УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от «_17_» __05_____2022_г., протокол №_4/22_
Председатель _____М.А. Волков___
(подпись, расшифровка подписи)
«_17_» ____05_____ 2022___г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Защита информации и информационная безопасность
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

Специальность (направление**): 02.03.03** «Математическое обеспечение и администрирование информационных систем»,
профиль «Технология программирования»
(код специальности (направления), полное наименование)
Форма обучения:_____очная_____
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «_01_»_____09_____2022_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	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационные технологии»
/_____/ ____Андреев А.С._/ *(подпись)* *(Ф.И.О.)* «_16_»_____05_____2022__г.	/__ _____/ ___Волков_М.А._/ *(подпись)* *(Ф.И.О.)* «_17_»_____05_____2022__г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Цель курса - заложить методически правильные основы знаний в области защиты информации и информационной безопасности, необходимые будущим специалистам в области прикладной информатики.

Информационная безопасность (ИБ) - сравнительно молодая, быстро развивающаяся область информационных технологий (ИТ), для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими ветвями ИТ, базис. Это - первая задача курса, для решения которой привлекается объектно-ориентированный подход.

Успех в области защиты информации и ИБ может принести только комплексный подход. Описание общей структуры и отдельных уровней такого подхода - вторая задача курса. Для ее решения рассматриваются меры законодательного, административного, процедурного и технического уровней.

Предполагается, что большинство понятий, введенных в данном курсе, станет предметом более детального рассмотрения в других, специальных курсах.

Задачи освоения дисциплины:

дать основы: методологии создания систем защиты информации и обеспечения информационной безопасности информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Защита информации и информационная безопасность» (Б1.В.1.11) изучается в 8 семестре и относится к числу обязательных дисциплин блока Б1.В.1, предназначенного для студентов, обучающихся по направлению подготовки бакалавриата **02.03.03** «Математическое обеспечение и администрирование информационных систем».

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Технология программирования»; «Теория информации; «Информационные системы и технологии»; «Интеллектуальные системы и технологии»; «Администрирование информационных систем».

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

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

способность использовать нормативные правовые документы;

способность анализировать проблемы и процессы;

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

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Современные системы автоматизации разработки информационных систем»; «Функциональное программирование»; «Параллельное программирование»; «Современные системы автоматизации разработки информационных систем».

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-2 - Способен использовать основные методы и средства автоматизации проектирования,	**Знать:** Основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов

реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов, а также способен использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов	Основные методы защиты интрасетей от вторжений **Уметь:** Использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов **Владеть:** Методами и средствами автоматизации, связанными с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов
ПК-3 - Способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств; операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности	**Знать:** Основные методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов **Уметь:** Использовать знания методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов с точки зрения обеспечения информационной безопасности **Владеть:** Навыками администрирования и модернизации программных продуктов и программных комплексов основных подсистем информационной безопасности объекта защиты
ПК-4 - Способен использовать основные концептуальные положения функционального, логического, объектно-ориентирован-ного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений	**Знать:** Основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений **Уметь:** Использовать основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования **Владеть:** Навыками использования основных концептуальных положений функционального, логического, объектно-ориентированного и визуального направлений

	программирования
ПК-5 - Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	**Знать:** Современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования **Уметь:** Использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования **Владеть:** Навыками использования современных методов разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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

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

Вид учебной работы	Количество часов (форма обучения дневная)			
	Всего по плану	В т.ч. по семестрам		
		8		
1	2	3	4	5
Контактная работа обучающихся с преподавателем	50	50/50		
Аудиторные занятия:	50	50/50		
Лекции	20	20/20		
Лабораторные работы (лабораторный практикум)	20	20/20		
Практические и семинарские занятия	10	10/10		
Самостоятельная работа	58	58		
Форма текущего контроля знаний и контроля самостоятельной работы: Тестирование, контр. работа,		-Тестирование на лаборатор-ных работах; - вопросы перед лекциями; - рефераты на заданные темы		

коллоквиум, реферат и др. (не менее 2 видов)				
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	Экзамен	Экзамен		
Всего часов по дисциплине:	144	144		

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			
1	2	3	4	5	6	7	8
Раздел 1. Основные положения защиты информации							
1	2	3	4	5	6	7	8
1. Основные понятия в области защиты информации	4	2				2	Тесты Т1, рефераты (№ 1,2,4,5,6,7,)
2. Источники угроз информационной безопасности в информационных системах		2		4		4	Тесты Т2, Реферат № 3), лаб. раб. 1
3. Правовой режим защиты государственной тайны		2				4	Тесты Т3, реферат (№ 8)
4. Правовые режимы защиты коммерческой, профессиональной тайн и служебной		2	2			6	Тесты Т4, реферат (№ 9)

информации							
5. Законодательство Российской Федерации по вопросам защиты персональных данных		2	2			6	Тесты Т5, рефераты (№ 2,10,11)
Раздел 2. Основные методы и средства обеспечения информационной безопасности							
6. Многоуровневая защита интрасетей		2	2	2		6	Тесты Т6, рефераты (№ 14,16), лаб. раб. 2
7. Технологии межсетевых экранов.		2	2	2		6	Тесты Т7, рефераты (№ 17,18,19), лаб. раб. 3
8. Идентификация, аутентификация и контроль несанкционированного доступа к информации		2	2	8		14	Тесты Т8, реферат (№ 13)
9. Виртуальные частные сети		2				4	Тесты Т9, рефераты (№ 20,21)
10. Методы и средства защиты информации от утечки по техническим каналам		2		4		6	Тесты Т10, рефераты (№ 12, 15), лаб. раб. № 7,8
Итого:	144	20	10	20		58	

5. СОДЕРЖАНИЕ КУРСА (МОДУЛЯ)

Раздел 1. Основные положения защиты информации

Тема 1. Основные понятия в области защиты информации.

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

Тема 2. Источники угроз информационной безопасности в информационных системах.

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

Тема 3. Правовой режим защиты государственной тайны.

Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны.

Тема 4. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации.

Понятие коммерческой, профессиональной тайн и служебной информации по российскому законодательству. Коммерческая, профессиональная тайны. Служебная тайна. Правовые режимы тайн. Юридическая ответственность за нарушения правовых режимов информации ограниченного доступа (дисциплинарная, гражданско-правовая, административная, уголовная).

Тема 5. Законодательство Российской Федерации по вопросам защиты персональных данных.

Основные мероприятия по вопросам защиты информации и документы, разрабатываемые на предприятии в соответствии с Федеральным законом РФ «О персональных данных».

Раздел 2. Основные методы и средства обеспечения информационной безопасности

Тема 6. Многоуровневая защита интрасетей.

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

Тема 7. Технологии межсетевых экранов.

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

Тема 8. Идентификация, аутентификация и контроль несанкционированного доступа к информации.

Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Пароли, сертификаты и электронные подписи. Методы аутентификации. Разграничение доступа по виду, характеру, назначению, степени важности и конфиденциальности информации.

Тема 9. Виртуальные частные сети.

Основные понятия и функции виртуальных частных сетей (VPN). Варианты построения виртуальных защищенных каналов. Средства обеспечения безопасности VPN.

Тема 10. Методы и средства защиты информации от утечки по техническим каналам.

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

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий

Раздел 1. Основные положения защиты информации

Тема 4. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации (семинар).

1. Правовые основы коммерческой тайны.
2. Правовые основы профессиональных тайн.
3. Правовые основы служебной тайны.
4. Юридическая ответственность за нарушения правовых режимов информации ограниченного доступа (дисциплинарная, гражданско-правовая, административная, уголовная).

Тема 5. Законодательство Российской Федерации по вопросам защиты персональных данных (семинар).

1. Основные шаги при создании системы защиты персональной тайны на предприятии.
2. Основные документы по защите персональных данных, разрабатываемые на предприятии.

Тема 6. Многоуровневая защита интрасетей.

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

Тема 7. Технологии межсетевых экранов.

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

Тема 8. Идентификация, аутентификация и контроль несанкционированного доступа к информации.

1. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации.
2. Понятия о НСД к информации. Основные системы защиты информации от НСД
3. Разграничение доступа по виду, характеру, назначению, степени важности и конфиденциальности информации.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 1. Основные положения защиты информации

Тема 2. Источники угроз информационной безопасности в информационных системах.

Лабораторная работа № 1. (4 часа). «Выработка концептуальных основ деятельности по обеспечению информационной безопасности предприятия».

Цель: Анализ информационных активов, используемых компанией и выработка концептуальных основ деятельности по обеспечению корпоративной информационной безопасности. Результат: отчет.

Методические указания: основное внимание должно быть уделено практическому выявлению угроз и базовых уязвимостей конкретных информационных активов предприятия, а также выбору методов и средств противодействия имеющимся угрозам информационной безопасности.

Раздел 2. Основные методы и средства обеспечения информационной безопасности

Тема 6. Многоуровневая защита интрасетей

Лабораторная работа № 2. (2 часа). «Разработка Политик ИБ предприятия».

Цель: Анализ информационных активов, используемых компанией и выработка

концепции основ деятельности по обеспечению корпоративной информационной безопасности. Результат: отчет.

Методические указания: основное внимание должно быть уделено практическому выявлению угроз и базовых уязвимостей конкретных информационных активов предприятия, а также выбору методов и средств противодействия имеющимся угрозам информационной безопасности.

Тема 7. Технологии межсетевых экранов.

Лабораторная работа № 3. Назначение и возможности встроенных межсетевых экранов (МЭ).

Цель: изучить возможности и научиться работать с встроенными МЭ (ОС и антивирусные пакеты). Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей встроенных МЭ.

Тема 8. Идентификация, аутентификация и контроль доступа к информации

Лабораторная работа № 4. «Электронный замок "Соболь". (2 часа). Назначение, возможности и порядок работы с Электронным замком "Соболь".

Цель: изучить возможности и научиться работать с электронным замком "Соболь". Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке, установке и практическому освоению возможностей электронного замка "Соболь".

Лабораторная работа № 5. (2 часа). «Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

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

Методические указания: основное внимание должно быть уделено настройке, установке и практическому освоению возможностей Программно-аппаратного комплекса средств защиты информации от НСД.

Лабораторная работа № 6. (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**».

Тема 10. Методы и средства защиты информации от утечки по техническим каналам.

Лабораторная работа № 7 (2 часа). «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 № 8 **(2 часа). «**Обнаружение радиозлучающих устройств с использованием сканирующего радиоприемника AR-3000A».

Цель работы: Ознакомление с техническими характеристиками изделия AR-3000A, изучение правил эксплуатации изделия, получение практических навыков работы с изделием.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика рефератов:

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Интересы личности (общества, государства) в информационной сфере.
3. Угрозы информационной безопасности Российской Федерации.
4. Информационная система как объект информационной безопасности.
5. Юридические аспекты защиты информации.
6. Законодательство РФ об информационной безопасности.
7. Требования Федерального закона РФ «Об информации, информационных технологиях и о защите информации».
8. Требования Федерального закона РФ «О государственной тайне».
9. Требования Федерального закона РФ «О коммерческой тайне».
10. Законодательство РФ в области защиты персональных данных.
11. Проблемы защиты персональных данных.
12. Основные каналы утечки информации при обработке на компьютерах.
13. Программные и аппаратные средства защиты информации от несанкционированного доступа.
14. Политики безопасности интрасети организации.
15. Основные методы защиты информации от утечки по техническим каналам.
16. Сетевой аудит.
17. Эталонная сетевая модель OSI.
18. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.
19. Технология межсетевых экранов.
20. Виртуальные частные сети (VPN).
21. Назначение и возможности ПАК «ViPNet».

8.2.1 Правила оформления рефератов

1. Объём реферата 7-10 листов печатного текста. К оформлению рефератов предъявляются такие же требования, как и к курсовым работам для студентов 3 курса, описанные в учебно-методическом пособии: Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Базовые понятия и определения информационной безопасности
2. Основные принципы организации защиты информации
3. Угрозы информационной безопасности и их проявления
4. Классификация источников угроз информационной безопасности
5. Модель действий нарушителя
6. Назначение и возможности сканирующего радиоприемника AR-3000A
7. Порядок отнесения сведений к государственной тайне.
8. Система защиты сведений, составляющих государственную тайну.

9. Информация как объект правоотношений (Закон РФ “Об информации, информационных технологиях и о защите информации”)
10. Виды и содержание тайн государства
11. Законодательная база охраны государственной тайны (Закон РФ «О государственно тайне»)
12. Законодательная база охраны персональных данных (Закон РФ “О персональных данных»
13. Правовые основы защиты служебной и профессиональных тайн
14. Правовое регулирование коммерческой тайны закон РФ «О коммерческой тайне»
15. Многоуровневая защита интрасетей. Политика безопасности интрасети организации.
16. Многоуровневая защита интрасетей. Сетевой аудит.
17. Основы идентификации и аутентификации
18. Классификация протоколов аутентификации
19. Первоочередные мероприятия по созданию системы защиты персональных данных на предприятии.
20. Методы пассивной и активной защиты
21. Классификация межсетевых экранов**.**
22. Функции межсетевых экранов**.**
23. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.
24. Назначение и возможности Электронного замка "Соболь".
25. Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.
26. Назначение и возможности системы защиты от НСД «Dallas Lock»
27. Назначение и возможности имитатора многофункционального «ИМФ-2»
28. Назначение и возможности прибора ST-032 «Пиранья»
29. Виртуальные частные сети (VPN). Основные понятия и функции VPN.
30. Назначение и возможности ПАК «ViPNet».

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Основные положения защиты информации. Тема 1. Основные понятия в области защиты информации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты и вопросы перед лекцией, экзамен
Раздел 1. Тема 2. Источники угроз информационной безопасности в информационных системах	Подготовка к лекции, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	4	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, экзамен
Раздел 1. Тема 3. Правовой режим защиты	Подготовка к лекции, подготовка рефератов,	4	Тесты и вопросы перед лекцией,

государственной тайны.	подготовка к сдаче экзамена		экзамен
Раздел 1. Тема 4. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации.	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	6	Тесты и вопросы перед лекцией, экзамен
Раздел 1. Тема 5. Законодательство Российской Федерации по вопросам защиты персональных данных.	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	6	Тесты и вопросы перед лекцией, экзамен
Раздел 2. Основные методы и средства обеспечения информационной безопасности. Тема 6. Многоуровневая защита интрасетей	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	6	Тесты и вопросы перед лекцией, экзамен
Раздел 2. Тема 7. Технологии межсетевых экранов.	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	6	Тесты и вопросы перед лекцией, экзамен
Раздел 2. Тема 8. Идентификация, аутентификация и контроль несанкционированного доступа к информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	14	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, экзамен
Раздел 2. Тема 9. Виртуальные частные сети	Подготовка к лекции, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	4	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, экзамен
Раздел 2. Тема 10. Методы и средства защиты информации от утечки по техническим каналам	Подготовка к лекции, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	6	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277
3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

дополнительная

1. Новиков В.К., Информационное оружие - оружие современных и будущих войн [Электронный ресурс] / Новиков В.К. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2013. - 262 с. - ISBN 978-5-9912-0166-7 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201667.html 2. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

1.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 02 июля 2021 года N 400)

1.3 Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации"

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/
1.4 Федеральный закон от 27.07.2006 N152-ФЗ "О персональных данных" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/
1.5 Федеральный закон от 29.07.2004 N98-ФЗ "О коммерческой тайне" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/
2. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. - Воронеж: ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html.
3. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности:
3.1 ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности. — Режим доступа: https://gostexpert.ru/gost/gost-27002-2021;
3.2 ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — Режим доступа https://gostexpert.ru/gost/gost-28147-89
4. Туманов С.А., Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" [Электронный ресурс]: / Туманов С.А. - Новосибирск: Изд-во НГТУ, 2016. - 56 с. - ISBN 978-5-7782-2826-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778228269.html.

учебно-методическая

1. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", «Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", «Системный анализ и управление» / А.С. Андреев, С.М. Бородин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54с. http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf
2. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Защита информации и информационная безопасность» для студентов бакалавриата по направлениям 09.03.03 «Прикладная информатика» и 02.03.03 «Математическое обеспечение и администрирование информационных систем» очной формы обучения / А. М. Иванцов. - Ульяновск: УлГУ, 2022. - 18 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13127.

Согласовано:

ДИРЕКТОР НБ	/ БУРХАНОВА М.М. /	/	2022
Должность сотрудника научной библиотеки	ФИО	подпись	дата

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, [2022]. – 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, [2022]. - 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, [2022]. – 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, [2022]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2022]. – 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, [2022]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2022]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : научно-информационная база данных EBSCO // EBSCOhost : [портал]. – URL: http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102 . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. База данных «Русский как иностранный» : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2022]. – URL: https://ros-edu.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2022].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий EastView : электронные журналы / ООО ИВИС. - Москва, [2022]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2022]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД Гребенников. – Москва, [2022]. – 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, [2022]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase : научно-информационная база данных EBSCO // EBSCOhost : [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал . – URL: http://window.edu.ru/ . – Текст : электронный.

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

7. Образовательные ресурсы УлГУ:

7.1. 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:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	/ 2022
должность сотрудника УИТиТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer;
- электронный замок "Соболь" – 3 комплекта;
- система защиты от НСД «Dallas Lock». 4 комплекта;
- программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ” – 1 комплект;
- имитатор многофункциональный имитатор «ИМФ-2»;
- прибор ST-032 «Пиранья»;
- сканирующий радиоприемник AR-3000A.

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

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

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

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

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

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

Разработчик: _____ доцент кафедры Иванцов Андрей Михайлович

подпись должность ФИО