УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от «_16_» ___05___ _2023_ г., протокол № _4/23_
Председатель _____ М.А. Волков___
(подпись, расшифровка подписи)
«___05___ 2023___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Обнаружение вторжений и защита информации
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационная безопасность и теория 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_____2023_г.

Программа актуализирована на заседании кафедры: протокол № 12 от 12.04.2023 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.)* «_13_»_____05_____2023__г.	/__ _____/ ___Волков _М.А._/ *(подпись)* *(Ф.И.О.)* «_13_»_____05_____2023__г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель курса: заложить методически правильные основы знаний, необходимые будущим специалистам - практикам в области защиты информации.

Задачи освоения дисциплины:

Основными задачами дисциплины являются:

- научить применять стандартные средства защиты от несанкционированного доступа в вычислительных сетях.

- ознакомить обучаемых с основным направлениями и методами защиты интрасетей от вторжений.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Обнаружение вторжений и защита информации» изучается в 8 семестре и относится к числу дисциплин блока Б1.В, 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: «Информационные технологии»; «Информационные сети»; «Архитектура вычислительных систем и компьютерных систем»; «Криптографические методы защиты информации».

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

знание базовых понятий в области информационных технологий и информационных сетей и основ криптографии;

способность использовать нормативные правовые документы;

способность анализировать социально-значимые проблемы и процессы.

Основные положения дисциплины используются в дальнейшем при защите информации в ходе дальнейшей трудовой 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-2 - Способен использовать основные методы и средства автоматизации проектирования, 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	**Знать:** Основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта 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-ориентированного 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, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на лабораторных работах; - вопросы перед лекциями; - рефераты на заданные темы		
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. Атаки на интрасети							
1	2	3	4	5	6	7	8
1. Основные понятия в области защиты информации	4	2				2	Тесты Т1
2. Источники угроз информационной безопасности в информационных системах	18	2		4		12	Тесты Т2, лаб. раб. 1
3. Классификация вторжений. Типовые удаленные атаки	6	2	2			2	Тесты Т2
4. Интрасети и причины, способствующие атакам	6	2				4	Тесты Т3
5. Основные методы, используемые нарушителями для проникновения в интрасети	8	2	2			4	Тесты Т4
Раздел 2. Основные методы и средства защиты интрасетей от вторжений							
6. Многоуровневая защита интрасетей	12	2	2	2		6	Тесты Т6, лаб. раб. 2
7. Технологии межсетевых экранов.	22	4	2	6		10	Тесты Т7, лаб. раб.3,4
8. Системы обнаружения вторжений	16	2	2	4		8	Тесты Т7, лаб. раб. 5
9. Методы и средства защиты информации от утечки по техническим каналам	16	2		6		10	Тесты Т9 лаб. раб. № 6,7
Итого:	144	20	10	20		58	

5. СОДЕРЖАНИЕ КУРСА (МОДУЛЯ)

Раздел 1. Атаки на интрасети

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. Классификация вторжений. Типовые удаленные атаки.

Дана краткая история вторжений (атак) на интрасети и определения основных понятий. Приведён вариант классификация вторжений (атак). Рассмотрены типовые удаленные атаки (анализ сетевого трафика, подмена доверенного субъекта, введение ложного объекта компьютерной сети, отказ в обслуживании). Приведены подходы к защите от типовых удаленных атак. Уязвимости интрасетей со стороны всевозможных атак. Роль администрирования интрасетей для защиты их от вторжений.

Тема 4. Интрасети и причины, способствующие атакам

Понятие интрасети и задачи её защиты. Виды интрасетей. Основные технологии, необходимые для создания интрасетей. Уязвимости интрасетей со стороны всевозможных атак. Роль администрирования интрасетей для защиты их от вторжений.

Тема 5. Основные методы, используемые нарушителями для проникновения в интрасети.

Основные методы развертывания атак на интрасети, а именно: классические методы (подбор пароля, метод «грубой силы», метод «зашифровать и сравнить», социальная инженерия); современные методы (перехват данных, мониторинг в системе X Window, подмена системных утилит, нападения с использованием сетевых протоколов ("Летучая смерть", SYN-бомбардировка, спуффинг).

Раздел 2. Основные методы и средства защиты интрасетей от вторжений

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. Системы обнаружения вторжений.

Классификация систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений. Роль хоста-бастиона при обнаружении вторжений.

Тема 9. 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. Атаки на интрасети

Тема 3. Классификация вторжений. Типовые удаленные атаки (семинар).

1. Обнаружение вторжений. Краткий исторический обзор.
2. Классификация вторжений (атак).

3. Типовые удаленные атаки (анализ сетевого трафика, подмена доверенного субъекта, введение ложного объекта компьютерной сети, отказ в обслуживании).

Тема 5. Основные методы, используемые нарушителями для проникновения в интрасети (семинар).

1. Классические методы (подбор пароля, метод «грубой силы», метод «зашифровать и сравнить», социальная инженерия).
2. Современные методы (перехват данных, мониторинг в системе X Window, подмена системных утилит, нападения с использованием сетевых протоколов ("Летучая смерть", SYN-бомбардировка, спуффинг).

Раздел 2. Основные методы и средства защиты интрасетей от вторжений

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. Системы обнаружения вторжений (семинар).

1. Классификация систем обнаружения вторжений.
2. Интеллектуальное и поведенческое обнаружение вторжений.
3. Роль хоста-бастиона при обнаружении вторжений.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 1. Атаки на интрасети.

Тема 3. 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 защиты интрасетей от вторжений

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. (2 часа). 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.

Лабораторная работа № 4. (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 8. Системы обнаружения вторжений.

Лабораторная работа № 5. (4 часа). Система SecretNet Studio. «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.

Тема 9. Методы и средства защиты информации от утечки по техническим каналам.

Лабораторная работа № 6 (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 № 7 (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.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Обнаружение вторжений (атак). Краткий исторический обзор.
2. Классификация вторжений (атак).
3. Типовые удаленные атаки. Анализ сетевого трафика.
4. Типовые удаленные атаки. Подмена доверенного субъекта.
5. Типовые удаленные атаки. Введение ложного объекта компьютерной сети.
6. Типовые удаленные атаки. Отказ в обслуживании.
7. Понятие интрасети и задачи ее защиты.
8. Проблемы безопасности интрасетей.
9. Классические методы**,** используемые нарушителями для проникновения в интрасети. Метод «подбор пароля».
10. Классические методы**,** используемые нарушителями для проникновения в интрасети. Метод «грубой силы».
11. Классические методы**,** используемые нарушителями для проникновения в интрасети. Метод «зашифровать и сравнить».
12. Классические методы**,** используемые нарушителями для проникновения в интрасети. Социальная инженерия.
13. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод «перехват данных».
14. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод «мониторинг в системе X Window».
15. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод «подмена системных утилит».
16. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов "Летучая смерть".
17. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов «SYN-бомбардировка».
18. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов «спуффинг».
19. Многоуровневая защита интрасетей. Политика безопасности интрасети организации.
20. Многоуровневая защита интрасетей. Сетевой аудит.
21. Классификация межсетевых экранов**.**
22. Функции межсетевых экранов**.**
23. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Экранирующий маршрутизатор.
24. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Шлюз сеансового уровня.
25. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Экранирующий маршрутизатор.
26. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Шлюз прикладного уровня.
27. Классификация систем обнаружения вторжений.
28. Интеллектуальное и поведенческое обнаружение вторжений.
29. Роль хоста-бастиона при обнаружении вторжений.
30. Базовые понятия и определения информационной безопасности
31. Основные принципы организации защиты информации
32. Угрозы информационной безопасности и их проявления
33. Классификация источников угроз информационной безопасности
34. Модель действий нарушителя

35. Назначение и возможности сканирующего радиоприемника AR-3000A
36. Назначение и возможности системы защиты от НСД «Dallas Lock»
37. Назначение и возможности прибора ST-032 «Пиранья»
38. Назначение, возможности и порядок работы с системой SecretNet Studio»

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Атаки на интрасети. 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	12	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, экзамен
Раздел 1. Тема 3. Правовой режим защиты государственной тайны.	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты и вопросы перед лекцией, экзамен
Раздел 1. Тема 4. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации.	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	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 сдаче экзамена	4	Тесты и вопросы перед лекцией, экзамен
Раздел 2. Основные методы и средства защиты интрасетей от вторжений. 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	10	Тесты и вопросы перед лекцией, экзамен
Раздел 2. Тема 8. Системы обнаружения вторжений.	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	8	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, экзамен

Раздел 2. Тема 9. Методы и средства защиты информации от утечки по техническим каналам	Подготовка к лекции, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	10	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 ос-

нове "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 «Обнаружение вторжений и защита информации» для студентов бакалавриата по направлению 02.03.03 «Математическое обеспечение и администрирование информационных систем» и 09.03.03 «Прикладная информатика» очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2020. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 363 КБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/4270

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. / ___ / 04.05.2023 /
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, [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 элек-

тронная 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»;
- система защиты от НСД «SecretNet Studio»
- 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