МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СТРОИТЕЛЬСТВА, ТРАНСПОРТА И АРХИТЕКТУРЫ имени Н.ИСАНОВА

УТВЕРЖДАЮ

Ректор КГУСТА, д.т.н., проф.

_____А.А. Абдыкалыков

«_01_» _____09._____ 2019 г.

ПРОГРАММА ИТОГОВОГО ГОСУДАРСТВЕННОГО ЭКЗАМЕНА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ БАКАЛАВРОВ

Направление подготовки: 590100 - Информационная безопасность

Профили подготовки: Безопасность автоматизированных систем,
Безопасность телекоммуникационных систем,

Академическая степень: бакалавр

БИШКЕК - 2019

УДК 004.056.

Программа итогового государственного экзамена составлена на основании государственного образовательного стандарта высшего профессионального образования по направлению подготовки 590100 «Информационная безопасность» (бакалавриат), утвержденного приказом Министерства образования и науки Кыргызской Республики от 15.09.2015г., № 1179\1 и учебного плана по основной образовательной программе высшего образования «Информационная безопасность».

Составители: Абдулаев А.А., к.т.н., доцент, зав. кафедрой ОБИС, старшие преподаватели: Оморова Н.А., Маматалиева Б.А., Сабирова Г.А.

Программа обсуждена и утверждена на заседании кафедры «Обеспечение безопасности информационных систем». Протокол №__2__ от __05.09.__2019 г.

Заведующий кафедрой ОБИС _____ А.А. Абдулаев
(подпись)

Программа одобрена на заседании Учебно-методического совета института новых информационных технологий, Протокол №__1__ от «__27__» __сентября__2019 г.

Председатель УМС ИНИТ _____ С.Ж. Карабаева
(подпись)

Программа итогового государственного экзамена согласована и рекомендована к утверждению:

Начальник УИУ КГУСТА _____ Р.А. Жумабаев
(подпись)

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические рекомендации «Программа государственного экзамена по направлению подготовки выпускников» предназначены для студентов, обучающихся по направлению подготовки 590100 «Информационная безопасность» (академическая степень «бакалавр») профили: «Безопасность автоматизированных систем», «Безопасность телекоммуникационных систем» и «Информационная безопасность оптических систем связи», а также научных руководителей и рецензентов выпускных квалификационных работ.

В рекомендациях приведены конкретные требования и указаны критерии оценок по сдачи государственного экзамена. Методические рекомендации построены в соответствии с требованиями действующих нормативных документов: ГОС ВПО направления подготовки бакалавра 590100 «Информационная безопасность», утвержденного приказом МОН КР от 15.09.2015 г., № 1179\1 и Положения об итоговой государственной аттестации выпускников высших учебных заведений Кыргызской Республики, утвержденного постановлением Правительства Кыргызской Республики от 20.05.2012 г., № 346 и приказов МОН КР, а также указаний и рекомендаций КГУСТА имени Н. Исанова.

Целью государственного междисциплинарного квалификационного экзамена является оценки уровня усвоения профессиональных компетенций, полученных за период обучения, в области информационной безопасности.

К государственному междисциплинарному квалификационному экзамену, допускается лицо, успешно завершившее в полном объеме освоение основной образовательной программы по направлению подготовки высшего образования.

1. ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ БАКАЛАВРА

Бакалавр в области информационной безопасности должен уметь решать задачи, соответствующие его квалификации по направлению подготовки 590100 «Информационная безопасность» (академическая степень «бакалавр») профили: «Безопасность автоматизированных систем», «Безопасность телекоммуникационных систем» и «Информационная безопасность оптических систем связи».

В процессе сдачи государственного междисциплинарного квалификационного экзамена осуществляется дальнейшее углубление и систематизация теоретических знаний, развитие прикладных умений при решении профессиональных задач, овладение методикой проведения исследований, развитие навыков самостоятельной работы, повышение общей и профессиональной эрудиции выпускника.

В ходе итоговой государственной аттестации оценивается полнота владения выпускником следующими компетенциями (в соответствии с ГОС ВПО по направлению 590100 «Информационная безопасность»):

ОК-2 - способен использовать базовые положения математических, естественных, гуманитарных, экономических наук при решении профессиональных задач;

ОК-4 - способен понимать и применять традиционные и инновационные идеи, находить подходы к их реализации и участвовать в работе над проектами, используя базовые методы исследовательской деятельности.

ИК-2 - способен логически верно, аргументировано и ясно строить свою устную и письменную речь на государственном и официальном языках;

ИК-5 - владеет основными методами, способами и средствами получения, хранения и переработки информации, навыками работы с компьютером, как средством управления информацией, в том числе в глобальных компьютерных сетях и корпоративных информационных системах;

ПК-2 - способен определять виды и формы информации, подверженной угрозам, виды и возможные методы, и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;

ПК-5 - способен применять системы программирования и программные средства системного, прикладного и специального назначения для решения задач обеспечения информационной безопасности;

ПК-6 - способен собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, а также проводить предварительный технико-экономический анализ и обосновать проектные решения по обеспечению информационной безопасности;

ПК-8 - способен принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

Выпускник по профилю подготовки «Безопасность автоматизированных систем» дополнительно должен обладать следующими профильно-специализированными компетенциями:

ПКП-1 - способен выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей;

ПКП-2 - способен разработать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации;

ПКП-3 - способен принимать участие в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности.

Выпускник по профилю подготовки «Безопасность телекоммуникационных систем» дополнительно должен обладать следующими профильно- специализированными компетенциями:

ПКП-1 - способен принимать участие в разработке устройств защищенных телекоммуникационных систем;

ПКП-2 - способен принимать участие в поведении технических расчетов при разработке архитектурных элементов защищенных телекоммуникационных систем;

ПКП-3 - способен выполнять необходимые математические расчеты в ходе экспериментальных исследований информационной безопасности телекоммуникационных систем.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПОДГОТОВКЕ ГОСУДАРСТВЕННОГО МЕЖДИСЦИПЛИНАРНОГО КВАЛИФИКАЦИОННОГО ЭКЗАМЕНА

Государственный междисциплинарный квалификационный экзамен является составной частью обязательной государственной итоговой аттестации выпускников по направлению подготовки 590100 – «Информационная безопасность» и призван оценить теоретическую и практическую подготовку к решению профессиональных задач в области исследования, разработки, внедрения и сопровождения информационных технологий и систем в соответствии с требованиями ГОС ВО КР.

В соответствии с этим Программа государственного междисциплинарного квалификационного экзамена охватывает тематику дисциплин теоретической и практической подготовки по направлению подготовки 590100 – «Информационная безопасность».

На заседании кафедры «Обеспечение безопасности информационных систем» рассмотрены и одобрены выбор дисциплин и перечень экзаменационных вопросов.

В программу включены вопросы по следующим дисциплинам:

– по базовому профессиональному циклу:

«Программно-аппаратные средства защиты информации»;

«Криптографические методы защиты информации»;

– по профилю «Безопасность автоматизированных систем»:

«Безопасность операционных систем»;

«Безопасность систем базы данных»;

– по профилю «Безопасность телекоммуникационных систем»:

«Техническая защита информации»;

«Безопасность вычислительных сетей».

Экзаменационный билет содержит три вопроса: первый два вопросы по базовому профессиональному циклу, а третий вопрос по профилю.

В процессе принятия экзамена в аудитории могут одновременно находится не более 8-ми экзаменующихся. Экзаменующимся выдаются установленные бланки листа устного ответа, и для подготовки к ответу отводится не более 30 минут.

Секретарь экзаменационной комиссии во время заседания ведет протокол, в котором фиксирует номер экзаменационного билета, а также итоговую оценку сдачи государственного экзамена по специальности.

3. КРИТЕРИИ ОЦЕНКИ ЗНАНИЙ

Знания, проявленные выпускником на государственном междисциплинарном квалификационном экзамене, оцениваются по четырех бальной системе

Оценка «отлично» – все три вопроса задания имеют полные решения. Содержание ответов свидетельствует об уверенных знаниях выпускника и о его умении решать профессиональные задачи.

Оценка «хорошо» – минимум два вопроса задания имеют полные решения. Содержание ответов свидетельствует о достаточных знаниях выпускника и о его умении решать профессиональные задачи.

Оценка «удовлетворительно» – минимум один вопрос задания имеет полное

решение. Содержание ответов свидетельствует о знаниях выпускника и о его ограниченном умении решать профессиональные задачи, соответствующие его будущей квалификации.

Оценка «неудовлетворительно» – все вопросы задания не имеют полного решения. Содержание ответов свидетельствует о слабых знаниях выпускника и о его неумении решать профессиональные задачи.

4. СОДЕРЖАНИЕ ПРОГРАММЫ ГОСУДАРСТВЕННОГО МЕЖДИСЦИПЛИНАРНОГО ЭКЗАМЕНА

4.1. Дисциплина «Программно-аппаратные средства защиты информации»

1. Информационная безопасность в компьютерных системах

Компьютерная система как объект защиты информации. Понятие угрозы информационной безопасности в КС. Классификация и общий анализ угроз информационной безопасности в КС. Случайные угрозы информационной безопасности.

2. Понятие политики безопасности в компьютерных системах

Разработка политики информационной безопасности. Методология политики безопасности компьютерных систем. Основные положения политики информационной безопасности. Жизненный цикл политики безопасности. Принципы политики безопасности.

3.Идентификации субъекта

Понятие протокола идентификации. Идентифицирующая информация. Пароли. Программно-аппаратные средства идентификации и аутентификации пользователей. Идентификации субъекта. Понятие протокола идентификации. Идентифицирующая информация. Пароли. Идентификация и аутентификация. Основные понятия и классификация.

4. Простая аутентификация

Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация, на основе сертификатов.

5. Биометрическая идентификация и аутентификация пользователей

Строгая аутентификация. Биометрическая идентификация и аутентификация пользователей. Строгая аутентификация. Протоколы аутентификации с симметричными алгоритмами шифрования. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций.

6. Аутентификация с использованием асимметричных алгоритмов шифрования

Электронная цифровая подпись (ЭЦП). Аутентификация, основанная на использовании цифровой подписи. Протоколы аутентификации с нулевой передачей значений.

Упрощенная схема аутентификации с нулевой передачей знаний. Параллельная схема аутентификации с нулевой передачей знаний.

7. Системы идентификации и аутентификации

Классификация систем идентификации и аутентификации. Особенности электронных систем идентификации и аутентификации. Организация хранения ключей (с примерами реализации) Комбинированные системы. Бесконтактные смарт-карты и USB-ключи. Гибридные смарт-карты. Биоэлектронные системы. Ключи. Организация хранения ключей. Распределение ключей. Использование комбинированной криптосистемы. Метод распределения ключей Диффи-Хеллмана. Протокол вычисления ключа парной связи ECKEP.

8. Основные подходы к защите данных от НСД

Защита ПЭВМ от несанкционированного доступа. Программно-аппаратные средства шифрования. Защита алгоритма шифрования. Необходимые и достаточные функции аппаратного средства криптозащиты. Построение аппаратных компонент криптозащиты данных. Устройства криптографической защиты данных серии КРИПТОН. Устройства для работы со смарт-картами. Системы защиты информации от несанкционированного доступа

9. Модель компьютерной системы

Методы и средства ограничения доступа к компонентам ЭВМ. Понятие изолированной программной среды. Понятие доступа и монитора безопасности. Обеспечение гарантий выполнения политики безопасности. Методология проектирования гарантированно защищенных КС. Метод генерации изолированной программной среды. Контроль доступа. Разграничения доступа. Иерархический доступ к файлам. Фиксация доступа к файлам. Способы фиксации фактов доступа. Доступ к данным со стороны процесса. Надежность систем ограничения доступа. Модели управления доступом. Системы разграничения доступа. Диспетчер доступа. Списки управления доступом к объекту. Списки полномочий субъектов. Атрибутные схемы.

10. Программные и аппаратные средства защиты компьютерных информационных систем

Защита программ от несанкционированного копирования. Подходы к защите информационных систем. Устойчивость к прямому копированию. Устойчивость к взлому. Аппаратные ключи. Структура системы защиты от несанкционированного копирования. Блок установки характеристик среды. Защита дискет от копирования. Электронные ключи HASP. Защита сетевого файлового ресурса. ЗАЩИТА ФАЙЛОВОЙ СИСТЕМЫ WINDOWS Шифрование. Разрешения для файлов и папок. Шифрующая файловая система (EFS) Encrypting File System. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing). Процесс шифрования. Процесс дешифрования. Процесс восстановления. Администрирование дисков в Windows. Защита программ. Защита программ на жестком диске. Обзор современных средств защиты. Защита файлов от изменения. Защита программ от изучения. Защита от дизассемблирования. Защита от

отладки. Защита от трассировки по прерываниям. Защита от исследований. проблемы хакера. Защита от исследований на уровне текстов. Защита от исследований в режиме отладки. Защита программ от трассировки.

4.2 Дисциплина «Техническая защита информации»

1. *Основы технической информации*

Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Свойства и виды информации Виды, источники и носители защищаемой информации.Демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники. Средства и методы технической разведки. Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой. Способы и средства перехвата сигналов. Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации.

2. *Каналы утечки информации*

Технические каналы утечки информации. Характеристики технических каналов утечки информации, физические принципы технических каналов передачи информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Электрические каналы утечки информации. Электромагнитные каналы утечки информации. Акустические каналы утечки информации. Виброакустические каналы утечки информации. Материально-вещественные каналы утечки информации. Комплексное использование каналов утечки информации. Средства обнаружения технических каналов утечки информации. Средства обнаружения и локализации закладных устройств. Нелинейные локаторы. Сканирующие приёмники. Детекторы электромагнитного поля. Программно-аппаратные автоматизированные комплексы. Досмотровая техника.

3. *Мероприятия по выявлению средств технической разведки*

Защита информации по ТКУИ и методы контроля защиты. Методы и средства защиты информации от утечки по техническим каналам. Пассивные и активные методы защиты. Скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов. Обнаружение и локализация закладных устройств, подавление их сигналов; экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания. Концепция и методы инженерно-технической защиты информации; методы и средства инженерной защиты и технической охраны объектов. Виды контроля эффективности защиты информации; физические принципы контроля защиты информации; основные положения методологии инженерно-технической защиты информации. Методы расчета и инструментального контроля показателей защиты информации. Средства измерения при инструментальном контроле.

4.3 Дисциплина «Безопасность вычислительных сетей»

1. Основные понятия компьютерных сетей

Основные понятия. История развития ЭВМ. Типы и характеристики линий связи: кабельные каналы; радиоканалы. Высокоскоростные системы цифровой передачи: методы передачи на канальном уровне; основные методы коммуникаций. Многоуровневый подход: декомпозиция задачи сетевого взаимодействия; протокол, интерфейс, стек протоколов. Модель OSI: общая характеристика модели; семь уровней эталонной модели. Стандартизация сетей: понятие «открытая система»; модульность и стандартизация; стандартные стеки коммуникационных протоколов. IP-адресация.

2. Локальные вычислительные сети (ЛВС)

Классификация сетей. Основные понятия локальных сетей. Организация взаимодействия устройств в сети: одноранговые сети; сети с выделенным сервером; технологии общего использования сетевых ресурсов. Сетевые топологии. Методы доступа и протоколы передачи в ЛВС. Стандарты в области локальных сетей института IEEE 802.x. Базовые технологии (архитектуры) локальных сетей: Ethernet; Token Ring; Arcnet; FDDI. Сравнение технологий и выбор конфигурации сети. Многоуровневая модель сети: компьютеры; коммуникационное оборудование; операционные системы; сетевые приложения. Аппаратные средства сетей: серверы; рабочие станции; сетевые карты; сетевое оборудование ЛВС; кабели. Программные компоненты: сетевые операционные системы; сетевые приложения. Подключение ПК к локальной сети. Настройка сетевых компонентов ЛВС. NAT. DNS.

3. Сетевые приложения Internet

Понятие браузера. Приложение Internet Explorer. Установка и настройка Internet Explorer. Методы подключение к Internet. Поиск информации. Работа с Web-страницами. Принципы работы электронной почты (SMTP, POP3, IMAP). Почтовые системы на основе WWW. Электронные адреса. Приложение Thunderbird. Настройка Thunderbird. Работа с сообщениями.

4.4 Дисциплина «Безопасность операционных систем»

1. Общие сведения об операционных системах

Понятие операционной системы. Цели и задачи операционной системы. Основная классификация операционных систем Общие сведения об операционных системах. Архитектура операционных систем. Основные принципы построения операционных систем. (принципы модульности, особого режима работы, виртуализации, мобильности, совместимости, генерируемости, открытости, обеспечение безопасности вычислений). Требования к современным операционным системам реального времени (RealTimeOS, RTOS). Понятие интерфейсов пользователя. Виды интерфейсов.

2. Файлы и каталоги. Управление правами доступа

Файловые системы. Цели и задачи файловой системы. Структура файловой системы. Иерархическая структура файловой системы. Типы файлов. Имена файлов. Атрибуты файлов. Основные операции при работе с файлами (создание, удаление, переименование, копирование, создание жесткой ссылки, вывод содержимого файла, вывод содержимого файла в соответствии с заданными условиями). Управление правами доступа. Категории

пользователей в операционных системах. Атрибуты защиты файла/каталога. Изменение кодов защиты для файлов/каталогов. Основные операторы задания прав доступа.

3. Сети и сетевые структуры

Сетевые и распределенные операционные системы. Классические и современные сетевые коммуникационные протоколы. Установка виртуальной компьютерной сети на основе операционных систем Windows. Установка и настройка протокола TCP/IP.

4. Установка и настройка операционных систем

Безопасность в операционных системах. Основные типы угроз. Основные типы вредоносных программ. Основные средства защиты: брандмауэры, антивирусные технологии, электронная подпись программ. Сетевая аутентификация на основе многоразового пароля. Аутентификация на основе сертификатов. Аутентификация на основе биометрических данных. Идентификация. Авторизация. UID. Security Account Manager. Политика безопасности. Политика аудита.

4.5 Дисциплина «Безопасность систем базы данных»

1. Работа с базами данных

Обзор баз данных SQL Server. Работа с файлами и файловыми группами. Перемещение файлов баз данных. Создание базы данных.

2. Аутентификация и авторизация пользователей

Проверка подлинности подключений к SQL Server. Авторизация имен входа (LOGIN) для доступа к базам данных. Авторизация на серверах. Работа с ролями сервера. Работа с фиксированными ролями базы данных. Создание пользовательских ролей базы данных.

3. Работа с типами данных

Использование типов данных. Работа с символьными данными. Преобразование типов данных. Специализированные типы данных.

4. Проектирование и реализация таблиц

Проектирование таблиц. Работа со схемами. Создание и изменение таблиц. Принудительное обеспечение целостности данных. Реализация сущностной и ссылочной целостности. PRIMARY KEY, CHECK, UNIQUE и FOREIGN KEY.

5. Проектирование и реализация представлений

Введение в представления. Создание и управление представлениями.

6. Проектирование и реализация хранимых процедур

Введение в хранимые процедуры. Работа с хранимыми процедурами. Работа с триггерами.

7. Модели восстановления SQL Server

Стратегии резервного копирования в SQL Server. Работа журнала транзакций в SQL Server. Резервное копирование баз данных и журналов транзакций. Управление резервными копиями базы данных. Работа с параметры резервного копирования. Общие сведения о процессе восстановления. Восстановление баз данных. Восстановление к точке по времени. Восстановление системных баз данных и отдельных файлов.

4.6. Дисциплина «Криптографические методы защиты информации»

1. Вводная лекция. Основные понятия криптографии. Задачи и цели дисциплины. Криптографическая система. Криптология- криптография и криптоанализ. Шифрование и дешифрование.

2. Исторические и классические шифры.Экскурс к истории криптографии. Криптографические системы –древнего мира, эпохи возраждения, XIX- века и начало XX века. Методы шифрования и дешифрования.

3. Классификация шифров и математическая модель шифров. Классификация классических система шифрования. Современная классификация. Математическая модель шифров. Поля, кольца, арифметика остатков.

4. Криптографические свойства и характеристики открытых текстов. Свойства открытых текстов. Методы сжатия информации. Избыточность открытых текстов. Криптоанализ классических шифров на основе частот букв различного алфавита

5. Теоретико-информационная стойкость шифров. Понятие стойкости шифров. Абсолютная стойкость. Дифференциальный и линейный анализ на стойкость. Методы атак на криптографические системы

6. Симметричные системы шифрования. Основы современных систем шифрования. Ключи и их размеры. Требования к системе и ключам. Классы реализующие симметричные системы шифрования на платформе .NET

7. Стандарт шифрования DES. Американский стандарт шифрования. Сеть Фейстеля. Количество раундов. Понятия S-блоков. Начальная и конечные перестановки. Анализ системы DES

8. Стандарт шифрования AES. Конкурс для нового стандарта. Алгоритмы. Шаги для шифрования. Отличия от DES. Программная реализация. Методы анализа шифра

9. Ассиметричные системы шифрования. Появление ассиметричной системы. Проблемы распределения ключей. Требования к ключам. Представители ассиметричных классов.

10. Криптографические библиотеки в операционных системах. Криптографические библиотеки и их применение. API. Доступ к библиотекам. Производительность шифров.

11. Стандарт шифрования RSA. История RSA. Алгоритм генерации ключа и процесса шифрования. Открытый и закрытый ключ. Криптоанализ.

12. Хэш-функции и стандарты. Стандарты генерации хеш значения и алгоритмы. Стойкость алгоритмов. Понятия коллизий.

13. Электронно-цифровая подпись RSA и DAS. Электронная подпись. Понятия подписи и верификации. Современные алгоритмы ЭЦП и их стойкость. Преимущества и недостатки.

14. Управление ключами и проблемы их распределения. Проблемы управления ключами. Инфраструктура открытых ключей. Симметричные и ассиметричные ключи. Удостоверяющий центр

15. Криптографические протоколы. Понятие протоколов. Криптографические протоколы и их классификация. Задачи решаемые протоколами. Применение протоколов в сетевой инфраструктуре.

5. ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

Список вопросов экзаменационного билета для государственного экзамена по направлению 590100 – «Информационная безопасность» составлен из следующих дисциплин:

Дисциплина «Программно-аппаратные средства защиты информации»

1. Простая аутентификация. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация, на основе сертификатов.
2. Биометрическая идентификация и аутентификация пользователей. строгая аутентификация. Биометрическая идентификация и аутентификация пользователей. Строгая аутентификация. Протоколы аутентификации с симметричными алгоритмами шифрования.
3. Аутентификация с использованием асимметричных алгоритмов шифрования. Электронная цифровая подпись (ЭЦП). Аутентификация, основанная на использовании цифровой подписи.
4. Системы идентификации и аутентификации. Классификация систем идентификации и аутентификации. Особенности электронных систем идентификации и аутентификации. Организация хранения ключей (с примерами реализации) Комбинированные системы.
5. Бесконтактные смарт-карты и USB-ключи. Гибридные смарт-карты. Биоэлектронные системы.
6. Ключи. Организация хранения ключей (с примерами реализации). Распределение ключей.
7. Использование комбинированной криптосистемы. Метод распределения ключей Диффи-Хеллмана. Протокол вычисления ключа парной связи ЕСКЕР.
8. Основные подходы к защите данных от НСД. Защита ПЭВМ от несанкционированного доступа.
9. Программно-аппаратные средства шифрования. Защита алгоритма шифрования. Необходимые и достаточные функции аппаратного средства криптозащиты.

Построение аппаратных компонент криптозащиты данных.

10. Методы и средства ограничения доступа к компонентам ЭВМ. Понятие изолированной программной среды. Понятие доступа и монитора безопасности.
11. Метод генерации изолированной программной среды.
12. Контроль доступа. Разграничения доступа. Иерархический доступ к файлам. Фиксация доступа к файлам. Способы фиксации фактов доступа. Доступ к данным со стороны процесса.
13. Программные и аппаратные средства защиты компьютерных информационных систем. Защита программ от несанкционированного копирования.
14. Подходы к защите информационных систем. Устойчивость к прямому копированию. Устойчивость к взлому. Аппаратные ключи. Структура системы защиты от несанкционированного копирования. Блок установки характеристик среды. Защита дискет от копирования.
15. Электронные ключи HASP
16. Защита сетевого файлового ресурса. Разрешения для файлов и папок. Шифрующая файловая система (EFS) Encrypting File System.
17. Взаимодействие файловой системы защиты NTFS и защиты ресурса общего доступа (Sharing). Процесс шифрования. Процесс дешифрования. Процесс восстановления. Администрирование дисков в Windows
18. Программные и аппаратные средства защиты компьютерных информационных систем. защита программ. Защита программ на жестком диске. Обзор современных средств защиты.
19. Защита файлов от изменения. Защита программ от изучения. Защита от дизассемблирования. Защита от отладки. Защита от трассировки по прерываниям. Защита от исследований. проблемы хакера. Защита от исследований на уровне текстов. Защита от исследований в режиме отладки. Защита программ от трассировки.
20. Базовые методы нейтрализации систем защиты от несанкционированного использования. Понятие и средства обратного проектирования.
21. Локализация кода модуля защиты посредством отлова WinAPI функций в режиме отладки. Базовые методы противодействия отладчикам.
22. Базовые методы противодействия дизассемблированию ПО.
23. Использование недокументированных инструкций и недокументированных возможностей процессора. Шифрование кода программы как универсальный метод противодействия отладке и дизассемблированию.
24. Защита от разрушающих программных воздействий. Компьютерные вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Классификация вирусов.
25. Механизмы заражения компьютерными вирусами. Признаки появления вирусов. Методы и средства защиты от компьютерных вирусов.
26. Компьютерные вирусы. Методы защиты. Антивирусные средства. Профилактика заражения вирусами компьютерных систем. Антивирус. Алгоритм работы. Проверочные механизмы. Постоянная проверка и проверка по требованию.
27. Структура антивирусной защиты предприятия. Функциональные требования. Общие требования. Пример вируса.
28. Программные методы защиты сетевых технологий в Internet структурах.

29. Защита данных в электронных платежных системах.
30. Принципы функционирования электронных платежных систем.

Дисциплина «Криптографические методы защиты информации»

1. Исторические шифры (Цезарь, Сцитала, Квадрат Полибия, шифр Виженера)
2. Управление, распределение ключей ассиметричных систем. Протоколы, выбор ключа и метод проверок протоколов
3. ЭЦП – задачи, технологии и алгоритмы
4. Хеш – алгоритмы и свойства
5. PKI – инфраструктура
6. Симметричные системы - модель, типы атак
7. Блочные и поточные шифры – преимущества и недостатки
8. Наука криптология – криптография и криптоанализ
9. Стандарт шифрования DES – ключи, раунды, способы реализации
10. Режимы сцепления блоков симметричных систем – цель и характеристики
11. Криптография в платформе .NET – иерархия и описание классов
12. Криптографическая система RSA – история, описания алгоритма
13. Стандарт шифрования AES – история конкурса, операции алгоритма
14. Ассиметричная система – проблемы и идеи
15. Характеристика открытых текстов, частотый анализ
16. Шифр Енигма
17. Математические основы криптографии – группы, кольца, модульная арифметика
18. Теоретико-информационная стойкость шифров
19. Криптографическая система – описание, состав
20. Задачи криптографии
21. Классификация шифров
22. Тест Казисского
23. Принцип Керкгоффса
24. Библиотеа CryptoAPI Windows
25. Алгоритмы ЭЦП-DSA
26. Алгоритмы ЭЦП-RSA
27. Гаммирование – выработка, алгоритмы и их характеристики
28. Теория абсолютно стойких систем
29. Дифференциальный и линейный анализ на стойкость
30. Применение «соли» в хеш алгоритмах

Дисциплина «Техническая защиты информации»

1. Источники конфиденциальной информации.
2. Организационные каналы обмена и передачи информации.
3. Виды технических каналов утечки информации
4. Электромагнитный канал утечки информации
5. Индукционный канал утечки информации
6. Виброакустический канал утечки информации
7. Параметрический канал утечки информации
8. Технические каналы утечки видовой информации
9. Технические каналы утечки информации. Структура и классификация.
10. Технические каналы утечки информации. Основные характеристики.
11. Технические каналы утечки информации при передаче ее по каналам связи.

12. Технические каналы утечки речевой информации
13. Демаскирующие признаки объектов. Общие положения.
14. Демаскирующие признаков в видимом диапазоне электромагнитного спектра.
15. Технические характеристики радиосигналов.
16. Системы технической защиты.
17. Концепция и методы инженерно-технической защиты информации
18. Понятие экранирования. Основные положения
19. Фильтрация информационных сигналов.
20. Виды помехоподавляющих фильтров
21. Методика выбора типа фильтров.
22. Типовые схемы фильтров

Дисциплина «Безопасность вычислительных сетей»

1. Модель TCP/IP.
2. Модель OSI.
3. Виртуальная частная сеть (VPN).
4. Прокси-серверы.
5. Сервис NAT.
6. ARP и RARP протоколы.
7. Адресация в IP сетях. Использование маски подсети.
8. TCP и UDP протоколы.
9. DNS протокол.
10. Сервис DHCP.
11. Утилита nslookup.
12. VLAN.
13. Демилитаризованная зона (DMZ).
14. Протоколы email (SMTP, POP3, IMAP).
15. Протокол SNMP.
16. Системы обнаружения вторжения (IDS).
17. Снифферы.

Дисциплина «Безопасность операционных систем»

1. Функции ОС.
2. Идентификация, аутентификация, авторизация.
3. Дискреционная модель разграничения доступа.
4. Мандатная модель разграничения доступа.
5. Политика безопасности.
6. Политика аудита.
7. Групповая политика.
8. Файловая система FAT, NTFS.
9. Межсетевой экран.
10. Реестр.
11. Механизм хранения паролей в ОС Windows и Linux.
12. ОС Linux, система прав доступа.
13. Вирусы. Черви. Троянские программы.
14. DoS, DDoS-атака.
15. Журналирование.
16. Сканирование портов.

17. Цифровая подпись.
18. Протокол аутентификации Kerberos.
19. Конфиденциальность.
20. Целостность.
21. Доступность.

Дисциплина «Безопасность систем базы данных»

1. DDL (язык определения данных).
2. DCL (язык управления данными).
3. DML (язык манипулирования данными).
4. Виды аутентификации в MS SQL Server.
5. Операторы GRANT и REVOKE.
6. Оператор DENY.
7. Резервное копирование базы данных.
8. Восстановление базы данных.
9. Фиксированные роли базы данных.
10. Нормализация базы данных.
11. Денормализация базы данных.
12. Какая разница между TRUNCATE и DELETE?
13. Понятие Триггер (trigger).
14. Понятие Представления (view).
15. Основные ограничения PRIMARY KEY, CHECK, UNIQUE и FOREIGN KEY.
16. Соединение таблиц. Типы join.
17. База данных model
18. Синтаксис использования предикатов BETWEEN, IN, LIKE в запросах SQL.
19. Модель «сущность-связь» или ER-модель.

Рекомендации обучающимся для успешной сдачи государственного аттестационного экзамена и выпускной квалификационной работы необходимо приобретение учащимися необходимых теоретических знаний и практических навыков, достаточных для использования современных информационных технологий для решения задач предотвращения и ликвидации ЧС, пожаров с целью минимизации времени, необходимого на принятие решения, а также оптимизации принимаемых действий.

Достижение этой цели последовательно осуществляется всеми формами проведения аудиторных занятий, при выполнении следующих действий обучающимися:

- лекционный курс – ведение конспекта, подготовка к теме лекции по рекомендованному списку литературы, просматривание записей предыдущей лекции с целью восстановления в памяти ранее изученного материала;
- лабораторные работы – подготовка к теме занятия по конспекту лекции, рекомендованным разделам учебных пособий.

Результаты учебной деятельности зависят от уровня самостоятельной работы обучающегося, который определяется личной подготовленностью к этому труду, желанием заниматься самостоятельно и возможностями реализации этого желания. Самостоятельная учебная деятельность является определяющим условием в достижении высоких результатов обучения, так как без самостоятельной работы невозможно превращение полученных знаний в умения и навыки.

Самостоятельная учебная деятельность должна строиться на следующих основных принципах:

– систематичности, последовательности, преемственности в самостоятельной работе;

– связи теории с практикой;

– сознательности и активности;

– прочности усвоения знаний.

К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет наличие у выпускников определенных способностей и умения самостоятельно добывать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной финансовой ситуации. Формирование такого умения происходит в течение всего периода обучения через участие студентов в практических занятиях, выполнение контрольных заданий и тестов, написание курсовых и выпускных квалификационных работ.

Учебный процесс в высшем учебном заведении в значительной степени строится на самостоятельной работе студентов, без которой трудно в полной мере овладеть сложным программным материалом и научиться в дальнейшем постоянно совершенствовать приобретенные знания и умения. Самостоятельная работа является внеаудиторной и предназначена для самостоятельного ознакомления студента с определенными разделами курса по рекомендованным педагогом материалам и подготовки к выполнению индивидуальных заданий по курсу.

Целью самостоятельной работы студентов является:

- научить студента осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение в дальнейшем непрерывно повышать свою квалификацию;

- закрепление, расширение и углубление знаний, умений и навыков, полученных студентами на аудиторных занятиях под руководством преподавателей;
изучение студентами дополнительных материалов по изучаемым дисциплинам и умение выбирать необходимый материал из различных источников;

- воспитание у студентов самостоятельности, организованности, самодисциплины, творческой активности, потребности развития познавательных способностей и упорства в достижении поставленных целей.

Правильный подход к освоению материала усиливает мотивацию к аудиторной и внеаудиторной активности, что обеспечивает необходимый уровень знаний по изучаемым дисциплинам и позволяет повысить готовность студентов к сдаче экзаменов.

Список литературы для подготовки к государственной итоговой аттестации по направлению подготовки 590100 -«Информационная безопасность»

Дисциплина «Программно-аппаратные средства защиты информации»

1. ЭБС «Znanium. com.» Хорев, П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с. – Режим доступа: http://znanium.com/
2. Борисов, М.А. Основы программно-аппаратной защиты информации : учеб. пособие для студентов вузов / М.А. Борисов, И.В. Заводцев, И.В. Чижов. - М. : ЛИБРОКОМ, 2012. - 376 с.
3. ЭБС «Znanium. com.» Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. – Режим доступа: http://znanium.com/
4. Основы информационной безопасности : учеб. пособие для студентов вузов / Е.Б. Белов [и др.]. - М. : Горячая линия - Телеком, 2006. - 544 с.

5. Мельников, В.П. Информационная безопасность и защита информации : учеб. пособие для студентов вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - М. : Академия, 2008. - 336 с.

Дисциплина «Криптографические методы защиты информации»

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.А. Основы криптографии. Учебное пособие. – М.:Гелиос-АРВ, 2011
2. Дернова Е.С., Молдовян Д.Н., Молдовян Н.А. – СПб. Изд. СПбГЭТУ, 2010.-100с.
3. П. Торстейнсон, Г. А. Ганеш. КРИПТОГРАФИЯ И БЕЗОПАСНОСТЬ В ТЕХНОЛОГИИ .NET. БИНОМ. Лаборатория знаний. 2013. 459 с.
4. Столлингс В. Криптография и защита сетей. Принципы и практика 2-е изд. – М: Вильямс, 2010
5. Варфоломеев А.А., Домнина О.С., Пеленицын М. Б. Управление ключами в системах криптографической защиты банковской информации.-М.:МИФИ, 2006

Дисциплина «Техническая защиты информации»

1. Власов, И.И. Техническая диагностика современных цифровых сетей связи. Основные принципы и технические средства измерений парамет-ров передачи для сетей PDH, SDH, IP, Ethernet и ATM / И.И. Власов, Э.В. Новиков, М.М. Птичников, Д.В. Сладких. - М.: ГЛТ , 2014. - 552 с.
2. Гагарина, Л.Г. Технические средства информатизации: Учебное пособие / Л.Г. Гагарина. - М.: ИД ФОРУМ, 2013. - 256 с.
3. Древс, Ю.Г. Технические и программные средства систем реального времени: Учебник / Ю.Г. Древс. - М.: Бином, 2015. - 334 с.
4. Зайцев, А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. - М.: РиС, 2014. - 442 с.
5. Зайцев, А.П. Технические средства и методы защиты информации: Учебное пособие / А.П. Зайцев, А.А. Шелупанов. - М.: ГЛТ, 2012. - 616 с.

Дисциплина «Безопасность вычислительных сетей»

1. Компьютерные сети. Принципы, технологии, протоколы. 4-е издание. В.Олифер, Н.Олифер. 2010
2. Компьютерные сети. 5-е издание. Э.Таненбаум, Д.Уэзеролл. 2012

Дисциплина «Безопасность операционных систем»

1. Внутреннее устройство Microsoft Windows. 6-е издание. Часть 1. М.Руссинович, Д.Соломон. 2013
2. Внутреннее устройство Microsoft Windows. 6-е издание. Часть 2. М.Руссинович, Д.Соломон. 2014
3. Утилиты Sysinternals. Справочник администратора. Руссинович Марк, Маргозис Аарон. 2012

Дисциплина «Безопасность систем базы данных»

1. Microsoft SQL Server 2012. Руководство для начинающих. Душан Петкович. 2013
2. SQL. Полное руководство. 3-е издание. Джеймс Грофф, Пол Вайнберг, Эндрю Оппель 2015

3. SQL Server 2008 R2. Black book. Published by: Dreamtech PRESS, 19-A, Ansari Road, Daryaganj, New Delhi, 2012 -1135 p
4. В.В.Дунаев. Базы данных Язык SQL для студента. 2-е издание . – СПб.: БХВ-Петербург, 2012. -320 с.
5. С.Д.Кузнецов. Базы данных. Модели данных. Учебник – М.: ООО «Бином-Пресс», 2008 г. 720 с.