Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Томский государственный университет систем управления и радиоэлектроники» (ТУСУР)



УТВЕРЖДАЮ
Ректор ТУСУР
_____ В.М. Рулевский
«__» _____ 2022 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

для поступающих в магистратуру
по направлению подготовки
10.04.01 «Информационная безопасность»

Магистерская программа подготовки
«Информационная безопасность объектов критической информационной инфраструктуры»

Томск 2022

Лист согласований

Программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 – «Информационная безопасность», утвержденного приказом Министерства образования и науки Российской Федерации № 1455 от 26 ноября 2020 г.

Программа рассмотрена и утверждена на заседании:

кафедры КИБЭВС от «30» ___августа____ 2022 г., протокол № 8

Программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки:

Декан ФБ Е.М. Давыдова

Зав. каф. КИБЭВС А.А. Шелупанов

Разработчик, д.т.н., профессор каф. КИБЭВС А.А. Шелупанов

Разработчик, к.т.н., доцент каф. КИБЭВС А.А. Конев

1. ОБЩИЕ ПОЛОЖЕНИЯ

Программа вступительных испытаний составлена на основании федерального государственного образовательного стандарта высшего образования подготовки бакалавриата по направлению 10.03.01 «Информационная безопасность» и охватывает базовые дисциплины подготовки бакалавров по указанному направлению.

Программа содержит перечень вопросов для вступительных испытаний и список рекомендуемой литературы для подготовки к экзамену. Форма вступительных испытаний и регламент проведения определяются Правилами приема в ТУСУР.

2. ЦЕЛЬ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Данные вступительные испытаний призваны определить уровень освоения компетенций и степень готовности абитуриента к освоению основной образовательной программы магистратуры по направлению 10.04.01 «Информационная безопасность», магистерская программа подготовки «Информационная безопасность объектов критической информационной инфраструктуры».

3. ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Тема 1. Основы информационной безопасности

Информация как объект защиты. Свойства информации, обеспечиваемые при её защите. Виды защищаемой информации.

Понятие «Угроза информационной без опасности». Классификация угроз. Способы реализации угроз.

Понятие «Система защиты информации». Направления защиты информации. Понятие «Уязвимость». Угрозы системе защиты информации.

Основные нормативно-правовые документы и принципы обеспечения защиты информации в области правового, технического, программно-аппаратного, криптографического и организационного направлений защиты информации.

Тема 2. Организационно-правовое обеспечение ИБ

Законодательство РФ в области информационной безопасности

Понятие и структура информационной безопасности. Основные задачи системы информационной безопасности. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Субъекты и объекты правоотношений в области информационной безопасности.

Отрасли законодательства, регламентирующие деятельность по защите информации.

Правовые основы защиты конфиденциальной информации. Конфиденциальная информация. Виды тайн. Коммерческая тайна. Профессиональные тайны. Служебная тайна. Персональные данные. Тайна

следствия и судопроизводства. Банковская тайна. Тайна телефонных переговоров и переписки.

Правовые основы защиты государственной тайны.

Государственная тайна, как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивание и рассекречивание. Система защиты государственной тайны. Органы защиты государственной тайны и их компетенции. Порядок допуска и доступ к государственной тайне. Перечень и содержание организационных мер, направленных на защиту государственной тайны.

Лицензирование и сертификация

Правовая основа лицензирования и сертификации в области защиты информации, в том числе защиты государственной тайны. Виды деятельности в информационной сфере, подлежащие лицензированию. Лицензирование деятельности по защите информации. Объекты

Нормы ответственности за правонарушения в сфере компьютерных технологий.

Уголовно-правовые нормы. Основные принципы и понятия уголовного права. Преступления в сфере компьютерной информации. Экспертиза компьютерных преступлений. Административные правонарушения.

Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.

Задачи организационного обеспечения информационной безопасности. Роль нормативных документов в защите информации. Инвентаризация информационных ресурсов организации. Построение моделей документооборота и информационных систем. Модели нарушителя информационной безопасности. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации.

Организация службы безопасности и работа с кадрами.

Служба безопасности объекта. Принципы деятельности службы безопасности. Задачи и функции службы безопасности. Структура службы безопасности. Функции сотрудников службы безопасности. Контроль состояния системы защиты, проведение служебных расследований. Подбор, расстановка и работа с кадрами. Внутренние угрозы информационной безопасности, социальная инженерия. Функции службы безопасности при подборе, увольнении сотрудников и текущей работе с ними. Нормативное обеспечение работы сотрудников организации с информацией ограниченного доступа.

Организация и обеспечения режима секретности.

Основные принципы организации и обеспечения секретного документооборота. Технологические меры поддержания информационной безопасности объектов. Организация совещания и переговоров. Регламентация предоставления сотрудникам допуска к информации ограниченного доступа. Регламентация выдачи (возврата) документов и работы с ними. Регламентация процедуры создания документа ограниченного доступа. Регламентация процедуры

снятие грифа с документов ограниченного доступа и их уничтожения. Регламентация обмена документами с другими организациями. Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно технического и экономического сотрудничества. Организация режима и охраны объектов в процессе транспортировки.

Организация пропускного и внутри объектового режима

Проектирование пропускного и внутри объектового режима. Категорирование помещений. Регламентация пропуска лиц в здания. Виды пропусков и порядок их оформления. Порядок пропуска автотранспорта на территорию организации. Регламентация приема и сдачи объекта под охрану. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения. Структура аварийного плана.

Тема 3. Программные средства

Основные понятия информационных сетей

История развития сетей ЭВМ. Место и роль вычислительных сетей в современном мире. Основные понятия и терминология. Общие представления о вычислительной сети. Общее понятие об иерархической структуре протоколов. Принципы многоуровневой организации локальных и глобальных сетей ЭВМ. Модель OSI. Стандартные стеки коммуникационных протоколов. Стандартизация в сетях. Классификация вычислительных сетей. Требования, предъявляемые к современным вычислительным сетям. Методы и технологии проектирования средств телекоммуникаций. Структуризации сети. Физическая и логическая топологии сетей. Основное коммуникационное оборудование.

Основы построения современных локальных сетей

Конфигурации локальных вычислительных сетей и методы доступа в них. Структура и функции локальных сетей. Содержание стандарта IEEE 802. Базовые технологии локальных сетей. IEEE 802.2 Ethernet. Оборудование локальных сетей. Программные средства телекоммуникации. Структура программного обеспечения локальной сети. Классификация программного обеспечения локальных сетей. Принципы построения сетевого программного обеспечения и сетевых операционных систем. Классификация серверов. Проектирование сетей ЭВМ по принципу «клиент-сервер».

Средства реализации межсетевого взаимодействия

Сетевой уровень передачи данных. IP-адресация. Реализация межсетевого взаимодействия средствами TCP/IP. Порядок распределения IP-адресов. Отображение IP-адресов на локальные адреса. ARP протокол. Принципы маршрутизации в IP-сетях. Протоколы маршрутизации. Понятие домена. Доменная адресация в IP-сетях. DNS протокол. Протокол IPv6. Протоколы транспортного уровня TCP и UDP.

Перспективные направления развития и проблемы информационных сетей

Современные тенденции развития телекоммуникационных систем. Интеграция различных типов сетей и сетевых служб. Виртуализация информационных систем. Облачные вычисления.

Основные понятия информационной безопасности сетей ЭВМ

Обеспечение безопасности телекоммуникационных связей и административный контроль. Основные понятия и терминология. Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность.

Технологии обеспечения безопасности в локальных сетях

Защита топологии сети. Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные экраны. Абонентское шифрование Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Безопасность ресурсов сети. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений Сканеры безопасности. Классы сканеров безопасности и особенности применения. Защита от вирусов

Обеспечение безопасности межсетевого взаимодействия

Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети. Уязвимости и защита базовых протоколов и служб: Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты

4. Список рекомендуемой литературы

Основная литература

1. Петренко, В. И. Теоретические основы защиты информации [Электронный ресурс]: учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2015. — 222 с. — Текст: электронный // Лань: электронно-библиотечная система. — Режим доступа: https://e.lanbook.com/book/155247

2. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Е. Б.Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва: Горячая линия-Телеком, 2011.— 558 с. — ISBN 5-93517-292-5. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: https://e.lanbook.com/book/111016

3. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // ЭБС Юрайт — Режим доступа: https://urait.ru/bcode/469235

4.. Построение защищенных корпоративных сетей [Электронный ресурс] [Электронный ресурс]: учебное пособие / Р.Н. Ачилов. — Электрон. дан. —

Москва : ДМК Пресс, 2013. — 250 с. — Режим доступа: https://e.lanbook.com/book/66472

Дополнительная литература

1. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnyedokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения: 03.05.2021).

2. Р 50.1.028-2001. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования [Электронный ресурс]: — Режим доступа: https://standartgost.ru/g/%D0%A0_50.1.028-2001 (дата обращения: 03.05.2021).

3. Федеральная служба по техническому и экспортному контролю приказ 11 февраля 2013 г. n 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17.

4. Федеральная служба по техническому и экспортному контролю методический документ методика оценки угроз безопасности информации [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g.

5. Федеральная служба по техническому и экспортному контролю утвержден ФСТЭК России 11 февраля 2014 г. методический документ меры защиты информации в государственных информационных системах [Электронныйресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument

6. Компьютерные сети и службы удаленного доступа [Электронный ресурс] [Электронный ресурс]: справочник / О. Ибе. — Электрон. дан. — Москва : ДМК Пресс, 2007. — 336 с. — Режим доступа: https://e.lanbook.com/book/1169

Вопросы для собеседования

Основы информационной безопасности

1. Типы объектов защиты информации и их определения.
2. Свойства информации, обеспечиваемые при её защите.
3. Категории доступа к информации. Степени секретности сведений, составляющих государственную тайну.
4. Виды информации, относящейся к сведениям конфиденциального характера.
5. Понятие «нарушение информационной безопасности». Примеры атак на информационные системы.
6. Понятие «угроза информационной безопасности». Формы представления информации.

7. Угрозы конфиденциальности информации, представленной в различных формах.
8. Угрозы целостности информации, представленной в различных формах.
9. Угрозы доступности информации, представленной в различных формах.
10. Способы реализации угроз, направленных на акустическую, видовую компьютерную информацию.
11. Способы реализации угроз информации, представленной в виде сигналов.
12. Понятие «обеспечение информационной безопасности организации». Примеры методов и средств защиты информации.
13. Понятие «система защиты информации». Направления защиты информации.
14. Элементы информационной системы, являющиеся объектами защиты.
15. Угрозы конфиденциальности и целостности, направленные на автоматизированные информационные системы.
16. Угрозы конфиденциальности и целостности, направленные на персонал организации.
17. Способы реализации угроз, направленных на автоматизированные информационные системы и системы защиты информации.
18. Понятие «Уязвимость». Причины возникновения уязвимостей.
19. Законодательные акты, регламентирующие работу со сведениями, составляющими государственную тайну, с персональными данными, служебную и коммерческую тайну.
20. Основные функции ФСБ России в области обеспечения информационной безопасности.
21. Основные функции ФСТЭК России в области обеспечения информационной безопасности.

Организационно-правовое обеспечение информационной безопасности

1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
2. Конституционные гарантии прав граждан на информацию и механизм их реализации.
3. Понятие и виды защищаемой информации по законодательству РФ.
4. Государственная тайна как особый вид защищаемой информации.
5. Конфиденциальная информация.
6.Система защиты государственной тайны.
7.Правовой режим защиты государственной тайны.
8. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.
9. Правовые режимы конфиденциальной информации.
10. Лицензирование и сертификация в области защиты информации, в том числе государственной тайны.
11. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.).
12. Защита интеллектуальной собственности.
13. Правовая регламентация охранной деятельности.
14. Международное законодательство в области защиты информации.

15. Преступления в сфере компьютерной информации.
16. Экспертиза преступлений в области компьютерной информации.
17. Криминалистические аспекты проведения расследований.

Безопасность сетей ЭВМ

1. История развития сетей ЭВМ. Место и роль вычислительных сетей в современном мире.
2. Основные понятия и терминология. Общие представления о вычислительной сети. Общее понятие об иерархической структуре протоколов. Принципы многоуровневой организации локальных и глобальных сетей ЭВМ.
3. Модель OSI. Стандартные стеки коммуникационных протоколов.
4. Стандартизация в сетях. Классификация вычислительных сетей. Требования, предъявляемые к современным вычислительным сетям.
5. Методы и технологии проектирования средств телекоммуникаций. Структуризации сети. Физическая и логическая топологии сетей. Основное коммуникационное оборудование
6. Конфигурации локальных вычислительных сетей и методы доступа в них. Структура и функции локальных сетей.
7. Содержание стандарта IEEE 802. Базовые технологии локальных сетей. IEEE 802.2 Ethernet.
8. Оборудование локальных сетей. Сетевой уровень передачи данных. IP-адресация. Реализация межсетевого взаимодействия средствами TCP/IP. Порядок распределения IP-адресов. Отображение IP-адресов на локальные адреса.
9. ARP протокол. Принципы маршрутизации в IP-сетях. Протоколы маршрутизации.
10. Понятие домена. Доменная адресация в IP-сетях. DNS протокол. Протокол IPv6. Протоколы транспортного уровня TCP и UDP.
11. Современные тенденции развития телекоммуникационных систем. Интеграция различных типов сетей и сетевых служб.
12. Обеспечение безопасности телекоммуникационных связей и административный контроль. Основные понятия и терминология. Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность.
13. Защита топологии сети. Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные экраны. Абонентское шифрование. Защита сетевого трафика и компонентов сети.
14. Защита компонентов сети от НСД. Безопасность ресурсов сети.
15. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
16. Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений
17. Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры
18. Интернет. Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов.
19. Виртуальные частные сети. Уязвимости и защита базовых протоколов и служб: Протоколы маршрутизации. Семейство TCP/IP. Службы поиска.

20. Безопасность WWW и электронной почты.
21. Сканеры безопасности. Классы сканеров безопасности и особенности применения.
22. Защита от вирусов. Программные средства телекоммуникации.
23. Структура программного обеспечения локальной сети. Классификация программного обеспечения локальных сетей.
24. Принципы построения сетевого программного обеспечения и сетевых операционных систем. Классификация серверов. Проектирование сетей ЭВМ по принципу «клиент-сервер».
25. Виртуализация информационных систем. Облачные вычисления.