Федеральное государственное автономное образовательное учреждение высшего образования
«Северо-Кавказский федеральный университет»
Институт информационных технологий и телекоммуникаций

Организация и технология защиты информации

Кафедра

ПРОГРАММА ИТОГОВОГО ГОСУДАРСТВЕННОГО ЭКЗАМЕНА ПО НАПРАВЛЕНИЮ 10.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки	10.03.01 Информационная безопасность
Профиль подготовки	Организация и технология защиты информации

г. Ставрополь, 2017

СОДЕРЖАНИЕ

ПРОГРАММА ИТОГОВОГО ГОСУДАРСТВЕННОГО ЭКЗАМЕНА ПО НАПРАВЛЕНИЮ 10.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1. Цели и задачи государственного экзамена

Заключительный этап теоретического обучения бакалавра в высшем учебном заведении состоит в подготовке и сдаче государственного экзамена. Государственный экзамен по направлению 10.03.01 «Информационная безопасность» преследует цель провести оценку степени профессиональной подготовки выпускника по использованию теоретических знаний, практических навыков и умений для решения профессиональных задач в области информационной безопасности на уровне, требуемом ФГОС ВО по направлению 10.03.01 «Информационная безопасность» с учетом специфики учебного процесса и региональных особенностей вуза.

Государственный экзамен по направлению 10.03.01 «Информационная безопасность» проводится в форме итогового междисциплинарного экзамена.

Основными задачами государственного экзамена являются:

– определение соответствия подготовки студента выпускного курса СКФУ требованиям ФГОС ВО по направлению 10.03.01 «Информационная безопасность» и уровня его подготовки;

– принятие решения о присвоении квалификации (степени) по результатам государственной итоговой аттестации и выдаче выпускнику Университета соответствующего диплома государственного образца о высшем профессиональном образовании;

– разработка рекомендаций, направленных на совершенствование качества подготовки специалистов, на основании результатов работы государственной аттестационной комиссии.

2. Перечень компетенций, которыми должен овладеть обучающийся в результате освоения образовательной программы и продемонстрировать на государственном экзамене

Выпускник бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность» должен обладать следующими компетенциями:

- общекультурными (ОК):

1) способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

2) способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

3) способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

4) способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

5) способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

6) способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

7) способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

8) способностью к самоорганизации и самообразованию (ОК-8);

9) способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9);

- общепрофессиональными (ОПК):

1) способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);

2) способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);

3) способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3);

4) способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);

5) способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);

6) способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);

7) способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);

- профессиональными (ПК):

эксплуатационная деятельность:

1) способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

2) способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

3) способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

4) способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

5) способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

6) способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

проектно-технологическая деятельность:

7) способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

8) способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

экспериментально-исследовательская деятельность:

9) способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

10) способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

11) способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);

12) способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

организационно-управленческая деятельность:

13) способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

14) способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

15) способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15);

- профессионально-специальными компетенциями (ПСК):

1) способностью проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики (ПСК-2.1);

2) способностью разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение (ПСК-2.2);

Выпускник бакалавриата по направлению подготовки «Информационная безопасность» должен

знать:

– основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире;

– основные разделы и направления философии, методы и приемы философского анализа проблем;

– лексический минимум в объеме 4 000 учебных лексических единиц общего и терминологического характера (для иностранного языка);

– основные экономические категории и закономерности, методы анализа экономических явлений и процессов, специфические черты функционирования хозяйственной системы на (микро- и макро-)уровнях, основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений;

– основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации;

– основные понятия и методы в области управленческой деятельности;

– основные понятия и методы математического анализа;

– основные понятия и методы аналитической геометрии;

– основные понятия и методы линейной алгебры и теории алгебраических систем;

– основные понятия и методы теории функций комплексного переменного;

– основные понятия и методы теории вероятностей и математической статистики;

– основные понятия и методы математической логики и теории алгоритмов, теории информации кодирования;

– математические методы обработки экспериментальных данных;

– основные понятия, законы и модели механики;

– основные понятия, законы и модели электричества и магнетизма;

– основные понятия, законы и модели теории колебаний и волн оптики, квантовой физики, физики твердого тела, статистической физики и термодинамики;

– особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности;

– основные понятия информатики;

– место и роль информационной безопасности в системе национальной безопасности Российской Федерации;

– методы программирования и методы разработки эффективных алгоритмов решения прикладных задач;

– современные средства разработки и анализа программного обеспечения на языках высокого уровня;

– аппаратные средства вычислительной техники;

– операционные системы персональных ЭВМ;

– основы администрирования вычислительных сетей;

– системы управления базами данных;

– принципы построения информационных систем;

– структуру систем документационного обеспечения;

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

– правовые нормы и стандарты по лицензированию в области

– обеспечения защиты государственной тайны и сертификации средств защиты информации;

– принципы и методы организационной защиты информации;

– технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

– принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;

– принципы организации информационных систем в соответствии с требованиями по защите информации;

– эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы;

– сигналы электросвязи, принципы построения систем и средств связи;

– методы анализа электрических цепей;

– принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них;

– основы схемотехники;

– опасные и вредные факторы системы "человек - среда обитания", методы анализа антропогенных опасностей, научные и организационные основы защиты окружающей среды и ликвидации последствий, аварий, катастроф, стихийных бедствий;

уметь:

– использовать в практической деятельности правовые знания; анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав;

– анализировать мировоззренческие, социально и личностно значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию; планировать и осуществлять свою деятельность с учетом результатов этого анализа;

– оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения;

– использовать математические методы и модели для решения прикладных задач;

– применять основные законы физики при решении прикладных задач;

– использовать программные и аппаратные средства персонального компьютера;

– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;

– составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;

– формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;

– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;

– анализировать и оценивать угрозы информационной безопасности объекта;

– применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

– пользоваться нормативными документами по защите информации;

– применять на практике методы анализа электрических цепей;

– анализировать и оценивать степень риска проявления факторов опасности системы "человек - среда обитания", осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности.

владеть:

– иностранным языком в объеме, необходимом для возможности получения информации по профессиональной тематике, и навыками устной речи;

– навыками письменного аргументированного изложения собственной точки зрения;

– навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений;

– навыками критического восприятия информации;

– навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;

– навыками обоснования, выбора, реализации и контроля результатов управленческого решения.

– методами количественного анализа процессов обработки, поиска и передачи информации;

– навыками проведения физического эксперимента и обработки его результатов;

– навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).

– методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;

– навыками выявления и уничтожения компьютерных вирусов;

– навыками работы с нормативными правовыми актами;

– методами и средствами выявления угроз безопасности автоматизированным системам;

– навыками организации и обеспечения режима секретности;

– методами технической защиты информации;

– методами формирования требований по защите информации;

– методами расчета и инструментального контроля показателей технической защиты информации;

– навыками чтения электронных схем;

– методами анализа и формализации информационных процессов объекта и связей между ними;

– методами организации и управления деятельностью

– служб защиты информации на предприятии;

– методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;

– профессиональной терминологией;

– навыками безопасного использования технических средств в профессиональной деятельности.

Коллектив кафедры организации и технологии защиты информации ставит перед собой задачу подготовить выпускников к принятию квалифицированных самостоятельных решений в различных аспектах проектирования, эксплуатации и модернизации систем защиты информации на объектах информатизации.

3. Структура государственного экзамена

Государственный экзамен включает вопросы, тесты (задачи) по следующим дисциплинам учебного плана подготовки бакалавров направления 10.03.01 «Информационная безопасность»:

1. Теоретические основы защиты информации.
2. Физические основы защиты информации.
3. Криптографические методы защиты информации
4. Организационно-правовое обеспечение информационной безопасности.
5. Техническая защита информации.

Экзамен предполагает:

1. Ответ экзаменуемого по теоретическим вопросам.
2. Практическое выполнение задания.

Структура экзаменационного билета состоит из 3 пунктов, соответствующих 3 различным дисциплинам. Каждый билет содержит 2 теоретических вопроса (базовой уровень) и практический вопрос (повышенный уровень).

4. Содержание государственного экзамена

Программа государственного экзамена по направлению 10.03.01 «Информационная безопасность» включает основополагающие темы следующих учебных дисциплин:

4.1 Теоретические основы защиты информации

Основные положения теории защиты информации. Угрозы безопасности информации. Основные свойства информации. Политика безопасности. Модели безопасности. Дискреционный контроль. Модель распространения прав доступа Take-Grant. Модели мандатного контроля и управления доступом. Модели контроля целостности. Ролевые модели доступа. Идентификация и аутентификация. Аудит информационной безопасности. Уязвимости. Атаки и вторжения.

4.2 Физические основы защиты информации

Технические каналы утечки информации. Основные направления инженерно-технической защиты информации. Теоретические основы акустики. Восприятие по амплитуде Акустика в помещениях. Электромагнитные волны. Антенны. Технические каналы утечки информации. Методы и средства защиты информации от утечки по техническим каналам. Защита информации в проводных телефонных системах. Возможности и способы несанкционированного подключения к телефонным линиям. Возможности обнаружения подключений средств снятия информации. Каналы утечки информации, образованные электромагнитным излучением.

4.3 Криптографические методы защиты информации

Общие сведения о криптографических методах защиты информации. Классификация шифров. Подходы к моделированию криптосистем. Криптографическая стойкость шифров. Принципы построения и

функционирования блочных шифров. Симметричные криптоалгоритмы. Принципы построения и функционирования поточных шифров. Принципы построения криптоалгоритмов с открытым ключом. Современные криптоалгоритмы с открытым ключом. Имитостойкость и помехоустойчивость шифров. Универсальные методы криптоанализа. Криптоанализ симметричных алгоритмов. Криптоанализ асимметричных алгоритмов. Криптографические хэш-функции. Электронная цифровая подпись. Управление криптографическими ключами. Реализации криптографических алгоритмов: программная, аппаратная, программно-аппаратная. Композиция криптографических методов в систему защиты информации. Криптографические стандарты. Криптографические протоколы.

4.4 Организационно-правовое обеспечение информационной безопасности

Информация как объект правового регулирования. Законодательство РФ в области информационной безопасности. Правовой режим защиты коммерческой тайны. Правовой режим защиты конфиденциальной информации. Лицензирование и сертификация в области обеспечения защиты государственной тайны. Защита интеллектуальной собственности. Компьютерные правонарушения. Правовое регулирование оперативно-розыскных мероприятий в оперативно-розыскной и частной детективной и охранной деятельности. Международное законодательство в области защиты информации. Принципы, силы, средства и условия организационной защиты информации. Организационные источники и каналы утечки информации. Организационные основы защиты информации на предприятии. Порядок засекречивания и рассекречивания сведений, документов и продукции. Организация допуска и доступа к государственной тайне. Допуск и доступ к конфиденциальной информации и документам. Направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации. Организация охраны предприятий. Организация внутриобъектового и пропускного режимов на предприятии. Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. Порядок доступа к конфиденциальной информации командированных лиц. Защита информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу. Защита информации при публикаторской и рекламной деятельности. Организация допуска предприятий к проведению работ со сведениями, составляющими государственную тайну. Организация служебного расследования по фактам разглашения конфиденциальной информации или утраты носителей информации. Организация аналитической работы по предупреждению утечки конфиденциальной информации. Планирование процессов организационной защиты информации. Организация контроля состояния защиты конфиденциальной информации на предприятии. Государственные, национальные и отраслевые стандарты по информационной безопасности. Международные стандарты информационной безопасности.

4.5 Техническая защита информации

Теоретические основы технической защиты информации. Место технической защиты информации в государственной системе защиты информации в РФ. Термины, определения и основы методологии в области технической защиты информации. Характеристика информации и информационных процессов как предмета технической защиты. Характеристика угроз безопасности информации в автоматизированных информационных системах. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Характеристика технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок. Специально создаваемые радиоэлектронные технические каналы утечки информации. Технические каналы утечки акустической (речевой) информации. Прямые акустические каналы утечки речевой информации. Составные акустические каналы утечки речевой информации. Способы и средства перехвата информации, передаваемой по каналам связи. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Методы, способы и средства защиты информации от утечки за счет ПЭМИН. Локализация побочных электромагнитных излучений и развязывание информационных сигналов. Энергетическое скрытие побочных электромагнитных излучений и наводок от средств вычислительной техники. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. Методы, способы и средства защиты речевой информации от утечки по техническим каналам. Звукоизоляция выделенных помещений. Системы и средства акустической и виброакустической маскировки. Способы и средства защиты телефонных каналов связи. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Оценка защищенности средств вычислительной техники от утечки за счет ПЭМИН. Средства измерения побочных электромагнитных излучений и наводок СВТ. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам. Оценка защищенности выделенных помещений от утечки речевой информации. Средства измерения акустических и вибрационных сигналов и шумов. Методы и средства выявления электронных устройств негласного получения информации. Методы и средства выявления электронных устройств негласного получения информации. Порядок проведения специальный обследований и исследований. Организация технической защиты информации. Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации. Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации.

В соответствии с данными дидактическими единицами и программами ФГОС ВО выбран перечень вопросов, представленных в разделе 4.

5. Перечень примерных вопросов для подготовки к государственному экзамену

– **теоретические вопросы к государственному экзамену (базовый уровень).**

Студенты, прошедшие курс обучения по направлению «Информационная безопасность», профилю «Организация и технология защиты информации» в результате обучения должны знать:

I. Теоретические основы защиты информации:

1. Основные положения теории защиты информации
2. Угрозы безопасности информации
3. Основные свойства информации
4. Политика безопасности
5. Модели безопасности
6. Дискреционный контроль
7. Модель распространения прав доступа Take-Grant
8. Модели мандатного контроля и управления доступом
9. Модели контроля целостности
10. Ролевые модели доступа
11. Идентификация и аутентификация
12. Аудит информационной безопасности
13. Уязвимости
14. Атаки и вторжения

II. Физические основы защиты информации:

1. Технические каналы утечки информации
2. Основные направления инженерно-технической защиты информации
3. Теоретические основы акустики
4. Электромагнитные волны. Антенны
5. Технические каналы утечки информации
6. Методы и средства защиты информации от утечки по техническим каналам
7. Защита информации в проводных телефонных системах
8. Возможности и способы несанкционированного подключения к телефонным линиям
9. Возможности обнаружения подключений средств снятия информации
10. Каналы утечки информации, образованные электромагнитным излучением.

III. Криптографические методы защиты информации:

1. Общие сведения о криптографических методах защиты информации
2. Классификация шифров
3. Подходы к моделированию криптосистем
4. Криптографическая стойкость шифров
5. Принципы построения и функционирования блочных шифров
6. Симметричные криптоалгоритмы
7. Принципы построения и функционирования поточных шифров
8. Принципы построения криптоалгоритмов с открытым ключом

9. Современные криптоалгоритмы с открытым ключом
10. Имитостойкость и помехоустойчивость шифров
11. Универсальные методы криптоанализа
12. Криптоанализ симметричных алгоритмов
13. Криптоанализ асимметричных алгоритмов
14. Криптографические хэш-функции
15. Электронная цифровая подпись
16. Управление криптографическими ключами
17. Реализации криптографических алгоритмов: программная, аппаратная, программно-аппаратная
18. Композиция криптографических методов в систему защиты информации
19. Криптографические стандарты
20. Криптографические протоколы

IV. Организационно-правовое обеспечение информационной безопасности:

1. Информация как объект правового регулирования
2. Законодательство РФ в области информационной безопасности
3. Правовой режим защиты коммерческой тайны
4. Правовой режим защиты конфиденциальной информации
5. Лицензирование и сертификация в области обеспечения защиты государственной тайны
6. Защита интеллектуальной собственности
7. Компьютерные правонарушения
8. Правовое регулирование оперативно-розыскных мероприятий в оперативно-розыскной и частной детективной и охранной деятельности
9. Международное законодательство в области защиты информации
10. Принципы, силы, средства и условия организационной защиты информации
11. Организационные источники и каналы утечки информации
12. Организационные основы защиты информации на предприятии
13. Порядок засекречивания и рассекречивания сведений, документов и продукции
14. Организация допуска и доступа к государственной тайне
15. Допуск и доступ к конфиденциальной информации и документам
16. Направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации
17. Организация охраны предприятий
18. Организация внутриобъектового и пропускного режимов на предприятии
19. Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации
20. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам

21. Порядок доступа к конфиденциальной информации командированных лиц

22. Защита информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу

23. Защита информации при публикаторской и рекламной деятельности

24. Организация допуска предприятий к проведению работ со сведениями, составляющими государственную тайну

25. Организация служебного расследования по фактам разглашения конфиденциальной информации или утраты носителей информации

26. Организация аналитической работы по предупреждению утечки конфиденциальной информации

27. Планирование процессов организационной защиты информации

28. Организация контроля состояния защиты конфиденциальной информации на предприятии

29. Государственные, национальные и отраслевые стандарты по информационной безопасности

30. Международные стандарты информационной безопасности

V. Техническая защита информации:

1. Термины, определения и основы методологии в области технической защиты информации

2. Характеристика информации и информационных процессов как предмета технической защиты

3. Характеристика угроз безопасности информации в автоматизированных информационных системах

4. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

5. Характеристика технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок

6. Специально создаваемые радиоэлектронные технические каналы утечки информации

7. Технические каналы утечки акустической (речевой) информации

8. Прямые акустические каналы утечки речевой информации

9. Составные акустические каналы утечки речевой информации

10. Способы и средства перехвата информации, передаваемой по каналам связи

11. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

12. Методы, способы и средства защиты информации от утечки за счет ПЭМИН

13. Локализация побочных электромагнитных излучений и развязывание информационных сигналов

14. Энергетическое скрытие побочных электромагнитных излучений и наводок от средств вычислительной техники

15. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

16. Методы, способы и средства защиты речевой информации от утечки по техническим каналам

17. Звукоизоляция выделенных помещений

18. Системы и средства акустической и виброакустической маскировки

19. Способы и средства защиты телефонных каналов связи

20. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

21. Оценка защищенности средств вычислительной техники от утечки за счет ПЭМИН

22. Средства измерения побочных электромагнитных излучений и наводок СВТ

23. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

24. Оценка защищенности выделенных помещений от утечки речевой информации

25. Средства измерения акустических и вибрационных сигналов и шумов

26. Методы и средства выявления электронных устройств негласного получения информации

27. Методы и средства выявления электронных устройств негласного получения информации

28. Порядок проведения специальный обследований и исследований

29. Организация технической защиты информации

30. Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации

31. Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации

– **практические вопросы к государственному экзамену (повышенный уровень).**

Студенты, прошедшие курс обучения по направлению «Информационная безопасность», профилю «Организация и технология защиты информации» в результате обучения должны уметь и владеть следующими навыками:

1. Смоделировать и исследовать в программе «Electronics Workbench» электрическую схему радиозакладного устройства.
2. Собрать лабораторную установку и провести исследования звукопоглощающих и звукоизолирующих свойств материалов.
3. Смоделировать и исследовать в программе «Electronics Workbench» принципы построения и работы схемы фильтрации опасных сигналов для защиты телефонной линии.
4. Смоделировать и исследовать в программе «Electronics Workbench» электрическую схему замещения системы высокочастотного навязывания.
5. Смоделировать и исследовать в программе «Mathcad» электрическое

поле от дискретного набора электрических зарядов.

6. Разработать приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для общеобразовательной организации.

7. Разработать приказ о назначении ответственного за обработку персональных данных для автотранспортного предприятия.

8. Разработать приказ о создании комиссии по организации и проведению работ по защите персональных данных для профессиональной образовательной организации.

9. Разработать перечень персональных данных, обрабатываемых в юридическом агентстве.

10. Разработать перечень информационных систем персональных данных и применяемых средств защиты информации для образовательной организации высшего образования.

11. Разработать перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним в организации дополнительного профессионального образования.

12. Разработать согласие субъекта персональных данных и журнал учета согласий субъектов персональных данных на обработку его персональных данных для агентства недвижимости.

13. Разработать уведомление о намерении осуществлять обработку персональных данных для дошкольной образовательной организации.

14. Составить заявление о предоставлении выписки из реестра операторов, осуществляющих обработку персональных данных для профессиональной образовательной организации.

15. Разработать перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных для образовательной организации высшего образования.

16. Определить актуальные угрозы безопасности персональных данных в информационных системах персональных данных для образовательной организации высшего образования.

17. Выполнить классификацию уровней защищенности персональных данных и составить акты классификации для городской детской поликлиники.

18. Выполнить классификацию автоматизированных систем и составить акты классификации для министерства здравоохранения края.

19. Разработать Концепцию обеспечения безопасности информации в автоматизированной системе автотранспортного предприятия.

20. Разработать Политику информационной безопасности для образовательной организации высшего образования.

21. Разработать План мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных дошкольной образовательной организации.

22. Разработать Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных городской детской поликлиники.

23. Разработать требования к мерам защиты информации, содержащейся в информационной системе образовательной организации высшего образования.

24. Разработать инструкцию администратора безопасности при использовании ресурсов объекта вычислительной техники профессиональной образовательной организации.

25. Разработать инструкцию администратора информационной системы персональных данных администрации города.

26. Разработать инструкцию ответственного за организацию резервирования и восстановления программного обеспечения и баз персональных данных организации дополнительного профессионального образования.

27. Подготовить заявки на аттестацию информационных систем персональных данных автотехцентра.

28. Подготовить необходимую организационно-распорядительную документацию на аттестацию информационных систем персональных данных городской больницы.

29. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия прибора: клавиатуры «С2000-К».

30. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия прибора: охранного извещателя «Фотон-16».

31. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия прибора: извещателя пожарного ручного «ИПР-И».

32. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия прибора: адресного расширителя «С2000- АР 8».

33. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия приборов: преобразователя интерфейсов RS-232/RS-485 и повторителя интерфейсов RS-485 «С 2000 ПИ».

34. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия прибора: контроллера двухпроводной линии связи «С2000-КДЛ».

35. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия прибора: извещателя акустического "Иволга".

36. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия прибора: световых табло "Выход"/"Пожар".

37. Продемонстрировать, воспользовавшись электронным тренажером и стендом, принципы работы системы контроля и управления доступом «Стил-Пост».

38. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия приборов: речевого оповещателя о пожаре "Рокот" и системы речевого оповещения "Орфей".

39. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия прибора: прибора приёмно-контрольного и управления автоматическими средствами пожаротушения и оповещателями «С2000 АСПТ».

40. На стенде «Интегрированная система охранно-пожарной сигнализации» продемонстрировать принцип действия прибора: извещателя пожарного «ИП 212 66».

41. Определить требуемый класс защиты для технических средств защиты ПДн используемых в ИСПДн для 3 уровня защищённости персональных данных.

42. Определить требуемый класс защиты для технических средств защиты ПДн используемых в ИСПДн для 2 уровня защищённости персональных данных.

43. Определить требуемый класс защиты для технических средств защиты ПДн используемых в ИСПДн для 1 уровня защищённости персональных данных

44. Оформить приказ о введении в действие перечня защищаемых сведений предприятия (организации).

45. Обнаружить радиозакладные устройства в помещении детектором поля Д-006.

46. Обнаружить радиозакладные устройства в помещении прибором Д-008 в режиме радиодетектора.

47. Обнаружить радиозакладные устройства в помещении детектором поля ST-107.

48. Обнаружить закладные устройства в линии 220В помещения прибором Д-008 в режиме анализатора проводных линий.

49. Обнаружить закладные устройства в телефонной линии помещения прибором Д-008 в режиме анализатора проводных линий.

50. Обнаружить закладные устройства в линии пожарной и охранной сигнализации помещения прибором Д-008 в режиме анализатора проводных линий.

51. Обнаружить закладные устройства в линии 220В помещения прибором ПСЧ-5.

52. Обнаружить закладные устройства в линии пожарной и охранной сигнализации помещения прибором ПСЧ-5.

53. Обнаружить закладные устройства в телефонной линии помещения прибором ПСЧ-5.

54. Обнаружить инфракрасный канал утечки информации в помещении прибором ПСЧ-5.

55. 11.Обнаружить акустический канал утечки информации помещении прибором ПСЧ-5.

56. Обнаружить вибро-акустический канал утечки информации в помещении прибором ПСЧ-5.

57. Обнаружить инфракрасный канал утечки информации в помещении прибором ПСЧ-5.

58. Обнаружить радиозакладные устройства в помещении специальным

сканирующим приёмником «Скорпион».

59. Заблокировать канал утечки информации по системам цифровой связи с использованием прибора «Квартет-2».

60. Заблокировать канал утечки информации по системам цифровой связи с использованием прибора «Филин-4».

61. Обнаружить и заблокировать радиоканалы утечки информации широкополосным генератором шума «Штора».

62. Обнаружить и заблокировать радиоканал утечки информации в помещении специальным сканирующим приёмником «Скорпион».

63. Обнаружить радиоканал утечки информации в помещении с использованием прибора ST-031 «Пиранья».

64. Обнаружить и заблокировать радиоканал утечки информации в помещении

65. Обнаружить канал утечки информации по линии 220В в помещении прибором ST-031 «Пиранья».

66. Обнаружить канал утечки информации по телефонной линии в помещении прибором ST-031 «Пиранья».

67. Обнаружить канал утечки информации по линии пожарной и охранной сигнализации в помещении прибором ST-031 «Пиранья».

68. Обнаружить акустический канал утечки информации в помещении прибором ST-031 «Пиранья».

69. Обнаружить вибро-акустический канал утечки в помещении прибором ST-031 «Пиранья».

70. Обнаружить инфракрасный канал утечки информации в помещении прибором ST-031 «Пиранья».

71. Провести обследование помещения на предмет наличия закладных устройств НРЛ «Лорнет».

72. Провести обследование помещения на предмет наличия закладных устройств НРЛ «NRL-900 EMS»

73. Продемонстрировать защиту переговоров по телефонной линии в помещении с использованием прибора «Гром-ЗИ-6»

74. Продемонстрировать защиту переговоров по телефонной линии в помещении с использованием прибора «МП-8 Сигма-РА»

75. Продемонстрировать защиту переговоров по телефонной линии в помещении с использованием прибора NG-305

76. Продемонстрировать подавление диктофонов в помещении с использованием комбинированного устройства «Тайфун-2».

77. Продемонстрировать защиту сотовых телефонов с использованием приборов «Ладья-Д» и «Кокон-Д» и пояснить принцип работы.

6. Список рекомендуемой литературы

6.1.Список основной литературы

1. Сагдеев К.М., Петренко В.И., Чипига А.Ф. Физические основы защиты информации: Учебное пособие. – Ставрополь: Изд-во СКФУ, 2015. – 394

с.

2. Петренко В.И. Теоретические основы защиты информации: Учебное пособие. – Ставрополь: Изд-во СКФУ, 2015. – 222 с.

3. Петренко В.И. Защита персональных данных в информационных системах: Учебное пособие. – Ставрополь: Изд-во СКФУ, 2016. – 201с.

4. Защита персональных данных в информационных системах: Лабораторный практикум / авт.-сост.: В.И. Петренко, И.В. Мандрица – Ставрополь: Изд-во СКФУ, 2018. – 118с.

5. Методы и средства инженерно-технической защиты информации: учебное пособие [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. - 2-е изд., стер. - М.: Флинта, 2011. - 187 с.

6. Организационно-правовое обеспечение информационной безопасности: учеб. пособие / [А. А. Стрельцов, В. С. Горбатов, Т. А. Поляков и др.]; под ред. А. А. Стрельцова. - М.: Академия, 2008. - 256 с. - (Высшее профессиональное образование). - Гриф: Рек. УМО для специальности "Информ. безопасность телеком. систем". - Библиогр.: с. 242-245. - 2500 экз. - ISBN 978-5- 7695-4240-4.

7. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2017. -586с.

6.2.Список дополнительной литературы

1. Девянин П.Н. Модели безопасности компьютерных систем. Учебное пособие. –М.: Издательский центр «Академия», 2015. – 144с.

2. Мельников, В. П. Информационная безопасность и защита ин-формации : учеб.пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 6-е изд., стер. – Москва : Академия, 2012. – 336 с.

3. Музыкантский А.И., Фурин В.В. Лекции по криптографии. – М.: МЦНМО, 2014. - 68 с.

4. Правовое обеспечение информационной безопасности [Электронный ресурс] /. - М.: Маросейка, 2008. - 368 с. Козлов, В. Е. Теория и практика борьбы с компьютерной пре-ступностью / В.Е. Козлов. – М.: Горячая линия-ТЕЛЕКОМ, 2002. – 336 с.

5. Разработка системы технической защиты информации : учебное пособие [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта, 2011. - 187 с. - ISBN 978-5-9765-1276-4. - URL:http://biblioclub.ru/index.php?page=book&id=93349

6. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. – М.: "Горячая линия-Телеком", 2014. - 229 с.

7. Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс / А.Н. Андрончик. - Екатеринбург: Издательство Уральского университета, 2014. - 179 с.

8. Степанов Е.А. «Информационная безопасность и защита информации». М.: ИНФР-М, 2014. – 353с.

9. Ярочкин В.И. «Информационная безопасность». 2014. – 640с.

7. Организация и проведение государственного экзамена

Государственный экзамен проводится в форме ответа на вопросы билета на открытом заседании экзаменационной комиссии при наличии не менее двух третей ее списочного состава.

При сдаче государственного экзамена допускается присутствие в аудитории не более 6 студентов.

Каждый студент самостоятельно выбирает экзаменационный билет один раз посредством произвольного извлечения.

Номер билета фиксируется секретарем ГЭК в соответствующем протоколе.

На подготовку к ответу на экзаменационный билет студенту отводится до 1 часа

При подготовке студент имеет право пользоваться программой государственного экзамена, а также с разрешения ГЭК – справочной литературой

Студенты, использующие при подготовке к ответу другую учебную литературу, с государственного экзамена удаляются

В протоколе после слов «Признать, что студент сдал государственный экзамен с оценкой» заносится запись «неудовлетворительно

Студент удален с государственного экзамена за списывание»

В экзаменационной ведомости студенту также проставляется оценка «неудовлетворительно».

В случае если студент по состоянию здоровья не смог ответить на вопросы экзаменационного билета, в протокол после слов «Общая характеристика ответа...» вносится запись «Студент по состоянию здоровья не смог ответить на вопросы экзаменационного билета».

Факт болезни должен быть подтвержден заключением медицинских работников.

По окончании ответа студента председатель и члены комиссии могут задавать дополнительные вопросы (как правило, не более трех).

Секретарь комиссии вносит в протокол вопросы билета, дополнительные вопросы членов комиссии, а также общую характеристику ответа студента на все вопросы.

В целом ответ студента на экзаменационный билет и дополнительные вопросы занимает, как правило, 30 минут.

По окончании ответов студентов академической группы объявляется совещание экзаменационной комиссии, на котором присутствуют только члены комиссии.

На совещании обсуждаются ответы каждого студента на вопросы билета и дополнительные вопросы.

По итогам обсуждения каждому студенту в протокол проставляется соответствующая оценка.

Секретарь комиссии заполняет экзаменационную ведомость и зачетные книжки студентов по итогам проведения государственного экзамена.

После совещания комиссии в аудиторию приглашаются студенты академической группы.

Председатель комиссии информирует студентов о результатах государственного экзамена.

8. Критерии выставления оценки

8.1 Итоги государственного экзамена Государственная экзаменационная комиссия подводит на закрытом заседании

Решение об оценках принимается простым большинством голосов членов комиссии, участвующих в заседании

8.2 В качестве критериев оценки ответа студентов выделяются:

- полнота раскрытия вопросов экзаменационного билета;
- логичность и последовательность изложения материала;
- аргументированность ответа студента;
- способность анализировать и сравнивать различные подходы к решению поставленной проблемы;
- готовность студента отвечать на дополнительные вопросы по существу экзаменационного билета.

8.3 Результаты государственного экзамена оцениваются как «**отлично**», «**хорошо**», «**удовлетворительно**», «**неудовлетворительно**».

8.4. Оценка «отлично» выставляется студенту, верно ответившему на вопросы экзаменационного билета и дополнительные вопросы, глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логично его излагающему, в ответе которого тесно связываются теория с практикой

При этом студент не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практической работы.

8.5. Оценка «хорошо» выставляется студенту, верно ответившему на 80% вопросов экзаменационного билета и дополнительных вопросов, твердо знающему программный материал, грамотно и по существу излагающему его, не допускающему существенных неточностей в ответе на вопрос, правильно применяющему теоретические положения при решении практических вопросов и задач, владеющему необходимыми знаниями и приемами их выполнения, демонстрирующему хорошие знания учебной литературы, нормативных актов, обладающему навыками анализа источников, знающему основные проблемы дисциплины, умеющему устанавливать основные причинно-следственные связи;

8.6 Оценка «удовлетворительно» выставляется студенту, верно ответившему на 60% вопросов экзаменационного билета и дополнительных вопросов, который имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает затруднения в применении нормативных актов.

8.7 Оценка «неудовлетворительно» выставляется студенту, верно ответившему менее чем на 60% вопросов экзаменационного билета и не ответившему на дополнительные вопросы, демонстрирующему слабое знание содержания дисциплины, плохо ориентирующемуся в основных понятиях курса, не знающему значительной части программного материала, допускающему существенные ошибки, неуверенно с большим затруднением формулирующему практические знания, слабо владеющему законодательным материалом, не умеющему устанавливать причинно-следственные связи.

8.8 Студент, не сдавший государственный экзамен, не имеет права быть допущенным к защите выпускной квалификационной работы

Студент, не прошедший итоговые аттестационные испытания, отчисляется из вуза.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ЧЛЕНАМ ГОСУДАРСТВЕННОЙ ЭКЗАМЕНАЦИОННОЙ КОМИССИИ ПО УЧАСТИЮ В ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

1 Перечень компетенций, знаний, умений, владений, уровень усвоения которых должен быть проверен на государственном экзамене

Цели и задачи государственного экзамена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 «Информационная безопасность» состоят в выявлении уровня теоретической подготовки специалиста и степени его подготовленности к профессиональной деятельности в области информационной безопасности.

Выпускник бакалавриата по направлению подготовки «Информационная безопасность» должен

знать:

– основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире;

– основные разделы и направления философии, методы и приемы философского анализа проблем;

– лексический минимум в объеме 4 000 учебных лексических единиц общего и терминологического характера (для иностранного языка);

– основные экономические категории и закономерности, методы анализа экономических явлений и процессов, специфические черты функционирования хозяйственной системы на (микро- и макро-)уровнях, основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений;

– основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации;

– основные понятия и методы в области управленческой деятельности;

– основные понятия и методы математического анализа;

– основные понятия и методы аналитической геометрии;

– основные понятия и методы линейной алгебры и теории алгебраических систем;

– основные понятия и методы теории функций комплексного переменного;

– основные понятия и методы теории вероятностей и математической статистики;

– основные понятия и методы математической логики и теории алгоритмов, теории информации кодирования;

– математические методы обработки экспериментальных данных;

– основные понятия, законы и модели механики;

– основные понятия, законы и модели электричества и магнетизма;

– основные понятия, законы и модели теории колебаний и волн оптики, квантовой физики, физики твердого тела, статистической физики и термодинамики;

– особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности;

– основные понятия информатики;

– место и роль информационной безопасности в системе национальной безопасности Российской Федерации;

– методы программирования и методы разработки эффективных алгоритмов решения прикладных задач;

– современные средства разработки и анализа программного обеспечения на языках высокого уровня;

– аппаратные средства вычислительной техники;

– операционные системы персональных ЭВМ;

– основы администрирования вычислительных сетей;

– системы управления базами данных;

– принципы построения информационных систем;

– структуру систем документационного обеспечения;

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

– правовые нормы и стандарты по лицензированию в области

– обеспечения защиты государственной тайны и сертификации средств защиты информации;

– принципы и методы организационной защиты информации;

– технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

– принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;

– принципы организации информационных систем в соответствии с требованиями по защите информации;

– эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы;

– сигналы электросвязи, принципы построения систем и средств связи;

– методы анализа электрических цепей;

– принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них;

– основы схемотехники;

– опасные и вредные факторы системы "человек - среда обитания", методы анализа антропогенных опасностей, научные и организационные основы защиты окружающей среды и ликвидации последствий, аварий, катастроф, стихийных бедствий;

уметь:

– использовать в практической деятельности правовые знания; анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав;

– анализировать мировоззренческие, социально и личностно значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию; планировать и осуществлять свою деятельность с учетом результатов этого анализа;

– оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения;

– использовать математические методы и модели для решения прикладных задач;

– применять основные законы физики при решении прикладных задач;

– использовать программные и аппаратные средства персонального компьютера;

– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;

– составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;

– формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;

– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;

– анализировать и оценивать угрозы информационной безопасности объекта;

– применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

– пользоваться нормативными документами по защите информации;

– применять на практике методы анализа электрических цепей;

– анализировать и оценивать степень риска проявления факторов опасности системы "человек - среда обитания", осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности;

владеть:

– иностранным языком в объеме, необходимом для возможности получения информации по профессиональной тематике, и навыками устной речи;

– навыками письменного аргументированного изложения собственной точки зрения;

– навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений;

– навыками критического восприятия информации;

– навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;

– навыками обоснования, выбора, реализации и контроля результатов управленческого решения.

– методами количественного анализа процессов обработки, поиска и передачи информации;

– навыками проведения физического эксперимента и обработки его результатов;

– навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).

– методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;

– навыками выявления и уничтожения компьютерных вирусов;

– навыками работы с нормативными правовыми актами;

– методами и средствами выявления угроз безопасности автоматизированным системам;

– навыками организации и обеспечения режима секретности;

– методами технической защиты информации;

– методами формирования требований по защите информации;

– методами расчета и инструментального контроля показателей технической защиты информации;

– навыками чтения электронных схем;

– методами анализа и формализации информационных процессов объекта и связей между ними;

– методами организации и управления деятельностью

– служб защиты информации на предприятии;

– методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;

– профессиональной терминологией;

– навыками безопасного использования технических средств в профессиональной деятельности.

Коллектив кафедры организации и технологии защиты информации ставит перед собой задачу подготовить выпускников к принятию квалифицированных самостоятельных решений в различных аспектах проектирования, эксплуатации и модернизации систем защиты информации на объектах информатизации.

Государственный экзамен проводится с соблюдением объективности и взаимного уважения студента и экзаменатора

Основными принципами процедуры оценивания ответа студента членами Государственной аттестационной комиссии на государственном экзамене являются: профессионализм, предметность, независимость, объективность, непредвзятость, беспристрастность, доброжелательность.

Основной задачей государственной аттестационной комиссии является определение соответствия подготовки выпускников квалификационным требованиям федерального государственного образовательного стандарта высшего профессионального образования по направлению 10.03.01 «Информационная безопасность»

При оценивании ответов студентов экзаменаторы руководствуются системой критериев:

Содержательное соответствие – соответствие содержания ответа поставленным на экзамене вопросам.

Методологическая обоснованность – построение ответа в соответствии с уровнями методологии научного знания, умение представить современное состояние развития информационных технологий, зарубежные научные подходы, теории и результаты исследований в критическом сравнении с достижениями отечественной науки.

Научный анализ – критический научный анализ излагаемых концепций, аргументированный конкретными результатами

Научный синтез – рассмотрение теоретических подходов, отдельных концепций и исследований в контексте научного знания в целом, демонстрирование понимания связи между отдельными элементами целостного научного знания, обобщение и систематизация научной информации при решении проблемы.

Системность – четкое выделение понятий, существенных элементов теорий или концепций, их характеристика, описание связей между ними, представление материала как цельной системы знаний.

Логичность – последовательное, непротиворечивое, четко структурированное изложение материала с выделением основополагающих и второстепенных положений; ясность изложения материала.

Понятийно-терминологическая обоснованность – использование при изложении материала адекватных научных профессиональных информационных и математических терминов и понятий, раскрытие их полного содержания, соответствующего современному уровню развития информационных технологий.

Проявление индивидуальной и профессиональной культуры.

При оценивании ответов студентов экзаменаторы отмечают достоинства ответов при их наличии, их соответствие указанным критериям, выделяют следующие типы несоответствий в виде неточностей или ошибок (при их наличии):

Неточность:

При изложении теоретического материала - незначительная погрешность, не искажающая смысла излагаемого материала, отсутствие в ответе ссылок на некоторых авторов конкретных теорий и исследований, изложение теорий или исследований без указания времени проведения исследований или создания концепций, имеющих отношение к вопросу.

При использовании терминологии – неполное представление о содержании понятий, использование жаргонных слов вместо научной терминологии при правильном изложении теоретического и эмпирического материала.

При изложении теоретических вопросов - слабая аргументированность, недостаточное подтверждение теоретических положений известными фактами и феноменами.

Ошибка:

При изложении теоретического материала - грубые искажения в описании научных теорий и концепций, неадекватное раскрытие содержания излагаемого вопроса; пропуски важных смысловых элементов материала; отсутствие в тексте или устном ответе описаний одного или более из основных теоретических подходов или ключевых компонентов излагаемой теории, перестановки и смещения в хронологии фактического или логического концептуального изложения материала.

При изложении эмпирического и (или) экспериментального материала - неадекватное использование или незнание методов, методик, тестов, измерительных параметров и процедур проведения исследований, существенных характеристик выборки, неадекватная интерпретация полученных основных результатов и выводов.

При использовании терминологии - неумение оперировать категориальным аппаратом, незнание основных научных информационных и математических терминов и понятий.

Форма оценивания членами ГЭК результатов освоения образовательной программы (уровня сформированности компетенций выпускника при сдаче государственного экзамена по направлению подготовки - 10.03.01 «Информационная безопасность» квалификация бакалавр)

№ п/п	Критерии оценки	отлично	хорошо	удовлетво-рительно	неудовле-твори-тельно
1.	Полнота раскрытия вопросов экзаменационного билета (указать ОК или ПК)				
2.	Аргументированность ответа студента (указать ОК или ПК)				
3.	способность анализировать и сравнивать различные подходы к решению поставленной проблемы (указать ОК или ПК)				
4.	готовность студента отвечать на дополнительные вопросы по существу экзаменационного билета (указать ОК или ПК)				
5.	Навыки защиты собственных научных идей, предложений и рекомендаций (указать ОК или ПК)				
6.	Общий уровень культуры общения (указать ОК или ПК)				
7.	Готовность к практической деятельности в условиях рыночной экономики, изменения при необходимости направления профессиональной деятельности в рамках предметной области знаний и практических навыков (указать ОК или ПК)				

Распределение оценок членов ГЭК по компетенциям для определения общего уровня сформированности требуемых компетенций при сдаче государственного экзамена

№ п/п	Члены ГЭК	Компетенции								
		ОК–1				……..	ОК–7	ПК–1	……	ПК–12
		Оценка по критерию								
		1	……..	7	сред-нее					
1.										
2.										
3.										
4.										
5.										
Сред-нее значе-ние по										

компе-тенции										