УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» мая 2024 г., протокол № 5/24

Председатель _____ / М.А. Волков
«21» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Обнаружение вторжений и защита информации**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	4 - очная форма обучения

Направление (специальность): 02.03.03 Математическое обеспечение и администрирование информационных систем
Направленность (профиль/специализация): Технология программирования
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Иванцов Андрей Михайлович	Кафедра информационной безопасности и теории управления	Доцент,Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Цель курса: заложить методически правильные основы знаний, необходимые будущим специалистам - практикам в области защиты информации.

Задачи освоения дисциплины:

Задачи освоения дисциплины:

Основными задачами дисциплины являются:

- научить применять стандартные средства защиты от несанкционированного доступа в вычислительных сетях.

- ознакомить обучаемых с основным направлениями и методами защиты интрасетей от вторжений.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Обнаружение вторжений и защита информации» относится к числу дисциплин блока Б1.В.1, предназначенного для студентов, обучающихся по направлению: 02.03.03 Математическое обеспечение и администрирование информационных систем.

В процессе изучения дисциплины формируются компетенции: ПК-2, ПК-3, ПК-4, ПК-5.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Эксплуатационная практика, Проектно-технологическая практика, Проектная деятельность, Подготовка к сдаче и сдача государственного экзамена, Проектирование информационных систем, Современные системы автоматизации разработки информационных систем, Разработка мобильных приложений, Инструментальные средства для визуального программирования, Программирование для Интернет, Высокопроизводительные вычисления, Программирование на языке Java, Информационные сети, 1С: Предприятие для программистов и системных администраторов, Открытые технологии разработки программного обеспечения, Объектно-ориентированное программирование, Системы реального времени, Метрология, стандартизация и сертификация информационных технологий, Компьютерная геометрия и графика, Методы программирования современных информационных систем, Администрирование информационных систем, Криптографические методы защиты информации, Преддипломная практика, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Методы разработки программного обеспечения, Технологическая (проектно-технологическая) практика, Представление знаний, Параллельное программирование, Методы и системы обработки больших данных, Сетевое программирование, Функциональное программирование, Интеллектуальные системы и технологии, Методы машинного обучения, Операционные системы, Графический дизайн, Базы данных, Web-технологии, Системы принятия решений, Имитационное моделирование, Теория систем и системный анализ, Численные методы, Управление стартапами в технологическом

предпринимательстве.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ПК-2 Способен использовать основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов, а также способен использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов	**знать**: Основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов Основные методы защиты интрасетей от вторжений **уметь**: Использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов **владеть**: Методами и средствами автоматизации, связанными с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов
ПК-3 Способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств; операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности	**знать**: Основные методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов **уметь**: Использовать знания методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов с точки зрения обеспечения информационной безопасности **владеть**: Навыками администрирования и модернизации программных продуктов и программных комплексов основных подсистем информационной безопасности объекта защиты
ПК-4 Способен использовать основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений	**знать**: Основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений **уметь**: Использовать основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования **владеть**: Навыками использования основных концептуальных положений функционального, логического, объектно-ориентированного и визуального направлений программирования

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-5 Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	**знать**: Современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования **уметь**: Использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования **владеть**: Навыками использования современных методов разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 4 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 144 часа

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		8
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	50	50
Аудиторные занятия:	50	50
Лекции	20	20
Семинары и практические занятия	10	10
Лабораторные работы, практикумы	20	20
Самостоятельная работа	58	58
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Экзамен (36)	Экзамен
Всего часов по дисциплине	144	144

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 1. Атаки на интрасети							
Тема 1.1. Основные понятия в области защиты информации	4	2	0	0	0	2	
Тема 1.2. Источники угроз информационной безопасности в информационных системах	16	2	0	2	0	12	Тестирование
Тема 1.3. Классификация вторжений. Типовые удаленные атаки	6	2	2	0	0	2	Тестирование
Тема 1.4. Интрасети и причины, способствующие атакам	6	2	0	0	0	4	Тестирование
Тема 1.5. Основные методы, используемые нарушител	8	2	2	0	0	4	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
ями для проникновения в интрасети.							
Раздел 2. Основные методы и средства защиты интрасетей от вторжений							
Тема 2.1. Многоуровневая защита интрасетей.	12	2	2	2	0	6	Тестирование
Тема 2.2. Технологии межсетевых экранов	22	4	2	6	6	10	Тестирование
Тема 2.3. Системы обнаружения вторжений	16	2	2	4	4	8	Тестирование
Тема 2.4. Методы и средства защиты информации от утечки по техническим каналам.	18	2	0	6	0	10	Тестирование
Итого подлежит изучению	108	20	10	20	10	58	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Атаки на интрасети

Тема 1.1. Основные понятия в области защиты информации

Цели и задачи курса. Объект и предмет изучения. Базовые понятия и определения. Общие принципы обеспечения защиты информации

Тема 1.2. Источники угроз информационной безопасности в информационных системах

Понятие угрозы. Классификация источников угроз информационной безопасности. Внешние источники угроз. Внутренние источники угроз. Противодействие угрозам. Модель нарушителя

Тема 1.3. Классификация вторжений. Типовые удаленные атаки

Дана краткая история вторжений (атак) на интрасети и определения основных по-нятий. Приведён вариант классификация вторжений (атак). Рассмотрены типовые удаленные атаки (анализ сетевого трафика, подмена доверенного субъекта, введение ложного объекта компьютерной сети, отказ в обслуживании). Приведены подходы к защите от типовых удаленных атак. Уязвимости интрасетей со стороны всевозможных атак. Роль администрирования интрасетей для защиты их от вторжений

Тема 1.4. Интрасети и причины, способствующие атакам

Понятие интрасети и задачи её защиты. Виды интрасетей. Основные технологии, необходимые для создания интрасетей. Уязвимости интрасетей со стороны всевозможных атак. Роль администрирования интрасетей для защиты их от вторжений.

Тема 1.5. Основные методы, используемые нарушителями для проникновения в интрасети.

Основные методы развертывания атак на интрасети, а именно: классические мето-ды (подбор пароля, метод «грубой силы», метод «зашифровать и сравнить», социальная инженерия); современные методы (перехват данных, мониторинг в системе X Window, подмена системных утилит, нападения с использованием сетевых протоколов ("Летучая смерть", SYN-бомбардировка, спуффинг).

Раздел 2. Основные методы и средства защиты интрасетей от вторжений

Тема 2.1. Многоуровневая защита интрасетей.

Рассматриваются уровни, обеспечивающие эффективную защиту сети. Она скла-дывается из следующих основных компонентов: политики безопасности интрасети организации; сетевого аудита; защиты на основе межсетевых экранов и систем обнаружения вторжений.

Тема 2.2. Технологии межсетевых экранов

Рассмотрена технология межсетевых экранов (МЭ) - одна из самых первых технологий защиты корпоративных сетей от внешних угроз. Показано, что МЭ способствует реализации политики безопасности, определяет разрешенные службы, типы доступа к ним и является реализацией этой политики в терминах сетевой конфигурации, хостов, маршрутизаторов и других мер защиты. Функции МЭ. Рассмотрена защита корпоративных сетей на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности

неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI (экранирующий маршрутизатор, шлюз сеансового уровня, шлюз прикладного уровня).

Тема 2.3. Системы обнаружения вторжений

Классификация систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений. Роль хоста-бастиона при обнаружении вторжений.

Тема 2.4. Методы и средства защиты информации от утечки по техническим каналам.

Основные методы и средства защиты информации от утечки в электромагнитном и акустическом (виброакустическом) каналах (экранирование, зашумление и фильтрация опасных сигналов). Средства противодействия перехвату «информации по техническим каналам.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Атаки на интрасети

Тема 1.3. Классификация вторжений. Типовые удаленные атаки

Вопросы к теме:

Очная форма

1. Обнаружение вторжений. Краткий исторический обзор.
2. Классификация вторжений (атак).
3. Типовые удаленные атаки (анализ сетевого трафика, подмена доверенного субъекта, введение ложного объекта компьютерной сети, отказ в обслуживании).

Тема 1.5. Основные методы, используемые нарушителями для проникновения в интрасети.

Вопросы к теме:

Очная форма

1. Классические методы (подбор пароля, метод «грубой силы», метод «зашифровать и сравнить», социальная инженерия).
2. Современные методы (перехват данных, мониторинг в системе X Window, подмена системных утилит, нападения с использованием сетевых протоколов ("Летучая смерть", SYN-бомбардировка, спуффинг).

Раздел 2. Основные методы и средства защиты интрасетей от вторжений

Тема 2.1. Многоуровневая защита интрасетей.

Вопросы к теме:

Очная форма

1. Политика безопасности интрасети организации.
2. Сетевой аудит.
3. Системы обнаружения вторжений и межсетевые экраны.

Тема 2.2. Технологии межсетевых экранов

Вопросы к теме:

Очная форма

1. Классификация межсетевых экранов.
2. Функции межсетевых экранов.
3. Особенности функционирования межсетевых экранов на различных уровнях мо-дели OSI (экранирующий маршрутизатор, шлюз сеансового уровня, шлюз прикладного уровня).

Тема 2.3. Системы обнаружения вторжений

Вопросы к теме:

Очная форма

1. Классификация систем обнаружения вторжений.
2. Интеллектуальное и поведенческое обнаружение вторжений.
3. Роль хоста-бастиона при обнаружении вторжений.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Выработка концептуальных основ деятельности по обеспечению информационной безопасности предприятия
Цели: Анализ информационных активов, используемых компанией и выработка концептуаль-ных основ деятельности по обеспечению корпоративной информационной безопасности.
Содержание: Содержание лабораторной работы: «Выработка концептуальных основ деятельности по обеспечению информационной безопасности предприятия». Методические указания: основное внимание должно быть уделено практическому выявлению угроз и базовых уязвимостей конкретных информационных активов предприятия, а также выбору методов и средств противодействия имеющимся угрозам информационной безопасности. Задачи: 1. Установить

номенклатуру информационных активов и оценить их значимость для выбранной компании (в соответствии с вариантом) в целом и для ее структурных подразделений. 2. Выявить виды и разновидности тайн, которые используются в деятельности рассматриваемой компании (в соответствии с вариантом). 3. Оценить риски информационной безопасности для рассматриваемой компании (в соответствии с вариантом). Порядок оформления и сдачи 1. Шрифт Times New Roman 14. Интервал 1. Поля стандартные. Страницы работы должны быть пронумерованы. Формат документа — MS Office. 2. Крайний срок сдачи лабораторного практикума до начала зачетной недели. Студенты, не представившие лабораторный практикум, к зачету не допускаются. Задание 1 Описание компании и ее структурных подразделений (Компания выбирается в соответствии с вариантом). a. Укажите наименование компании и адрес ее корпоративного сайта (придумать свой собственный адрес). b. Дайте описание деятельности компании, её направлений (3-4) и бизнес-целей (3-4). c. Опишите основные показатели деятельности компании, характеризующие её масштабы (3-4 показателя), и приведите примерные числовые значения за какой-то период или дату; d. В MS Visio или другом графическом редакторе составьте функциональную блок-схему компании в выбранном варианте. Детализацию производить до уровня отделов. e. Постройте схему, характеризующую архитектуру ИТ-сети компании, ее программные и аппаратные компоненты. Задание 2 Определение номенклатуры информационных активов a. Определите базовые уязвимости и угрозы в сфере информационной безопасности для деятельности компании. b. Для каждого структурного подразделения определите информационные активы. Заполните Таблицу 1. Ниже рассмотрен вариант для наиболее актуальных активов. Таблица 1 Вид актива Наименование актива Владелец (наименование отдела) Угрозы (Уязвимости) Обоснование выбранной степени важности (от 1 до 10 баллов) Персональные данные БД на сервере Рук. ИТ отдела - Пожар - Хищение - Отключение электропитания - Землетрясение - - ……. - …….. …….. …….. …… …… …… ……. Перс. данные на бумажных носителях Рук. Отдела кадров …….. …… Коммерческая тайна Финансы, НОУ-ХАУ и др. Рук. Производств. отделов …….. …… Банковская тайна Служебная тайна Государственная тайна Для выполнения данного пункта необходимо внимательно ознакомиться: - с пунктом 7 стандарта ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. (Ранее был ГОСТ Р ИСО/МЭК 17799-2005); - с текстом ФЗ «О коммерческой тайне»; - с текстом ФЗ «О персональных данных». Задание 3 Определите примерный перечень сведений, составляющих коммерческую (служебную, банковскую) тайну компании. Заполните Таблицу 2. Таблица 2 № п/п Сведения, составляющие коммерческую (служебную) тайну Сотрудники каких подразделений допущены к данным сведениям 1. Ноу-хау Вашего предприятия 2. Инф, входящая в финансовые документы и др. … Для выполнения данного пункта (в отношении информации, относящейся к коммерческой тайне) необходимо внимательно ознакомиться с текстом ФЗ «О коммерческой тайне». Задание 4 Для сведений, составляющих тайны, и информационных активов, включающих соответствующие данные, определите – на каких носителях эти данные находятся. Заполните Таблицу 3. Таблица 3 № п/п Вид тайны В состав какого информационного актива входят соответствующие данные На каких носителях распространяются соответствующие данные Задание 5 Для сведений, составляющих тайны, и информационных активов, включающих соответствующие данные, определите представляющие наибольшую угрозу. Заполните Таблицу 4. Таблица 4 № п/п Вид тайны В состав какого информационного актива входят соответствующие данные Способы дистанционного добывания 1. Коммерческая Интернет, ……. 2. Персональные данные 3. Банковская Задание 6 Распределите информационные активы, содержащие сведения, составляющие тайны, по зонам доступа. Заполните Таблицу 5. Таблица 5 № п/п Информационные активы Какие виды тайн содержат В какой зоне должны находиться На территории предприятия В охраняемой

зоне (в помещении) В сейфе охраняемого помещения …….. Задание 7 Определите наиболее опасные каналы утечки информации, способы и средства противодействия утечке. Заполните Таблицу 6. Таблица 6 № п/п Информационные активы Наиболее опасные каналы утечки для каждого актива Средство противодействия утечке 1 База данных персонал - Интернет -хищение носителей - излучения и наводки - вербовка – сотрудников - ……. - Межсетевые экраны, установка Спец. систем противодействия вторжениям - физическая защита и др. - специальные системы зашумления и др. - ……. - ……
Результаты: Проведён анализ информационных активов, используемых компанией и выработаны концептуальные основы деятельности по обеспечению корпоративной информационной безопасности. Подготовлен отчёт
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4270
Разработка Политик ИБ предприятия
Цели: Анализ информационных активов, используемых компанией и выработка концепции основ деятельности по обеспечению корпоративной информационной безопасности.
Содержание: Разработка основных частных политик выбранного предприятия
Результаты: Проанализированы информационные активы, используемых компанией и выработана концепция основ деятельности по обеспечению корпоративной информационной безопасности. Результат: отчет.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4270
Назначение и возможности встроенных межсетевых экранов (МЭ).
Цели: - изучить возможности встроенных межсетевых экранов (МЭ) на примере выбранного МЭ; - научиться администрировать выбранный МЭ.
Содержание: Методика выполнения лабораторной работы включает в себя следующие положения: 1. Если исследуемый МЭ – встроенный брандмауэр используемой операционной системы, то надо просто зайти в него. 2. Если исследуемый МЭ – не является встроенным, то необходимо его загрузить. 3. Произвести выборочное администрирование МЭ, изменяя те или иные параметры. Фиксировать изменения фильтрации трафика.
Результаты: - изучены возможности встроенных межсетевых экранов (МЭ) на примере выбранного МЭ; - студентами продемонстрированы навыки администрирования выбранного МЭ.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4270
«Назначение и возможности системы защиты от НСД «Dallas Lock».
Цели: Изучить программно-аппаратный комплекс средств защиты информации Dallas Lock -K (C) и получить навыки установки, настройки и практического использования комплекса.
Содержание: Методика выполнения лабораторной работы включает в себя следующие положения: 1. Если на компьютере уже установлена система защиты, ее необходимо удалить. 2. Необходимо убедиться, что на диске C имеется необходимое свободное пространство для установки системы защиты. 3. Проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows, и устранить выявленные дефекты. 4. Рекомендуется произвести дефрагментацию диска. 5. Проверить компьютер на отсутствие компьютерных вирусов. 6. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы. 7. Закрыть все запущенные приложения, так как установка системы потребует принудительной перезагрузки.
Результаты: Изучены возможности программно-аппаратного комплекса средств защиты информации Dallas Lock -K (C) и получены навыки установки, настройки и практического использования комплекса.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4270

Система SecretNet Studio. «Назначение, возможности и порядок работы с системой SecretNet Studio».
Цели: изучить возможности и научиться работать с системой SecretNet Studio. Результат: отчет.
Содержание: В данной работе необходимо произвести установку СЗИ и настройку локальной защиты АРМ пользователя. Для локальной защиты необходимо: - обозначить его права по доступу к ресурсам, находящимся на АРМ; - ограничить использование внешних носителей; - настроить механизм замкнутой программной среды (список программ, возможных к запуску); - настроить механизм теневого копирования и маркировки; - обеспечить контроль целостности ресурсов, находящихся на АРМ. Методика выполнения лабораторной работы включает в себя следующие положения: 1. Ознакомление с теоретической частью «Secret Net Studio». 2. Установка программного обеспечения средства защиты информации «Secret Net Studio» на локальный ПК. 3. Подготовка средства защиты информации к инициализации. 4. Инициализация «Secret Net Studio». 5. Подготовка к эксплуатации. 6. Настройка и эксплуатация «Secret Net Studio». 7. Удаление программного обеспечения «Secret Net Studio».
Результаты: Изучены возможности и получены навыки работы с системой SecretNet Studio. Результат: отчет.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4270
«Изучение методов поиска и локализации специальных технических средств с использованием прибора ST-032 Пиранья».
Цели: Изучить возможности прибора ST 032 «Пиранья» и научиться осуществлять поиск и локализацию специальных технических средств несанкционированного получения информации
Содержание: Работа проводится в игровом варианте попарно в два этапа. Первый студент – «злоумышленник» (З), второй – сотрудник службы безопасности (СБ). На первом этапе З изучает технические характеристики и правила эксплуатации многофункционального имитатора ИМФ-2 (Приложение 1), а СБ – технические характеристики, правила эксплуатации и методику поиска каналов утечки информации с помощью поискового комплекса «Пиранья ST-032». Перед началом практических действий оба игрока отвечают на контрольные вопросы преподавателя с целью проверки уровня их подготовки. Контрольные вопросы приведены ниже. Затем, СБ на некоторое время (1…2 мин) покидает аудиторию. За это время З должен включить ИМФ-2 в режим радиозакладки и где-либо замаскировать или спрятать в личных вещах присутствующих в аудитории студентов. Для создания акустического фона, вызывающего функционирование ИМФ-2 может использоваться магнитофонная запись или доклад одного из присутствующих студентов. Вошедший в аудиторию СБ начинает поиск радиозакладки с использованием ST-032. При этом фиксируется время начала и окончания поиска. На втором этапе игроки меняются ролями. Аналогично работает вторая и последующие пары игроков в группе. Победители определяются в двух номинациях: среди сотрудников службы безопасности и «злоумышленников». В первом случае лучшим признается тот студент, который затратил минимальное время на обнаружение и локализацию радиозакладки, во втором – тот, чью закладку искали максимальное время. Выполнение работы оценивается «зачет» – «не зачет». Изучение других режимов поиска осуществляется демонстрационным методом. Для этого ИМФ-2 последовательно переводится в различные режимы работы для имитации работы закладок по ИК-каналу, телефонной линии и сети электропитания. Переключением режимов работы ST-032 обнаруживаются каналы утечки. Для проверки детектора низкочастотных полей целесообразно продемонстрировать съем информации с наушников, подключенных к сотовому телефону в режиме воспроизведения музыкального файла.
Результаты: Изучены возможности прибора ST 032 «Пиранья», получены навыки поиска и локализацию специальных технических средств несанкционированного получения информации

Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4270
«Обнаружение радиозлучающих устройств с использованием сканирующего радиоприемника AR-3000A».
Цели: Ознакомление с техническими характеристиками изделия AR-3000A, изучение правил эксплуатации изделия, получение практических навыков работы с изделием.
Содержание: При подготовке к использованию прибора по назначению необходимо выполнить следующие операции: - Подсоедините соответствующую антенну к байонетному разъему на задней панели. - Подсоедините к приемнику нужный источник питания, используя либо данный блок питания, либо 12-ти вольтовой кабель. - После включения установите уровень громкости в положение «10», ручку бесшумной настройки в положение 12 и убедитесь, что переключатель дистанционного управления в положении (OFF). - Включите питание. Убедитесь, что ни один из указанных символов <KEYLOCK>, <RMT>, <PAUSE> не появился на ЖКИ-дисплее при первом включении. - Уберите эти символы с дисплея при их появлении как указано выше. - После указанной процедуры приемник готов к вводу частоты и режима приема. Основные действия в каждом отдельном режиме приема Режим ввода: - В этом режиме можно выбрать частоту для немедленного прослушивания, ввод частоты произойдет после нажатия кнопки (DIAL). Выбор частоты приема можно осуществить с помощью десятичных кнопок, кнопок (UP/DOWN) или ручки настройки. Прямой ввод с помощью кнопок: Выберите частоту коммерческого авиационного диапазона 133,7 МГц в режиме AM. - Нажмите [DIAL]. - Нажмите [MODE]. Нажмите [UP/DOWN] или поверните ручку настройки, пока на ЖКД не появится индикатор <AM>. Нажмите [ENTER]. - Последовательно нажмите клавиши [STEP] [2] [5] [ENTER]. В данном случае в этом нет необходимости, однако тем самым Вы установите разнос между каналами в 25 кГц, предусмотренный для коммерческого авиационного диапазона, и приемник в дальнейшем будет точно настраиваться на другие станции при вращении ручки настройки. Если Вы желаете прослушивать только частоту 133,7 МГц без дальнейшей перестройки, этот пункт может быть опущен. - Последовательно нажмите клавиши [1] [3] [3] [.] [7] [ENTER]. Теперь приемник точно настроен на частоту 133,7 МГц в режиме AM. Если при наборе частоты Вы допустили ошибку, нажмите клавишу [ENTER] и начните набор сначала. Режим программного поиска в диапазоне 118-138 МГц с шагом 25 кГц, в режиме AM: - Нажмите последовательно [2nd F] [SEARCH SET]. На дисплее появится мигающий символ <SEARCH>. Кнопкой [UP/DOWN] установите режим AM, затем нажмите клавишу [ENTER]. - На дисплее появится мигающий символ <STEP>. Нажмите [2] [5] [ENTER], чтобы установить шаг, равный 25 кГц. - На дисплее появится символ <L> - приемник запрашивает нижнюю (исходную) частоту. Нажмите [1] [1] [8] [ENTER]. - На дисплее появится символ <H> - приемник запрашивает верхнюю (конечную) частоту. Нажмите [1] [3] [8] [ENTER]. На дисплее появится символ <P>, приемник автоматически начинает поиск. При обнаружении сигнала - поиск приостановится. Для его возобновления, пока присутствует сигнал, Вы можете слегка покрутить ручку настройки или нажать [UP/DOWN]. - Для прекращения программного поиска нажмите [SEARCH], для его возобновления повторно нажмите [SEARCH]. Введенные Вами параметры занесены в память, они не пропадут даже при выключении приемника. Чтобы вести поиск в имеющихся в памяти диапазонах, выберите соответствующий диапазон и нажмите [SEARCH]. Более подробное описание основных практических действий с приёмником AR3000A приведено в Приложении 2. Полное описание практических действий изложено в технической документации на поисковый приёмник AR3000A.
Результаты: Студенты ознакомились с техническими характеристиками изделия AR-3000A, получены практические навыки работы с изделием.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/4270

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Базовые понятия и определения информационной безопасности
2. Основные принципы организации защиты информации
3. Угрозы информационной безопасности и их проявления
4. Классификация источников угроз информационной безопасности
5. Модель действий нарушителя
6. Обнаружение вторжений (атак). Краткий исторический обзор
7. Классификация вторжений (атак)
8. Типовые удаленные атаки. Анализ сетевого трафика
9. Типовые удаленные атаки. Подмена доверенного субъекта
10. Типовые удаленные атаки. Введение ложного объекта компьютерной сети
11. Типовые удаленные атаки. Отказ в обслуживании
12. Понятие интрасети и задачи ее защиты
13. Проблемы безопасности интрасетей
14. Классические методы, используемые нарушителями для проникновения в интрасети. Метод «подбор пароля»
15. Классические методы, используемые нарушителями для проникновения в интрасети. Метод «грубой силы»
16. Классические методы, используемые нарушителями для проникновения в интрасети. Метод «зашифровать и сравнить».
17. Классические методы, используемые нарушителями для проникновения в интрасети. Социальная инженерия
18. Современные методы, используемые нарушителями для проникновения в интрасети. Метод «перехват данных»
19. Современные методы, используемые нарушителями для проникновения в интрасети. Метод «мониторинг в системе X Window»
20. Современные методы, используемые нарушителями для проникновения в интрасети. Метод «подмена системных утилит»
21. Современные методы, используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов "Летучая смерть"
22. Современные методы, используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов «SYN-бомбардировка»
23. Современные методы, используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов «спуффинг»
24. Многоуровневая защита интрасетей. Политика безопасности интрасети организации
25. Многоуровневая защита интрасетей. Сетевой аудит
26. Классификация межсетевых экранов
27. Функции межсетевых экранов
28. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

Экранирующий маршрутизатор
29. Особенности функционирования межсетевых экранов на различных уровнях моделиOSI. Шлюз сеансового уровня
30. Особенности функционирования межсетевых экранов на различных уровнях моделиOSI. Экранирующий маршрутизатор
31. Особенности функционирования межсетевых экранов на различных уровнях моделиOSI. Шлюз прикладного уровня
32. Назначение и возможности системы защиты информации от НСД«Dallas Lock»
33. Классификация систем обнаружения вторжений
34. Интеллектуальное и поведенческое обнаружение вторжений
35. Роль хоста-бастиона при обнаружении вторжений
36. Назначение, возможности и порядок работы с системой SecretNet Studio»
37. Назначение и возможности сканирующего радиоприемника AR-3000A
38. Назначение и возможностиприбора ST-032 «Пиранья»

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Атаки на интрасети			
Тема 1.1. Основные понятия в области защиты информации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Вопросы к экзамену
Тема 1.2. Источники угроз информационной безопасности в информационных системах	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	12	Вопросы к экзамену, Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Тема 1.3. Классификация вторжений. Типовые удаленные атаки	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Вопросы к экзамену, Тестирование
Тема 1.4. Интрасети и причины, способствующие атакам	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 1.5. Основные методы, используемые нарушителями для проникновения в интрасети.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Раздел 2. Основные методы и средства защиты интрасетей от вторжений			
Тема 2.1. Многоуровневая защита интрасетей.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Вопросы к экзамену, Тестирование
Тема 2.2. Технологии межсетевых экранов	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Вопросы к экзамену, Тестирование
Тема 2.3. Системы обнаружения вторжений	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Вопросы к экзамену, Тестирование
Тема 2.4. Методы и средства защиты информации от утечки по техническим каналам.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Вопросы к экзамену, Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Щеглов А. Ю. Защита информации: основы теории : учебник / А. Ю. Щеглов, К. А. Щеглов. - Москва : Юрайт, 2024. - 349 с. - (Высшее образование). - URL: https://urait.ru/bcode/557073 . - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - ISBN 978-5-534-19762-4. / .— ISBN 0_546557

2. Внуков А. А. Защита информации : учебное пособие / А. А. Внуков. - 3-е изд. ; пер. и доп. - Москва : Юрайт, 2024. - 161 с. - (Высшее образование). - URL: https://urait.ru/bcode/537247 . - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - ISBN 978-5-534-07248-8 : 759.00. / .— ISBN 0_529450

3. Зенков А. В. Информационная безопасность и защита информации : учебное пособие / А. В. Зенков. - 2-е изд. ; пер. и доп. - Москва : Юрайт, 2024. - 107 с. - (Высшее образование). - URL: https://urait.ru/bcode/544290 . - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - ISBN 978-5-534-16388-9 : 389.00. / .— ISBN 0_529148

дополнительная

1. Новиков В.К. Информационное оружие - оружие современных и будущих войн : монография / В.К. Новиков ; Новиков В.К. - Москва : Горячая линия - Телеком, 2013. - 262 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991201667.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0166-7. / .— ISBN 0_242555

2. Туманов С.А. Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" : учебно-методическое пособие / С.А. Туманов, И.Л. Рева ; Туманов С.А.; Рева И.Л. - Москва : НГТУ, 2016. - 56 с. - URL: https://www.studentlibrary.ru/book/ISBN9785778228269.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-7782-2826-9. / .— ISBN 0_249836

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Обнаружение вторжений и защита информации» для студентов бакалавриата по направлению 02.03.03 «Математическое обеспечение и администрирование информационных систем» и 09.03.03 «Прикладная информатика» очной формы обучения / А. М. Иванцов ; УлГУ, Фак. математики, информ. и авиац. технологий. - 2020. - Загл. с экрана. - Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 363 КБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/4270. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_37889.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Академическая лицензия на УМК ViPNet "Защита сетей"
- Альт рабочая станция
- Комплект «Максимальная защита» Средства защиты информации Secret Net Studio 8

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Доцент Кандидат технических наук, Доцент	Иванцов Андрей Михайлович
	Должность, ученая степень, звание	ФИО