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 10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки	10.04.01 Информационная безопасность
Магистерская программа	Комплексная защита объектов информатизации

г. Ставрополь, 2017

Содержание

Введение

1. В соответствии с образовательным стандартом по направлению подготовки 10.04.01 «Информационная безопасность» и образовательной программой по направлению подготовки 10.04.01 «Информационная безопасность», утвержденной Учёным советом СКФУ в состав государственной итоговой аттестации входят:

- государственный экзамен по направлению подготовки 10.04.01 «Информационная безопасность;

-защита выпускной квалификационной работы.

2. Программа ГИА составлена в соответствии с требованиями:

- образовательного стандарта по направлению подготовки 10.04.01 «Информационная безопасность»;

- образовательной программы по направлению подготовки 10.04.01 «Информационная безопасность», утвержденной Учёным советом СКФУ;

- Приказа Министерства образования и науки Российской Федерации от 19 декабря 2013 г. №1367 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;

– Положения об учебно-методическом обеспечении образовательных программ высшего образования в ФГАОУ ВО «Северо-Кавказский федеральный университет», утвержденного приказом ректора СКФУ от 08.09.2014г. №1376–о;

3. В результате освоения образовательной программы по направлению 10.04.01 «Информационная безопасность», обучающийся должен овладеть, и продемонстрировать ходе государственной итоговой аттестации, следующими:

общекультурными компетенциями (ОК):

– способностью к абстрактному мышлению, анализу, синтезу (ОК-1);

– способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые (ОК-2);

общепрофессиональными компетенциями (ОПК):

- способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности (ОПК-1);

- способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2);

профессиональными компетенциями (ПК):

− способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность (ПК-1);

− способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2);

− способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной

безопасности объектов защиты на основе российских и международных стандартов (ПК-3);

− способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4);

− способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления (ПК-5);

− способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов (ПК-6);

− способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7);

− способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8);

− способностью проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9);

− способностью проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10);

− способностью проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности (ПК-11);

− способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12);

− способностью организовать управление информационной безопасностью (ПК-13);

− способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14);

− способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15);

− способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной (ПК-16).

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 10.04.01 «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 ВПО по направлению 10.04.01 «Информационная безопасность» с учетом специфики учебного процесса и региональных особенностей вуза.

Государственный экзамен по направлению 10.04.01 «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 10.04.01 «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 магистратуры по направлению подготовки «Информационная безопасность» должен обладать следующими

общекультурными компетенциями (ОК):

– способностью к абстрактному мышлению, анализу, синтезу (ОК-1);

– способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые (ОК-2);

общепрофессиональными компетенциями (ОПК):

- способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности (ОПК-1);

- способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности (ОПК-2);

профессиональными компетенциями (ПК):

а) проектная деятельность:

− способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность (ПК-1);

− способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2);

− способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов (ПК-3);

− способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК-4);

б) научно-исследовательская деятельность:

− способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления (ПК-5);

− способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов (ПК-6);

− способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента (ПК-7);

− способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи (ПК-8);

в) вид деятельности: контрольно-аналитическая:

− способностью проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9);

− способностью проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10);

г) вид деятельности: педагогическая:

− способностью проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности (ПК-11);

д) вид деятельности: организационно-управленческая:

− способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения (ПК-12);

− способностью организовать управление информационной безопасностью (ПК-13);

− способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК-14);

− способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности (ПК-15);

− способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной (ПК-16).

Выпускник магистратуры по направлению подготовки «Информационная безопасность» должен:

знать:

- основные теории и методы макро и микроэкономики;
- экономическое планирование и прогнозирование, методику оценки хозяйственной деятельности (применительно к отрасли обеспечения информационной безопасности);
- основные типы статистических задач и математические методы их решения;
- основные математические методы исследования случайных процессов;
- основные теоретико-числовые методы применительно к задачам защиты информации;
- физические основы функционирования технических средств и систем обработки и передачи информации;
- физические основы образования технических каналов утечки информации;

уметь:

- анализировать, оценивать и прогнозировать экономические эффекты и последствия реализуемой и планируемой деятельности;
- самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач;
- применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации;
- применять системы компьютерной математики для решения типовых задач;
- использовать физические эффекты для обеспечения технической защиты информации;
- применять на практике методы физики при исследовании технических каналов утечки информации;
- осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;
- обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности;
- организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;

владеть:

- навыками управления информационной безопасностью простых объектов;
- приемами экономического анализа и планирования, навыками реализации и контроля результатов управленческого решения по экономическим критериям;
- навыками аналитического и численного решения задач математической статистики;
- методами проведения физического эксперимента при выявлении технических каналов утечки информации;

- основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем;

- методы концептуального проектирования технологий обеспечения информационной безопасности.

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 магистров направления 10.04.01 «Информационная безопасность»:

1. Теоретические основы компьютерной безопасности.
2. Технологии обеспечения информационной безопасности объектов.
3. Защищённые информационные системы.
4. Основы научных исследований.

Экзамен предполагает:

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

Структурно экзаменационный билет 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 10.04.01 «Информационная безопасность» включает основополагающие темы следующих учебных дисциплин:

Теоретические основы компьютерной безопасности

Структуризация методов защиты информации в АС. Уровни защиты. Защита от угрозы нарушения конфиденциальности информации на уровне представления. Защита от угрозы нарушения конфиденциальности информации на уровне содержания (семантическая защита). Защита от угрозы нарушения целостности информации на уровне представления. Защита от угрозы нарушения целостности информации на уровне содержания (семантическая защита). Сравнительная характеристика методов обеспечения целостности информации на уровне представления (контрольное суммирование, имитозащита и электронная подпись). Защита от сбоев программно-аппаратной среды. Обеспечение отказоустойчивости ПО АС. Сокрытие логики работы АС и её защищенных функций реализованных программно и (или) программно-аппаратно. Понятие монитора безопасности. Аксиомы безопасности. .Понятие модели безопасности. Разрешимость модели безопасности. Дискреционные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Take-Grant. Расширенная модель Take-Grant. Модель мандатного управления доступом.

Модель Белла-ЛаПадула, модель Биба. Ролевая модель управления доступом. Особенности управления доступом в семействе ОС Windows NT. Привилегии. Привилегия овладевания. Наследование прав на объекты объектами. Домены безопасности. Модель доменов и типов для POSIX систем. Понятие шлюза безопасности, его назначение и структура. Виртуализация.

Технологии обеспечения информационной безопасности объектов

Значение информационной безопасности и ее место в системе национальной безопасности. Сущность и понятие защиты информации. Теоретические и концептуальные основы защиты информации объектов. Критерии, условия и принципы отнесения информации к защищаемой. Состав и классификация носителей защищаемой информации. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию Каналы и методы несанкционированного доступа к конфиденциальной информации. Объекты защиты информации. Классификация видов, методов и средств защиты информации. Кадровое и ресурсное обеспечение защиты информации. Технологическое обеспечение защиты информации на объекте. Структура систем защиты информации объекта. Аудит информационной безопасности объекта.

Защищённые информационные системы

Механизмы защиты операционной системы. Интеграция защищенных операционных систем. Типовые угрозы сетевой безопасности. Методы и средства обеспечения информационной безопасности в вычислительных сетях. Теоретические основы безопасности в СУБД. Механизмы обеспечения конфиденциальности, целостности и высокой готовности СУБД.

Основы научных исследований

Научное исследование, его сущность и организация. Структура научного знания. Основы методологии научных исследований. Общая характеристика метода и методологии научного исследования. Основные этапы планирования и проведения научного исследования. Источники научной информации. Методика работы с источниками научной информации. Оформление и защита научных работ. Методика работы над рукописью исследования. Особенности презентации и защиты результатов исследования.

5. Перечень примерных вопросов для подготовки к государственному экзамену

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

Студенты, прошедшие курс обучения по направлению «Информационная безопасность», магистерской программе «Комплексная защита объектов информатизации» в результате обучения должны знать:

I. Теоретические основы компьютерной безопасности:

1. Структуризация методов защиты информации в АС. Уровни защиты.
2. Защита от угрозы нарушения конфиденциальности информации на

уровне представления.

3.Защита от угрозы нарушения конфиденциальности информации на уровне содержания (семантическая защита).

4.Защита от угрозы нарушения целостности информации на уровне представления.

5.Защита от угрозы нарушения целостности информации на уровне содержания (семантическая защита).

6.Сравнительная характеристика методов обеспечения целостности информации на уровне представления (контрольное суммирование, имитозащита и электронная подпись).

7.Защита от сбоев программно-аппаратной среды.

8.Обеспечение отказоустойчивости ПО АС.

9.Сокрытие логики работы АС и её защищенных функций реализованных программно и (или) программно-аппаратно.

10.Понятие монитора безопасности. Аксиомы безопасности.

11.Понятие модели безопасности. Разрешимость модели безопасности.

12.Дискреционные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Take-Grant. Расширенная модель Take-Grant.

13.Модель мандатного управления доступом. Модель Белла-ЛаПадула, модель Биба.

14.Ролевая модель управления доступом. Особенности управления доступом в семействе ОС Windows NT. Привилегии. Привилегия овладевания.

15.Наследование прав на объекты объектами.

16.Домены безопасности. Модель доменов и типов для POSIX систем.

17.Понятие шлюза безопасности, его назначение и структура. Виртуализация.

II. Технологии обеспечения информационной безопасности объектов:

1. Значение информационной безопасности и ее место в системе национальной безопасности
2. Сущность и понятие защиты информации
3. Теоретические и концептуальные основы защиты информации объектов
4. Критерии, условия и принципы отнесения информации к защищаемой
5. Состав и классификация носителей защищаемой информации
6. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию Каналы и методы несанкционированного доступа к конфиденциальной информации
7. Объекты защиты информации
8. Классификация видов, методов и средств защиты информации
9. Кадровое и ресурсное обеспечение защиты информации
10. Технологическое обеспечение защиты информации на объекте
11. Структура систем защиты информации объекта
12. Аудит информационной безопасности объекта.

III. Защищённые информационные системы

1. Механизмы защиты операционной системы
2. Интеграция защищенных операционных систем
3. Типовые угрозы сетевой безопасности
4. Методы и средства обеспечения информационной безопасности в вычислительных сетях
5. Теоретические основы безопасности в СУБД
6. Механизмы обеспечения конфиденциальности, целостности и высокой готовности СУБД

IV. Основы научных исследований

1. Научное исследование, его сущность и организация
2. Структура научного знания
3. Основы методологии научных исследований
4. Общая характеристика метода и методологии научного исследования
5. Основные этапы планирования и проведения научного исследования
6. Источники научной информации
7. Методика работы с источниками научной информации
8. Оформление и защита научных работ
9. Методика работы над рукописью исследования
10. Особенности презентации и защиты результатов исследования.

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

Студенты, прошедшие курс обучения по направлению «Информационная безопасность», магистерской программе «Комплексная защита объектов информатизации» в результате обучения должны уметь и владеть следующими навыками:

1 Составьте модель персонального компьютера.
2 Представьте угрозы персональным компьютерам.
3 Опишите средства защиты персонального компьютера.
4 Составьте архитектуру безопасности.
5 Опишите систему управления базами данных.
6 Организуйте криптографический алгоритм.
7 Опишите алгоритм Евклида.
8 Составьте математические методы анализа политики безопасности.
9 Постройте модель сети, в которой будет минимум уязвимостей.
10 Постройте атаку на тройной DES с помощью линейного криптоанализа.
11 Проведите анализ схем шифрования, использующих многократно один блочный шифр.
12 Проведите анализ возможных направлений утечки информации и способы борьбы с ними.
13 Провести классификацию объектов защиты.

14 Опишите порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

15 Составьте список всех типов мер защиты информации

16 Опишите архитектуру программных средств защиты информации.

17 Организуйте криптографический алгоритм.

18 Компенсируйте отсутствие CLI-интерфейса в МСЭ «Континент».

19 Составьте собственный криптографический алгоритм.

20 Постройте модель сети, в которой будет минимум уязвимостей.

21 Постройте полную модель сети предприятия и организуйте ее защиту.

22 Проведите отладку трафика с помощью ACL.

23 Проведите анализ возможных направлений утечки информации и способы борьбы с ними.

24 Создание защищенной инфраструктуры на базе ОС Windows, с использованием ПО Zone Alarm.

25 Создание защищенной инфраструктуры на базе ОС Windows, с использованием ПО Panda Firewall.

26 Создание защищенной инфраструктуры на базе ОС Windows, с использованием брандмауэра Windows Server 2003.

27 Создание защищенной инфраструктуры на базе ОС Linux, с использованием ПО IPCop.

28 Создание защищенной инфраструктуры на базе ОС Linux, с использованием ПО Shorewall.

29 Создание защищенной инфраструктуры на базе ОС Linux, с использованием ПО Uncomplicate Firewall.

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

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

32 Разработать Политику информационной безопасности для образовательной организации высшего образования.

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

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

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

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

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

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

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

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

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

42 Обнаружить акустический канал утечки информации помещении прибором ПСЧ-5.

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

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

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

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

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

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

49 Обнаружить и заблокировать радиоканал утечки информации в помещении

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

6. Список рекомендуемой литературы

6.1.Список основной литературы

1. Алферов, А.П. Основы криптографии: Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2005.

2. Бабенко, Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. – М: Гелиос АРВ, 2006.

3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. М.: Горячая линия - Телеком, 2005. – 416 с.

4. Корнеев И.К. Защита информации в офисе: учеб. – М.: ТК Велби, Изд-во Проспект, 2008. – 336 с.

5. Корт С.С. Теоретические основы защиты информации: Учебное пособие. - М.: –Гелиос АРВ, 2004. – 240с.

6. Организация и современные методы защиты информации /Под общей редакцией Диева С.А., Шаваева А.Г./ - М.: Концерн «Банковский Деловой Центр», 2006. – 472с.

7. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 2009. – 568с

8. Правовое обеспечение информационной безопасности: учебник / [под общ.науч. ред. В. А. Минаева и др.]. – Изд. 2-е, расш. и доп. - Москва: Ма-

росейка, 2008. - 368 с.

9. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности. – М.: Гелиос АРВ, 2004. – 224 с.

10. Шевцов В.А., Куприянов А.И., Сахаров А.В. Основы защиты информации. – М. Издательский дом «Академия», 2008. – 256 с.

6.2.Список дополнительной литературы

11. Алферов, А.П. Основы криптографии: Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2005.

12. Бабенко, Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. – М: Гелиос АРВ, 2006.

13. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. М.: Горячая линия - Телеком, 2005. – 416 с.

14. Корнеев И.К. Защита информации в офисе: учеб. – М.: ТК Велби, Изд-во Проспект, 2008. – 336 с.

15. Корт С.С. Теоретические основы защиты информации: Учебное пособие. - М.: –Гелиос АРВ, 2004. – 240с.

16. Организация и современные методы защиты информации /Под общей редакцией Диева С.А., Шаваева А.Г./ - М.: Концерн «Банковский Деловой Центр», 2006. – 472с.

17. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 2009. – 568с

18. Правовое обеспечение информационной безопасности: учебник / [под общ.науч. ред. В. А. Минаева и др.]. - Изд. 2-е, расш. и доп. - Москва: Маросейка, 2008. – 368 с.

19. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности. – М.: Гелиос АРВ, 2004. – 224 с.

20. Шевцов В.А., Куприянов А.И., Сахаров А.В. Основы защиты информации. – М. Издательский дом «Академия», 2008. – 256 с.

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 5 студентов. Каждый студент самостоятельно выбирает экзаменационный билет один раз посредством произвольного извлечения. Номер билета фиксируется секретарем ГАК 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 ГАК – 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

Итоги государственного экзамена Государственная экзаменационная комиссия подводит на закрытом заседании. Решение об оценках принимается простым большинством голосов членов комиссии, участвующих в заседании.

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.

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

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 прак-

тикой. 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.

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;

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.

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.

Студент, не сдавший государственный экзамен, не имеет права быть допущенным к защите выпускной квалификационной работы. Студент, не прошедший итоговые аттестационные испытания, отчисляется из вуза.