

МИНОБРНАУКИ РОССИИ



Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГАОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность

Код и наименование направления подготовки/специальности

Организация и технологии защиты государственной тайны

Наименование направленности (профиля)/ специализации

Уровень высшего образования: магистратура

Форма обучения: очная, очно-заочная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2026

Защищённые информационные системы
Рабочая программа дисциплины

Составитель:

Кандидат технических наук, зав. кафедрой комплексной защиты информации
Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры КЗИ

№ 5 от 25.12.2025

ОГЛАВЛЕНИЕ

| | |
|--|--|
| 1. Пояснительная записка | 4 |
| 1.1. Цель и задачи дисциплины | 4 |
| 1.2. Перечень планируемых результатов обучения по дисциплине, соотнесённых с индикаторами достижения компетенций | 4 |
| 1.3. Место дисциплины в структуре образовательной программы | 5 |
| 2. Структура дисциплины | 5 |
| 3. Содержание дисциплины | 6 |
| 4. Образовательные технологии | 8 |
| 5. Оценка планируемых результатов обучения | 10 |
| 5.1. Система оценивания | 10 |
| 5.2. Критерии выставления оценки по дисциплине | 11 |
| 5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине | 12 |
| 6. Учебно-методическое и информационное обеспечение дисциплины | 15 |
| 6.1. Список источников и литературы | 15 |
| 6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» | 17 |
| 7. Материально-техническое обеспечение дисциплины | 17 |
| 8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов | 18 |
| 9. Методические материалы | 19 |
| 9.1. Планы практических занятий | 19 |
| <i>Приложение 1</i> | Ошибка! Закладка не определена. |

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – профессиональная подготовка магистрантов, необходимая для освоения методов и технологий защиты государственной тайны при работе в автоматизированных информационных системах.

Задачи дисциплины:

дать знания:

- о нормативных правовых актах в области защищённых информационных систем;
- о методах и средствах разработки защищённых информационных систем.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесённых с индикаторами достижения компетенций

| Компетенция (код и наименование) | Индикаторы компетенций (код и наименование) | Результаты обучения |
|--|---|--|
| <i>УК-4 – Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</i> | <i>УК-4.1 – Знает современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации</i> | <i>Знать:</i> <ul style="list-style-type: none"> • <i>современные коммуникативные технологии на государственном и иностранном языках;</i> • <i>закономерности деловой устной и письменной коммуникации</i> |
| | <i>УК-4.2 – Умеет применять на практике коммуникативные технологии, методы и способы делового общения</i> | <i>Уметь:</i> <ul style="list-style-type: none"> • <i>применять на практике коммуникативные технологии, методы и способы делового общения</i> |
| | <i>УК-4.3 – Владеет методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств</i> | <i>Владеть:</i> <ul style="list-style-type: none"> • <i>методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств</i> |
| <i>ОПК-1 – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание</i> | <i>ОПК-1.1 – Знает основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности</i> | <i>Знать:</i> <ul style="list-style-type: none"> • <i>основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности</i> |
| | <i>ОПК-1.2 – Умеет проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности</i> | <i>Уметь:</i> <ul style="list-style-type: none"> • <i>проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности</i> |
| | <i>ОПК-1.3 – Владеет</i> | <i>Владеть:</i> |

| | | |
|---|---|---|
| | <i>навыками участия в разработке системы обеспечения информационной безопасности объекта</i> | <ul style="list-style-type: none"> • <i>навыками участия в разработке системы обеспечения информационной безопасности объекта языковых форм и средств</i> |
| <i>ОПК-2 – Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности</i> | <i>ОПК-2.1 – Знает методы концептуального проектирования технологий обеспечения информационной безопасности</i> | <i>Знать:</i> <ul style="list-style-type: none"> • <i>методы концептуального проектирования технологий обеспечения информационной безопасности</i> |
| | <i>ОПК-2.2 – Умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности</i> | <i>Уметь:</i> <ul style="list-style-type: none"> • <i>выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности</i> |
| | <i>ОПК-2.3 – Владеет навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности</i> | <i>Владеть:</i> <ul style="list-style-type: none"> • <i>навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности</i> |

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Защищённые информационные системы» относится к обязательной части блока дисциплин учебного плана.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 5 з.е., 180 академических часа (ов).

Структура дисциплины для очной формы обучения

Объём дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

| Семестр | Тип учебных занятий | Количество часов |
|---------|--------------------------|------------------|
| 1 | Лекции | 36 |
| 1 | Практические работы | 44 |
| 1 | Промежуточная аттестация | 18 |
| Всего: | | 98 |

Объём дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 82 академических часа(ов).

Структура дисциплины для очно-заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

| Семестр | Тип учебных занятий | Количество часов |
|---------|--------------------------|------------------|
| 2 | Лекции | 16 |
| 2 | Практические работы | 24 |
| 2 | Промежуточная аттестация | 18 |
| Всего: | | 58 |

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 122 академических часа(ов).

3. Содержание дисциплины

Тема 1. Основные понятия защищённых информационных систем. Общие принципы построения защищённых информационных систем

Понятие «информационная система». Концепция безопасности информационной системы. Цели обеспечения информационной безопасности. Санкционированный и несанкционированный доступ. Угрозы безопасности и каналы реализации угроз. Уровни защиты информации. Стандарты безопасности. Классы защищённости информационных систем. Нормативная база Российской Федерации и иностранных государств. Современная доктрина информационной безопасности Российской Федерации.

Тема 2. Архитектура информационных систем на основе баз данных. Технологии проектирования баз данных

Трёхуровневая архитектура информационных систем на основе баз данных. Модели данных.

Структура данных. Целостность реляционных данных. Основные этапы проектирования баз данных. Технологии проектирования на основе нормализации. Технологии проектирования на основе модели «Сущность-связь».

Тема 3. Разграничения доступа к ресурсам информационной системы

Основные понятия систем разграничения доступа. Сущность и определение политики безопасности. Основные типы политик безопасности: мандатные, ролевые, контроля целостности информационных ресурсов, избирательного разграничения доступа. Субъектно-объектная модель информационной системы.

Тема 4. Средства обеспечения целостности информационных систем на основе баз данных. Средства обеспечения конфиденциальности информации в системах на основе баз данных

Угрозы целостности информации. Способы противодействия. Понятие и основные свойства транзакций. Механизм блокировок. Декларативная и процедурная ссылки целостности. Способы поддержания ссылочной целостности. Триггеры и правила. Угрозы конфиденциальности информации.

Средства идентификации и аутентификации в СУБД. Средства управления доступом. Виды привилегий.

Использование механизма ролей. Метки безопасности. Использование представлений для обеспечения конфиденциальности информации.

Тема 5. Способы хранения конфиденциальной информации

Положение о конфиденциальной информации в электронном виде. Контентная категоризация. Классификация информации по уровню конфиденциальности. Метки документов. Способы хранения конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация.

Тема 6. Основные направления защиты информации. Организационные меры защиты информации в организации

Защита документов. Защита каналов утечки конфиденциальной информации. Мониторинг действий пользователей. Классификация внутренних нарушителей: неосторожные, манипулируемые, саботажники, нелояльные, мотивированные извне.

Другие градации. Кадровая политика. Определение прав локальных пользователей. Стандартизация программного обеспечения. Организация процедуры хранения физических носителей информации.

Определение уровней контроля информационных потоков. Режимы архива, сигнализации, активной защиты.

Тема 7. Классификация межсетевых экранов. Их политики. Типы окружений межсетевых экранов. Политика безопасности межсетевых экранов

Классификация. Установление TCP-соединения. Пакетные фильтры, набор правил. Пограничные маршрутизаторы.

Межсетевые экраны (МЭ) на основе технологий Stateful Inspection и Host-based. Персональные МЭ и их персональные устройства. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Гибридные технологии МЭ. Трансляция сетевых адресов (NAT). Статическая и скрытая трансляция NAT. Принцип построения окружения МЭ. DMZ-сети. Конфигурация с одной DMZ-сетью. Service Leg конфигурация.

Конфигурация с двумя DMZ-сетями. Виртуальные частные сети. Расположение VPN-серверов. Интранет.

Экстранет. Компоненты инфраструктуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях.

Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы. SMTP-серверы.

Политика МЭ. Реализация его набора правил. Тестирование политики МЭ. Возможные подходы к эксплуатации МЭ а. Сопровождение МЭ и управление им. Физическая безопасность окружения МЭ. Администрирование МЭ. Стратегия восстановления после сбоев. Возможность создания логов МЭ. Инциденты безопасности.

Тема 8. Системы обнаружения атак

Понятие системы обнаружения атак (IDS). Типы и базовая структура IDS. Совместное расположение Host и Target. Разделение Host и управления. Полностью распределённое управление. Network-based IDS, Host-based IDS, Application-based IDS.

Анализ, выполняемый IDS. Определение злоупотреблений. Активные и пассивные ответные действия. Использование SNMP TRAPS. Системы анализа и оценки уязвимостей. Host-based и Network-based анализ уязвимостей. Способы взаимодействия сканера уязвимостей и IDS.

Тема 9. Безопасное использование службы доменных имён (DNS)

Безопасность DNS. Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности. Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS. Name-серверы, Авторитетные и кэширующие Name-серверы. Resolver'ы. Транзакции DNS. Запрос/ответ DNS. Зонная пересылка. Динамические обновления. Безопасность окружения DNS. Угрозы для ПО и данных DNS.

Тема 10. Обеспечение безопасности WEB-серверов. Безопасность WEB-ориентированного контента

Причины уязвимости WEB-сервера. Планирование развёртывания WEB-сервера. Безопасное инсталлирование и конфигурирование используемой ОС. Удаление или запрещение ненужных сервисов и приложений. Управление ресурсами на уровне ОС. Альтернативные платформы для WEB-сервера. Использование Appliances для WEB-сервера. Специально усиленные ОС и WEB-серверы. Тестирование безопасности ОС.

Безопасное инсталлирование и конфигурирование WEB-сервера. Соответствующий список действий. Разграничение доступа для ПО WEB-сервера. Управление доступом к директории содержимого WEB-сервера. Публикации информации на WEB-сайтах.

Обеспечение безопасности технологий создания активного содержимого.

URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента.

Уязвимости технологий создания содержимого на стороне сервера. Необходимые действия для обеспечения безопасности WEB-содержимого.

Тема 11. Технологии аутентификации и шифрования

Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic и Digest аутентификации. SSL/TLS. Возможности и слабые места SSL/TLS. Пример SSL/TLS сессии. Схемы шифрования SSL/TLS. Список действий при использовании технологий аутентификации и шифрования. Firewall прикладного уровня для Web: ModSecurity.

4. Образовательные технологии

| № п/п | Наименование раздела | Виды учебных занятий | Образовательные технологии |
|--------------|---|--|---|
| 1 | 2 | 3 | 4 |
| 1. | <i>Тема 1. Основные понятия защищённых информационных систем. Общие принципы построения защищённых информационных систем.</i> | <i>Лекция 1.1 Лекция 1.2 Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |
| 2 | <i>Тема 2. Архитектура информационных систем на основе баз данных. Технологии проектирования баз данных.</i> | <i>Лекция 2.1 Лекция 2.2 Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |
| 3 | <i>Тема 3. Разграничения доступа к ресурсам информационной системы</i> | <i>Лекция 3.1 Лекция 3.2 Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |
| 4 | <i>Тема 4. Средства обеспечения</i> | <i>Лекция 4.1 Лекция 4.2</i> | <i>Традиционная лекция с использованием презентаций</i> |

| | | | |
|---|--|--|--|
| | <i>целостности информационных систем на основе баз данных. Средства обеспечения конфиденциальности информации в системах на основе баз данных.</i> | <i>Лекция 4.3 Практическое занятие 1. Самостоятельная работа</i> | <i>Выполнение и защита практического задания Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |
| 5 | <i>Тема 5. Способы хранения конфиденциальной информации</i> | <i>Лекция 5.1 Лекция 5.2 Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |
| 6 | <i>Тема 6. Основные направления защиты информации. Организационные меры защиты информации в организации</i> | <i>Лекция 6.1 Лекция 6.2 Практическое занятие 2. Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Выполнение и защита практического задания Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |
| 7 | <i>Тема 7. Классификация межсетевых экранов. Их политики. Типы окружений межсетевых экранов. Политика безопасности межсетевых экранов.</i> | <i>Лекция 7.1 Лекция 7.2 Лекция 7.3 Практическое занятие 3. Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Выполнение и защита практического задания Работа с литературой Консультирование и проверка заданий посредством</i> |
| 8 | <i>Тема 8. Системы обнаружения атак.</i> | <i>Лекция 8.1 Лекция 8.2 Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |
| 9 | <i>Тема 9. Безопасное использование службы доменных имён (DNS)</i> | <i>Лекция 9.1 Лекция 9.2 Практическое занятие 4. Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Выполнение и защита практического задания Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |

| | | | |
|----|--|---|--|
| 10 | <i>Тема 10. Обеспечение безопасности WEB-серверов. Безопасность WEB-ориентированного контента.</i> | <i>Лекция 10.1 Лекция 10.2 Практическое занятие 5. Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Выполнение и защита практического задания Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |
| 11 | <i>Тема 11. Технологии аутентификации и шифрования.</i> | <i>Лекция 11.1 Лекция 11.2 Практическое занятие 6. Самостоятельная работа</i> | <i>Традиционная лекция с использованием презентаций Выполнение и защита практического задания Работа с литературой Консультирование и проверка заданий посредством электронной почты</i> |

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

| Форма контроля | Макс. количество баллов | |
|--|----------------------------------|------------------------------------|
| | За одну работу | Всего |
| Текущий контроль: - опрос - практическое занятие 1-5 - практическое занятие 6 | 2 баллов 6 баллов 8 баллов | 22 баллов 30 баллов 8 баллов |
| Промежуточная аттестация – экзамен | | 40 баллов |
| Итого за семестр | | 100 баллов |

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

| | | |
|--------------------|--------------------|------------|
| 100-балльная шкала | Традиционная шкала | Шкала ECTS |
|--------------------|--------------------|------------|

| | | | |
|----------|---------------------|------------|----|
| 95 – 100 | отлично | зачтено | A |
| 83 – 94 | | | B |
| 68 – 82 | хорошо | | C |
| 56 – 67 | | | D |
| 50 – 55 | | | E |
| 20 – 49 | неудовлетворительно | не зачтено | FX |
| 0 – 19 | | | F |

5.2. Критерии выставления оценки по дисциплине

| Баллы/ Шкала ECTS | Оценка по дисциплине | Критерии оценки результатов обучения по дисциплине |
|-------------------------|--|---|
| 100-83/ A,B | «отлично»/ «зачтено (отлично)»/ «зачтено» | <p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p> |
| 82-68/ C | «хорошо»/ «зачтено (хорошо)»/ «зачтено» | <p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p> |
| 67-50/ D,E | «удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено» | <p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p> |
| 49-0/ F,FX | «неудовлетворительно»/ не зачтено | <p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не</p> |

| Баллы/ Шкала ECTS | Оценка по дисциплине | Критерии оценки результатов обучения по дисциплине |
|-------------------------|-------------------------|--|
| | | <p>владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p> |

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

| № | Вопрос | Реализуемая компетенция |
|-----|--|-------------------------|
| 1. | Что такое информационная система? | УК-4, ОПК-1, ОПК-2 |
| 2. | Основные положения Доктрины информационной безопасности Российской Федерации | УК-4, ОПК-1, ОПК-2 |
| 3. | Основные этапы проектирования баз данных. | УК-4, ОПК-1, ОПК-2 |
| 4. | Что такое нормализация отношений? | УК-4, ОПК-1, ОПК-2 |
| 5. | Основные нормальные формы | УК-4, ОПК-1, ОПК-2 |
| 6. | Особенности ДКНФ | УК-4, ОПК-1, ОПК-2 |
| 7. | Основные понятия систем разграничения доступа | УК-4, ОПК-1, ОПК-2 |
| 8. | Сущность и определение политики безопасности. | УК-4, ОПК-1, ОПК-2 |
| 9. | Основные типы политик безопасности | УК-4, ОПК-1, ОПК-2 |
| 10. | Понятие и основные свойства транзакций | УК-4, ОПК-1, ОПК-2 |
| 11. | Механизм блокировок | УК-4, ОПК-1, ОПК-2 |
| 12. | Средства идентификации и аутентификации в СУБД | УК-4, ОПК-1, ОПК-2 |
| 13. | Межсетевые экраны их виды. Администрирование межсетевых экранов. | УК-4, ОПК-1, ОПК-2 |
| 14. | Демилитаризованная зона, её понятие и структура | УК-4, ОПК-1, ОПК-2 |
| 15. | Составляющие защиты периметра. | УК-4, ОПК-1, ОПК-2 |
| 16. | Особенности периметра современных КС | УК-4, ОПК-1, ОПК-2 |
| 17. | Реализация механизма VPN | УК-4, ОПК-1, ОПК-2 |
| 18. | VPN-клиент, VPN-сервер и шлюз безопасности VPN. | УК-4, ОПК-1, ОПК-2 |
| 19. | Классификация сетей VPN. | УК-4, ОПК-1, ОПК-2 |
| 20. | Протокол PPTP. Структура пакета. | УК-4, ОПК-1, ОПК-2 |
| 21. | Процедура установления SSL-сессии. | УК-4, ОПК-1, ОПК-2 |
| 22. | Защита беспроводных сетей | УК-4, ОПК-1, ОПК-2 |
| 23. | Архитектура стека протоколов IPSec | УК-4, ОПК-1, ОПК-2 |
| 24. | Защита передаваемых данных с помощью протоколов AH и ESP | УК-4, ОПК-1, ОПК-2 |
| 25. | Протокол аутентифицирующего заголовка. | УК-4, ОПК-1, ОПК-2 |
| 26. | Применение протокола AH в транспортном и туннельном | УК-4, ОПК-1, ОПК-2 |

| | | |
|-----|--|--------------------|
| | режимах | |
| 27. | Протокол инкапсулирующей защиты, применение протокола ESP в транспортном и туннельном режимах. | УК-4, ОПК-1, ОПК-2 |
| 28. | Протокол управления криптоключами IKE | УК-4, ОПК-1, ОПК-2 |
| 29. | Задачи, решаемые протоколами IKE | УК-4, ОПК-1, ОПК-2 |
| 30. | Установление безопасной ассоциации | УК-4, ОПК-1, ОПК-2 |
| 31. | Базы данных SAD и SPD | УК-4, ОПК-1, ОПК-2 |
| 32. | Основные схемы применения IPSec | УК-4, ОПК-1, ОПК-2 |
| 33. | Практические аспекты защиты веб-порталов от информационных атак | УК-4, ОПК-1, ОПК-2 |
| 34. | Типовая архитектура веб-портала | УК-4, ОПК-1, ОПК-2 |
| 35. | Подсистемы антивирусной защиты | УК-4, ОПК-1, ОПК-2 |
| 36. | Подсистемы контроля целостности | УК-4, ОПК-1, ОПК-2 |
| 37. | Подсистемы разграничения доступа | УК-4, ОПК-1, ОПК-2 |
| 38. | Подсистемы обнаружения вторжений | УК-4, ОПК-1, ОПК-2 |
| 39. | Сервисы DNS | УК-4, ОПК-1, ОПК-2 |
| 40. | Основные механизмы безопасности для сервисов DNS | УК-4, ОПК-1, ОПК-2 |
| 41. | Причины уязвимости WEB-сервера | УК-4, ОПК-1, ОПК-2 |

Промежуточная аттестация (примерные вопросы для экзамена)

1. Понятие «информационная система». Концепция безопасности информационной системы. Цели обеспечения информационной безопасности. Санкционированный и несанкционированный доступ.
2. Угрозы безопасности и каналы реализации угроз. Уровни защиты информации. Стандарты безопасности.
3. Классы защищённости информационных систем.
4. Нормативная база Российской Федерации и иностранных государств. Современная доктрина информационной безопасности Российской Федерации.
5. Трёхуровневая архитектура информационных систем на основе баз данных. Модели данных.
6. Структура данных. Целостность реляционных данных. Основные этапы проектирования баз данных.
7. Технологии проектирования на основе нормализации.
8. Технологии проектирования на основе модели «Сущность-связь».
9. Основные понятия систем разграничения доступа. Сущность и определение политики безопасности.
10. Основные типы политик безопасности.
11. Угрозы целостности информации. Способы противодействия. Понятие и основные свойства транзакций.
12. Механизм блокировок. Оптимистическая и пессимистическая блокировки
13. Декларативная и процедурная ссылочные целостности.
14. Способы поддержания ссылочной целостности. Триггеры и правила.
15. Средства идентификации и аутентификации в СУБД. Средства управления доступом. Виды привилегий.
16. Положение о конфиденциальной информации в электронном виде. Контентная категоризация.
17. Классификация информации по уровню конфиденциальности. Метки документов.
18. Способы хранения конфиденциальной информации.
19. Защита документов. Защита каналов утечки конфиденциальной информации. Мониторинг действий пользователей.
20. Классификация внутренних нарушителей.

21. Другие градации. Кадровая политика. Определение прав локальных пользователей.
22. Стандартизация программного обеспечения. Организация процедуры хранения физических носителей информации.
23. Определение уровней контроля информационных потоков. Режимы архива, сигнализации, активной защиты.
24. Классификация МЭ. Установление TCP-соединения. Пакетные фильтры, набор правил. Пограничные маршрутизаторы.
25. МЭ на основе технологий Stateful Inspection и Host-based. Персональные МЭ и их персональные устройства. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Гибридные технологии МЭ.
26. Трансляция сетевых адресов (NAT). Статическая и скрытая трансляция NAT.
27. DMZ-сети. Конфигурация с одной DMZ-сетью.
28. Service Leg конфигурация.
29. Конфигурация с двумя DMZ-сетями.
30. Виртуальные частные сети. Расположение VPN-серверов. Интранет.
31. Экстранет. Компоненты инфраструктуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях.
32. Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы. SMTP-серверы.
33. Политика МЭ. Реализация его набора правил. Тестирование политики МЭ.
34. Возможные подходы к эксплуатации МЭ.
35. Сопровождение МЭ и управление им.
36. Физическая безопасность окружения МЭ.
37. Администрирование МЭ.
38. Стратегия восстановления после сбоев. Возможность создания логов МЭ. Инциденты безопасности.
39. Понятие системы обнаружения атак. Типы и базовая структура IDS. Совместное расположение Host и Target.
40. Разделение Host и управления. Полностью распределённое управление. Network-based IDS, Host-based IDS, Application-based IDS.
41. Анализ, выполняемый IDS. Определение злоупотреблений.
42. Активные и пассивные ответные действия. Использование SNMP TRAPS.
43. Системы анализа и оценки уязвимостей. Host-based и Network-based анализ уязвимостей. Способы взаимодействия сканера уязвимостей и IDS.
44. Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности.
45. Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS.
46. Транзакции DNS. Запрос/ответ DNS. Зонная пересылка.
47. Динамические обновления. Безопасность окружения DNS. Угрозы для ПО и данных DNS.
48. Причины уязвимости WEB-сервера. Планирование развёртывания WEB-сервера. Безопасное инсталлирование и конфигурирование используемой ОС.
49. Удаление или запрещение ненужных сервисов и приложений. Управление ресурсами на уровне ОС. Альтернативные платформы для WEB-сервера. Использование Appliances для WEB-сервера. Специально усиленные ОС и WEB-серверы. Тестирование безопасности ОС.
50. Безопасное инсталлирование и конфигурирование WEB-сервера. Соответствующий список действий.
51. Разграничение доступа для ПО WEB-сервера. Управление доступом к директории содержимого WEB-сервера. Публикации информации на WEB-сайтах.
52. Обеспечение безопасности технологий создания активного содержимого.
53. URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента.

54. Уязвимости технологий создания содержимого на стороне сервера. Необходимые действия для обеспечения безопасности WEB-содержимого.
55. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic и Digest аутентификации.
56. SSL/TLS. Возможности и слабые места SSL/TLS. Пример SSL/TLS сессии. Схемы шифрования SSL/TLS.
57. Список действий при использовании технологий аутентификации и шифрования.
58. Технологии RADIUS и TACAS+

Примерные тестовые задания

1. Виртуальная защищённая сеть VPN – это

а) объединение компьютеров в сеть через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть для обеспечения безопасности циркулирующих данных.

б) объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

в) объединение локальных сетей и отдельных компьютеров через глобальную сеть Интернет в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

г) объединение отдельных компьютеров и мобильных устройств через глобальную сеть Интернет в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

2. По признаку «рабочего» уровня модели OSI различают следующие группы VPN:

- а) VPN канального уровня;
- б) VPN прикладного уровня;
- в) VPN сеансового уровня.
- г) VPN сетевого уровня;
- д) VPN транспортного уровня;
- е) VPN представительского уровня.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

основные

1. *Федеральный закон «Об информации, информационных технологиях и о защите информации»* от 27.07.2006 № 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

2. *Федеральный закон «О персональных данных»* от 27.07.2006 № 152-ФЗ (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.

3. *Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)*. (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/bazovaya-model-ot-15-fevralya-2008-g>, свободный. – Загл. с экрана.

дополнительные

4. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-30-marta-1992-g>, свободный. – Загл. с экрана.

5. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-3>, свободный. – Загл. с экрана.

6. *Приказ ФСТЭК России* от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17>, свободный. – Загл. с экрана.

7. *Приказ ФСТЭК России* от 18 февраля 2013 г. № 21. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.. [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21>, свободный. – Загл. с экрана.

Литература

основная

1. *Краковский, Ю. М.* Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. – 3-е изд., перераб. – Санкт-Петербург : Лань, 2021. – 236 с. – ISBN 978-5-8114-5632-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/156401>. -- Режим доступа: для авториз. пользователей.

2. *Запечников, С. В.* Основы построения виртуальных частных сетей: Учебное пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. - Москва : Гор. линия-Телеком, 2011. - 249 с. (Специальность). ISBN 5-93517-139-2, 3000 экз. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/563048>. – Режим доступа: по подписке.

3. *Полищук, Ю. В.* Базы данных и их безопасность : учебное пособие / Ю.В. Полищук, А.С. Боровский. — Москва : ИНФРА-М, 2022. – 210 с. – (Высшее образование: Специалист). – DOI 10.12737/1011088. – ISBN 978-5-16-014924-0. – Текст : электронный. – URL: <https://znanium.com/catalog/product/1811408>. – Режим доступа: по подписке.

дополнительная

4. *Белоус, А. И.* Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. – 692 с. – ISBN 978-5-9729-0486-0. – Текст : электронный. - URL: <https://znanium.com/catalog/product/1167736>. – Режим доступа: по подписке.

5. *Тузовский, А. Ф.* Проектирование и разработка web-приложений : учебное пособие для вузов / А. Ф. Тузовский. — Москва : Издательство Юрайт, 2024. — 219 с. — (Высшее образование). — ISBN 978-5-534-16300-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/537106>.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. *Банк данных угроз безопасности информации.* [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : URL: <https://bdu.fstec.ru/threat>, свободный. – Загл. с экрана.

2. *Методика* определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380>, свободный. – Загл. с экрана.

3. *Видео уроки Cisco Packet Tracer.* Курс молодого бойца. [Электронный ресурс] : Режим доступа : <https://rutube.ru/channel/41927358/videos/>, свободный. – Загл. с экрана.

Национальная электронная библиотека (НЭБ) www.rusneb.ru
 ELibrary.ru Научная электронная библиотека www.elibrary.ru
 Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

| №п /п | Наименование ПО | Производитель | Способ распространения (лицензионное или свободно распространяемое) |
|-------|-----------------------------|---------------|---|
| 1 | Microsoft Office 2010 | Microsoft | лицензионное |
| 2 | Windows 10 Pro | Microsoft | лицензионное |
| 3 | Kaspersky Endpoint Security | Kaspersky | лицензионное |

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

| №п /п | Наименование ПО | Производитель | Способ распространения (|
|-------|--------------------------------|---------------|--------------------------|
| 1 | Microsoft Office 2010 или выше | Microsoft | лицензионное |
| 2 | | | |
| 3 | Kaspersky Endpoint Security | Kaspersky | лицензионное |
| 4 | Cisco Packet Tracer v.8 | Cisco Systems | условно свободное |
| 5 | VMware Workstation 15 Player | VMware, Inc | свободное |
| 6 | или VirtualBox 6.0 | Oracle | свободное |
| 7 | Дистрибутивы Linux (например | Canonical | свободное |

| | | | |
|---|--|----------------------------|-----------|
| | Ubuntu 14) | | |
| 8 | WEB-сервер Apache 2.0 | Apache Software Foundation | свободное |
| 9 | Microsoft SQL Server 2008 R2 (или более поздняя версия) выпуск Express Edition | Microsoft | свободное |

Средства вычислительной техники, сетевое оборудование, техническое, программное и программно-аппаратные средства защиты информации и средствами контроля защищенности информации.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.

- для глухих и слабослышащих: в печатной форме, в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.

Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика практических занятий соответствует программе дисциплины.

Практическое занятие 1

Тема – *Обеспечение целостности информационных систем на основе баз данных*

Продолжительность – 12 уч.ч.

Задания:

1. Разработать макет базы данных в MS SQL Server.
2. Провести нормализацию отношений (таблиц).
3. Ввести в каждую таблицу не менее пяти строк.
4. Создать формы или представления
5. В полученной базе данных в СУБД Microsoft SQL Server создать таблицы персонала, где должны быть указаны подразделения и сотрудники: кадров, руководства, бухгалтерии, финансового подразделения, менеджеров по работе с клиентами, поставок, заказов, склада и т.д.
6. Присвоить соответствующие роли.
7. Создать правила разграничения доступа на основе ролей.
8. Ответить на теоретические вопросы в конце практической работы.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Оформить отчёт по практической работе. Приложением к отчёту служат файлы БД

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС Windows 10 Pro и Microsoft Office 2010.
2. Виртуальная машина с установленной СУБД Microsoft SQL Server

Практическое занятие 2**Тема – Организационные меры защиты информации в организации****Продолжительность – 4 уч.ч.**

Задания:

1. Выбрать организацию из списка предложенных преподавателем.
2. Предложить организационные меры защиты информации.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Составить отчёт о практическом занятии.
3. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010

Практическое занятие 3 Тема – Администрирование межсетевых экранов**Продолжительность – 8 уч.ч.**

Задания:

1. Работа с межсетевым экраном Cisco ASA.
2. Администрирование межсетевых экранов в программе Cisco Packet Tracer.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Собрать схему по топологии в Cisco Packet Tracer в индивидуальном адресном пространстве.
3. Обратит внимание на ограничение лицензии при работе с Cisco ASA в Cisco Packet Tracer
4. При работе в чужом адресном пространстве или с чужой учётной записью задание считается невыполненным.
5. Составить отчёт о практическом занятии.
6. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer

Практическое занятие 43**Тема – Безопасное использование службы доменных имён****Продолжительность – 8 уч.ч.**

Задания:

1. Собрать в Cisco Packet Tracer выданную преподавателем схему.
2. Провести настройку DNS-сервера.
3. Присвоить имена компьютерам.
4. Провести имитацию атаки на сервер.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Использовать IP-адреса только из своего адресного пространства.
3. Имитацию атаки провести с использованием стороннего подключения через терминал
4. При работе в чужом адресном пространстве или с чужой учётной записью задание считается невыполненным.
5. Составить отчёт о практическом занятии.
6. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer

Практическое занятие 5

Тема – Настройка WEB-сервера

Продолжительность – 10 уч.ч.

Задания:

1. Развернуть на виртуальной машине сервер Apache 2.0, MySQL и PHP.
2. Провести настройку WEB-сервера с учётом защиты информации.
3. Создать простой сайт с использованием СУБД MySQL.
4. Атаковать сайт с использованием SQL-инъекций.
5. Добавить код с использованием встроенных функций защиты PHP.
6. Атаковать сайт с использованием SQL-инъекций.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Составить отчёт о практическом занятии.
3. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, виртуальная машина с Apache 2.0, MySQL и PHP

Практическое занятие 6

Тема – Изучение протокола RADIUS

Продолжительность – 10 уч.ч.

Задания:

1. Собрать в Cisco Packet Tracer выданную преподавателем схему.
2. Настроить центр авторизации AAA.
3. Провести настройку DNS-сервера.
4. Присвоить имена компьютерам.
5. Провести имитацию атаки на сервер.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Собрать схемы по топологии в Cisco Packet Tracer в индивидуальном адресном пространстве.
3. При работе в чужом адресном пространстве задание считается невыполненным.
4. Составить отчёт о практическом занятии.
5. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины: профессиональная подготовка магистрантов, необходимая для освоения методов и технологий защиты государственной тайны при работе в автоматизированных информационных системах.

Задачи:

дать знания:

- о нормативных правовых актах в области защищённых информационных систем;
- о методах и средствах разработки защищённых информационных систем.

В результате освоения дисциплины обучающийся должен:

Знать:

современные коммуникативные технологии на государственном и иностранном языках;

закономерности деловой устной и письменной коммуникации;

основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности;

методы концептуального проектирования технологий обеспечения информационной безопасности;

Уметь:

применять на практике коммуникативные технологии, методы и способы делового общения;

проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности;

выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности;

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме оценивания выступлений, докладов на практических занятиях, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 5 зачетные единицы.