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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации
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

СОГЛАСОВАНО
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
/ _____ / Андреев А.С. / *(подпись)* *(Ф.И.О.)* «12» 05 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Дисциплина «Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации» 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 контроля состояния технической защиты конфиденциальной информации (ТЗКИ).

Задачи освоения дисциплины:

изучить основные методы и средства контроля состояния ТЗКИ;

обеспечить освоение студентами умений и навыков по вопросам контроля состояния ТЗКИ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации» изучается в 7 семестре и относится к дисциплинам блока Б1.В. Дисциплина основывается на знаниях, полученных при изучении дисциплин «Основы информационной безопасности», «Профессиональный электив. Организационно-правовые основы технической защиты конфиденциальной информации», «Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от НСД», «Организационное и правовое обеспечение информационной безопасности».

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

- знание базовых профессиональных понятий и определений в области информационной безопасности;
- способность использовать нормативные правовые документы;
- способность использовать основные положения и методы социальных и гуманитарных наук;
- способность анализировать социально-значимые проблемы и процессы.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: «Безопасность операционных систем», «Безопасность вычислительных сетей», «Защита информации от утечки по техническим каналам», а также в ходе всех видов практик и в повседневной деятельности.

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**
ПК-7 - Способен проводить работы по техническому обслуживанию защищён-ных технических средств обработки информации	**Знает:** Технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении Порядок аттестации объектов информатизации на

	соответствие требованиям безопасности информации Порядок устранения неисправностей технических средств обработки информации в защищенном исполнении и организации их ремонта **Умеет:** 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 **Владеет:** Навыками проведения технического обслуживания защищенных технических средств обработки информации
ПК-8 - Способен проводить работы по установке, настройке и испытаниям технических средств обработки информации	**Знает:** 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 электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электро-питания 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 **Умеет:** Проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами. Производить установку и монтаж защищенных технических средств обработки информации **Владеет:** Навыками установки и монтажа защищенных технических средств обработки информации. Навыками настройки защищенных технических средств обработки информации

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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

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		
		7		
Контактная работа обучающихся с преподавателем	54	54/54*		
Аудиторные занятия:	54	54/54*		
Лекции	18	18/18*		
Практические и семинарские занятия	18	18/18*		
Лабораторные работы (лабораторный практикум)	18	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 на семинарах; - вопросы при защите лабора-торных работ		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	зачет	зачет		
Всего часов по дисциплине	108	108		

* 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 и разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практические занятия, семинары	Лабораторные работы			
Раздел 1. Основы организации контроля состояния ТЗКИ							
1. Основные задачи контроля состояния ТЗКИ	4	2				2	Тесты Т1
2. Организационный и технический контроль состояния ТЗКИ	10	2	4			4	Тесты Т2
Раздел 2. Методы и средства контроля защищенности конфиденциальной информации							
3. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН	20	2	2	4		12	Тесты Т3, лаб. работы 1,2
4. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам	18	2	2	6		8	Тесты Т4, лаб. работа 3
5. Методы и средства контроля защищенности конфиденциальной информации от НСД	16	2	2	4		8	Тесты Т5 лаб. работа 4
Раздел 3. Мониторинг информационной безопасности средств и систем информатизации							
6. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации	8	2	2			4	Тесты Т6
7. Обнаружение и идентификация инцидентов безопасности информации	16	2	2	4		8	Тесты Т7 лаб. работа 5
8. Планирование мер по устранению инцидентов	8	2	2			4	Тесты Т8

безопасности информации							
9. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации	8	2	2			4	Тесты Т9
Итого:	108	18	18	18		54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Основы организации контроля состояния ТЗКИ

Тема 1. Основные задачи контроля состояния ТЗКИ

Основные термины и определения в области состояния ТЗКИ. Сущность и задачи контроля состояния ТКЗИ. Система документов по контролю состояния ТЗКИ. Вопросы, подлежащие проверке при контроле состояния ТКЗИ в организации.

Тема 2. Организационный и технический контроль состояния ТЗКИ

Классификация видов контроля состояния ТКЗИ. Организационный и технический контроль состояния ТЗКИ. Система документации по контролю состояния ТЗКИ.

Раздел 2. Методы и средства контроля защищенности конфиденциальной информации

Тема 3. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

Основные методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Методика оценки защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

Тема 4. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам.

Обобщённая структура технического канала утечки. Основные методы контроля защищенности конфиденциальной акустической речевой информации от утечки. Основные средства контроля защищенности конфиденциальной акустической речевой информации от утечки

Тема 5. Методы и средства контроля защищенности конфиденциальной информации от НСД.

Основные методы и средства контроля защищенности конфиденциальной информации от НСД. Документирование результатов контроля. Требования к средствам контроля защищенности конфиденциальной информации.

Раздел 3. Мониторинг информационной безопасности средств и систем информатизации

Тема 6. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации.

Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации. Состав и структура системы мониторинга информационной безопасности средств и систем информатизации. Порядок и методы мониторинга информационной безопасности средств и систем информатизации.

Тема 7. Обнаружение и идентификация инцидентов безопасности информации

Понятие события и инцидента ИБ. Система управления инцидентами ИБ. Этапы процесса управления инцидентами ИБ. Политика управления инцидентами ИБ.

Обнаружение и идентификация инцидентов безопасности информации, а также событий, приводящих к возникновению инцидентов. Оценка последствий инцидентов безопасности информации.

Тема 8. Планирование мер по устранению инцидентов безопасности информации

Планирование мер по устранению инцидентов безопасности информации, в том числе по восстановлению систем информатизации, их сегментов и средств, входящих в их состав, в случае отказа в обслуживании или после сбоев. Устранение последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса. Примерное содержание плана обеспечения непрерывности бизнеса. Контроль за событиями безопасности и действиями пользователей в средствах и системах информатизации.

Тема 9. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации

Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в средствах и системах информатизации. Разработка предложений (рекомендаций) по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) систем защиты информации систем информатизации, повторной оценке эффективности систем защиты информации систем информатизации или проведении дополнительных работ по оценке эффективности систем защиты информации систем информатизации

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Основы организации контроля состояния ТЗКИ

Тема 2. Организационный и технический контроль состояния ТЗКИ (семинар).

1. Сущность и задачи контроля состояния ТКЗИ
2. Вопросы, подлежащие проверке при контроле состояния ТКЗИ в организации
3. Классификация видов контроля состояния ТКЗИ. Организационный и технический контроль состояния ТЗКИ

4. Система документации по контролю состояния ТЗКИ

Раздел 2. Методы и средства контроля защищенности конфиденциальной информации

Тема 3. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН (семинар).

1. Основные методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН
2. Методика оценки защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН

Тема 4. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам (семинар)**.**

1. Обобщённая структура технического канала утечки
2. Основные методы контроля защищенности конфиденциальной акустической речевой информации от утечки

3. Основные средства контроля защищенности конфиденциальной акустической речевой информации от утечки

Тема 5. Методы и средства контроля защищенности конфиденциальной информации от НСД (семинар)**.**

1. Основные методы контроля защищенности конфиденциальной информации от НСД

2. Основные средства контроля защищенности конфиденциальной информации от НСД

3. Документирование результатов контроля. Требования к средствам контроля защищенности конфиденциальной информации.

Раздел 3. Мониторинг информационной безопасности средств и систем информатизации

Тема 6. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации (семинар).

1. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации

2. Состав и структура системы мониторинга информационной безопасности средств и систем информатизации.

3. Порядок и методы мониторинга информационной безопасности средств и систем информатизации.

Тема 7. Обнаружение и идентификация инцидентов безопасности информации (семинар).

1. Понятие события и инцидента ИБ
2. Система управления инцидентами ИБ
3. Этапы процесса управления инцидентами ИБ
4. Политика управления инцидентами ИБ

Тема 8. Планирование мер по устранению инцидентов безопасности информации (семинар).

1. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса

2. Примерное содержание плана обеспечения непрерывности бизнеса

Тема 9. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации (семинар)**.**

1. Содержание протоколов аттестационных испытаний и заключения по результатам аттестационных испытаний информационных (автоматизированных) систем

2. Содержание протоколов аттестационных испытаний и заключения по результатам аттестационных испытаний выделенных (защищаемых) помещений

3. Оформление аттестата соответствия на выделенное (защищаемое) помещение

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 2. Методы и средства контроля защищенности конфиденциальной информации

Тема 3. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН

Лабораторная работа № 1. «Изучение методов поиска и локализации специальных технических средств с использованием прибора ST-032 Пиранья».

Цель работы: Изучить возможности прибора ST-032 «Пиранья» и научиться осуществлять поиск и локализацию специальных технических средств несанкционированного получения информации.

Методические указания: основное внимание должно быть уделено практической

эксплуатации в ходе поиска и локализации специальных технических средств несанкционированного получения информации.

Лабораторная работа № 2. (2 часа). «Защита каналов передачи информации генератором шума «Гром-ЗИ-4».

Цель работы: Ознакомление с техническими характеристиками генератора шума «Гром-ЗИ-4», изучение правил его эксплуатации и получение практических навыков работы с генератором шума Гром-ЗИ-4».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с генератором шума Гром-ЗИ-4».

Тема 4. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам.

Лабораторная работа № 3. (6 часов) «Ознакомление с техническими характеристиками селективного микровольтметра В6-9».

Цель работы: Получение практических навыков в работе с селективным микровольтметром в ходе измерения опасных сигналов.

Методические указания: основное внимание должно быть уделено практическим навыкам работы с селективным микровольтметром В6-9.

Тема 5. Методы и средства контроля защищенности конфиденциальной информации от НСД

Лабораторная работа № 4. (4 часа). Назначение, возможности и порядок работы с системой SecretNet Studio.

Цель: изучить возможности и научиться работать с системой SecretNet Studio. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей системы SecretNet Studio.

Раздел 3. Мониторинг информационной безопасности средств и систем информатизации

Тема 7. Обнаружение и идентификация инцидентов безопасности информации

Лабораторная работа № 5. (4 часа Назначение и возможности системы защиты от НСД «Dallas Lock».

Цель: изучить возможности и научиться работать с системой защиты от НСД. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей «**Dallas Lock**».

Все лабораторные работы проводятся в интерактивной форме, а именно используются:

диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами, группами студентов;

элементы деловых игр, «мозговой штурм» или дискуссии по рассматриваемым вопросам.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Контрольные работы и рефераты не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика курсовых работ:

1. Методика контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.
2. Методика контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам.
3. Методика средства контроля защищенности конфиденциальной информации от НСД.
4. Обнаружение и идентификация инцидентов безопасности информации.
5. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации.
6. Методика выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных системах.
7. Сертификация средств защиты информации от НСД.
8. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД.
9. Методы выявления и оценки возможности реализации угроз безопасности информации.
10. Требования международных и национальных стандартов по защите информации.

8.3.1 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 ЗАЧЁТУ

1. Основные задачи контроля состояния ТЗКИ.
2. Нормативные и методические документы по контролю ТЗКИ.
3. Вопросы, подлежащие проверке при контроле состояния ТЗКИ.
4. Организация и порядок проведения контроля состояния ТЗКИ.
5. Оценка защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.
6. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.
7. Проведение контроля защищенности конфиденциальной информации от утечки за счет ПЭМИН с использованием программно-аппаратных комплексов.
8. Методика инструментального контроля выполнения норм показателя защищенности акустической речевой конфиденциальной информации.
9. Оценка защищенности акустической речевой информации.
10. Методы и средства контроля защищенности акустической речевой информации.
11. Проведение контроля защищенности акустической речевой информации с использованием программно-аппаратных комплексов.
12. Методы контроля защищенности конфиденциальной информации от НСД.

13. Средства контроля защищенности конфиденциальной информации от НСД.

14. Порядок проведения сертификационных испытаний средств защиты информации основных классов.

15. Задачи и функции мониторинга информационной безопасности средств и систем информатизации.

16. Порядок и методы мониторинга информационной безопасности средств и систем информатизации.

17. Контроль за событиями безопасности и действиями в средствах и системах информатизации.

18. Контроль (анализ) защищенности информации, содержащейся в средствах и системах информатизации.

19. Порядок и метода мониторинга информационной безопасности средств и систем информатизации.

7. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Основы организации контроля состояния ТЗКИ. Тема 1. Основные задачи контроля состояния ТЗКИ	Подготовка к лекции, подготовка к сдаче зачёта	2	Тесты перед лекцией, зачёт
Раздел 1. Тема 2 Организационный и технический контроль состояния ТЗКИ	Подготовка к лекции, к семинару, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 2. Методы и средства контроля защищенности конфиденциальной информацией. Тема 3. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН	Подготовка к лекции, семинару, к лабораторным работам, подготовка к сдаче зачёта	12	Тесты перед лекцией, тесты на семинаре, защита лабораторных работ, зачёт
Раздел 2. Тема 4. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам	Подготовка к лекции, семинару, к лабораторной работе, подготовка к сдаче зачёта	8	Тесты перед лекцией, тесты на семинаре, защита лабораторных работ, зачёт
Раздел 2. Тема 5. Методы и средства контроля защищенности конфиденциальной информации от НСД	Подготовка к лекции, семинару, к лабораторной работе, подготовка к сдаче зачёта	8	Тесты перед лекцией, тесты на семинаре, защита лабораторных работ, зачёт

Раздел 3. Мониторинг информационной безопасности средств и систем информатизации. Тема 6. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации	Подготовка к лекции, к семинару, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 3. Тема 7. Обнаружение и идентификация инцидентов безопасности информации	Подготовка к лекции, семинару, к лабораторной работе, подготовка к сдаче зачёта	8	Тесты перед лекцией, тесты на семинаре, защита лабораторных работ, зачёт
Раздел 3. Тема 8. Планирование мер по устранению инцидентов безопасности информации	Подготовка к лекции, к семинару, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 3. Тема 9. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации	Подготовка к лекции, к семинару, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты на семинаре, зачёт

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. 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

2. Гродзенский, Я. С. Информационная безопасность : учебное пособие / Гродзенский Я. С. - Москва : РГ-Пресс, 2020. - 144 с. - ISBN 978-5-9988-0845-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785998808456.html

дополнительная

1.1 Иванцов А. М. Основы информационной безопасности : курс лекций : учебное пособие. Ч. 1 / А. М. Иванцов, В. Г. Козловский; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2019. - 72 с.

1.2 Иванцов А. М. Основы информационной безопасности : курс лекций : учебное пособие. Ч. 2 / А. М. Иванцов, В. Г. Козловский; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2020. - 118 с.

2. Техническая защита информации : учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева [и др.]. — Самара : ПГУТИ, 2020. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255575

3. Исаева, М. Ф. Техническая защита информации : учебное пособие / М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2017. — 49 с. — ISBN 978-5-7641-1008-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/101600

4. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам/ Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 — URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html

5. 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

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов. - Ульяновск: УлГУ, 2022. - 19 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/14064.

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:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer;
- система защиты от НСД «Dallas Lock». 4 комплекта;
- имитатор многофункциональный имитатор «ИМФ-2»;
- прибор ST-032 «Пиранья»;
- генератор шума «Гром-ЗИ-4;
- селективный микровольтметр В6-9;
- система защиты от НСД SecretNet Studio.

Аудитории для проведения занятий — 2/24б, 3/317.

Аудитории укомплектованы 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