МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. И. РАЗЗАКОВА

СПО (КОЛЛЕДЖ)

«УТВЕРЖДАЮ»
Директор СПО (Колледж)
_____ Дербишева Э.Д.
(попись)
«___» _____ 2024 г.

ПРОГРАММА
ИТОГОВОЙ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

Уровень основной профессиональной образовательной программы	**Среднее профессиональное образование (СПО)**
Специальность	**100203 «Информационная безопасность автоматизированных систем»**
Квалификация	**Техник по защите информации**
Форма обучения	**Очная**

Бишкек – 2024

Программа итоговой государственной аттестации для студентов среднего профессионального образования по специальности 100203 «Информационная безопасность автоматизированных систем» / КГТУ им. И. Раззакова; Сост. Н.А.Оморова, Б.А. Маматалиева, Б.Т.Ткачева. – Бишкек, 2024. – 16 с.

Предназначена для студентов 3 курса среднего профессионального образования по специальности 100203 «Информационная безопасность автоматизированных систем» СПО (Колледжа) КГТУ им. И. Раззакова.

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Программа итоговой государственной аттестации (далее - ИГА) разработана на основе:

- Закона Кыргызской Республики «Об образовании».
- Положении об итоговой государственной аттестации выпускников образовательной организации среднего профессионального образования Кыргызской Республики, утвержденный ПП КР от 4 июля 2012 года N 470.
- Государственного образовательного стандарта среднего профессионального образования по специальности «Информационная безопасность автоматизированных систем», утвержденного Министерством образования и науки КР № 863\1 от 10.05.2022 г.
- Типового учебного плана утвержденного приказом МОиН КР № 443\1 от 13.04.2018 г.

2. Итоговая аттестация представляет собой форму оценки степени и уровня освоения обучающимися основной образовательной программы.

3. Итоговая аттестация проводится на основе принципов объективности и независимости оценки качества подготовки обучающихся.

4. Целью государственной итоговой аттестации является установление степени готовности обучающегося к самостоятельной деятельности, сформированности профессиональных компетенций в соответствии с Государственного образовательного стандарта среднего профессионального образования по специальности 100203 «Информационная безопасность автоматизированных систем».

5. Главной задачей по реализации требований Государственного образовательного стандарта является реализация практической направленности подготовки специалистов со средним профессиональным образованием. Конечной целью обучения является подготовка специалиста, обладающего не только и не столько совокупностью теоретических знаний, но, в первую очередь, специалиста, готового решать профессиональные задачи.

6. Формой государственной итоговой аттестации выпускников специальности СПО 100203 «Информационная безопасность автоматизированных систем» является сдача итогового междисциплинарного экзамена по дисциплинам:

- Криптографические методы и защиты информации;
- Программно-аппаратные средства автоматизированных систем;
- Основы информационной безопасности.

7. В программе государственной итоговой аттестации определены:

- материалы по содержанию итоговой аттестации;

- сроки проведения государственной итоговой аттестации;
- условия подготовки и процедуры проведения государственной итоговой аттестации;
- критерии оценки уровня качества подготовки выпускника.

8. Программа государственной итоговой аттестации, а также критерии оценки знаний выпускников рассматриваются на заседании предметно-цикловой комиссии «ИБАС» и отделения «Управление и IT» протокол №2 от 04 октября 2019 года и утверждаются председателем методического совета СПО (Колледжа) КГТУ им. И. Раззакова протокол №5 от 27 декабря 2019 года.

1. ПАСПОРТ ПРОГРАММЫ ИТОГОВОЙ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

1.1. Область применения программы итоговой государственной аттестации

Программа итоговой государственной аттестации (далее - ИГА) является частью программы подготовки специалистов среднего звена в соответствии с ГОС СПО по специальности 100203 «Информационная безопасность автоматизированных систем» в части освоения видов профессиональной деятельности:
- Эксплуатация подсистем безопасности автоматизированных систем;
- Применение программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности в автоматизированных системах;

и соответствующих профессиональных компетенций: **профессиональными (ПК):**

ПК-1. Владеть основными методами и средствами разработки программного обеспечения.
ПК-5. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах;
ПК-6. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах;
ПК-9. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;
ПК-10. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

1.2. Цели и задачи итоговой государственной аттестации

Целью итоговой государственной аттестации является установление соответствия уровня освоенности компетенций, обеспечивающих соответствующую квалификацию и уровень образования обучающихся, макету государственному образовательному стандарту среднего профессионального образования. ИГА призвана способствовать систематизации и закреплению знаний и умений обучающегося по специальности при решении конкретных профессиональных задач, определить уровень подготовки выпускника к самостоятельной работе.

2. СТРУКТУРА И СОДЕРЖАНИЕ ИТОГОВОЙ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

2.1. Форма проведения итоговой государственной аттестации

Итоговая государственная аттестация выпускников специальности «Информационная безопасность автоматизированных систем» состоит из итоговых экзаменов по дисциплинам:

- Криптографические методы и защиты информации;
- Программно-аппаратные средства защиты информации;
- Основы информационной безопасности.

Итоговый экзамен по отдельной дисциплине должен определять уровень усвоения студентом материала, предусмотренного учебной программой, и охватывать все минимальное содержание данной дисциплины, установленное соответствующим государственным образовательным стандартом.

2.2. Содержание программы итоговой государственной аттестации

Дисциплина «Криптографические методы и защиты информации»

Тема. Основные понятия криптографии.

Криптографическая система. Криптология, криптография и криптоанализ. Шифрование и дешифрование. Исторические и классические шифры. Экскурс к истории криптографии. Криптографические системы – древнего мира, эпохи возрождения, XIX–века и начало XX века.

Тема. Методы шифрования и дешифрования.

Классификация шифров и математическая модель шифров. Классификация классических система шифрования. Современная классификация. Математическая модель шифров. Поля, кольца, арифметика остатков. Криптографические свойства и характеристики открытых текстов. Свойства открытых текстов. Методы сжатия информации. Избыточность открытых текстов. Криптоанализ классических шифров на основе частот букв различного алфавита

Тема. Теоретико-информационная стойкость шифров.

Понятие стойкости шифров. Абсолютная стойкость. Дифференциальный и линейный анализ на стойкость. Методы атак на криптографические системы.

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

Тема. Стандарт шифрования.

Стандарт шифрования DES. Американский стандарт шифрования. Сеть Фейстеля. Количество раундов. Понятия S-блоков. Начальная и конечные перестановки. Анализ системы DES. Стандарт шифрования AES. Конкурс для нового стандарта. Алгоритмы. Шаги для шифрования. Отличия от DES. Программная реализация. Методы анализа шифра. Ассиметричные системы шифрования. Появление ассиметричной системы. Проблемы распределения ключей. Требования к ключам. Представители ассиметричных классов.

Тема. Криптографические библиотеки в операционных системах.

Криптографические библиотеки и их применение API. Доступ к библиотекам. Производительность шифров. Стандарт шифрования RSA. История RSA. Алгоритм генерации ключа и процесса шифрования. Открытый и закрытый ключ. Криптоанализ. Хэш-функции и стандарты. Стандарты генерации хеш значения и алгоритмы. Стойкость алгоритмов. Понятия коллизий.

Тема. Электронно-цифровая подпись

-цифровая подпись RSA и DAS. Электронная подпись. Понятия подписи и верификации. Современные алгоритмы ЭЦП и их стойкость. Преимущества и недостатки. Управление ключами и проблемы их распределения. Проблемы управления ключами. Инфраструктура открытых ключей. Симметричные и ассиметричные ключи. Удостоверяющий центр. Криптографические протоколы. Понятие протоколов. Криптографические протоколы и их классификация. Задачи решаемые протоколами. Применение протоколов в сетевой инфраструктуре.

Дисциплина «Программно-аппаратные средства защиты информации»

Тема. 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.

Тема. 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.

Тема. 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. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация, на основе сертификатов. Строгая аутентификация. Биометрическая идентификация и аутентификация пользователей. Строгая аутентификация. Протоколы аутентификации с симметричными алгоритмами шифрования. Протоколы, основанные на использовании однонаправленных ключевых хэш-функций.

Тема. 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. 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 ЕСКЕР.

Тема. 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

Тема. 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.

Тема. 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.

Дисциплина «Основы информационной безопасности»

Тема. Концепция информационной безопасности.

Введение в понятие информационной безопасности. Основные составляющие информационной безопасности. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.

Тема. Угрозы безопасности информации

Основные определения и критерии классификации угроз. Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.

Тема. Основные направления защиты информации

Международные и государственные стандарты информационной безопасности и их использование в практической деятельности. Законодательный, административный и процедурный уровень информационной безопасности. Программно-технического уровня информационной безопасности. Основные понятия, механизмы безопасности, классы безопасности, информационная безопасность распределенных систем, рекомендации X.800, администрирование средств безопасности. Стандарты информационной безопасности и критерии оценки безопасности компьютерных систем и сетей. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".

Тема. Способы защиты информации

Методология защиты информации. Сервиса безопасности, анализ защищенности, обеспечение отказоустойчивости, обеспечение безопасного восстановления. Идентификация и аутентификация, управление доступом. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит. Многоуровневая защита корпоративных сетей. Экранирование. Туннелирование.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ИТОГОВОЙ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

3.1. Общие требования к организации и проведению итоговой государственной аттестации

1. Для проведения ИГА создается Государственная аттестационная комиссия в порядке, предусмотренном в Положении об итоговой государственной аттестации выпускников образовательной организации среднего профессионального образования Кыргызской Республики, утвержденный ППКР от 4 июля 2012 года N 470, которая формируется из преподавателей колледжа, лиц, приглашенных из сторонних организаций и представителей работодателей по профилю подготовки.

2. Основными функциями государственной аттестационной комиссии являются:

- определение соответствия подготовки выпускника требованиям макета государственного образовательного стандарта среднего профессионального образования;

принятие решения о присвоении профессиональной квалификационной или академической степени по результатам итоговой государственной аттестации и выдаче выпускнику соответствующего документа государственного образца о среднем профессиональном образовании;

разработка рекомендаций, направленных на совершенствование подготовки выпускников на основании результатов работы государственной аттестационной комиссии.

3. Кандидатура председателя государственной аттестационной комиссии по специальности утверждается Министерством образования и науки Кыргызской Республики.

4. Государственные аттестационные комиссии действуют в течение одного календарного года.

5. Государственную аттестационную комиссию возглавляет председатель, который организует и контролирует деятельность комиссии, обеспечивает единство требований, предъявляемых к выпускникам.

6. Председатель государственных аттестационных комиссий утверждается Министерством образования и науки Кыргызской Республики.

7. Государственная аттестационная комиссия формируется из преподавателей организации профессионального образования и лиц, приглашенных из сторонних учреждений: преподавателей других образовательных организаций и специалистов предприятий, организаций, учреждений по профилю подготовки выпускников.

3.2. Порядок проведения итоговой государственной аттестации

1. К итоговой аттестации допускаются лица, завершившие полный курс обучения по специальности 100203 «Информационная безопасность автоматизированных систем» и успешно прошедшие все предшествующие аттестационные испытания, предусмотренные учебным планом.

2. Сдача итоговых экзаменов проводятся на открытых заседаниях аттестационной комиссии с участием не менее двух третей ее состава.

3. Результаты аттестационных испытаний, включенных в итоговую государственную аттестацию, определяются оценками "отлично", "хорошо", "удовлетворительно", "неудовлетворительно" и объявляются в тот же день после оформления в установленном порядке протоколов заседаний государственных аттестационных комиссий.

4. Решения государственных аттестационных комиссий принимаются на закрытых заседаниях простым большинством голосов членов комиссии. При равном числе голосов голос председателя является решающим.

5. Присвоение соответствующей квалификации выпускнику организации профессионального образования и выдача ему документа о среднем профессиональном образовании осуществляется при условии успешного прохождения всех установленных видов аттестационных испытаний, включенных в итоговую государственную аттестацию.

6. Студенту, имеющему оценку "отлично" не менее чем по 75% дисциплин учебного плана, оценку "хорошо" по остальным дисциплинам и прошедшему итоговую государственную аттестацию только с отличными оценками, выдается диплом с отличием.

7. Студент, не прошедший в течение установленного срока обучения аттестационные испытания, входящие в состав итоговой государственной аттестации, отчисляется из образовательной организации и получает академическую справку установленного Министерством образования и науки Кыргызской Республики образца.

8. Выпускники, не прошедшие итоговые аттестационные испытания, допускаются к повторной сдаче не ранее чем через один год, после прохождения итоговой государственной аттестации.

9. Ежегодный отчет о работе государственной аттестационной комиссии обсуждается на Педсовете колледжа в двухмесячный срок после завершения итоговой государственной аттестации.

3.3. Критерии оценивания результатов итоговой государственной аттестации

1. Оценка ответа студента на государственном экзамене определяется в ходе заседания ГАК. Решения ГАК принимаются на закрытых заседаниях простым большинством голосов членов комиссии, участвующих в заседании, при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов голос председательствующего на заседании ГАК является решающим.

2. Результаты решения ГАК определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка "ОТЛИЧНО" ставится студенту, показавшему повышенный уровень готовности к профессиональной деятельности.

Оценка "ХОРОШО" ставится студенту, показавшему пороговый (допустимый) уровень готовности к профессиональной деятельности.
Оценка "УДОВЛЕТВОРИТЕЛЬНО" ставится студенту, показавшему пороговый (критический) уровень готовности к профессиональной деятельности.
Оценка "НЕУДОВЛЕТВОРИТЕЛЬНО" ставится студенту, не достигшему пороговый уровень готовности к профессиональной деятельности.

4. ПРИМЕРНЫЕ ВОПРОСЫ К ПОДГОТОВКЕ СДАЧИ ИТОГОВОЙ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ

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 «Основы информационной безопасности»

1. Понятие информационной безопасности. Основные составляющие. Важность проблемы.
2. Основные определения и критерии классификации угроз.
3. Вредоносное программное обеспечение.
4. Наиболее распространенные угрозы.
5. Понятие мобильные агенты, вирусов, "червей" статической и динамической целостностью.
6. Законодательный уровень информационной безопасности.
7. Понятие национальной безопасности.
8. Виды безопасности личности, общества и государства.
9. Роль информационной безопасности в обеспечении национальной безопасности государства.
10. Обеспечение информационной безопасности в нормальных и чрезвычайных ситуациях.
11. Основные правовые и нормативные акты в области информационной безопасности.
12. Стандарты и спецификации в области информационной безопасности.
13. Административный уровень информационной безопасности.
14. Управление рисками.
15. Политика и программа безопасности
16. Процедурный уровень информационной безопасности.
17. Сервиса безопасности.
18. Анализ защищенности.
19. Обеспечение отказоустойчивости.
20. Обеспечение безопасного восстановления.
21. Основные программно-технические меры.
22. Идентификация и аутентификация, управление доступом.
23. Моделирование и аудит, шифрование, контроль целостности.
24. Многоуровневая защита корпоративных сетей.
25. Экранирование.
26. Туннелирование.
27. Механизмы безопасности, классы безопасности.
28. Информационная безопасность распределенных систем.

СПИСОК ЛИТЕРАТУРЫ ДЛЯ ПОДГОТОВКИ К ИГА ПО СПЕЦИАЛЬНОСТИ 100203 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

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: / 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 / 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. – 100 с.
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 «Основы информационной безопасности»

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с.
2. Ищейнов В.Я. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.
3. Партыка Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2016. - 432 с.
4. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.