 с.
2. Зак С. М. Математика. Арифметика. Геометрия. 6 класс. Все домашние работы. К учебнику и задачнику Е. А. Бунимовича. М.: Стандарт, ЛадКом, 2014. 256 с.
3. Боженкова Л. И. Научные основы школьного курса геометрии в обучении // Образовательные ресурсы и технологии. 2016. №2 (14). URL: https://cyberleninka.ru/article/n/-nauchnye-osnovy-shkolnogo-kursa-geometrii-v-obuchenii (дата обращения: 27.04.2018).
4. Виситаева М. Б. Пропедевтическое изучение геометрического материала в 5-6-х классах как основа развития личности школьника // Акмеология образования. Психология развития. 2013. №4. URL: https://cyberleninka.ru/article/n /propedevticheskoe-izuchenie-geometricheskogo-materiala-v5-6-x-klassah-kak-osnova-razvitiya-lichnosti-shkolnika (дата обращения: 27.04.2018).

АНАЛИЗ МОДЕЛЕЙ ТЕСТИРОВАНИЯ

В. П. Коротченко, П. А. Рыженко
руководитель – канд. техн. наук, доцент ***И. Н. Топчиев***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрены модели тестов и тестовых заданий, выявлены их достоинства. Предложена модель тестового задания, сочетающая в себе классическую и современную теорию тестирования. Проанализировано преимущество использования политомической оценки тестового балла.

Ключевые слова: современная теория тестирования, теория моделирования и параметризации тестов, модель Раша, модель Бирнбаума, тестовое задание, политомическая оценка.

На данный момент существует два подхода к теории тестирования:
– современная теория;
– классическая теория.

И классическая теория тестирования, и современная теория применяются параллельно друг с другом. Каждая теория использует собственные модели тестирования, которые представляют тестовые задания (ТЗ) [1, с. 339].

Относительно к современной теории тестирования, в основе её моделей лежит функция, определяющая отношение вероятности верного решения задания к уровню подготовленности участника тестирования и параметров задания [2, с. 431]. Такая функция является функцией успеха, и каждая модель современной теории имеет свою функцию успеха.

В современной теории тестирования существует два множества моделей:

1. Множество Бирнбаума.
2. Множество Раша [3, с. 12].

Рассматривая множество моделей Раша следует выделить:

1. Модель Пуассона.
2. Модель с фиксированными (произвольными) промежуточными категориями выполнения заданий.
3. Дихотомическая модель Раша.

Среди множества моделей Бирнбаума выделяют двухпараметрическую и трехпараметрическую модель.

Так как наибольшее распространение на практике получили однопараметрическая модель Раша и двухпараметрическая модель Бирнбаума, рассмотри функции успеха этих моделей:

Функция успеха модели Раша имеет следующий вид:

$$P = \frac{1}{1+e^{-(\theta-\delta)}} \quad (1)$$

где P – вероятность успешного выполнения тестового вопроса, θ – уровень подготовленности, δ – характеристическая функция трудностей, а $\theta = \delta$. График функции успеха для модели Раша представлен на рисунке 1.

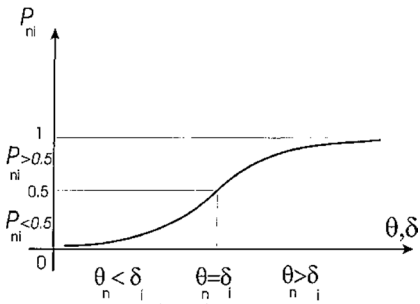


Рисунок 1. График функции успеха модели Раша

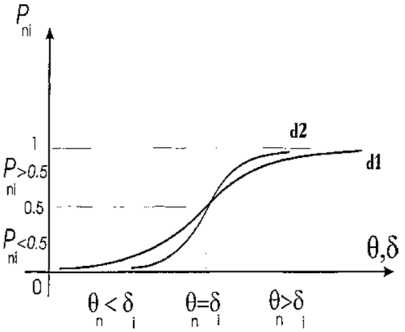


Рисунок 2. Модель ТЗ Бирнбаума

Пример модели тестового задания Бирнбаума с различными параметрами представлен на рис. 2.

Недостатком рассмотренных моделей является то, что необходимо экспериментальным путем определять параметры тестовых заданий [4, с. 1].

Используя за основу современную и классическую теорию тестирования, предлагается модель тестовых заданий, дополненная добавлением ключевых слов к описанию и ответам тестового задания. Предлагаемая модель в итоге состоит из следующих частей:

1. Сложность тестового задания.

2. Текст ТЗ и ответов на него, с добавлением ключевых слов к ним.

Основываясь на предложенной модели можно установить взаимосвязь между тестовыми заданиями, которая поможет увеличить эффективность тестирования. Для повышения точности и эффективности тестовых заданий необходимо применять политомическую оценку, которая предусматривает несколько категорий ответов, за каждый из которых дается разный балл. Используя политомическую оценку, предлагается использовать следующую формулу:

$$T = B(P - N)/F, \quad (2)$$

где T – тестовый балл, B – балл за правильный ответ, P – количество выбранных правильных вариантов, N – количество выбранных неправильных вариантов, F – общее количество правильных вариантов.

Если среди выбранных ответов неправильных ответов больше чем правильных, начисляется 0 баллов. Такой подход избавит от случаев, когда тестируемый может выбрать большинство вариантов ответа и получить некоторое число баллов.

Предложенную формулу оценки можно применить к различным типам тестовых заданий, таких как ТЗ множественного выбора, ТЗ на сопоставление, а также ТЗ на установление правильной последовательности. Перечисленные типы заданий имеют некоторые особенности, которые можно рассмотреть на примере тестового задания множественного выбора.

Приведем пример расчета для ТЗ множественного выбора:

Пусть общее количество доступных ответов равно 6, для ответа на задание необходимо выбрать 4 варианта. Тогда, при различных ответах тестируемого получим следующие результаты:

1) P = 4, N = F, T = B * (4-0) /4 = B – тестируемый получает полный балл;

2) P = 3, N = 1, T = B * (3-1) /4 = B /2 – тестируемый получает половину от балла;

3) P = 4, N = 1, T = B * (4-1) /4 = 3 B/4 – тестируемый получает 3/4 от балла за задание;

4) P = 4, N = 2, T = B * (4-2) /4 = B/4 – тестируемый получает 1/4 от балла за задание.

Первые три случая позволяют отразить действительные знания тестируемого, но в последнем варианте есть большая вероятность ошибки, так как тестируемый может выбрать все предлагаемые варианты ответов, тем самым получив в 1/4 от тестового балла за задание. Такой вариант не позволит отразить действительный уровень знаний тестирования, поэтому, чтобы избежать подобной ошибки при оценке тестового задания множественного выбора необходимо, чтобы количество неправильных ответов в тестовом задании или превосходило, или было равно количеству правильных вариантов ответа. Таким образом, при выборе всех предлагаемых от-

ветов тестируемый не получит тестовых баллов, что позволит точнее отразить уровень подготовленности тестируемого.

Литература

1. Андронов А. М. Теория вероятностей и математическая статистика / А. М. Андронов, Е. А. Копытов, Л. Я. Гринглаз. Спб.: Питер, 2004. 464 с.

2. Башмаков А. И. Разработка компьютерных учебников и обучающих систем / А. И. Башмаков, И. А. Башмаков. М.: Изд-во «Филинъ», 2002. 616 с.

3. Карданова Е. Ю. Основные модели современной теории тестирования / Е. Ю. Карданова, Ю. М. Нейман // Вопросы тестирования в образовании. 2003. № 9. С. 12-37.

4. Челышкова М. Б. Математические модели современной теории тестов // Тез. докл. школа-семинар "Научные проблемы тестового контроля знаний". М.: Исследовательский, центр проблем качества подготовки специалистов. С. 42-57.

РАЗВИТИЕ САМОСТОЯТЕЛЬНОСТИ МЛАДШИХ ШКОЛЬНИКОВ ЧЕРЕЗ ВНЕДРЕНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Т. В. Малюта
руководитель – канд. пед. наук, доцент ***А. Х. Ардеев***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассмотрены вопросы введения ФГОС в систему общего образования и, обусловленные этим, существенные изменения в деятельности педагога. Проанализированы особенности развития самостоятельности младших школьников через внедрение информационно-коммуникационных технологий, рассмотрены преимущества использования электронных учебных материалов.

Ключевые слова: самостоятельность, информационно-коммуникационные технологии, мультимедиа презентация, моделирование.

XXI век – век новых технологий который значительно расширил степень влияния окружающего мира на подрастающее поколение. Все чаще сверстники общаются друг с другом с помощью гаджетов используя всевозможные чаты, форумы, электронную почту тем самым заменяя «живое слово». Поэтому можно целесообразно использовать широкие возможности, предоставляемые Интернетом, для приобщения обучающихся к информационной культуре. Поэтому имеет большое значение за короткое время научить ребенка работать с информацией. Это позволит учителя совмещать традиционные методы и современные информационные технологии, в том числе и компьютерные. На уроках компьютер позволяет урок сделать более мобильным, дифференцированным и индивидуальным.

Подкованность педагогов школы в данном направлении говорит о ценности продуктивного использования информационных технологий, заключающееся в увеличении уровня самостоятельности обучающихся.

Наглядность и простое использование, безусловно, делает более успешным учебный процесс, развивает творческие способности, вызывает

познавательный интерес школьников, благоприятно способствует на положительную мотивацию к самоообразованию [7, с. 258].

Преимущественно использования ИКТ раскрываются с начала его использования, и по мере применения, дают толчок к саморазвитию учителя, дают возможность оставаться ему современным, мобильным и интересным.

Планируя, мультимедийный урок, учитель осуществляет огромную работу – продумывает последовательность технологических операций, формы и способы подачи информации на большой экран, решает, как будет управлять учебным процессом, как будет обеспечивать общение на уроке, обратную связь с обучающимися, достигать развивающего эффекта обучения.

Применение ИКТ помогает организовать самоконтроль знаний в работе с тестами, дает возможность систематизировать знания, повторить, закреплять полученные знания, решать интерактивные упражнения, развивать мышление, память [5, с. 21-23].

Наиболее ярким достоинством уроков с применением ИКТ выступает усиление наглядности, которое благоприятно способствует развитию художественного и эстетического вкуса обучающихся, повышению их эмоциональной сферы [6, с. 82].

Медиапособия, которые создают педагоги, чаще всего включают изображения, видео-, аудиоматериалы, тестовые задания.

Эффект уроков с мультимедиа поддержкой усиливается с помощью музыкального сопровождения, анимированными и звуковыми эффектами. Такие уроки чаще сопровождаются вопросами познавательного характера, которые вызывают ребенка на диалог, комментирование происходящего [1, с. 50-54].

При самостоятельной разработке мультимедийных пособий, педагоги уделяют больше внимания цветовому решению слайдов, так как, она благоприятно воздействует на познавательную деятельность, учитывают возрастные особенности.

Проводя анализ уроков с использованием, можно отметить: высокую плотность урока, интенсивность смены видов деятельности.

Уроки, в которых применяется презентационный материал, мультимедийные пособия, наиболее ярко эмоционально окрашены, выразительны, чаще применяются игровые приемы, что благоприятно влияет на повышение качества усвоения учебного материала.

Чаще всего школьный класс оснащен 1-2 компьютерами, что позволяет использовать индивидуальные формы работы. В таком случае можно в классе организовать фронтальную работу, а один - два ученика получают индивидуальное задание, оценка которого запрограммирована в компьютере.

При проведении обобщающих уроков по нескольким темам можно использовать данное электронное пособие в классе, оснащенным одним компьютером, подключенным к компьютеру. В данном случае будет уместна фронтальная форма работы, в рамках которой будет организована систематизация, обогащение или углубления знаний учащихся.

Также единственный компьютер в классе может быть использован учителем, при применении групповой деятельности обучающихся, в ходе которой 2-4 ученика дается одинаковое задание, которое необходимо выполнить при помощи электронного пособия. В этом случае будет важен не только результат работы, но и способ их взаимодействия в процессе работы. В связи с этим учителю заранее нужно продумать все возможные способы взаимодействия учащихся, при работе с пособием.

При использовании электронного пособия можно организовать индивидуальную форму работы, которая будет более эффективной, если учителем будет предлагаться индивидуальная серия заданий, направленная на коррекцию его типичных ошибок. Также можно предложить задания более высокого уровня наиболее успешным ученикам [2, с. 49-51].

Итак, различные виды средств обучения являются носителями специфических свойств и функций, определяющих их дидактические возможности. Такое представление о средствах обучения служит теоретическим обоснованием дифференцированного подхода к их использованию.

Литература

1. Баженова Л. М. Медиаобразование как средство художественного развития младших школьников // Начальная школа. 2012. №5. С.50-54.

2. Дурова А. И. Современные технологии в учебном процессе / А. И. Дурова, А. А. Вахрушев // Начальная школа. 2017. №12. С.49-51.

3. Комарова И. Использование информационных технологий в совершенствовании системы образования // Народное образование. 2016. №2. С.157-159.

4. Павлова С. И. Информационно-технические средства обучения в начальной школе // Начальная школа. 2016. №4. С.110-112.

5. Соколова Т. Е. Воспитание познавательных интересов младших школьников средствами новых информационных технологий // Начальная школа. 2014. №3. С.21-23.

6. Суворова Г. Ф. Средства обучения и методика их использования в начальной школе / Г. Ф. Суворова, Я. В. Владимирова, А. В. Поляков. М.: Просвещение, 2010. 160 с.

7. Щукина Г. И. Проблема познавательного интереса в педагогике. М.: «Просвещение», 2015. 368 с.

ЭЛЕКТРОННЫЙ ОБРАЗОВАТЕЛЬНЫЙ РЕСУРС ДЛЯ ИЗУЧЕНИЯ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Д. В. Мезенцев
руководитель – канд. техн. наук, доцент ***И. Н. Топчиев***
Северо-Кавказский федеральный университет, г. Ставрополь

Проведен обзор программных сред и оболочек для создания электронных образовательных ресурсов; представлено описание электронного образовательного ресурса для приобретения студентами компетенций создания программных систем с использованием нейросетевых технологий для решения различных технических задач.

Ключевые слова: электронные образовательные ресурсы, дистанционное обучение, образовательные интеграционные платформы, Moodle, прогрессивные педагогические методики, мультимедиа ресурсы.

Информационные технологии развиваются колоссальными темпами. В современном образовании происходят значительные изменения, развивается и совершенствуется новая технология – дистанционное образование, что влечет за собой все более серьезные требования, предъявляемые к его организации.

В настоящее время дистанционное обучение, развивающееся на стыке передовых научно-технических достижений и прогрессивных педагогических методик, позволяет не только использовать инновационные образовательные технологии, различные организационные формы, средства и способы организации обучения, но и создавать условия для социализации различных категорий обучающихся, независимо от места их нахождения, состояния здоровья, мобильности [1].

Организационно-дидактической основой дистанционного обучения является электронная информационно-образовательная среда, создаваемая с помощью информационно-коммуникационных и интернет-технологий, среди которых особое место занимают, обеспечивающие обмен учебной информацией на расстоянии, и реализующие систему педагогического сопровождения и администрирования процесса подготовки обучающихся.

Правильный выбор программного средства для создания дистанционного учебного курса позволяет реализовать все дидактические возможности и преимущества дистанционных технологий обучения. Программных сред и оболочек для создания дистанционного курса существует сейчас большое множество. Например, такие средства как: ATutor, Claroline, Dokeos, LAMS, OLAT, OpenACS, Sakai, Moodle и др. [2].

При подготовке ИТ-специалистов использование электронных ресурсов является наиболее оправданным. В рамках исследования был разработан электронный образовательный ресурс на платформе Moodle для приобретения студентами компетенций создания программных систем с использованием нейросетевых технологий для решения различных технических задач.

Начальная страница (рис. 1) была создана с учетом стандартов оформления электронных образовательных ресурсов. В ней содержится верхняя строка с указанием учебного заведения для которого создавался электронный ресурс, ниже расположены ссылки на официальный сайт учебного заведения, нормативные документы, инструкции по работе с ресурсом и контакты для оказания технической поддержки. Ниже находится строка с ссылкой на главную страницу данного электронного учебника; а также идентификационный логотип данного учебника. Логотип электронного курса представляет собой официальный логотип учебного заведения.

Раздел управления курсом для преподавателя (рис. 3) включает в себя пункт «Управление курсом» с подразделами: режим редактирования (раздел редактирования содержимого курса); редактировать настройки (раздел редактирования курса с пунктами несвязанными с наполнением); пользователи (список пользователей которым доступен курс); фильтры (фильтры применимые к данному курсу); отчеты (отчеты обучающихся по прохождению курса); оценки (оценки обучающихся); значки (возможные значки достижений по выбранному курсу) [2, 3].

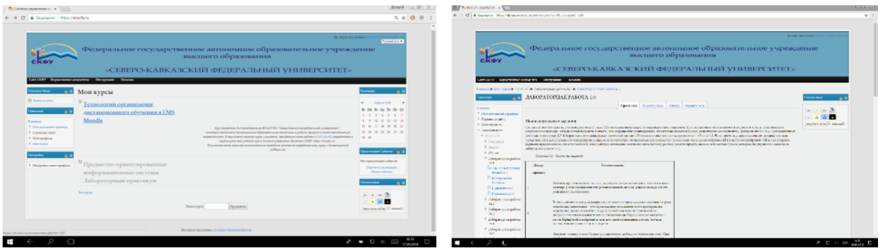


Рисунок 1. Страницы электронного образовательного ресурса

Слева находится навигационное меню электронного ресурса (рис. 2), которое включает пункты для ускорения процесса нахождения нужной информации.

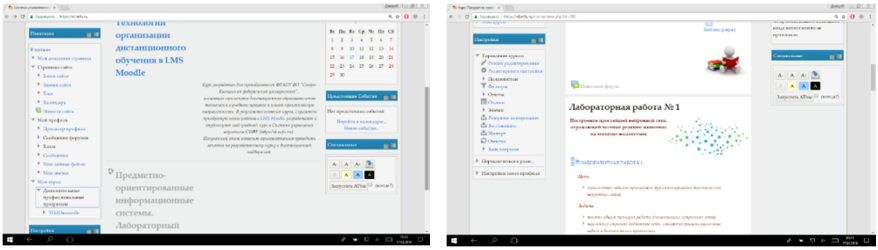


Рисунок 2. Навигационное меню

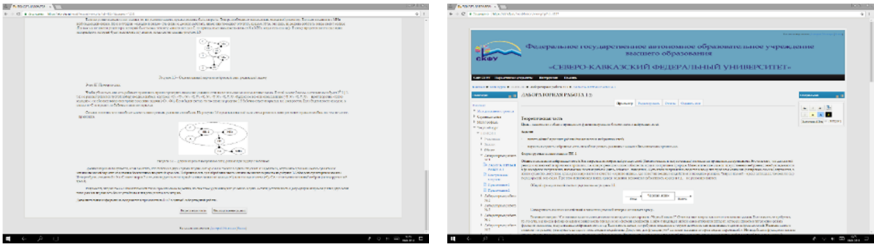


Рисунок 3. Представление теоретического материала

Электронный образовательный ресурс содержит 6 лабораторных работ: построение простейшей нейронной сети, отражающей частные реакции животных на внешние воздействия; общее знакомство со средой Matlab и созданием в ней искусственных нейронных сетей; создание простой нейронной сети с помощью nntool; создание и обучение нейронной сети на языке высокого уровня среды Matlab; пример создания и обучения нейронных сетей для задач классификации в среде Matlab (часть 1 и часть 2). Каждая лабораторная работа включает в себя теоретическую часть (рис. 3) и индивидуальные задания (рис. 1) переключение между которыми выполняется кнопками внизу страницы (рис. 3).

Использование разработанного образовательного ресурса целесообразно как при проведении лабораторных занятий в компьютерном классе, так и при самостоятельной работе студентов.

Литература

1. Terry Anderson. The Theory and Practice of Online Learning: Second Edition = Athabasca University Press, 2008.

2. Мациевский С. В. Развитие научных основ ИТ-образования // Дистанционное и виртуальное обучение. 2007. N 9. С. 13-17.

3. Ольнев А. С. Использование новых технологий в дистанционном обучении // Актуальные проблемы современной науки. 2011. N 1. С. 96.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СРЕДСТВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ОБРАЗОВАНИИ

И. С. Павлова, Е. А. Кобзева
руководитель – канд. пед. наук, доцент ***Т. А. Куликова***
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье рассматривается применение информационно-коммуникационных технологий и проводится анализ проблем, связанных с внедрением ИКТ в образование. Рассмотрены преимущества информационных технологий перед традиционной системой образования. В результате исследования заключительной точкой стала необходимость совершенствования методов и форм обучения, а также развитие образования не только с технической стороны, но и с педагогической.

Ключевые слова: информационно-коммуникационные технологии, образование, качество образования, цифровые технологии, виды информационных технологий, средства ИКТ, использование ИКТ.

В настоящее время, применение информационно-коммуникационных технологий в сфере образования способствует повышению качества образовательных технологий, появлению новых форм обучения (электронное, мобильное, совместное обучение и т. д.), созданию электронных образова-

тельных ресурсов и доступа к ним обширного круга обучающихся, а также повышает доступность и качество образования.

Исходя из этого, появляется проблема перехода от устаревшей системы образования к цифровому обучению [1].

Основными причинами данной проблемы являются недостаточное моральное и материальное стимулирование деятельности преподавателей по внедрению ИКТ, малое количество и низкое качество готовых учебных материалов для организации самостоятельной работы студентов на базе-ИКТ, отсутствие у вуза технических возможностей.

Так как цифровые технологии [2] все более активно распространяются, сфера образования подвергается существенным изменениям.

Существуют следующие виды информационных технологий в образовании:

- мобильное обучение;
- социальные медиа;
- смарт-книга;
- облачные технологии;
- массовые открытые онлайн-курсы.

Внедрение информационно-коммуникационных технологий значительно расширяет возможности образования.

Использование ИКТ в обучении помогает решить задачи, представленные на рис. 1.

Рисунок1. Задачи, решаемые с использованием ИКТ в процессе обучения

Рассмотрим преимущества использования ИКТ в образовании перед традиционным обучением, которые Е.И. Машбиц относит к набору существенных преимуществ использования компьютера в обучении перед традиционными:

1. Информационные технологии расширяют возможности предъявления учебной информации. Воспроизвести реальную обстановку деятельности позволяет применение цвета, графики, звука, всех современных средств видеотехники.

2. Существенное повышение мотивации студентов к обучению, за счет применения адекватного поощрения правильных решений задач.

3. ИКТ вовлекают учащихся в учебный процесс, способствуя активизации умственной деятельности и наиболее широкому раскрытию их способностей.

4. В учебном процессе использование ИКТ повышает возможности постановки учебных задач и управления процессом их решения. Компьютеры позволяют строить и анализировать модели различных ситуаций, предметов, явлений.

5. Качественное изменение контроля деятельности учащихся и обеспечение мобильности управления учебным процессом.

6. Обучающая программа дает возможность обучающимся наглядно представить результат своих действий, определить этап в решении задачи, на котором сделана ошибка, и исправить ее. Компьютер способствует формированию у учащихся рефлексии [3].

В педагогической практике имеется классификация средств ИКТ по области методического назначения (рис. 2).

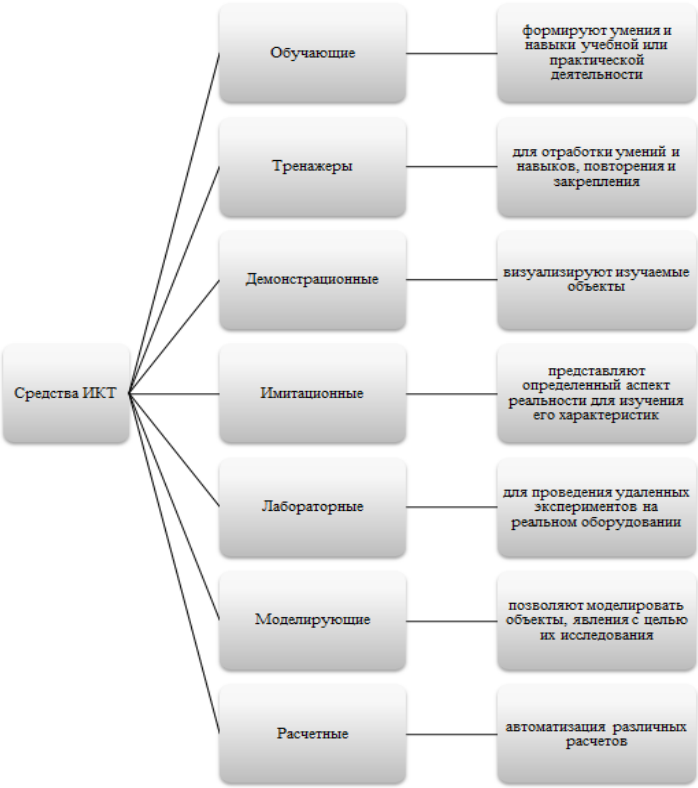


Рисунок 2. Классификация средств ИКТ по области методического назначения

Помимо преимуществ существуют также недостатки при использовании средств ИКТ. На рис. 3 представлены недостатки в образовательном процессе.

Рисунок 3. Недостатки и проблемы использования средств ИКТ

В современных условиях педагогу недостаточно быть только пользователем, необходимо говорить о повышении компетентности педагога в области ИКТ, являющейся его профессиональной характеристикой, составляющей педагогического мастерства.

Таким образом, в процессе образования неизбежно приходится изменять все компоненты образовательной системы и внедрять средства информационных и коммуникационных технологий в профессиональную деятельность педагогов, в предметные области и организацию управления учебно – воспитательным процессом. Поэтому, для того чтобы улучшать методы и формы обучения, нужна специальная подготовка работников системы образования в области использования средств информационных технологий, а также современное оборудование и программное обеспечение, электронные средства учебного и образовательного назначения [4].

Литература

1. Загвязинский В. И. Вузовская лекция в структуре современного учебного процесса // Образование и наука. 2014. С. 34-46.

2. Захарова, И.Г. Информационные технологии в образовании: Учеб. пособие для студентов высш. пед. учеб. заведений. М., 2003. 105 с.

3. Информационные и коммуникационные технологии в образовании / под ред. Д. Бадарча. М.: ИИТО ЮНЕСКО, 2013. 320 с.

4. Образовательные технологии XXI века: информационная культура и медиаобразование. ОТ'13: сб. ст. междунар. науч.-практ. конф. / под ред.: С. И. Гудилиной, К. М. Тихомировой, Д. Т. Рудаковой. СПб.: Нестор-История, 2013. 373 с.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ОБУЧЕНИИ ХИМИИ

Э. В. Паршукова
руководитель – канд. пед. наук, доцент ***Г. И. Шевченко***
Северо-Кавказский федеральный университет, г. Ставрополь

Актуальность темы исследования обусловлена тем, что непросто успешно овладеть даже базовым уровнем школьного курса химии. Поэтому перед педагогом остро стоит задача включения каждого обучающегося в активную деятельность, обеспечивающую формирование и развитие познавательной деятельности, повышающей интерес к химии. Одним из способов повышения эффективности обучения химии является использование информационных и коммуникационных технологий, которые позволяют применять в обучении химии различные методы и организационные формы, включить каждого обучающегося в процесс самостоятельной деятельности, учитывая его индивидуальные способности.

Ключевые слова: информационные и коммуникационные технологии, интегративные функции, система обучения и методы обучения химии, мотивация**,** задачи обучения, познавательная активность.

Реальность современного мира такова, что необходимо быть не только образованным и способным понимать и правильно реагировать на постоянно изменяющееся положение человека в мире, но быть конкурентоспособным на рынке труда. Поэтому современным школьникам, для соответствия требованиям общества, необходимо быть высокообразованными, коммуникабельными, толерантными, владеющими новыми технологиями [2].

Информационные и коммуникационные технологии (ИКТ) – образовательные технологии, основу которых составляют современные способы обработки информации с помощью компьютера, их периферийных устройств, программных средств, мультимедиа, компьютерных сетей. На основе ИКТ осуществляется процесс подготовки и передачи информации школьнику. В процессе использования ИКТ обучающийся становится активным участником образовательного процесса, потому что повышается интерес к предмету, развиваются возможности самореализации и самовыражения [1].

В настоящее время, когда химия как наука становится все более востребованной, проникающей во все сферы жизни человека, овладеть ею без кропотливого труда, терпения, усидчивости просто невозможно.

Задача любой учебной дисциплины, в том числе и химии, «может быть достигнута только благодаря реализации комплекса интегративных функций. К их числу следует отнести: образовательно-мировоззренческую, воспитательно-мобилизующую, профессионально-прикладную, жизненно-практическую и развивающую».

В связи с этим становится актуальным совершенствование форм и методов обучения химии, которые стимулируют мыслительную деятельность школьников, развивают их познавательную активность, учат практически использовать химические знания [7, 8].

Учитель химии с помощью ИКТ может осуществлять анализ:

– всех видов учебной и внеклассной деятельности, например, проводить анкетирование обучающихся;

– своего опыта педагогической деятельности;

– итогов успеваемости;

– самостоятельного конструирования электронных пособий и т.д.

Как показывает практика **х**имия – один из самых сложных общеобразовательных предметов. Успешно овладеть даже базовым уровнем школьного курса химии непросто. Поэтому задача педагога состоит в том, чтобы включить каждого обучающегося в активную деятельность, обеспечивающую формирование и развитие познавательной деятельности и повышающую мотивацию обучения химии, поскольку качество знаний во многом определяется интересом к учебному предмету [6].

Современная система обучения представляет собой информационную инфраструктуру, которая включает различные технологии и участников

образовательного процесса, обладающих знаниями и практическим опытом, способных обмениваются им друг с другом [9, 10].

Образовательная деятельность сегодня не может обойтись без использования ИКТ. Применение на уроках химии различных мультимедийных средств и интерактивных комплексов дает возможность обучающимся увидеть и изучить пространственное строение молекул органических соединений, что достаточно сложно сделать это в рамках учебника и представленном в нем плоскостном изображении. В особенности удобными являются задания для самоконтроля и тестирования, которые позволяют оперативно проверить уровень усвоения материала не только учителем, но и самими обучающимися.

Ключевой проблемой при любом обучении является проблема удержания внимания обучающихся. ИКТ способствуют удерживанию внимания обучающихся в течение всего урока, благодаря тому, что эти технологии позволяют поддерживать смену ярких впечатлений от увиденного. Наглядность, возможность изменять темп и формы изучения материала, его образно – художественное представление – все это делает компьютер незаменимым помощником учителя в деле снижения утомляемости обучающихся [7, 8]. К достоинствам компьютера в качестве помощника следует отнести практически неограниченные его возможности, предоставляемые учителю при творческом построении урока.

Применение ИКТ способствует изменению взаимодействия «учитель-ученик» – не только передавать знания обучающимся, но и развивать у них логику, мышление, чтобы они выступали не в роли пассивных слушателей, а в роли активных участников, создателей урока [5].

Проанализировав психолого-педагогическую и методическую литературу по теме исследования, изучив формы использования ИКТ в обучении химии, и на основании экспериментального преподавания и изучения передового опыта учителей химии было выявлено влияние ИКТ на образовательный процесс [4]. Грамотное использование в обучении химии таких методов как:

1) экспертное оценивание (в качестве экспертов выступают педагоги);
2) целенаправленное наблюдение за учебным процессом;
3) обобщение независимых характеристик;
4) анкетирование обучающихся;
5) тестирование обучающихся (входящий контроль: предварительная диагностика уровня усвоения химических понятий; выходной контроль для выявления динамики развития обучающихся);
6) моделирование и проектирование учебного процесса;
7) праксиметрические методы (анализ результатов деятельности).

Позволило определить одну из важнейших задач обучения химии – пробуждение удивления, любопытства, заинтересованности обучающихся. Как только учитель «зацепит» сферу интересов обучающихся, он сможет

пробиться через стену отчужденности и безразличия, вызвать простое, естественное удивление перед фактом или теоретическим выводом. Учитель открывает перед обучающимися конкретную область знаний как источник интереса, делая активной и устойчивой мотивацию к процессу обучения.

В заключение следует заметить, что сегодня ИКТ становятся важной частью практически всех профессий, прочно входят в наш быт, образование и культуру. В частности, ИКТ в образовании позволяют включить каждого обучающегося в процесс самостоятельной деятельности, учитывая его индивидуальные способности. Они расширяют сферу самостоятельной познавательной деятельности, позволяют осуществлять переход от простых знаний к более сложным знаниям.

Использование средств ИКТ (компьютера, интерактивной доски и др.) на уроках химии повышает заинтересованность обучающихся, улучшает качество восприятия ими учебного материала. А учителю позволяют понять обучающегося, объективнее оценить его способности и знания. Все это, в конечном счете, побуждает учителя к поиску новых, нетрадиционных форм и средств обучения [3].

Литература

1. Горовая В. И., Шевченко Г. И. Управленческая парадигма и ее реализация в образовательной практике современного вуза // Вестник Университета (Государственный университет управления). 2008. № 6. С. 35-39.

2. Далингер В. А. Компетентностный подход и образовательные стандарты общего образования // Образовательно-инновационные технологии: теория и практика: монография / под ред. О. И. Кирикова. Книга 2. Воронеж: Изд-во ВГПУ, 2009. С. 7-18.

3. Дендербер С. В., Ключникова О. В. Современные технологии в процессе преподавания химии. М., 2007.

4. Загорский В. В. Интернет–ресурсы для учителя // Химия в школе. 2003. № 9. С. 2-7.

5. Использование современных информационных и коммуникационных технологий в образовательном процессе: Учебно-методический комплект для системы педагогического образования / под общ.ред. А. М. Семибратова. М.: АПК и ПРО, 2004. 200 с.

6. Нечитайлова Е. В. Информационные технологии на уроках химии // Химия в школе. 2005. № 3. С. 13-15.

7. Паршукова Э. В. ИКТ в обучении химии. Ставрополь: Изд-во СКФУ, 2017.

8. Паршукова Э. В. Игровые компьютерные технологии в деятельности учителя химии. Ставрополь: Изд-во СКФУ, 2017.

9. Шевченко Г. И. Образовательная электронная среда: сущность, назначение // Информационные технологии в науке и образовании. Материалы международной научно-практической интернет-конференции и V Всероссийского семинара «Применение MOODLE в сетевом обучении». Под редакцией А.Э. Попова. 2012. С. 72-74.

10. Шевченко Г. И. Образовательная электронная среда и модификация управленческой деятельности преподавателя вуза // Информатика и образование. 2010. № 12. С. 98-100.

ОСНОВНЫЕ ПРОБЛЕМЫ ОРГАНИЗАЦИИ И ВОПРОСЫ ПОСТРОЕНИЯ МОДЕЛИ ЭЛЕКТРОННОГО ОБУЧЕНИЯ В ВУЗЕ

Д. А. Решетникова
руководитель – канд. пед. наук, доцент ***О. П. Панкратова***
Северо-Кавказский федеральный университет, г. Ставрополь

В статье рассматриваются основные проблемы организации электронного обучения на протяжении последних нескольких лет, перспективы его дальнейшего развития. Предлагаются меры по решению данных проблем и улучшению организации такого обучения в ВУЗе. Анализируются различные модели электронного обучения и выдвигаются требования, которые необходимо соблюдать при их создании.

Ключевые слова: электронное обучение, проблемы электронного обучения, организация электронного обучения, модель электронного обучения.

В настоящее время информационные технологии присутствуют в жизни и оказывают влияние на каждого человека. Они настолько глубокого внедрились и в сферу образования, что это способствовало развитию инновационных форм обучения, например, электронного обучения [4, с. 8].

Вопросам развития, особенностям применения, технологиям и средствам электронного обучения в вузе посвящены работы многих отечественных и зарубежных ученых [1].

В данной статье представлен обзор ряда научных материалов по проблемам организации электронного обучения в ВУЗе за последние несколько лет, а также предложены меры по разрешению основных проблем, стоящих перед организаторами электронного обучения сегодня.

В федеральном законе «Об образовании Российской Федерации» под электронным обучением понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. А при реализации образовательных программ с применением только электронного обучения, непосредственно должны быть созданы условия для функционирования электронной информационно-образовательной среды [6, с. 54]. Отсюда и вытекает ряд проблем по организации электронного обучения в вузе.

Так в 2014 году А. А. Воронина в своей статье выделяла следующую проблему организации электронного обучения в ВУЗе – «недостаточность материальной базы для широкого использования возможностей электронных ресурсов, а также неспособность преподавательского состава методически обеспечить функционирование электронного образовательного кон-

тента на необходимом уровне качества» [3]. Решением данных проблем занимаются и по сей день. Большинство преподавателей готовы методически обеспечить его функционирование, однако проблема материальной базы остается актуальной.

В 2016 году И. А. Болкунов основной проблемой в вопросах организации электронного обучения выделил финансовую составляющую. По его мнению, она содержит в себе не только вопросы разработки и применения стандартов на электронные учебные пособия, но и затраты непосредственно на разработку электронных курсов, а также их последующее усовершенствование [2, с. 129].

Существует еще множество проблем по организации электронного обучения, решением которых занимаются на протяжении нескольких лет. Построение модели электронного обучения была и остается одной из самых актуальных проблем в данной области.

Существует множество моделей электронного обучения. Н. С. Силкина и Л. Б. Соколинский в своей научной работе выделяют и представляют обзор следующих моделей:

1. Концептуальная модель среды электронного обучения, в основе которой лежит база знаний, содержащая образовательный контент (рис. 1).
2. Модель данных для взаимодействия с образовательными объектами.

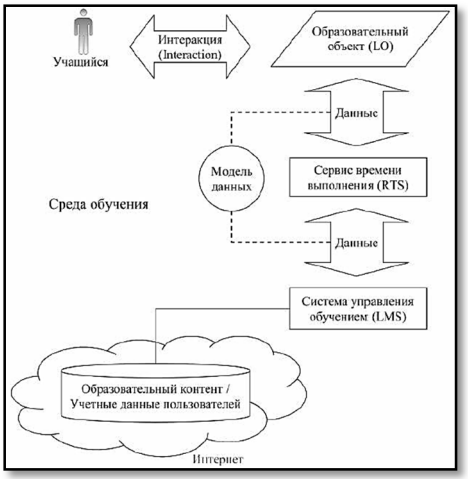


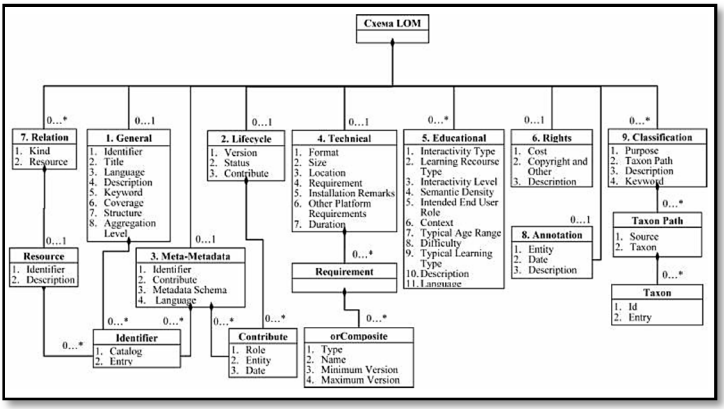
Рисунок 1. Концептуальная модель среды электронного обучения

3. Модели накопления контента, описывающие компоненты, которые используются в образовательных системах, а также способы их обмена и описания для поиска и использования, упаковки контента. Такие модели они подразделяются на:

a. Модель метаданных, предназначенная для описания структуры и свойств образовательных объектов (рис. 2, а);

b. Модель структуры контента, определяющая структуру электронного учебного курса в соответствии с требованиями (рис. 2, б);

c. Модель упаковки контента, определяющая стандартный набор структур данных (рис. 2, в);



а) Модель метаданных

Иерархия	Уровень	Структура курса
Программа (Curriculum)	1.	
Курс (Course)	2.	Блок
Глава (Chapter)	3.	Блок
Раздел (Subchapter)	4.	Блок
Модуль (Module)	5.	
Урок (Lesson)	6.	Назначаемый элемент (Assignable Unit)
Понятие (Topic)	7.	
Кадр (Frame)	8.	
Объект (Object)	9.	

б) Модель структуры контента

в) Модель упаковки контента

Рисунок 2. Модели накопления контента

4. Модель среды выполнения, определяющая структуру прикладного программного интерфейса (рис. 3).

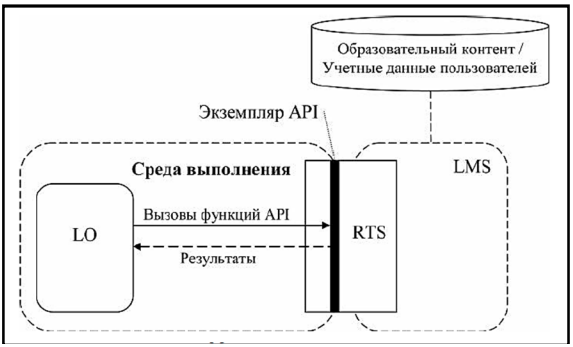


Рисунок 3. Модель среды выполнения

5. Модель простого упорядочения, определяющая метод, с помощью которого можно задать план изучения образовательного контента.

6. Модель компетенций, использующаяся непосредственно для спецификации знаний, умений и навыков в LMS и в компетентностных профилях учащихся и другие модели электронного обучения (рис. 4) [5, с. 6-33].

Проанализировав представленные модели, мы пришли к выводу, что при построении модели электронного обучения необходимо руководствоваться следующими требованиями:

1. Обучение должно содержать в себе элементы адаптивности – в частности, гибкую траекторию обучения. Не мало важным остается при этом модульный подход к представлению учебного материала, позволяющий осуществлять обучение в зависимости от уровня знаний.

2. Обучение должно быть максимально ориентировано на самостоятельную работу обучающегося, а также обеспечивать его заинтересованность в процессе обучения.

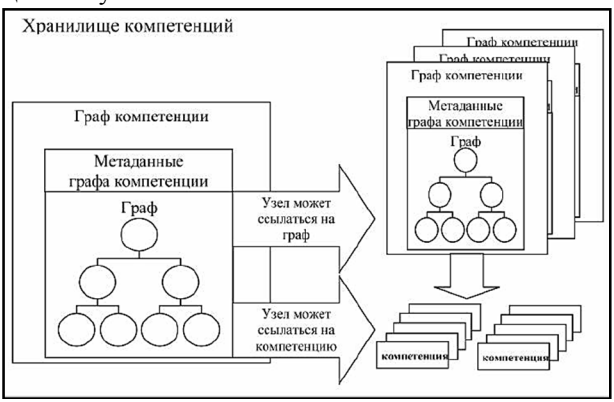


Рисунок 4. Модель компетенций

3. Должна учитываться специфика обучения в профессиональной сфере (должна быть организована практически непрерывная возможность обучения в различных условиях, например:

a) ограниченных финансовых ресурсов,

b) территориальной удаленности;

c) невозможности отрыва персонала от основного места работы на длительный срок и др.

4. Обучение обязательно должно включать в себя элементы активного обучения, которые предусматривают визуализацию учебного материала, использование технологий мультимедиа и применение современных компьютерных технологий.

5. Компьютерные средства обучения должны включать наиболее востребованный учебный материал и быть снабжены актуальной нормативной базой.

6. Средства обучения должны быть ориентированы на использование в Web-среде.

7. Необходимо обеспечить непрерывность и цикличность процесса обучения и тестирования.

Каждая модель электронного обучения предусматривает наличие методической базы, как правило, представленной двумя уровнями:

– создание комплекса электронных энциклопедий по определенным областям знаний;

– создание электронных учебных курсов на основе уже существующих энциклопедий, при помощи экспорта учебных блоков и организации их в иерархическую структуру, адекватно реализующих рабочие учебные программы в соответствии с требованиями нормативно-правовой базы.

Таким образом, сейчас необходимо заниматься комплексным решением отмеченных проблем электронного обучения. Конечно, решение таких проблем невозможно без прямого участия Государственных органов управления образованием, ВУЗов и компаний, работающих на рынке информационных технологий. Тогда, и только тогда электронное обучение в системе российского образования будет развиваться и совершенствоваться.

Литература

1. Баринова Н. В. Проблемы развития дистанционного и электронного образования в России // ИТпортал, 2017. №2 (14). Крым: Крымский федеральный университет им. В. И. Вернадского [Научная статья]. Режим доступа: http://itportal.ru/science/tech/problemy-razvitiya-distantsionnogo-/ (дата обращения 22.04.2018).

2. Болкунов И. А. Электронное обучение: проблемы, перспективы, задачи/ Таврический научный обозреватель, 2016. №11 (16). С.128–132.

3. Воронина А. А. Проблемы внедрения электронного Обучения в России/ XI международная научно-методическая конференция «Новые образовательные технологии в вузе». Екатеринбург: Российский государственный профессионально-педагогический университет [Научная статья]. Режим доступа: http://elar.urfu.ru/bitstream/10995/24767/1/notv-2014-049.pdf (дата обращения 25.04.2018).

4. Набатова М. С. Дистанционное обучение // Альманах мировой науки, 2016. № 4-3 (7), С. 8-9.

5. Силкина Н. С., Соколинский Л. Б. Модели и стандарты электронного обучения/ Вестник ЮУрГУ. Серия: вычислительная математика и информатика, Издательский центр ЮУрГУ, 2014. Том 3. № 4. С. 5-35.

6. Федеральный закон «Об образовании в Российской Федерации». М.: Издательство «Омега-Л», 2013. С. 134.

ОБЗОР И АНАЛИЗ СИСТЕМ АТТЕСТАЦИИ СИЛ ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

П. А. Рыженко, В. П. Коротченко
руководитель – канд. техн. наук, доцент ***И. Н. Топчиев***
Северо-Кавказский федеральный университет, г. Ставрополь

Актуальность исследования определена в соответствии с приказом Министерства Транспорта России N 231 «Об утверждении требований к знаниям, умениям, навыкам сил обеспечения транспортной безопасности», а также тем, что к подготовке, переподготовке, и повышению квалификации в настоящее время, предъявляются высокие требования [1, с. 1].

В статье рассмотрена проблема использования компьютерных систем тестирования для проверки знаний сотрудников, приведены критерии оценки типовых систем, выявлены недостатки существующих систем аттестации. В результате проведенного обзора и анализа систем аттестации сил обеспечения транспортной безопасности можно сделать вывод, что существующие системы не способны в полной мере решать поставленные перед ними задачи, поэтому необходимо разработать систему, лишенную недостатков других аналогов.

Ключевые слова: компьютерная система тестирования, аттестация, оценивание знаний, обеспечение транспортной безопасности, автоматизированное рабочее место, система оценок.

Аттестация – это форма оценки работы сотрудников, соответствия их занимаемой должности. Проведение аттестаций на основе тестирования является одним из самых эффективных способов контроля знаний. Такой стандартизованный метод проверки знаний, умений и навыков сотрудников позволяет обеспечить непредвзятость, а также определить точную систему оценок. Для повышения эффективности тестирований используются компьютерные системы тестирования (КСТ) [2, с. 1].

1. Обзор и анализ систем аттестации

Рассматривая системы в сфере аттестации сил обеспечения транспортной безопасности следует выделить систему АО «Транссеть». Этой компанией разработана единая система аттестации сил обеспечения транспортной безопасности на железнодорожном транспорте. Система проводит проверки по 8 категориям специалистов [3, с. 1].

Система содержит несколько модулей, осуществляющих различные функции:

1. Модуль «Администрирование» используется для работы с Аттестуемыми лицами, назначает и согласовывает билеты по группам аттестуемых лиц.

2. Модуль проверки позволяет проводить проверку знаний умений и навыков аттестуемых лиц по восьми категориям сил ОТБ.

3. Модуль «Отчеты», включает в себя Протоколы проверок, Реестры проверок и Аналитическую отчетность.

4. Модуль «Автоматизированных рабочих мест (далее – АРМ)», включает в себя: АРМ Руководителя проверок; АРМ Технического специалиста; АРМ Полиграффолога; АРМ Специалиста по физической подготовке; АРМ Специалиста по стрельбе [4, с. 1].

Преимущества данной системы заключаются в следующем: ориентированность на разветвленную филиальную структуру аттестующей организации; удаленный доступ к системе; настройка системы под требования любой организации; ограничение доступа пользователям, не имеющим данных для входа в систему.

Однако, используя находящиеся на сайте компании в открытом доступе руководства пользователя и администратора, можно сделать несколько выводов о функциональности системы и ее недостатках.

При изучении системы можно сделать вывод, что она построена на основе системы управления обучением Moodle – модульной объектно-ориентированной дистанционной учебной среде.

Одной из главных проблем систем, построенных на основе систем с открытым исходным кодом является защищенность данных. Некоторые возможности системы Moodle позволяют пользователям добавлять непроверенные файлы, HTML коды, которые потенциально могут быть использованы с целью получения прав администратора [5, с. 1113].

Согласно руководству пользователя системы, протокол итогов проведения аттестации формируется в бумажной форме, а также в формате файла Microsoft Word. Для того, чтобы обеспечить независимость формата выходного документа от используемой операционной системы, необходимо формировать отчет в формате PDF. Формат PDF является более защищенным, он стандартизирован международной организацией по стандартизации ISO для архивного хранения электронных документов, что является еще одним преимуществом перед другими форматами.

Самым серьезным недостатком системы аттестации сил обеспечения транспортной безопасности от компании «Транссеть» является организация обмена информацией между ЕГИС ОТБ Минтранса России и информационной системой проведения проверок. Во избежание вмешательства в результаты аттестации, протокол, формирующийся после проведения проверок должен в автоматическом режиме передаваться в единую государ-

ственную информационную систему обеспечения транспортной безопасности (ЕГИС ОТБ).

Согласно регламенту информационного взаимодействия подсистемы аттестации сил обеспечения транспортной безопасности, с внешними информационными системами проведения проверок, обмен информацией должен осуществляться посредством обмена файлами установленного формата по протоколу FTP путем передачи данных в формате XML, а также файлов с материалами аудио-видео фиксации, документов и фотографий.

Поскольку при информационном обмене осуществляется передача персональных данных, не предназначенных для открытого использования, необходимо обеспечить защиту передаваемых данных от несанкционированного доступа.

2. Критерии оценки типовых компьютерных систем тестирования

В связи с большим количеством компьютерных систем тестирования, требуется выявить основные критерии сравнения таких систем.

Анализируя системы, можно сделать вывод, что критерии сравнения могут быть разделены на пять групп: критерии, относящиеся к созданию тестовых материалов; критерии, относящиеся к возможностям использования графики, аудио и видео; критерии, относящиеся к обработке результатов тестирования; критерии, относящиеся к административным функциям, а также критерии проведения тестирования.

В компьютерных системах тестирования важную роль играет обеспечение защиты данных о тестовых вопросах и ответах, а также о самих тестируемых. В КСТ компрометация или несанкционированное изменение данных делает бессмысленной ее функционирование. Для обеспечения защиты данных во время тестирования необходимо использовать одностороннее шифрование тестовых заданий, а также ограничить доступ к системе тестирования при помощи ввода логина и пароля. Защита тестовых материалов обеспечивает объективность тестирования, вследствие чего является одним из самых важных факторов.

На основе выделенных критериев проведем анализ компьютерных систем тестирования. Для сравнения были выбраны такие системы как: «xDLS», «SunRav TestOfficePro», «Socrat XXI», «Perception», «Ellekta», «Usatic», «Прометей», «WebQuiz XP», «Aírame», «UniTest». На рисунке 1 представлены результаты сравнения функциональности выбранных систем по выбранным критериям (рис. 1).

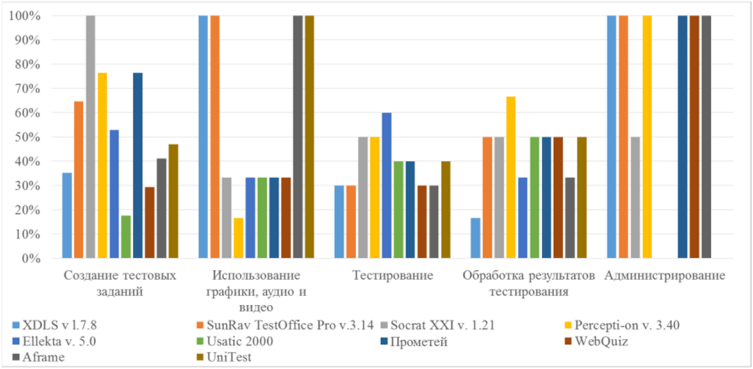


Рисунок 1. Сравнение систем компьютерного тестирования

Литература

1. Приказ Министерства Транспорта России от 21.08.2014 N 231 «Об утверждении требований к знаниям, умениям, навыкам сил обеспечения транспортной безопасности.

2. Студенческая онлайн-библиотека: [Электронный ресурс]. URL:http://studbooks.-net/1452597/menedzhment/attestatsiya_naibolee_rasprostranennaya_forma_otsenki_raboty_personala. (Дата обращения: 26.01.2018)

3. Приказ Минтранса России от 09.09.2014 № 243 от 8 сентября 2014 г. N 243 «Об утверждении типовых дополнительных профессиональных программ в области подготовки сил обеспечения транспортной безопасности».

4. АО «Транссеть»: [Электронный ресурс]. URL: http://transset.ru. (Дата обращения: 26.01.2018).

5. Логинова А. В. Модульная объектно-ориентированная среда обучения (Moodle): эффективная или несовершенная форма организации обучения? // Молодой ученый. 2015. №9. С. 1112-1114. URL https://moluch.ru/archive/89/17853/ (дата обращения: 26.01.2018).

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ ПРИ ОБУЧЕНИИ МАТЕМАТИКЕ

Д. А. Семенова
руководитель – канд. физ.-мат. наук, доцент ***Н. А. Поддубная***
Северо-Кавказский федеральный университет, г. Ставрополь

В данной статье проведен анализ проблем, связанных с внедрением информационных и коммуникационных технологий (ИКТ) в образование, рассмотрены особенности применения средств ИКТ в обучении математике, проанализированы методы и формы обучения с использованием электронных образовательных ресурсов (ЭОР), выявлены принципы совершенствования процесса обучения математике с использованием ЭОР.

Ключевые слова: образование, качество образования, информационные и коммуникационные технологии, электронный образовательный ресурс, средства ИКТ, принципы обучения.

Математика занимает особое место в науке, общественной жизни и культуре, одной из важнейшей составляющей мирового научно-технического прогресса. Обучение математике играет системообразующую роль в образовании, развивая познавательные способности человека, в том числе и к логическому мышлению, влияя на изучение и других дисциплин. На сегодняшний день, качественное математическое образование необходимо для благополучной жизни в современном обществе [5].

Математическое образование должно:

– предоставлять каждому обучающемуся возможность достижения такого уровня математических знаний, который необходим для дальнейшей успешной жизни в обществе;

– обеспечивать каждого обучающегося развивающей интеллектуальной деятельностью на доступном ему уровне, используя при этом всю красоту и увлекательность, присущую математике.

Информационные технологии не только облегчают доступ к информации и открывают различные возможности изменения учебной деятельности, но и позволяют по-новому организовать взаимодействие всех субъектов обучения, построить образовательную систему так, что каждый обучающийся будет инициативным и равноправным участником образовательного процесса.

Особенность предмета «Математика» в том, что для организации учебной деятельности требуется наличие огромного количества наглядного учебного материала по изучаемым темам. Частичным решением проблемы по обеспечению наглядным материалом может быть использование на уроках математики электронных образовательных ресурсов (ЭОР)[3].

ЭОР предназначены для лучшего освоения содержания курса математики, отработки умения понимать и применять на практике математические средства наглядности (графики, схемы, таблицы, диаграммы и др.) для иллюстрации и аргументации, что особо важно для современного образованного человека.

Уже сейчас становится явным тот факт, что одной из главных составляющих профессиональной компетентности учителя является степень его готовности использовать на своих уроках современные информационные и коммуникационные технологии (ИКТ), а также разрабатывать и собственные электронные образовательные ресурсы.

Успех в результате реализуемой образовательной деятельности является существенным способом для мотивации участников образовательного процесса. Использование электронных образовательных ресурсов в обучении математике, таких как электронные приложения к учебникам по математике, интерактивные наглядные пособия, презентации по различным темам, включающие видеофрагменты, примеры решенных задач, схемы, графики, таблицы, ведет к развитию у обучающихся способностей самостоятельно и результативно осваивать новый материал. Это обусловлено

применением различных форм представления информации в ЭОР, что делает учебный материал более интересным и доступным для усвоения обучающимися, и вместе с использованием традиционных форм, методов и средств обучения позволяет существенно повысить качество и эффективность урока [3].

Для закрепления знаний и контроля степени усвоения материала учащимися рационально использовать тренажёры, такие как «Уроки математики 5-6 класс» и «Домашний тренажер по математике». В зависимости от сложности заданий учащийся может сам выбрать систему оценивания. В конце работы компьютер выставляет оценку и показывает результат выполнения заданий в процентном, графическом и оценочном коэффициентах.

На уроках математики, где применяется электронные образовательные ресурсы, в большей степени реализуются принципы наглядности и доступности, обеспечивается получение большего объема информации и заданий за короткий период. Обычная школьная доска не может вместить тот объем информации, который можно показать на экране[4].

Экспериментально можно обосновать преимущества использования электронных образовательных ресурсов на уроках математики. По масштабу педагогические эксперименты бывают глобальные, т.е. охватывающие большое число испытуемых, локальные и микро эксперименты, в которых задействовано минимальное количество участников. В последнее время получает всё большую популярность открытый характер эксперимента.

Школьники, которые вовлечены в опытную проверку гипотетических новаторских разработок, становятся участниками поиска. Их самонаблюдение, мнение, эмоциональные состояния дают ценные материалы о качестве и результативности экспериментально испытываемых разработок.

При проведении эксперимента обычно выделяю две группы испытуемых. Первая получает статус экспериментальной группы, а вторая — контрольной. В экспериментальной группе реализуется инновационное решение. В контрольной – те же проблемы воспитания реализуются с использованием традиционных форм обучения. Благодаря этому появляется возможность сравнить два результата, доказывающих или опровергающих верность выдвинутой гипотезы о преимуществах использования средств информационных и коммуникационных технологий на уроках математики. Сравнивается традиционное усвоение определенного раздела математики при последовательном изучении программных тем и с применением электронных образовательных ресурсов [1].

Анализ результатов тестовых проверочных работ констатирующего и контрольного этапа эксперимента для двух групп может быть представлен с использованием критерия Вилкоксона-Манна-Уитни (рис. 1).

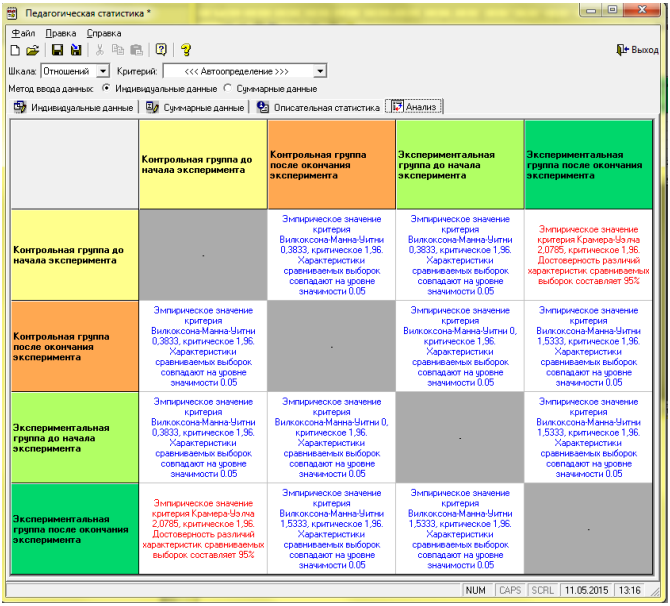


Рисунок 1. Анализ данных экспериментальной и контрольной групп до и после эксперимента по критерию Вилкоксона–Манна–Уитни

Анализ результатов проведенного исследования позволяет выявить явные превосходства инновационных методик обучения математике с использованием ЭОР перед традиционными. Очевидно, что ожидать повышения эффективности и качества образования можно только лишь при условии, что разработанные образовательные продукты будут обладать инновационными качествами. Они отличаются в основном базой представления текста и иллюстраций – материал представляется на экране компьютера, а не на бумаге. Так же ЭОР имеют существенные отличия в навигации по тексту. В ЭОР можно указать неизвестный термин и немедленно получить его определение в дополнительном окне, или быстро сменить содержимое экрана при указании ключевого слова или словосочетания и т.д. [3].

Использование электронных образовательных ресурсов позволит заменить различные традиционные средства обучения. Во многих случаях эта замена эффективна, поскольку позволяет поддерживать у учащихся интерес к изучаемому предмету, позволяет создавать информационную обстановку, которая побуждает интерес и любознательность ребенка. В школе компьютер дает возможность учителю сочетать различные средства, способствующие более углубленному и осознанному усвоению изучаемого материала, позволяет организовать процесс обучения по индивидуальным программам, экономит время урока [2].

Использование электронных образовательных ресурсов при обучении математике расширяет рамки образовательного процесса, повышает его практическую направленность. Достигаются необходимые предметные, метапредметные, а также личностные результаты обучения, повышается мотивация и познавательная активность учащихся, создаются условия, способствующие их успешной самореализации в будущем.

Литература

1. Захарова И. Г. Информационные технологии в образовании: Учебное пособие для студентов высших педагогических учебных заведений. 2003. 15 с.
2. Климанова Л. Ф. Универсальные учебные действия обучающихся: примеры формирования // Управление начальной школой. 2010. № 10. С. 20-25.
3. Кузнецова М. В. Использование ЭОР в процессе обучения в основной школе // Академия АйТи. 2011. С. 3-4.
4. Осипова Н. В. Показатели сформированности универсальных учебных действий обучающихся / Н. В. Осипова, И. А. Головинская, С. В. Брюханова // Формирование УУД средствами ИКТ. 2010. № 10. С. 8-12.
5. Ячменникова Т. С. Деятельностный подход в формировании универсальных учебных действий на уроках математики. Как формировать на уроке универсально-учебные действия, предусмотренные ФГОС нового поколения? // Муниципальное образование: эксперимент и инновации. 2011. № 1. С. 25-31.

ЭСТЕТИЧЕСКОЕ ВОСПИТАНИЕ ШКОЛЬНИКОВ ПРИ ИЗУЧЕНИИ ИНФОРМАТИКИ

М. Р. Сулейманова
руководитель – старший преподаватель ***З. М. Муцурова***
ФГБОУ ВО Чеченский государственный педагогический университет, г. Грозный

В данной статье рассмотрена основная проблема нынешнего общества – эстетическое воспитание школьников. Основная цель современного образования – это воспитание рационально мыслящей, и духовно развитой личности. Важной задачей считается совершенствование художественного образования и эстетического воспитания учащихся. Задачи эстетического воспитания – приобретение теоретических знаний и формирование практических умений.

Ключевые слова: эстетическое воспитание, информатика, современное образование, формирование.

Одной из ключевых проблем нынешнего общества является эстетическое воспитание. В современном обществе наблюдается избыток информации о современном и древнем искусстве, но, чаще всего, различий между ними мы не замечаем. Единственный аспект, согласно которому в настоящее время обуславливается важность произведений искусства, считается его рейтинг и популярность в Интернете. В нынешнем обществе такое понятие

как эстетика утратило своё значение, по этой причине подросткам сложно оценить эстетическую красоту художественного произведения или произведения искусства. Однако, ни в коем случае не стоит утверждать, что всё общество утратило способность наслаждаться прекрасным.

Основная цель современного образования – это воспитание рационально мыслящей, и духовно развитой личности. В данном процессе эстетическому воспитанию отводится не последняя роль. Важной задачей считается совершенствование художественного образования и эстетического воспитания учащихся. Важно совершенствовать чувство прекрасного, формировать эстетические вкусы, умение понимать и ценить произведения искусства и архитектуры. Для этого необходимо использовать все возможности, которые нам предоставляются, ведь в наше время обществу доступна любая информация, мы должны уметь в полной мере использовать возможности каждого учебного предмета. Не малую роль в этом играют учебные предметы, такие как литература, изобразительное искусство, мировая художественная культура, музыка, и пр. Безусловно, значимую роль в эстетическом воспитании нужно уделить учебному предмету такому как информатика, так как данная отрасль науки в современном обществе просто необходима, и она заполонила весь мир.

Понятие информационная культура включает в себя не только умение правильно использовать различного рода информацию, но также и умение красиво ее оформлять. На уроках Информатики имеется возможность эстетически правильно реализовать оформление дизайна программы, ее интерфейса, красиво и грамотно изложить решение в процессе ее реализации.

Примером эстетического воспитания школьников, может служить учебник «Занимательная информатика» Златопольского Д.М. В этой работе особое внимание уделяется созданию различных игр в Microsoft Excel, изучению истории появления термина информатика. Или же учебник Босовой Людмилы Леонидовны, автор уже с 5-го класса предлагает к изучению различные компоненты Microsoft Office и всячески пытается заинтересовать учеников. Школьники должны выполнить работы в ходе реализации которых они научатся правильно, но в то же время интересно, красочно с использованием анимации оформлять презентации, и создавать слайд – шоу.

Эстетическое воспитание, если оно правильно и обширно реализуется, оказывает эффективное влияние на нравственное формирование учащихся, и на эстетику их поведения. Каждый человек должен осознавать прекрасное. Какой бы деятельностью не занимались учащиеся, будь то математика, литература информатика, необходимо стремиться придавать ей яркие формы, красочное исполнение, элементы эстетики.

Трудности, всплывающие на пути эстетического воспитания целесообразно рассматривать и обсуждать на самых высоких уровнях, искать их всевозможное решение, отвечать на всплывающие в процессе обучения вопросы непосредственно с помощью компьютера. На первый взгляд со-

здается впечатление, что компьютер и эстетическое воспитание мало совместимы и в педагогической литературе встречаются весьма редко, однако российские и иностранные ученные всё чаще совершают успешные попытки интеграции и возведение в целостное единство, таких понятий как искусство, воспитание, компьютер.

Таким образом, мы приходим к выводу, что эстетическое воспитание ученика может благополучно осуществляться на уроках информатики, с помощью компьютера. Создание определенного дизайна прививает чувство стиля и эстетической красоты, а также напоминает ученикам о культуре как современного, так и древнего мира. Люди часто приходят к предположениям, что современные технологии всячески мешают развитию и познанию ребенком эстетических ценностей, эти предположения ошибочны, так как благодаря современным технологиям ребенок может получить наглядную информацию, услышать и прочувствовать ее, и благодаря всему этому эстетика сама зарождается в нем.

Литература

1. Комарова Т. С. Школа эстетического воспитания. М.: Мозаика-синтез, 2009. 352 с.

СРАВНЕНИЕ СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ SQLITE, MYSQL И POSTGRESQL

М. А. Тупикина
руководитель – старший преподаватель ***А. В. Шипулин***
Северо-Кавказский федеральный университет, г. Ставрополь

Актуальность обусловлена востребованностью систем управления базами данных (СУБД) в разработки приложений для предприятия. Рассмотрены три широко используемые системы. Цель – сравнить и выявить наиболее подходящую СУБД для разработки приложения узкой направленности с использованием небольшого количества функций. Сравнение проводилось на основе данных, известных об этих системах. В результате выявлен лидер, после рассмотрения разных аспектов программ.

Ключевые слова: система управления базами данных (СУБД), SQLite, MySQL, PostgreSQL, база данных, разработка проектов, разработка, структурирование, функциональность.

SQLite – это система управления базой данных, которая отлично подходит для работы с приложениями и имеет большой спектр инструментов, в отличие от сетевых СУБД, ещё работа происходит непосредственно с файлами, вместо портов и сокетов (сетевые СУБД). Благодаря технологиям используемых библиотек SQLite считается очень быстрой и сравнительно мощной.

У SQLite есть несколько преимуществ, например, файловая структура, так как база состоит из одного файла, проблем с перемещением на разные устройства не возникает. Также, она удобна в тестировании и при разработке.

Одним из недостатков является отсутствие системы пользователей. Этот минус не слишком критичен, так как по большей части эта СУБД применяется в небольших приложениях. Если рассматривать этап проектирования, то данная база будет уступать другим в возможности увеличить производительность [1].

Использование SQLite возможно во встроенных приложениях, когда масштабируемость не стоит на первом месте. Если вам понадобится создать простое приложение, но с использованием достаточного количества функций, то данная СУБД подходит для этого идеально, так как оно многофункционально и проста в использовании.

Использование SQLite нецелесообразно для создания многопользовательских приложений и логичней будет использовать полноценную СУБД, например, MySQL. Также не стоит использовать данную СУБД, когда предстоит запись большого объема данных. В SQLite разрешено добавление только по одной записи, что достаточно снижает производительность [2].

MySQL, на данный момент, одна из самых распространённых СУБД. Также, благодаря её востребованности, имеется большое количество плагинов и расширений, которые помогают в работе с системой. Есть достаточно большой перечень инструментов, с учетом того, что в этой СУБД представлен функционал SQL не полностью.

Преимуществами MySQL является простота в работе, возможность установки дополнительных приложений, которые обеспечивают лёгкую работу с БД. Достаточно богатая функциональность, безопасность, масштабируемость и скорость в разы облегчают работу, особенно если используются большие объемы данных. [3]

Из недостатков можно отметить медленную разработку, иногда у пользователей появляются жалобы на процессы разработки, но, несмотря на это, на базе MySQL созданы достаточно успешные СУБД такие, как MariaDB. Также могут возникнуть проблемы с надежностью или известные ограничения по функционалу, которые могут понадобиться для требовательных приложений.

MySQL находит себе применения в случаях, когда функционала SQLite может быть уже недостаточно, например, используются для разработки веб сайтов и веб приложений.

MySQL не стоит использовать, если вы планируете перейти на СУБД с полной поддержкой SQL, так как рассматриваемая СУБД не полностью соответствует стандартам SQL. Также могут быть проблемы с параллельными операциями чтения-записи и поддержанием полнотекстового поиска.

Рассмотрим последнюю из данных систем. PostgreSQL самая профессиональная из представленных в статье систем управления базами данных. Помимо максимального соответствия стандартам SQL, в PostgreSQL происходит своевременное обновление ANSI/ISO SQL стандартов, также имеется поддержка объектно-ориентированного или реляционного подхода к базам данных [1]. Postgre весьма производителен, в нем реализовано управление многовариантного параллелизма (MVCC), также упрощено использование постоянно повторяемых операций с помощью хранимых процедур. Хоть PostgreSQL не на столько популярен, как MySQL, существует достаточно большой перечень приложений, которые могут в разы облегчить с ним работу.

Одним из важнейших достоинств является бесплатное ПО, которое соответствует стандарту SQL, ещё имеется большое сообщество поддержки, в котором можно найти ответы интересующие вопросы [1]. Также PostgreSQL имеет большое количество дополнений и расширений, что увеличивает и без того не скудный функционал.

Одним из недостатков является замедление сервера при простых операциях чтения. Используется PostgreSQL, когда требуется целостность и надежность данных, процедуры пользователей, или, если вы планируете переходить на платную СУБД. Также она позволяет создавать более структурированные данных, не жертвуя какими-либо аспектами.

Не стоит использовать PostgreSQL, если для вас самое важное это быстрое чтение или если вам нужна простая настройка, так как на настройку данной СУБД может уйти слишком много времени [3]. Также нецелесообразно использовать Postgre, если вы собираетесь создавать базу, которую с легкостью могли бы сделать на MySQL.

Проанализировав плюсы и минусы дынных программ, сравнив их применение, можно сказать, что каждая из них будет хороша в использовании в разных случаях. Для работы над небольшими приложениями будет удобно использовать SQLite. Для разработки более крупных проектов, лучше использовать MySQL, так как она достаточна обширна по функциональной составляющей, и быстра в работе, по сравнению с PostgreSQL. PostgreSQL, в свою очередь, хоть непопулярна, но прекрасно подходит для составления больших и сложных баз данных, но при этом стоит учитывать, что она весьма медленно работает.

Литература

1. Статья «SQLite vs MySQL vs PostgreSQL: сравнение систем управления базами данных» [Электронный ресурс]. Режим доступа: http://devacademy.ru/posts/sqlite-vs-mysql-vs-postgresql/ (дата обращения 23.04.2018).

2. Статья «Сравнение SQL баз данных» [Электронный ресурс]. Режим доступа: http://usanov.net/1970-sravnenie-sql-baz-dannyx (дата обращения 23.04.2018).

3. Форум «SQL.ru» [Электронный ресурс]. Режим доступа: http://www.sql.ru/forum/-1075807/access-ili-sqlite-2-3-komputera (дата обращения 23.04.2018).

ХАРАКТЕРИСТИКА СОВРЕМЕННЫХ СПОСОБОВ И ПРИЕМОВ ОРГАНИЗАЦИИ ВАРИАТИВНОГО ОБУЧЕНИЯ ИНФОРМАТИКЕ И ИКТ

А. С. Швецова
руководитель – канд. пед. наук, доцент ***О. П. Панкратова***
Северо-Кавказский федеральный университет, г. Ставрополь

В период перехода к информационному обществу важным достижением любого человека является его умение оперативно и качественно работать с информацией, его способность к всесторонней социализации и анализу информации, и результатов ее обработки,а также к принятию обоснованных и своевременных решений на основе имеющейся информации. Этому надо планомерно и непрерывно учить, начиная с первых шагов в школе. А для этого должны быть сформированы требования к структуре знаний по всем дисциплинам информационно-компьютерного направления на всех уровнях обучения, выстроена логическая и непрерывная последовательность изучаемых дисциплин, а в них разделов и тем. Кроме того, необходимо создать соответствующие условия для вариативного обучения во всех образовательных учреждениях любого уровня и, в первую очередь, в школе.

Ключевые слова: вариативное обучение, информатика и ИКТ, школа, профильное обучение.

Важнейшая черта современного обучения - его направленность на то, чтобы готовить учащихся не только приспосабливаться, но и активно осваивать ситуации социальных перемен. В этой связи предпринята попытка в поиске условий, направленных на реализацию вариативного образования школьников в соответствии с их наклонностями и психолого-физиологическими возможностями.

Информатика, в настоящее время, – одна из фундаментальных областей научного знания. Она способствует формированию современного научного мировоззрения, развитию интеллектуальных способностей и познавательных интересов школьников; освоение базирующихся на этой науке информационных технологий необходимо школьникам, как в самом образовательном процессе, так и в их повседневной и будущей жизни. Поэтому вариативная часть учебного плана в школе обеспечивает реализацию федерального компонента образовательного стандарта, а также школьного и регионального компонентов образования.

Предмет «Информатика и информационно-коммуникационные технологии (ИКТ)» является элементом системы школьных учебных дисциплин, поэтомусодержание и структура определяются общими принципами построения и функционирования этой системы.

Базисный учебный план для среднего (полного) общего образования (2004 год) предлагает несколько вариантов возможных профилей.

- федеральный компонент;
- инвариантная часть;

– вариативная часть;
– региональный (национально-региональный);
– компонент;
– компонент образовательного учреждения.

В состав инвариантного ядра входятти традиционные темы компьютерной области,содержание которых не зависит от конкретной модели компьютера или конкретного вида программного продукта. К этим темам относятся: техническая часть компьютера, информационно-коммуникационные технологии,классификация программного обеспечения, основы алгоритмизации и программирования, основы кодирования и др.

Вариативная составляющая содержания школьного курса информатики определяется современным уровнем развития компьютерной технологии, обеспеченной соответствующими программными продуктами. Конкретная программная среда рассматривается с позиций приобретения учащимися технологических навыков работы с программным инструментарием и использования его как при моделировании, так и при создании информационных объектов. Изучению различных программных сред должно быть уделено достаточно много внимания,но это не должно быть основным направлением и целью обучения. Недопустимо в школьном курсе информатики изучать только технологию работы в различных программных средах. Следует познакомить учащихся с широким спектром разноплановых задач, где эффективно может применяться компьютерная технология.

Кроме того, учитывая требования Государственного стандарта по информатике и ИКТ, в состав вариативной составляющей вводится раздел, посвященный изучению основ технологии программирования. Следует заметить, что данный раздел призван обеспечить только ориентировочную деятельность учащегося. Ни в коей мере нельзя требовать от школьника, у которого маршрут освоения данного учебного предмета определяется базовым уровнем, тех знаний и умений, которые проверяются в ЕГЭ.

Системно-информационная концепция отражает точку зрения на информатику и ИКТ, как на учебный предмет с двух позиций. С одной стороны, содержание учебного материала должно способствовать развитию интеллектуальных и творческих способностей ребенка, умению анализировать сущность объектов, явлений и процессов, проводить их целенаправленное исследование и делать на этой основе выводы. С другой стороны, оно призвано обеспечить школьника необходимыми знаниями и умениями использования современного компьютерного инструментария, что и составляет суть вариативной составляющей.

С внедрением данной программы появляется возможность на уроках информатики и ИКТ закреплять и углублять знания, полученные по другим предметам. На реально может быть реализован принцип межпредметных связей. Это достигается в процессе решения многочисленных задач из разных предметных областей, используя для этого два методических подхода.

Первый подход состоит в том, что освоение любой программной среды осуществляется в процессе реализации (решения) конкретной задачи. Целью является получение результата, а для этого учащемуся предлагается необходимый компьютерный инструментарий и тщательно разработанная методика его освоения. Второй подход определяется тем, что после освоения технологии работы в офисных программных средах большое внимание уделяется исследованию. С этой целью учащиеся занимаются компьютерным моделированием объектов, процессов, явлений из любых предметных областей в ранее освоенной программной среде.

Вариативное обучение предоставляет много новых возможностей в развитии новых методик обучения. Их многообразие позволяет реально на практике обеспечивать индивидуальные потребности учащихся, профильные интересы детей, то есть повсеместно в массовой школе реализовать педагогику развития ребенка. Традиционные методики обогатились новыми мощными визуально-наглядными средствами обучения, позволяющими оснастить новыми информационными массивами поисковую и исследовательскую работу учащихся, включая сбор, анализ и обработку отобранной или самостоятельно подготовленной детьми информации.

Литература

1. Гин А. А. Приемы педагогической техники: свобода выбора. Открытость. Деятельность. Обратная связь. Идеальность. Пособие для учителя. 3-е изд. М.: Вита-Пресс, 2013.

2. Макарова Н. В., Степанов А. Г. Информатика в системе непрерывного образования. Международный банковский институт. Санкт-Петербург, 2015.

3. Сборник нормативных документов. Информатика и ИКТ / сост. Э. Д. Днепров, А. Г.Аркадьев. 3-е изд., стетеотип. М.: Дрофа, 2016.

4. Стратегия модернизации содержания общего образования: Материалы для разработки документов по обновлению общего образования. М.: 2012.

Научное издание

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Сборник материалов VIII Всероссийской
научно-технической конференции
(г. Ставрополь, 22-23 мая 2018 года)

Часть 2

Издается в авторской редакции

Печатается с электронного макета, предоставленного заказчиком

Подписано в печать 31.05.2018
Формат 60x84 1/8 Усл. печ. л. 20,41 Уч.-изд. л. 19,84
Бумага офсетная Заказ Тираж 300 экз.

Отпечатано в Издательско-полиграфическом комплексе
ФГАОУ ВО «Северо-Кавказский федеральный университет»
355029, г. Ставрополь, пр-т Кулакова, 2