УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от «_18_» __05__ 2021 г., протокол №_4/21_
Председатель _____ М.А. Волков
(подпись, расшифровка подписи)
«_18_» ___05_____ 2021___г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Обнаружение вторжений и защита информации
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

Направление бакалавриата: **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_____2021_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.)* «_12_»___05_____2021_	/_____/ _ Волков _М.А._ / *Подпись* *(Ф.И.О.)* «_18_»_____05_____2021__г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели 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 ГИА.

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 модернизация	**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

цией программных продуктов и программных комплексов	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) 5.

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 семестр		
1	**2**	**3**	**4**	**5**
Контактная работа обучающихся с преподавателем	80	80/80*		
Аудиторные занятия:	80	80/80*		
Лекции	20	20/20*		
Практические и семинарские занятия	20	20/20*		
Лабораторные работы (лабораторный практикум)	40	40/40*		
Самостоятельная работа	64	64		
Форма текущего контроля знаний и контроля самостоятельной работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		Тестирование на семинарах и лабораторных работах; - вопросы и тесты перед лекциями		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	экзамен 36	экзамен 36		
Всего часов по дисциплине:	180 с экзаменом	180 с экзаменом		

* 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 дневная

Название разделов и тем	Виды учебных занятий						
	Всего	Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практич. занятия, семинар	Лабораторные работы			
Раздел 1. Атаки на интрасети							
1. Введение в курс дисциплины.	3	2				1	Тесты Т1
2. Классификация вторжений. Типовые удаленные атаки.	6	2	2			2	Тесты Т2
3. Интрасети и причины, способствующие атакам.	5	2	2			1	Тесты Т3
4. Основные методы, используемые нарушителями для проникновения в интрасети.	10	2	4			4	Тесты Т4
Раздел 2. Основные методы защиты интрасетей от вторжений							
5. Многоуровневая защита интрасетей.	22	2	2	6		12	Тесты Т5, лаб.раб. 1
6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.	24	4	4	6		10	Тесты Т6, лаб.раб. 2
7. Системы обнаружения вторжений.	12	4	4			4	Тесты Т7
8. Виртуальные частные сети.	8	2	2			4	Тесты Т8
Раздел 3. Средства защиты информации от несанкционированного доступа.							
9. Персональные средства аутентификации данных - USB-ключи и смарт-карты eToken.	8			4		4	лаб.раб. 3
10. Электронный замок "Соболь".	10			6		4	лаб.раб. 4
11. Система защиты от НСД «Dallas Lock».	12			6		6	лаб.раб. 5
12. Система защиты конфиденциальной информации и персональных данных «Secret Disk»	12			6		6	лаб.раб. 6

13. Программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ”.	8			6		6	лаб.раб. 7
Итого:	144	20	20	40		64	

5. СОДЕРЖАНИЕ КУРСА (МОДУЛЯ)

Раздел 1. Атаки на интрасети

Тема 1. Введение в курс дисциплины.

Во введении рассмотрена актуальность изучаемой дисциплины «Обнаружение вторжений и защита информации». Дана краткая история вторжений (атак) на интрасети и определения основных понятий. Перечислены организации, которые наиболее часто подвержены попыткам осуществления атак: финансовые учреждения и банки; сервис-провайдеры Internet; фармацевтические компании; правительственные и оборонные предприятия; партнеры и заказчики различных правительственных учреждений; международные корпорации.

Тема 2. Классификация вторжений. Типовые удаленные атаки.

Дан 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.

Тема 3. 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 4. Основные методы, используемые нарушителями для проникновения в интрасети.

В данной теме рассмотрены 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 защиты интрасетей от вторжений

Тема 5. 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 6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

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 7. Системы обнаружения вторжений.

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

Тема 8. Виртуальные частные сети.

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

Раздел 3. Средства защиты информации от несанкционированного доступа

Тема 9. Персональные средства аутентификации и защищенного хранения данных - USB-ключи и смарт-карты eToken.

Назначение, возможности и порядок работы с персональными средствами аутентификации и защищённого хранения данных (USB-ключи и смарт-карты eToken).

Тема 10. Электронный замок "Соболь".

Назначение, возможности, установка и порядок работы с Электронным замком "Соболь".

Тема 11. Система защиты от НСД «Dallas Lock».

Назначение, возможности, установка и использование системы защиты от НСД «Dallas Lock».

Тема 12. Система защиты конфиденциальной информации и персональных данных «Secret Disk».

Назначение, возможности, установка и использование системы защиты от НСД «Secret Disk».

Тема 13. Программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ”.

Назначение, возможности, установка и использование программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

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 2. 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 3. Интрасети и причины, способствующие атакам (семинар).

1. Понятие интрасети и задачи ее защиты.
2. Сегментирование интрасетей.
3. Проблемы безопасности интрасетей.

Тема 4. 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 защиты интрасетей от вторжений

Тема 5. Многоуровневая защита интрасетей (семинар).

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

Тема 6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI (семинар).

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 7. Системы обнаружения вторжений (семинар).

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

Тема 8. Виртуальные частные сети (VPN) (семинар).

1. Основные понятия и функции VPN.
2. Варианты построения виртуальных защищенных каналов.
3. Средства обеспечения безопасности VPN.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 2. Основные методы защиты интрасетей от вторжений

Тема 5. Многоуровневая защита интрасетей.

Лабораторная работа № 1. (8 часов). «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.

Тема 6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

Лабораторная работа № 2 (6 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.

Раздел 3. Средства защиты информации от несанкционированного доступа

Тема 9. Персональные средства аутентификации и защищённого хранения данных - USB-ключи и смарт-карты eToken.

Лабораторная работа № 3. (4 часа). Назначение, возможности и порядок работы с персональными средствами аутентификации и защищённого хранения данных (USB-ключи и смарт-карты eToken).

Цель: Изучить возможности и научиться работать с персональными средствами аутентификации данных. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей персональных средств аутентификации.

Тема 10. Электронный замок "Соболь".

Лабораторная работа № 4. (4 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".

Тема 11. Система защиты от НСД «**Dallas Lock**».

Лабораторная работа № 5. (6 часов). 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 12. Система защиты конфиденциальной информации и персональных данных «Secret Disk».

Лабораторная работа № 6 (6 часов). Назначение и возможности Системы защиты от НСД «Secret Disk».

Цель: изучить возможности и научиться работать с Системой защиты от НСД «Secret Disk». Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке, установке и практическому освоению возможностей Системы защиты от НСД «Secret Disk».

Тема 13. Программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ”.

Лабораторная работа № 7 (6 часов). Назначение и возможности программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

Цель: изучить возможности и научиться работать с программно-аппаратным комплексом средств защиты информации 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.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые, контрольные работы и рефераты 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. Виртуальные частные сети (VPN). Основные понятия и функции VPN.

31. Варианты построения виртуальных защищенных каналов.

32. Средства обеспечения безопасности виртуальных частных сетей (VPN).

33. Назначение и возможности персональных средств аутентификации и защищенного хранения данных (USB-ключи и смарт-карты eToken).

34. Назначение и возможности Электронного замка "Соболь".

35. Назначение и возможности системы защиты конфиденциальной информации и персональных данных «Secret Disk».

36. Назначение и возможности системы защиты информации от НСД «Dallas Lock».

37. Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1	2	3	4
Раздел 1. Атаки на интрасети. Тема 1. Введение в курс дисциплины	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, вопросы и тесты на семинаре, экзамен
Раздел 1. Тема 2. Классификация вторжений. Типовые удаленные атаки	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты и вопросы на семинаре, экзамен
Раздел 1. Тема 3. Интрасети и причины, способствующие атакам	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, вопросы и тесты на семинаре, экзамен
Раздел 1. Тема 4. Основные методы, используемые нарушителями для проникновения в интрасети	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, вопросы и тесты на семинаре, экзамен
Раздел 2. Основные методы защиты интрасетей от вторжений. Тема 5. Многоуровневая защита интрасетей	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	12	Тесты перед лекцией, тесты и вопросы на семинаре, вопросы на лабораторной работе экзамен
Раздел 2. Тема 6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	10	Тесты перед лекцией, тесты и вопросы на семинаре, вопросы на лабораторной работе экзамен
Раздел 2. Тема 7. Системы обнаружения вторжений	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты и вопросы на семинаре, экзамен
Раздел 2. Тема 8. Виртуальные частные сети	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты и вопросы на семинаре, экзамен
Раздел 3. Средства защиты информации от несанкционированного доступа Тема 9. Персональные средства аутентификации данных - USB-ключи и смарт-карты eToken	Подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	4	Вопросы на лабораторной работе, экзамен
Раздел 3. Тема 10. Элек-	Подготовка рефератов,	4	Вопросы на лабора-

тронный замок "Соболь"	подготовка к лабораторным работам, подготовка к сдаче экзамена		торной работе, экзамен
Раздел 3. Тема 11. Система защиты от НСД «Dallas Lock».	Подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	6	Вопросы на лабораторной работе, экзамен
Раздел 3. Тема 12. Система защиты конфиденциальной информации и персональных данных «Secret Disk».	Подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	6	Вопросы на лабораторной работе, экзамен
Раздел 3. Тема 13. Программно-аппаратный комплекс средств защиты информации от НСД «Аккорд–АМДЗ».	Подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	6	Вопросы на лабораторной работе, экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Шелухин О.И., Обнаружение вторжений в компьютерные сети (сетевые аномалии) [Электронный ресурс]: Учебное пособие для вузов / Под ред. профессора О.И. Шелухина. - М.: Горячая линия - Телеком, 2013. - 220 с. - ISBN 978-5-9912-0323-4 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203234.html.

2. Защита информации: основы теории: учебник для бакалавриата и магистратуры / Щеглов А. Ю., Щеглов К. А. – М.: Издательство Юрайт, 2019. – 309 с. https://biblio-online.ru/viewer/zaschita-informacii-osnovy-teorii-433715.

3. Бирюков А.А., Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А. А. - М. : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785970604359.html.

дополнительная

1. 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 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

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 до-

ступа: 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 Р ИСО/МЭК 27002-2012 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-27002-2012;

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.

URL: ftp://10.2.96.134/Text/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:

Гл.библ-рь НБ УлГУ	Попина И.Ю		04.05.2021
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. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2021]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2021]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2021]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача : электронно-библиотечная система : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2021]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2021]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2021]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2021]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // 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. Русский язык как иностранный : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2021]. – 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, [2021].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2021]. – 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, [2021]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2021]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2021]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase // 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 / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://window.edu.ru/ . – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО

ЦРГОП и ИТ. – URL: http://www.edu.ru. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ : модуль 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.	/	04.05.2021
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;
- система защиты конфиденциальной информации и персональных данных «Secret Disk. Базовый комплект с USB-ключом – 4 комплекта;
- персональные средства аутентификации и защищенного хранения данных - USB-ключи и смарт-карты eToken – 3 комплекта.

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