МИНИСТЕРСТВО ОБРАЗОВАНИЯ И КУЛЬТУРЫ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ

КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
им. И. Раззакова

«ОДОБРЕНО»
Председатель УМС
_____
«___» _____20 г.

«УТВЕРЖДАЮ»
Ректор КГТУ
_____проф.М.Дж. Джаманбаев
«___» _____20 г.

РАБОЧАЯ ПРОГРАММА

ГОСУДАРСТВЕННОГО ЭКЗАМЕНА ПО НАПРАВЛЕНИЮ
для студентов специальности 590001 «Информационная безопасность»
специализации - " БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ "

дневной формы обучения

Рабочая программа составлена в соответствии с требованиями
Государственного образовательного стандарта
по специальности 590001 «Информационная безопасность»
Разработал: доцент кафедры ИВТ Исраилова Н.А.
Рассмотрена и утверждена на заседании кафедры ИВТ
Протокол № ____ от «___»_____20__ г. _____
(подпись зав. каф.)

Бишкек-2020

1. Цель Государственного экзамена по направлению

Итоговый государственный экзамен проводится по специальным дисциплинам с целью определения соответствия знаний, умений и навыков студентов по комплексу специальных дисциплин требованиям государственного образовательного стандарта.

Порядок проведения и программа государственного экзамена по специальности 590001 «Информационная безопасность» определяются вузом на основании методических рекомендаций и соответствующих примерных программ, разработанных УМО в области автоматизации, электроники, вычислительной техники, а также на основании Положения об итоговой государственной аттестации выпускников высших учебных заведений.

2. Общие требования к выпускнику, предусмотренные ГОС

Требования к профессиональной подготовленности дипломированного специалиста.

Выпускник должен уметь решать задачи, соответствующие его квалификации, указанные в государственном образовательном стандарте.

Инженер по специальности 590001 «Информационная безопасность»

Знать: математические, теоретические и организационно-правовые основы информационной безопасности, теорию и практику операционных систем, систем управления базами данных, сетевых технологий, криптографических, технических, программно-аппаратных средств информационной безопасности, основные технологии программирования и разработки программного обеспечения, основные положения различных парадигм программирования, технологии разработки программ в рамках этих направлений, возможные сферы их приложений при решении практических задач, принципы функционирования сетей передачи данных, возможные атаки и защиты от этих атак.

Уметь: решать задачи в профессиональной деятельности, а именно:

- сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем;
- подготовка научно-технических отчетов, обзоров, докладов, публикаций по результатам выполненных исследований;
- моделирование и исследование свойств защищенных автоматизированных систем;
- анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;
- разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;
- сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;
- разработка политик информационной безопасности автоматизированных систем;
- разработка защищенных автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;

- выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
- разработка систем управления информационной безопасностью автоматизированных систем;
- контроль работоспособности и эффективности применяемых средств защиты информации;
- выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;
- проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;
- организационно-управленческая деятельность:
- организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
- организационно-методическое обеспечение информационной безопасности автоматизированных систем;
- организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;
- контроль реализации политики информационной безопасности;
- реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;
- администрирование подсистем информационной безопасности автоматизированных систем;
- мониторинг информационной безопасности автоматизированных систем;
- управление информационной безопасностью автоматизированных систем;
- обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;
- разработка и исследование моделей информационно-технологических ресурсов, модели угроз и модели нарушителей информационной безопасности в распределенных информационных системах;
- удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;
- аудит защищенности информационно-технологических ресурсов;
- координация деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятиях и в учреждениях. Владеть:
- способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах,
- способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах, способностью проводить аудит защищенности инфор

3. Перечень дисциплин, включенных в государственный экзамен и форма экзамена

В соответствии с требованиями государственного образовательного стандарта к минимуму содержания и уровню профессиональной подготовки специальности в программу государственного экзамена включены вопросы по дисциплинам специальности из разделов: «Языки программирования и СУБД» «Безопасность операционных систем, баз данных и вычислительных сетей», «Организационные и правовые основы обеспечения информационной безопасности», «Криптографические методы защиты информации» «Технические средства защиты информации».

Экзаменационный билет состоит из двух теоретических вопросов и одной задачи.

4. Перечень вопросов по разделам

Раздел «Криптографические методы защиты информации»

1. Блочные шифры. Математическая модель. Разновидности блочных шифров.
2. Эллиптические кривые над конечным полем. Сложение точек, порядок точки, образующая точка. Теорема Хассе. Подпись Эль-Гамаля на эллиптической кривой.
3. Цифровая подпись, атаки и угрозы. Подписи RSA и Эль-Гамаля. Национальные стандарты DSA.
4. Асимметричные криптосистемы. Понятие односторонней функции. Проблемы факторизации и дискретного логарифмирования. Криптосистемы RSA и ЭльГамаля.
5. Функции хэширования, требования к ним. Схема Меркла-Дамгарда. Хэш-функции на основе блочных шифров.
6. Управление ключами в асимметричных криптосистемах. Инфраструктура открытых ключей. Сертификаты. Стандарт X.509.
7. Ключи симметричной криптосистемы. Жизненный цикл ключей. Требования к обеспечению безопасности жизненного цикла ключей. Управление ключами в криптографических системах. Примеры для ИБ.
8. Идентификация и аутентификация. Парольные схемы. Протоколы рукопожатия.
9. Интерактивные системы доказательства.
10. Криптографические протоколы – основные виды и типы, область применения.
11. Разделение секрета. Идеальность и совершенность схем разделения секрета.
12. Совершенные и идеальные шифры по Клоду Шеннону. Избыточность языка на букву сообщения. Ложные ключи и расстояние единственности.
13. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры.
14. Ключевая системы шифра. Атаки и угрозы шифрам. Вычислительная и теоретическая стойкость.

Раздел «Безопасность операционных систем, баз данных и вычислительных сетей»

1. Основные сетевые стандарты, протоколы взаимодействия в сетях. Модели OSI и TCP/IP. Сетевое оборудование на 2 и 3 уровнях модели OSI. Пример.
2. Аутентификация и защита канала в сетях VPN – семейства протоколов IPSec и SSL\TLS. Пример.

3. Понятие процесса, потока. Жизненный цикл процесса. Основные цели и алгоритмы планирования процессов. Пример.
4. Средства обеспечения защиты данных от несанкционированного доступа, средства идентификации и аутентификации объектов БД, языковые средства разграничения доступа, организация аудита в системах БД. Задачи и средства администратора безопасности БД. Пример.
5. Безопасность баз данных – механизмы управления (разграничения) доступом пользователей к данным. Пример.
6. Безопасность баз данных – механизмы восстановления данных после программных и\или аппаратных сбоев, откат транзакций. На своем примере.
7. Безопасность баз данных - использование шифрования и криптографических протоколов. Пример.
8. Типовые функциональные дефекты ОС, приводящие к созданию каналов утечки данных.
9. Контроль доступа к данным в ОС: основные понятия, модели доступа.
10. Основные сервисы безопасности ОС.
11. Основные угрозы безопаности в ОС. Меры противодействия (на своем примере).
12. Формализованные требования к защите ОС.
13. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресуров и технологии разграничения доступа пользователей к ресурсам сети. Монитор безопасности. На своем примере.
14. Протоколы IP v4 и IP v6. Совместное использование в рамках одной корпоративной сети.
15. Технологии обеспечения безопасности корпоративной сети с использованием оборудования 2-го уровня модели OSI. На своем примере.
16. Технологии обеспечения безопасности корпоративной сети с использованием оборудования 3-го уровня модели OSI. На своем примере.
17. Понятие неразделяемого ресурса. Гонки. Методы взаимного исключения с активным ожиданием (метод блокирующей переменной, строгое чередование, алгоритм Деккера, алгоритм Петерсона).
18. Технологии обеспечения безопасности беспроводных сетей. На своем примере.

Раздел «Алгоритмы, теория языков программирования, базы данных»

1. Задачи о кратчайших расстояниях на графах. Основные алгоритмы для решения задач о кратчайших расстояниях.
2. Алгоритмы поиска. Использование деревьев в задачах поиска: бинарные, сбалансированные, красно-черные деревья поиска.
3. Алгоритмы сортировки. Постановка задачи, классификация, анализ эффективности.
4. Основные алгоритмы (обмен, выбор, вставка, шейкер, метод Шелла, быстрая,поразрядная, пирамидальная).
5. Абстрактные типы данных. Классы. Инкапсуляция. Наследование. Полиморфизм.
6. Спецификация и реализация в разных языках программирования.
7. Процессы и потоки. Объекты межпроцессной синхронизации. Понятие гонок и взаимной блокировки
8. Общие понятия реляционного подхода к организации БД. Основные понятия реляционной теории: домен, атрибут, кортеж, первичный ключ, отношение.
9. Фундаментальные свойства отношений. Нормализация. На своем примере для небольшой базы.

10. Синтаксис оператора SELECT. Обзор его подразделов (списка выборки, секций FROM,WHERE, GROUP BY, HAVING, OREDER BY).. Способы упорядочивания итогового набора в секции OREDER BY. Модификация данных с использованием Data Manipulation Language (DML). Операторы INSERT, UPDATE, DELETE. На примересвоей небольшой базы.

Раздел «Технические средства и методы защиты информации»

1. Технические каналы утечки информации, классификация и характеристика. На своем примере.
2. Радиоэлектронные каналы утечки информации. На своем примере.
3. Способы и средства инженерной защиты и технической охраны объектов. На своем примере.
4. Видеокамеры. Организация охраны объекта с помощью видеокамер. На своем примере.
5. Способы и средства информационного скрытия речевой информации от подслушивания. Энергетическое скрытие акустического сигнала. На своем примере.
6. Принцип действия активных средств поиска прослушивающих устройств. Метод нелинейной локации. На своем примере.
7. Принцип действия пассивных средств поиска прослушивающих устройств. На своем примере.

Раздел «Организационные и правовые основы обеспечения информационной безопасности»

1. Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ. На примере своей ИС.
2. Требования доктрины информационной безопасности КР и ее реализация в существующих системах информационной безопасности. На примере своей ИС.
3. Принципы обработки ПДн. Условия обработки ПДн. Согласие на обработку ПДн. Пример согласия. Порядок отправления запросов к оператору ПДн и ответов на них. Пример запроса.
4. Порядок сертификации средств защиты информации. Основные участники процесса. Необходимость сертификации. Виды и схемы сертификации средств защиты информации. Понятия техническое условие, задание по безопасности и профиль защиты.
5. Основные положения ПП-1119. Классификация ИСПДн. Определение уровня защищенности. Основные характеристики ИСПДн. Перечень мер в зависимости от уровня защищенности. На примере своей ИСПДн.
6. Условия обработки биометрических и специальных ПДн. Виды ИСПДн. Условия трансграничной передачи ПДн
7. Понятие средства защиты инфорации. Классификации средств защиты информации с примерами. Типы сертифицированных средств защиты информации с примерами.
8. Введение режима коммерческой тайны в организации. На своем примере.
9. Ответственность за нуршение закона. Определение СКЗИ. Виды СКЗИ. Основные понятия. Условия эксплуатации СКЗИ
10. Этапы разработки, внедрения и эксплуатации системы защиты информации на своем примере. Техническое задание и технический проект на создание системы защиты информации. Порядок аттестации информационной системы.

5. Учебно-методическое и информационное обеспечение дисциплины.

Основная литература:

1. Фихтенгольц Г. М. Основы математического анализа / Г. М. Фихтенгольц. - СанктПетербург: Лань. - (Учебники для вузов. Специальная литература) Ч. 2. - 2001. - 464 с.

2. Дегтев, А. Н. Алгебра и логика: учеб. пособие по спец. "Математика"/ А. Н. Дегтев. - 3-е изд.. - Тюмень: Изд-во Тюм. гос. ун-та, 2008. - 88 с.

3. Гмурман, В. Е.. Теория вероятностей и математическая статистика: учеб. пособие для студ. вузов/ В. Е. Гмурман. - 12-е изд., перераб.. - Москва: Высшее образование, 2008. - 479 с.

4. Крамаров С.О. Криптографическая защита информации: учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — М.: РИОР: ИНФРА-М, 2018. — 321 с. — (Высшее образование). — DOI: https://doi.org/ 10.12737/1716-6 [Электронный ресурс]. - URL: http://znanium.com/catalog/product/ 901659 (29.01.2018).

5. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс]: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск: Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. – Режим доступа: http://znanium.com/catalog/product/441493 (дата обращения: 23.04.2018).

6. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс]: учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск: Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. Режим доступа – URL: http://znanium.com/catalog/product/463037 (18.05.2018)

7. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс]: учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск: Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. . Режим доступа – URL: http://znanium.com/catalog/product/463061 (18.05.2018).

8. Агальцов В.П. Базы данных. В 2-х кн. Книга 2. Распределенные и удаленные базы данных: учебник / В.П. Агальцов. — М.: ИД «ФОРУМ»: ИНФРА-М, 2017. — 271 с. http://znanium.com/catalog/product/652917 (18.05.2018).

9. Агальцов В.П. Базы данных. В 2-х кн.Кн. 1. Локальные базы данных: учебник / В.П. Агальцов. - 2-е изд., перераб. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 352 с. http:// znanium.com/catalog/product/326451 (18.05.2018).

10. Операционные системы, среды и оболочки: учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М.: ФОРУМ : ИНФРА-М, 2017. — 560 с. http:// znanium.com/catalog/product/552493 (18.05.2018).

Дополнительная литература:

1. Демидович, Б. П.. Сборник задач и упражнений по математическому анализу: учебное пособие для студентов математических и физических специальностей вузов/ Б. П. Демидович. - 13-е изд., испр.. - Москва: Сервисная компания, 2014. - 624 с

2. Вейль, Г.. Алгебраическая теория чисел = Algebraic theory of Numbers/ Г. Вейль; Пер. с англ. Л. И. Копейкина. - 3-е изд., стереотип.. - Москва: Едиториал УРСС, 2004. - 224 с.

3. Ростовцев, А. Г. Алгебраические основы криптографии/ А. Г. Ростовцев. - СанктПетербург: Мир и семья: Интерлайн, 2000. - 354 с. 20

4. Бабаш А.В. Криптографические методы защиты информации. Том 3: Учебнометодическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: 60x88 1/8. - (Высшее образование: Бакалавриат). ISBN 978-5-369-01304-5. [Электронный ресурс]. – URL: http://znanium.com/catalog/product/432654 (23.04.2018).

5. Душкин А.В. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с. http://znanium.com/catalog/product/977192 (18.05.2018).

6. Федорова М. Ю. Нормативно-правовое обеспечение образования: учебное пособие для студентов вузов/ М. Ю. Федорова. - 4-е изд., испр. - Москва: Академия, 2013. - 176с.

7. Гринберг, А. С. Информационные технологии управления [Электронный ресурс]: учебное пособие / А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. - М.: ЮнитиДана, 2012. - 479 с. - 5-238-00725-6. Режим доступа: http://znanium.com/catalog/product/ 396629 (18.05.2018).

Технические средства и материально-техническое обеспечение дисциплины: Для проведения итогового междисциплинарного экзамена используется аудитория, оборудованная мультимедиа проектором и персональным компьютером.

6. Критерии оценки знаний студентов

Ответ выпускника оценивается по 100 балльной системе с последующим переводом в пятибалльную систему.

Решения государственной экзаменационной комиссии принимается на закрытых заседаниях. Оценка студенту за ответ каждым членом комиссии выставляется:

ОТЛИЧНО, если студент показал глубокие знания программного материала, грамотно и логично его излагает, быстро принимает правильные решения;

ХОРОШО, если студент проявил полное знание программного материала, освоил основную литературу, обнаружил стабильный характер знаний, но допустил небольшие ошибки или неточности в ответе;

УДОВЛЕТВОРИТЕЛЬНО, если студент имеет знания только основного материала, но не усвоил его деталей, не допускает грубых ошибок в ответе, требует в отдельных случаях наводящих вопросов для принятия правильного решения, допускает отдельные неточности или оговорки;

НЕУДОВЛЕТВОРИТЕЛЬНО, если студент допускает грубые ошибки в ответе, не может применять полученные знания на практике.

Общая оценка знаний студента каждым членом комиссии выводится по частным оценкам за ответы на вопросы билета.

Итоговая оценка студента за экзамен выставляется по результатам оценок каждого члена комиссии простым большинством голосов членов комиссии, участвующих в заседании. При равном числе голосов председатель комиссии (или заменяющий его заместитель председателя комиссии) обладает правом решающего голоса.