УТВЕРЖДЕНО
решением Ученого совета ФМИАТ
«16» мая 2023 г., протокол № 4/23
Председатель _____ Волков М.А.
(подпись, расшифровка подписи)
«16» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Разработка и эксплуатация автоматизированных систем в защищённом исполнении
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

Специальность: 10.05.03 "Информационная безопасность автоматизированных систем"
(код специальности (направления), полное наименование)

Специализация: "Безопасность открытых информационных систем"
полное наименование

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: « 01 » 09 2023 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	ИБ и ТУ	Кандидат технических наук, доцент
Клочков Андрей Евгеньевич	ИБ и ТУ	Старший преподаватель

СОГЛАСОВАНО
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
_____ / Андреев А.С. / *(подпись) (Ф.И.О.)* « 11 » 05 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Основной целью освоения дисциплины «Разработка и эксплуатация автоматизированных систем в защищённом исполнении» является формирование у студентов знаний о защищённых автоматизированных системах, их разработке и эксплуатации. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач по обеспечению необходимого уровня информационной безопасности автоматизированных систем.

Задачи освоения дисциплины:

- изучение принципов эксплуатации защищённых автоматизированных систем;
- овладение средствами и методами проектирования и разработки защищенных автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Разработка и эксплуатация автоматизированных систем в защищённом исполнении» изучается в 8 семестре и относится к обязательной части дисциплин блока Б1.О специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Курс учебной дисциплины тесно увязан с другими учебными дисциплинами, в первую очередь с курсами «Физика», «Электроника и схемотехника», «Безопасность операционных систем», «Основы информационной безопасности», «Методы и средства защиты информации от утечки по техническим каналам», «Системы и сети передачи информации», «Языки программирования», позволяющими понять физическую сущность разработки и эксплуатации защищённых автоматизированных систем.

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области физики, вычислительной техники, электроники и схемотехники;

способность использовать нормативные правовые документы;

способность анализировать проблемы и процессы;

способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Безопасность сетей ЭВМ»; «Аттестация объектов информатизации»; «Инструментальные средства контроля защищенности информации»; «Сертификация средств защиты информации».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	**Знать:** основные задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации **Уметь:** решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи **Владеть:** навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий
ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	**Знать:** основные средства криптографической защиты информации, используемые при решении задач профессиональной деятельности **Уметь:** правильно использовать основные средства криптографической защиты информации при решении задач профессиональной деятельности **Владеть:** навыками правильного использования основных средств криптографической защиты информации при решении задач профессиональной деятельности
ОПК-14 - Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	**Знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах **Уметь:** осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования типовых проектных решений **Владеть:** навыками осуществления разработки, внедрения и эксплуатации автоматизированных систем с учетом требований по защите информации

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 5.

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

Вид учебной работы	**Количество часов (форма обучения ___*очная*_____)**			
	Всего по плану	**В т.ч. по семестрам**		
		8 семестр		
Контактная работа обучающихся с преподавателем	90/90	90/90*		
Аудиторные занятия:	90/90	90/90*		
Лекции	36/36	36/36*		
Практические и семинарские занятия	18/18	18/18*		
Лабораторные работы (лабораторный практикум)	36/36*	36/36*		
Самостоятельная работа	54	54		
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на лекциях; - вопросы при защите лабораторных работ		
Курсовая работа		+		
Виды промежуточной аттестации (экзамен, зачет)	экзамен	экзамен 36		
Всего часов по дисциплине:	180 с экзаменом	180 с экзаменом		

* В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения очная

Название разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практ. занятия, семинар	Лабораторные работы			
Раздел 1. Понятия и сущность защищённых автоматизированных систем							
1. Основные понятия и классификация защищен-ных автоматизированных систем	10	4	2			4	Тесты Т1,
2. Основы защиты информации в защищенных автоматизированных системах	10	4	2			4	Тесты Т2,
3. Угрозы безопасности информации в защищенных автоматизированных системах	16	4	2	4		6	Тесты Т3, лаб. раб. 1
4. Программно-техничес-кий уровень защиты автоматизированных систем	20	4	2	8	8	6	Тесты Т4, лаб. раб. 2-3
Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем							
5. Основы организации разработки защищенных АС	10	4	2			4	Тесты Т5,
6. Общие принципы проектирования защищенных АС	10	4	2			4	Тесты Т6,
7. Основы эксплуатации защищенных АС	20	4	2	8	8	6	Тесты Т7, лаб. раб. 4
8. Криптографические протоколы обеспечения безопасности	16	4	2	4		6	Тесты Т9, лаб. раб. 5
9. Основы администрирования АС	32	4	2	12	2	14	Тесты Т9, лаб. раб. 6-7
Итого:	144	36	18	36	18	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Понятия и сущность защищённых автоматизированных систем

Тема 1. Основные понятия и классификация защищенных автоматизированных систем

Классификация автоматизированных систем (АС). Информационные технологии, используемые в АС. Жизненный цикл АС. Основные угрозы безопасности информации в автоматизированных системах. Отказоустойчивость АС.

Тема 2. Основы защиты информации в защищенных автоматизированных системах

Понятия информации и информационных ресурсов. Предмет защиты информации. Объект защиты информации. Понятие информационной безопасности. Понятие политики информационной безопасности. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем. Стадия выработки требований. Стадия определения способов защиты. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты. Основные принципы обеспечения информационной безопасности в автоматизированной системе (АС). Принципы, позволяющие реализовать положения по защите АС. Принцип системности. Принцип комплексности. Принцип непрерывной защиты.

Тема 3. Угрозы безопасности информации в защищенных автоматизированных системах

Понятие угрозы безопасности. Понятие атаки. Понятие злоумышленника. Источники угроз. Окно опасности. Базовые признаки угроз информационной безопасности. Классификация угроз. Доступность информации. Угроза доступности. Целостность информации. Угроза нарушения целостности. Конфиденциальность информации. Угроза нарушения конфиденциальности. Угроза раскрытия параметров АС. Методы обеспечения информационной безопасности. Структуризация методов обеспечения информационной безопасности. Уровни доступа к защищаемой информации. Основные направления и методы реализации угроз информационной безопасности. Классификация злоумышленников.

Тема 4. Программно-технический уровень защиты автоматизированных систем

Подходы к обеспечению защиты информации. Сервисы безопасности. Основные и вспомогательные сервисы безопасности. Виды сервисов безопасности. Понятия идентификации, аутентификации и авторизации пользователей. Виды аутентификации. Проблема надежной аутентификации и пути ее решения. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам автоматизированных сетей. Криптографическое обеспечение аутентификации пользователей. Парольная аутентификация. Виды парольной аутентификации. Преимущества и недостатки парольной аутентификации. Повышение надежности парольной аутентификации. Средства и методы защиты от компрометации и подбора паролей. Биометрическая аутентификация. Общая схема биометрической аутентификации. Преимущества и недостатки биометрической аутентификации. Достоинства и недостатки различных схем биометрической аутентификации. Требования к защите компьютерной информации. Общие положения. Характеристики подходов к защите компьютерной информации. Классификация требований к системам защиты. Формализованные требования к набору и параметрам механизмов защиты. Необходимые требования. Дополнительные требования. Формализованные требования к защите информации от несанкционированного доступа.

Нормативные документы ФСТЭК, регламентирующие защиту информации от несанкционированного доступа. Формализованные требования к защите компьютерной информации АС. Основные подсистемы и группы механизмов защиты АС. Требования к защите конфиденциальной информации. Требования к защите секретной информации. Различия требований и основополагающих механизмов защиты от несанкционированного доступа.

Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем

Тема 5. Основы организации разработки защищенных АС

Последовательность и содержание этапов разработки АС. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Методы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС.

Тема 6. Общие принципы проектирования защищенных АС

Проектирование защищенных АС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторской документации. Структура и содержание технического задания. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АС. Организация хранения информации в защищенных АС.

Тема 7. Основы эксплуатации защищенных АС

Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС. Порядок обеспечения защиты информации при эксплуатации АС. Организация технического обслуживания защищенных АС. Средства диагностирования защищенных АС. Аппаратно-программные средства диагностики АС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.

Тема № 8. Криптографические протоколы обеспечения безопасности

Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

Тема № 9. Основы администрирования АС

Задачи администрирования подсистем АС. Взаимодействие подсистем АС. Средства администрирования АС. Настройка сетевой подсистемы защищенной АС. Принципы функционирования информационных сервисов АС. Установка и настройка работы информационных сервисов АС. Удаленное администрирование компонентов АС.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Понятия и сущность защищённых автоматизированных систем

Тема 1. Основные понятия и классификация защищенных автоматизированных систем (семинар)

1. Классификация автоматизированных систем (АС).
2. Информационные технологии, используемые в АС.

3. Жизненный цикл АС.

4. Основные угрозы безопасности информации в автоматизированных системах.

Тема 2. Основы защиты информации в защищенных автоматизированных системах (семинар)

1. Понятие информационной безопасности. Понятие политики информационной безопасности.

2. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем.

3. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем.

4. Основные принципы обеспечения информационной безопасности в автоматизированной системе (АС).

Тема 3. Угрозы безопасности информации в защищенных автоматизированных системах (семинар)

1. Понятие угрозы безопасности. Понятие атаки. Понятие злоумышленника.

2. Источники угроз. Окно опасности. Базовые признаки угроз информационной безопасности.

3. Классификация угроз.

4. Основные методы обеспечения информационной безопасности.

Тема 4. Программно-технический уровень защиты автоматизированных систем (семинар)

1. Подходы к обеспечению защиты информации. Сервисы безопасности.

2. Понятия идентификации, аутентификации и авторизации пользователей. Виды аутентификации.

3. Протоколы передачи аутентификационной информации по каналам автоматизированных сетей.

4. Требования к защите компьютерной информации. Общие положения.

5. Различия требований и основополагающих механизмов защиты от несанкционированного доступа.

Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем

Тема 5. Основы организации разработки защищенных АС (семинар)

1. Последовательность и содержание этапов разработки АС.

2. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.

3. Методы и средства обеспечения отказоустойчивости автоматизированных систем.

4. Критерии оценки защищенности АС.

Тема 6. Общие принципы проектирования защищенных АС (семинар)

1. Проектирование защищенных АС. Методы проектирования.
2. Содержание этапов проектирования. Основы ведения конструкторской документации.
3. Структура и содержание технического задания.
4. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД.

Тема 7. Основы эксплуатации защищенных АС (семинар)

1. Аттестация АС по требованиям безопасности.

2. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации.

3. Особенности эксплуатации АС на объекте защиты.

4. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС.

Тема № 8. Криптографические протоколы обеспечения безопасности (семинар)

1. Протоколы аутентификации на прикладном уровне.
2. Протокол Kerberos.
3. Протоколы аутентификации на транспортном уровне.

4. Протокол SSL/TLS.

Тема № 9. Основы администрирования АС (семинар)

1. Задачи администрирования подсистем АС. Взаимодействие подсистем АС.
2. Средства администрирования АС.
3. Настройка сетевой подсистемы защищенной АС.
4. Принципы функционирования информационных сервисов АС. Установка и настройка работы информационных сервисов АС.

5. Удаленное администрирование компонентов АС.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 1. Понятия и сущность защищённых автоматизированных систем

Тема 3. Основные понятия и классификация защищенных автоматизированных систем

Лабораторная работа № 1 (4 часа). «Анализ сетевого трафика (Wireshark)».

Цель работы: Ознакомление с возможностями программ перехвата и просмотра трафика в сети.

Ход работы:

1. Установить ПО Whireshark. Дистрибутив можно скачать с общего диска:
\\nas\Distr
2. Запустить Whireshark и начать захват пакетов на вашей сетевой карте.
3. Открыть браузер и перейти по адресу
http://www.lab24b.ulsu.local/
4. Отфильтровать перехваченные пакеты в соответствии с протоколом и изучить все заголовки протоколов.
5. Попробовать пройти авторизацию на сайте указав произвольный логин и пароль.
6. Найти в ПО Whireshart пакеты авторизации и продемонстрировать отправленную на сервер информацию, а также ответ сервера.
7. Зайти на вашу электронную почту на любом из внешних сервисов (yandex, gmail, mail и д.р.). Продемонстрировать перехват пакетов. Объяснить разницу.

Тема 4. Программно-технический уровень защиты автоматизированных систем

Лабораторная работа № 2 (4 часа). «Получение информации о устройстве в сети ».

Цель работы: Ознакомление с возможностями утилиты с открытым исходным кодом для исследования сети и проверки безопасности.

Задание:

- получить все работающие устройства в сети 192.168.24.0\24;
- определить открытые порты на сервере dc и mssql;
- найти DNS сервер;
- составьте список всех MAC адресов лаборатории.

Лабораторная работа № 3 (4 часа). «Получение информации о домене (WHOIS)».

Цель работы: Ознакомление с возможностями сетевого протокола прикладного уровня, базирующегося на протоколе TCP. Основное применение — получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем.

Задание:

- Определить автономную сеть для IP адреса: 3165290846.
- Узнать владельца сайта www.iptk.ru.
- Узнать номер автономной сети.

Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем

Тема 7. Основы эксплуатации защищенных АС

Лабораторная работа № 4 (8 часов). «Основы маршрутизации».

Цель работы: Познакомится с маршрутизацией пакетов.

Задание:

Настроить маршрутизацию на ОС Linux для обеспечения доступа в Интернет с ВМ Windows. (Настроить Linux для работы в качестве роутера)

Ход работы:

Настройка внутренней сети виртуальных машин

1. Конфигурируем новые сетевые адаптеры обоих виртуальных машин для работы в одной IP сети. (Запрещено использовать следующие сети: 192.168.24.0/24, 10.2.0.0/16)
2. Проверяем доступность каждого из компьютеров по протоколу ICMP (пингуем друг друга).
3. Включаем маршрутизацию IP
4. Раскомментируем строчки
5. Перезагружаем машину
6. Проверяем включена ли маршрутизация пакетов
7. Добавляем правило для firewall, разрешающее работу NAT
8. Внимание enp0s3 - название вашего сетевого интерфейса. (Укажите правильное название)
9. На ОС Windows установите в качестве шлюза IP адрес вашего Linux сервера.
10. Проверьте доступность адреса внутренней сети лаборатории **192.168.24.200**
11. Проверьте доступность узла сети Интернет **www.yandex.ru**
12. Измените параметры сети и загрузите в браузере страницу **www.yandex.ru**

Тема № 8. Криптографические протоколы обеспечения безопасности

Лабораторная работа № 5 (4 часа). «Знакомство с аппаратными маршрутизаторами».

Цель работы: Познакомиться с работой сетевого интерфейса на примере использования аппаратных маршрутизаторов.

В лаборатории установлено несколько аппаратных маршрутизаторов компании Microtik.

Подключение к Microtik

IP адреса маршрутизаторов смотри на схеме лаборатории.

router01.lab24b.ulsu.local
router02.lab24b.ulsu.local

router03.lab24b.ulsu.local
router04.lab24b.ulsu.local

Ход работы

В данном примере в качестве виртуальной машины используется Ubuntu 20 Linux Server

1. Через ПО Winbox подключимся к маршрутизатору
2. Откроем список доступных интерфейсов маршрутизатора
3. Изучим свойства интерфейсов. Параметры работы протоколов L2
4. Обратим внимание на интерфейс типа bridge (сетевой мост)
5. Настройки сетевых мостов производятся в разделе Bridge.
6. Настройка VLAN на Mikrotik
7. Настройка VLAN на виртуальных машинах VirtualBox

Тема № 9. Основы администрирования АС

Лабораторная работа № 6 (6 часов). «Изучение технологии NAT».

Цель работы: Изучение технологии NATЗадание №1.

Ход работы:

1. Выбрать для работы один из роутеров Microtik
2. Сбросить все настройки выбранного роутера. Смотри статью: Резервное копирование и восстановление настроек Microtik
3. Настроить виртуальную машину с OS Linux в соответствии с схемой работы.
4. Пропинговать роутер с VM Linux и обратно
5. Добавить правило NAT так, чтобы все компьютеры сети 192.168.1YY.0\24 могли работать с сервисами в сети 192.168.24.0\24, например, заходить на сайт www.lab24b.ulsu.local
6. Подключить VM Windows к сети 192.168.24.0
7. Пропинговать VM Windows с VM Linux
8. Запустить анализатор пакетов Wireshark на VM Windows и продемонстрировать работу NAT.
9. После успешной демонстрации установить настройки роутера по-умолчанию.

Задание №2

1. На ОС Linux установить Web сервер Apache
2. Откройте в браузере ваш IP адрес. Вы должны увидеть приветственную страницу Apache2
3. Перейдите в VM Windows и попробуйте открыть ваш IP адрес.
4. Настройте правило трансляции адресов NAT так, чтобы ваш сайт был доступен из сети 192.168.24.0\24.

Лабораторная работа № 7 (6 часов). «Основы работы IP сетей».

Цели работы:

- Определить MAC и IP адреса компьютера в сети Ethernet.
- Изучение команд ipconfig и ping.
- Получение информации о настройках

Задание №1:

1. Получите информацию о текущей конфигурации сети.
2. Покажите используемый сетевым адаптером MAC адрес устройства.
3. Измените MAC адрес в настройках виртуальной машины и посмотрите как

изменится конфигурация сети.

Задание №2

1.Отключите автоматическое получение адресов.

2.Установите IP адрес из сети 192.168.38.0 mask 255.255.255.0

3.Для второй виртуальной машины установите адрес из такой же сети.

4.Установите дополнительные IP адреса на обоих ОС из сети 192.168.48.0 mask 255.255.255.0

Задание №3

1. Пропинговать ip адреса ваших виртуальных машин
2. Каждая машина должна успешно пинговать другую машину
3. Изучить возможности команды PowerShell
4. Пропинговать доменные адреса:

a. yandex.ru
b. ya.ru
c. google.com
d. google.ru

Задание №4

1.Изучить вывод команды arp -a

2.Объяснить почему не все IP адреса присутствуют в списке

3.Изучить возможности команды

Задание №5

1.Установить адрес шлюза 192.168.32.1

2.Пропинговать 10.2.0.1

3.Объяснить результат

4.Установить адрес шлюза 192.168.24.100

5.Пропинговать 10.2.0.1

6.Объяснить результат

Задание №6

Изменить IP адреса серверов DNS.

1.192.168.24.100.

a. Выполнить nslookup ya.ru
b. Выполнить nslookup ya.ru 192.168.24.100
c. Объяснить результаты

2. 10.2.0.1

a. Выполнить nslookup ya.ru
b. Выполнить nslookup ya.ru 10.2.0.1
c. Выполнить nslookup www.lab24b.ulsu.local
d. Объяснить результаты

3. 8.8.8.8

a. Выполнить nslookup www.google.com
b. Объяснить результаты

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Контрольные работы и рефераты не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика курсовых работ:

1. Проблемы энергетического скрытия речевой информации в телефонных линиях связи и принципы их решения.

2. Анализ электромагнитных каналов утечки информации.
3. Анализ акустических каналов утечки информации.
4. Анализ эффективности использования физических средств защиты.
5. Принципы обнаружения и локализации радиозакладок.
6. Сравнительный анализ характеристик средств обнаружения радиозакладок.
7. Оптические каналы утечки информации и их локализация.
8. Реализация защиты информации от утечки через ПЭМИН.
9. Предотвращение утечки информации по цепям электропитания и заземления.
10. Способы увеличения дальности скрытного наблюдения в оптическом видимом и инфракрасном диапазонах.

8.2.1 Правила оформления курсовых работ

Требования к курсовым работам для студентов отражены в учебно-методическом пособии: Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Классификация автоматизированных систем (АС)
2. Информационные технологии, используемые в АС
3. Жизненный цикл АС
4. Основные угрозы безопасности информации в автоматизированных системах
5. Отказоустойчивость АС
6. Основные понятия и классификация защищенных автоматизированных систем
7. Понятия информации и информационных ресурсов. Предмет защиты информации
8. Понятие информационной безопасности
9. Понятие политики информационной безопасности
10. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем
11. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем
12. Стадия выработки требований
13. Стадия определения способов защиты
14. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты
15. Основные принципы обеспечения информационной безопасности в автоматизированной системе
16. Принципы, позволяющие реализовать положения по защите АС
17. Угрозы безопасности информации в защищенных автоматизированных системах
18. Базовые признаки угроз информационной безопасности. Классификация угроз
19. Уровни доступа к защищаемой информации
20. Подходы к обеспечению защиты информации. Сервисы безопасности
21. Виды аутентификации. Проблема надежной аутентификации и пути ее решения
22. Средства и методы хранения эталонных копий аутентификационной информации
23. Средства и методы защиты от компрометации и подбора паролей
24. Требования к защите компьютерной информации
25. Нормативные документы ФСТЭК, регламентирующие защиту информации от несанкционированного доступа

26. Основные подсистемы и группы механизмов защиты АС
27. Последовательность и содержание этапов разработки АС
28. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем
29. Методы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС
30. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС
31. Проектирование защищенных АС. Основные методы проектирования
32. Основы ведения конструкторской документации
33. Структура и содержание технического задания
34. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД
35. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации
36. Особенности эксплуатации АС на объекте защиты
37. Организация технического обслуживания защищенных АС
38. Аппаратно-программные средства диагностики АС
39. Протоколы аутентификации на прикладном уровне
40. Протоколы аутентификации на транспортном уровне
41. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI
42. Задачи администрирования подсистем АС. Средства администрирования АС
43. Настройка сетевой подсистемы защищенной АС
44. Принципы функционирования информационных сервисов АС
45. Установка и настройка работы информационных сервисов АС
46. Удаленное администрирование компонентов АС

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Понятия и сущность защищённых автоматизированных систем			
Тема 1. Основные понятия и классификация защищенных автоматизированных систем (АС)	Подготовка к лекции, подготовка к сдаче экзамена	4	Тесты перед лекцией, экзамен
Тема 2. Основы защиты информации в защищенных АС	Подготовка к лекции, подготовка к сдаче экзамена	4	Тесты перед лекцией, экзамен
Тема 3. Угрозы безопасности информации в защищенных АС	Подготовка к лекции, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	6	Тесты перед лекцией, вопросы на лабораторной работе, экзамен
Тема 4. Программно-технический уровень	Подготовка к лекции, подготовка к семинару,	6	Тесты перед лекцией, вопросы на

защиты АС	лабораторным работам, подготовка к сдаче экзамена		лабораторной работе, экзамен
Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем			
Тема 5. Основы организации разработки защищенных АС	Подготовка к лекции, подготовка к сдаче экзамена	4	Тесты перед лекцией, экзамен
Тема 6. Общие принципы проектирования защищенных АС	Подготовка к лекции, подготовка к сдаче экзамена	4	Тесты перед лекцией, экзамен
Тема 7. Основы эксплуатации защищенных АС	Подготовка к лекции, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	6	Тесты перед лекцией, вопросы на лабораторной работе, экзамен
Тема 8. Криптографические протоколы обеспечения безопасности	Подготовка к лекции, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	6	Тесты перед лекцией, вопросы на лабораторной работе, экзамен
Тема 9. Основы администрирования АС	Подготовка к лекции, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	14	Тесты перед лекцией, вопросы на лабораторной работе, экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / Шаньгин В. Ф. - Москва: ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785940747680.html

2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084

3. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268

дополнительная

1 Милёхина, О. В. Информационные системы: теоретические предпосылки к построению: учеб. пособие / Милёхина О. В. - Новосибирск: Изд-во НГТУ, 2013. - 282 с. - ISBN 978-5-7782-2220-5. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785778222205.html

2. Некоммерческая интернет-версия СПС "КонсультантПлюс":

2.1 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». - URL: http://www.consultant.ru/document/cons_doc_LAW_2481/

2.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации» - URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

2.3 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации") - URL: http://www.consultant.ru/document/cons_doc_LAW_208191/

3. Малюк А.А., Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев и др.. Под ред. В.С. Горбатова. - М.: Горячая линия - Телеком, 2011. - 288 с. - ISBN 978-5-9912-0160-5 - URL: http://www.studentlibrary.ru/book/ISBN9785991201605.html

4. Захарова, Е. Я. Информационные системы : учеб. пособие / Е. Я. Захарова, О. В. Милёхина - Новосибирск : Изд-во НГТУ, 2010. - 126 с. - ISBN 978-5-7782-1535-1. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785778215351.html

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» для студентов специалитета по специальности 10.05.03 очной

формы обучения / А. М. Иванцов; УлГУ, ФМИиАТ. - Ульяновск: УлГУ, 2021. - 18 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/10731

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. / ___ / 04.05.2023 /
должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

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, [2023]. – 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, [2023]. - 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, [2023]. – 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, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – 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, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - 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, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – 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.

Согласовано:

Инженер ведущий	Щуренко Ю.В.		04.05.2023
Должность сотрудника УИТТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских, лабораторных занятий: 2/26, 3/316, 3/317, 2/24б.

Аудитория 2/24б укомплектована специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

– для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

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 кафедры Иванцов Андрей Михайлович
подпись должность ФИО

Разработчик: _____ ст. преподаватель кафедры Клочков Андрей Евгеньевич
подпись должность ФИО