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	**Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	3

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:

Дисциплина «Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа» является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Дисциплина реализует требования профессионального стандарта «Специалист по технической защите информации" и направлена на получение студентами знаний, умений и навыков по вопросам технической защиты конфиденциальной информации (ТЗКИ) от несанкционированного доступа (НСД).

Задачи освоения дисциплины:

изучить основные методы и средства ТЗКИ от НСД;

обеспечить освоение студентами умений и навыков по вопросам ТЗКИ от НСД.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа» относится к числу дисциплин блока Б1.В.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ПК-7, ПК-8.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа, Эксплуатационная практика, Подготовка к сдаче и сдача государственного экзамена, Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации, Профессиональный электив. Организационно-правовые основы технической защиты конфиденциальной информации.

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-7 Способен проводить работы по техническому обслуживанию защищённых технических средств обработки информации	**знать**: Технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении Порядок аттестации объектов информатизации на соответствие тре-бованиям безопасности информации Порядок устранения неисправностей технических средств обработки

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	информации в защищенном исполнении и организации их ремонта **уметь**: Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией Проводить устранение выявленных неисправностей защищенных технических средств обработки информации **владеть**: Навыками проведения технического обслуживания защищенных техниче-ских средств обработки информации
ПК-8 Способен проводить работы по установке, настройке и испытаниям технических средств обработки информации	**знать**: Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и эксплуатации защищенных технических средств обработки информации. Технические каналы утечки информации, возникающие за счет побочных электро-магнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах. Способы защиты информации от утечки по техническим каналам **уметь**: Проводить настройку защищенных технических средств обработки инфор-мации в соответствии с инструкциями по эксплуатации и эксплуатацион-но-техническими документами. Производить установку и монтаж защищенных технических средств обработки информации **владеть**: Навыками установки и монтажа защищенных технических средств обрабо-тки информации. Навыками настройки защищенных технических средств обработки инфор-мации

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 3 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 108 часов

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		6
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:	54	54
Лекции	18	18
Семинары и практические занятия	18	18
Лабораторные работы, практикумы	18	18
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	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачет (0)	Зачет
Всего часов по дисциплине	108	108

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. Угрозы безопасности информации, связанные с НСД							
Тема 1.1. Понятие и общая классификация угроз безопасности информаци	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
и, связанных с НСД							
Тема 1.2. Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах	4	2	0	0	0	2	Тестирование
Тема 1.3. Банк данных угроз безопасности информации, включающих базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах	14	2	6	0	0	6	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
Раздел 2. Меры и средства защиты информации от НСД							
Тема 2.1. Общая характеристика и классификация мер и средств защиты информации от НСД	8	2	2	0	0	4	Тестирование
Тема 2.2. Средства защиты информации от НСД	38	4	2	12	0	20	Тестирование
Тема 2.3. Общий порядок сертификации средств защиты информации от НСД	8	2	2	0	0	4	Тестирование
Тема 2.4. Определение факта доступа к файлам. доступ к данным со стороны процесса	20	2	2	6	0	10	Тестирование
Тема 2.5. Мероприятия по физической защите объекта информатизации и отдельных технических средств, и	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
сключающих НСД к техническим средствам, их хищение и нарушение работоспособности							
Итого подлежит изучению	108	18	18	18	0	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Угрозы безопасности информации, связанные с НСД

Тема 1.1. Понятие и общая классификация угроз безопасности информации, связанных с НСД

Основные термины и определения в области НСД. Источники угроз безопасности информации. Модели угроз безопасности информации, связанных с НСД.

Тема 1.2. Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах

Методы выявления уязвимостей информационных систем. Порядок и содержание работ по анализу уязвимостей программного обеспечения информационных систем, в том числе средств защиты информации информационных систем.

Тема 1.3. Банк данных угроз безопасности информации, включающих базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах

Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE. Общая система оценки уязвимостей (стандарт CVSS).

Раздел 2. Меры и средства защиты информации от НСД

Тема 2.1. Общая характеристика и классификация мер и средств защиты информации от НСД

Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД.

Тема 2.2. Средства защиты информации от НСД

Межсетевые экраны, требования к ним и способы применения. Системы обнаружения вторжений, требования к ним и способы применения. Средства антивирусной защиты, требования к ним и способы применения. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета. Средства (механизмы) обеспечения целостности информации. Криптографические средства защиты информации. DLP-системы, их возможности и перспективы применения.

Тема 2.3. Общий порядок сертификации средств защиты информации от НСД

Стандарты по сертификации средств защиты информации от НСД. Порядок проведения сертификационных испытаний на соответствие классам защищённости СВТ. Отчетность по результатам испытаний.

Тема 2.4. Определение факта доступа к файлам. доступ к данным со стороны процесса

Основные способы определения факта доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа. Понятие электронного замка. Механизмы контроля аппаратной конфигурации ПЭВМ.

Тема 2.5. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности

Общая характеристика объекта информатизации. Система физической защиты объекта информатизации и отдельных технических средств. Основные мероприятия по физической защите объекта информатизации и отдельных технических средств.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Угрозы безопасности информации, связанные с НСД

Тема 1.1. Понятие и общая классификация угроз безопасности информации, связанных с НСД

Вопросы к теме:

Очная форма

1. Основные термины и определения в области НСД.
2. Источники угроз безопасности информации.
3. Модели угроз безопасности информации, связанных с НСД.

Тема 1.3. Банк данных угроз безопасности информации, включающих базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах

Вопросы к теме:

Очная форма

1. Общая характеристика Банка данных угроз безопасности информации
2. Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.
3. Методы выявления уязвимостей информационных систем. Порядок и содержание работ по анализу уязвимостей программного обеспечения информационных систем, в том числе средств защиты информации информационных систем
4. Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE.
5. Общая система оценки уязвимостей (стандарт CVSS).

Раздел 2. Меры и средства защиты информации от НСД

Тема 2.1. Общая характеристика и классификация мер и средств защиты информации от НСД

Вопросы к теме:

Очная форма

1. Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе.
2. Классификация мер и средств защиты информации от НСД (управление доступом; регистрация и учет; обеспечение целостности; антивирусная защита; межсетевое экранирование и сегментирование сетей; анализ защищенности и обнаружение вторжений и т.д.)

Тема 2.2. Средства защиты информации от НСД

Вопросы к теме:

Очная форма

1. Межсетевые экраны, требования к ним и способы применения.
2. Системы обнаружения вторжений, требования к ним и способы применения.
3. Средства антивирусной защиты, требования к ним и способы применения.
4. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа.
5. Средства регистрации и учета.
6. Средства (механизмы) обеспечения целостности информации.
7. Криптографические средства защиты информации.
8. DLP-системы, их возможности и перспективы применения.

Тема 2.3. Общий порядок сертификации средств защиты информации от НСД

Вопросы к теме:

Очная форма

1. Сертификация средств вычислительной техники (СВТ) по требованиям защищенности от НСД к информации
2. Порядок проведения сертификационных испытаний на соответствие классам защищенности СВТ.
3. Отчетность по результатам испытаний.

Тема 2.4. Определение факта доступа к файлам. доступ к данным со стороны процесса

Вопросы к теме:

Очная форма

1. Способы определения факта доступа
2. Журналы доступа. Критерии информативности журналов доступа
3. Механизмы контроля аппаратной конфигурации ПЭВМ

Тема 2.5. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности

Вопросы к теме:

Очная форма

1. Общая характеристика объекта информатизации.
2. Система физической защиты объекта информатизации и отдельных технических средств.
3. Основные мероприятия по физической защите объекта информатизации и отдельных

технических средств.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Назначение и возможности встроенных межсетевых экранов (МЭ).
Цели: - изучить возможности встроенных межсетевых экранов (МЭ) на примере выбранного МЭ; - научиться администрировать выбранный МЭ.
Содержание: 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: - изучить и продемонстрировать основные возможности МЭ. - составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/13989.
Системы обнаружения вторжений на примере Системы защиты от НСД «Dallas Lock»
Цели: изучить возможности Системы обнаружения вторжений «Dallas Lock» и научиться работать с ней. Результат: отчет.
Содержание: 1. Если на компьютере уже установлена система защиты, ее необходимо удалить. 2. Необходимо убедиться, что на диске С 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: - изучить и продемонстрировать основные возможности Dallas Lock как системы защиты информации от НСД. - составить отчет о проделанной работе и защитить его у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/13989.
Назначение, возможности, установка и порядок работы с Электронным замком "Соболь".
Цели: Изучить возможности Электронного замка "Соболь" и получить навыки настройки, установки и практического использования электронного замка.
Содержание: 1. Ознакомление с теоретической частью электронного замка "Соболь". 2. Установка программного обеспечения комплекса "Соболь". 3. Подготовка комплекса к инициализации. 4. Инициализация электронного замка "Соболь". 5. Подготовка электронного замка к эксплуатации. 6. Настройка и эксплуатация комплекса "Соболь". 7. Удаление программного обеспечения электронного замка "Соболь".
Результаты: - изучить электронный замок «Соболь» и научиться устанавливать, настраивать и эксплуатировать его; - составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/13989.
Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа на примере Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

Цели: Изучить возможности и научиться работать с комплексом средств защиты от несанкционированного доступа (НСД).
Содержание: 1. Ознакомление с теоретической частью СЗИ НСД «Аккорд- АМДЗ». 2. Установка платы контроллера и программного обеспечения комплекса, включающая три основных этапа: - установка платы контроллера в свободный слот ПЭВМ и регистрацию администратора безопасности информации (БИ) (супервизора), в том числе, настройка комплекса в соответствии с конфигурацией технических средств ПЭВМ; - регистрация пользователей, назначение пользователям личных ТМ-идентификаторов, паролей и времени доступа; - назначение списка дисков, файлов, разделов реестра, контролируемых на целостность. 3. Инициализация СЗИ НСД «Аккорд- АМДЗ»: - регистрация супервизора (администратора безопасности информации); - регистрация нового пользователя. 4. Эксплуатация комплекса «Аккорд- АМДЗ». 5. Снятие средств защиты комплекса «Аккорд- АМДЗ».
Результаты: - изучить СЗИ НСД «Аккорд- АМДЗ» и научиться устанавливать, настраивать и эксплуатировать его; - составить отчет о проделанной работе и отчитаться по нему у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/13989.
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.
Результаты: - изучить «Secret Net Studio» и научиться устанавливать, настраивать, эксплуатировать и корректно удалять СЗИ с компьютера; - подготовить письменный отчет о проделанной работе и защитить его у преподавателя.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/13989.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Основные термины и определения в области НСД

2. Источники угроз безопасности информации, связанные с НСД

3. Методы выявления уязвимостей информационных систем

4. Методы выявления уязвимостей информационных систем

5. Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах

6. Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE

7. Общая система оценки уязвимостей (стандарт CVSS)

8. Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе

9. Меры защиты информации от НСД

10. Основные средства защиты информации от НСД

11. Общая характеристика межсетевых экранов

12. Системы обнаружения вторжений, требования к ним и способы применения

13. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа

14. Средства регистрации и учета

15. Средства (механизмы) обеспечения целостности информации

16. DLP-системы, их возможности и перспективы применения

17. Криптографические средства защиты информации

18.

19. Порядок проведения сертификационных испытаний на соответствие классам защищённости СВТ. Отчетность по результатам испытаний

20. Основные способы определения факта доступа. Журналы доступа

21. Выявление следов несанкционированного доступа к файлам

22. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя

23.

24. Общая характеристика объекта информатизации. Система физической защиты объекта информатизации и отдельных технических средств

25. Основные мероприятия по физической защите объекта информатизации и отдельных технических средств

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. Угрозы безопасности информации, связанные с НСД			
Тема 1.1. Понятие и общая классификация угроз безопасности информации, связанных с НСД	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 1.2. Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 1.3. Банк данных угроз безопасности информации, включающих базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Тестирование
Раздел 2. Меры и средства защиты информации от НСД			
Тема 2.1. Общая характеристика и классификация мер и средств защиты информации от НСД	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 2.2. Средства защиты информации от НСД	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	20	Тестирование
Тема 2.3. Общий порядок сертификации средств защиты информации от НСД	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 2.4. Определение факта доступа к файлам. доступ к данным со стороны процесса	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Тестирование
Тема 2.5. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Суворова Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. - 2-е изд. ; пер. и доп. - Москва : Юрайт, 2024. - 277 с. - (Высшее образование). - URL: https://urait.ru/bcode/544029 . - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - ISBN 978-5-534-16450-3 : 1169.00. / .— ISBN 0_529150

2. Гродзенский Я.С. Информационная безопасность : учебное пособие / Я.С. Гродзенский ; Гродзенский Я.С. - Москва : РГ-Пресс, 2020. - 144 с. - URL: https://www.studentlibrary.ru/book/ISBN9785998808456.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9988-0845-6. / .— ISBN 0_260443

дополнительная

1. Иванцов А. М. Основы информационной безопасности : курс лекций : учебное пособие. Ч. 1 / А.

М. Иванцов, В. Г. Козловский ; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2019. - Загл. с экрана. - Электрон. текстовые дан. (1 файл : 776 КБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/1396. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_36065

2. Иванцов А. М. Основы информационной безопасности : курс лекций : учебное пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем». Часть 2 / А. М. Иванцов, В. Г. Козловский ; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2020. - Загл. с экрана. - Электрон. текстовые дан. (1 файл : 1,41 МБ). - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/8697. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_42171

3. 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 «Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов. - 2022. - 15 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13989. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_476606.

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