УТВЕРЖДЕНО

решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Разработка и эксплуатация автоматизированных систем в защищенном исполнении**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	4

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 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:

Основной целью освоения дисциплины «Разработка и эксплуатацияавтоматизированных 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 безопасностиавтоматизированных систем.

Задачи освоения дисциплины:

- изучение принципов эксплуатации защищённых автоматизированных систем;

- овладение средствами и методами проектирования и разработки защищенныхавтоматизированных систем;

- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-9, ОПК-10, ОПК-14.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Программно-аппаратные средства защиты информации, Методы и средства криптографической защиты информации, Сети и системы передачи информации, Разработка и эксплуатация автоматизированных систем в защищенном исполнении, Научно-исследовательская работа, Защита информации от утечки по техническим каналам, Проектная деятельность, Подготовка к сдаче и сдача государственного экзамена, Системы управления базами данных, Организационное и правовое обеспечение информационной безопасности, Базы данных, Криптографические протоколы, Основы информационной безопасности, Теоретико-числовые методы в криптографии, Организация электронно вычислительных машин и вычислительных систем.

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
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 сос-тояния и тенденций развития информационных технологий, средств тех-нической 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 теку-щего состояния и тенденций развития информационных технологий
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 ав-томатизированных системах **уметь**: осуществлять разработку, внедрение и эксплуатацию автоматизиро-ванных 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 автома-тизированных систем с учетом требований по защите информации
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 криптографичес-кой защиты информации при решении задач профессиональной дея-тельности

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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

4.2. Объем дисциплины по видам учебной работы (в часах): 180 часов

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	90	90
Аудиторные занятия:	90	90
Лекции	36	36
Семинары и практические занятия	18	18
Лабораторные работы, практикумы	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	Тестирование
Курсовая работа	Курсовая работа	Курсовая работа
Виды промежуточной аттестации (экзамен, зачет)	Экзамен (18)	Экзамен
Всего часов по дисциплине	180	180

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. Понятия и сущность защищённых автоматизированных систем							
Тема 1.1. Основные понятия и классификация защищенных автоматизированн	10	4	2	0	0	4	Вопросы к Экзамену, 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
ых систем							
Тема 1.2. Основы защиты информации в защищенных автоматизированных системах	10	4	2	0	0	4	Вопросы к Экзамену, Тестирование
Тема 1.3. Угрозы безопасности информации в защищенных автоматизированных системах	16	4	2	4	0	6	Вопросы к Экзамену, Тестирование
Тема 1.4. Программно-технический уровень защиты автоматизированных систем	20	4	2	8	0	6	Вопросы к Экзамену, Тестирование
Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем							
Тема 2.1. Основы организации и разработки защищенных АС	10	4	2	0	0	4	Вопросы к Экзамену, Тестирование
Тема 2.2. Общие принципы проектирования	10	4	2	0	0	4	Вопросы к Экзамену, 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
защищенных АС							
Тема 2.3. Основы эксплуатации защищенных АС	20	4	2	8	0	6	Вопросы к Экзамену, Тестирование
Тема 2.4. Криптографические протоколы обеспечения безопасности	16	4	2	4	0	6	Вопросы к Экзамену, Тестирование
Тема 2.5. Основы администрирования АС	32	4	2	12	0	14	Вопросы к Экзамену, Тестирование
Итого подлежит изучению	144	36	18	36	0	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Понятия и сущность защищённых автоматизированных систем

Тема 1.1. 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 1.2. 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 1.3. 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 1.4. 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 2.1. 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 2.2. 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 2.3. 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 2.4. 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 2.5. 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

Раздел 1. Понятия и сущность защищённых автоматизированных систем

Тема 1.1. Основные понятия и классификация защищенных автоматизированных систем

Вопросы к теме:

Очная форма

1. Классификация автоматизированных систем (АС).
2. Информационные технологии, используемые в АС.
3. Жизненный цикл АС.
4. Основные угрозы безопасности информации в автоматизированных системах.

Тема 1.2. Основы защиты информации в защищенных автоматизированных системах

Вопросы к теме:

Очная форма

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 1.3. Угрозы безопасности информации в защищенных автоматизированных системах

Вопросы к теме:

Очная форма

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 1.4. Программно-технический уровень защиты автоматизированных систем

Вопросы к теме:

Очная форма

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 2.1. Основы организации разработки защищенных АС

Вопросы к теме:

Очная форма

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 2.2. Общие принципы проектирования защищенных АС

Вопросы к теме:

Очная форма

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 2.3. Основы эксплуатации защищенных АС

Вопросы к теме:

Очная форма

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 2.4. Криптографические протоколы обеспечения безопасности

Вопросы к теме:

Очная форма

1. Протоколы аутентификации на прикладном уровне.
2. Протокол Kerberos.
3. Протоколы аутентификации на транспортном уровне.
4. Протокол SSL/TLS.

Тема 2.5. Основы администрирования АС

Вопросы к теме:

Очная форма

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, ПРАКТИКУМЫ

Анализ сетевого трафика (Wireshark)
Цели: Ознакомление с возможностями программ перехвата и просмотра трафика в сети.
Содержание: 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.
Результаты: Продемонстрировать возможности программ перехвата и просмотра трафика в сети
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10731
Получение информации о устройстве в сети
Цели: Ознакомление с возможностями утилиты с открытым исходным кодом для исследования сети и проверки безопасности
Содержание: - 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.

Результаты: Продемонстрировать возможности утилиты с открытым исходным кодом для исследования сети и проверки безопасности
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10731
Получение информации о домене (WHOIS)
Цели: 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.
Содержание: - Определить автономную сеть для IP адреса: 3165290846. - Узнать владельца сайта www.iptk.ru. - Узнать номер автономной сети
Результаты: Продемонстрировать возможности сетевого протокола прикладного уровня, базирующегося на протоколе TCP.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10731
Основы маршрутизации
Цели: Познакомится с маршрутизацией пакетов
Содержание: 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
Результаты: Продемонстрировать умение работать с маршрутизацией пакетов
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10731
Знакомство с аппаратными маршрутизаторами
Цели: Познакомиться с работой сетевого интерфейса на примере использования аппаратных маршрутизаторов
Содержание: 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
Результаты: Продемонстрировать навыки работы сетевого интерфейса на примере использования аппаратных маршрутизаторов
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10731
Технология NAT
Цели: Изучение технологии NAT
Содержание: 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.
Результаты: Продемонстрировать навыки работы с технологией NAT
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10731
Основы работы IP сетей
Цели: – Определить MAC и IP адреса компьютера в сети Ethernet. – Изучение команд ipconfig и ping. – Получение информации о настройках
Содержание: 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
Результаты: Продемонстрировать навыки работы с IP сетями
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/10731

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Темы курсовой работы

Тема 1. Программная реализация некоторых быстрых алгоритмов декодирования кодов Рида-Соломона

Тема 2. Разработка системы защищённой передачи данных в современных мессенджерах

Тема 3. Высокоскоростная программная реализация некоторых симметричных криптосистем

Тема 4. Разработка модуля генератора случайных последовательностей для криптопровайдера КриптоПро CSP

Тема 5. Программная реализация некоторых совершенных схем разделения секрета

Тема 6. Программная реализация некоторых протоколов аутентификации на основе симметричных шифров
Тема 7. Разработка системы защиты обучающего комплекса для подготовки специалистов по эксплуатации программного-аппаратного обеспечения ViPNet

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Классификация автоматизированных систем (АС)
2. Информационные технологии, используемые в АС
3. Жизненный цикл АС
4. Отказоустойчивость АС
5. Основные понятия и классификация защищенных автоматизированных систем
6. Понятия информации и информационных ресурсов.Предмет защиты информации
7. Понятие информационной безопасности
8. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем
9. Стадия выработки требований
10. Стадия определения способов защиты
11. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты
12. Основные угрозы безопасности информации в автоматизированных системах
13. Понятие политики информационной безопасности
14. Угрозы безопасности информации в защищенных автоматизированных системах
15. Базовые признаки угроз информационной безопасности. Классификация угроз
16. Уровни доступа к защищаемой информации
17. Подходы к обеспечению защиты информации. Сервисы безопасности
18. Виды аутентификации. Проблема надежной аутентификации и пути ее решения
19. Средства и методы хранения эталонных копий аутентификационной информации
20. Средства и методы защиты от компрометации и подбора паролей
21. Требования к защите компьютерной информации
22. Нормативные документы ФСТЭК, регламентирующие защиту информации от несанкционированного доступа
23. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем
24. Основные подсистемы и группы механизмов защиты АС
25. Последовательность и содержание этапов разработки АС
26. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем
27. Методы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС
28. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС
29. Проектирование защищенных АС. Основные методы проектирования
30. Основы ведения конструкторской документации
31. Структура и содержание технического задания
32. Построение комплексной защиты АС. Основы проектирования комплексной защиты

информационной безопасности от НСД
33. Основные принципы обеспечения информационной безопасности в автоматизированной системе
34. Принципы, позволяющие реализовать положения по защите АС
35. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации
36. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации
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 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. Понятия и сущность защищённых автоматизированных систем			
Тема 1.1. Основные понятия и классификация защищенных автоматизированных систем	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	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 1.2. Основы защиты информации в защищенных автоматизированных системах	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 1.3. Угрозы безопасности информации в защищенных автоматизированных системах	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Тема 1.4. Программно-технический уровень защиты автоматизированных систем	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем			
Тема 2.1. Основы организации разработки защищенных АС	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 2.2. Общие принципы проектирования защищенных АС	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 2.3. Основы эксплуатации защищенных АС	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Тема 2.4. Криптографические протоколы обеспечения безопасности	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Тема 2.5. Основы администрирования АС	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	14	Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Шаньгин В.Ф. Информационная безопасность и защита информации : учебное пособие / В.Ф. Шаньгин ; Шаньгин В.Ф. - Москва : ДМК-пресс, 2014. - 702 с. - URL: https://www.studentlibrary.ru/book/ISBN9785940747680.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-94074-768-0. / .— ISBN 0_243296

2. Суворова Галина Михайловна. Информационная безопасность : учебное пособие для вузов / Г.М. Суворова ; Г. М. Суворова. - Москва : Юрайт, 2023. - 253 с. - (Высшее образование). - URL: https://urait.ru/bcode/519780 (дата обращения: 10.02.2023). - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-13960-0 : 1039.00. / .— ISBN 0_490325

дополнительная

1. Милёхина О.В. Информационные системы: теоретические предпосылки к построению : учебное пособие / О.В. Милёхина, Е.Я. Захарова, В.А. Титова ; Милёхина О.В.; Захарова Е.Я.; Титова В.А. - Москва : НГТУ, 2014. - 283 с. - URL: https://www.studentlibrary.ru/book/ISBN9785778224056.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-7782-2405-6. / .— ISBN 0_249899

2. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам : учебное пособие / Г.А. Бузов ; Бузов Г.А. - Москва : Горячая линия - Телеком, 2015. - 586 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204248.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0424-8. / .— ISBN 0_251025

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. - 2021. - 18 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/10731. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_261317.

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