УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» 06 2019 г., протокол № 5/19
Председатель _____ М.А. Волков
(подпись, расшифровка подписи)
«21» 06 2019 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**: 09.03.03** «Прикладная информатика»,
профиль «Информационная среда» (Квалификация (степень) - «бакалавр»)
код направления (специальности), полное наименование *полное наименование*

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «_01_»_____09_____2019_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.)* «_19_»_____06_____2019_г.	/_____/ Волков М.А. / *(подпись)* *(Ф.И.О.)* «_21_»_____06_____2019__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:

- ознакомить обучаемых с основным направлениями и методами защиты интрасе-тей от вторжений;

- научить применять стандартные средства защиты от вторжений (атак).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Обнаружение вторжений и защита информации» изучается в 8 семестре и относится к числу обязательных дисциплин блока Б1.В, предназначенного для студентов, обучающихся по направлению подготовки бакалавриата 09.03.03 «Прикладная информатика».

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 изучении таких дисциплин как: «Современные системы автоматизации разработки информационных систем»; «Программирование для Интернет».

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**
ОПК-1 - Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	**Знать:** Основные методы математического анализа и моделирования, теоретического и экспериментального исследования **Уметь:** Применять основные методы математического анализа и моделирования, теоретического и экспериментального исследования в своей профессиональной деятельности **Владеть:** Методологией использования основных методов математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности
ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной	**Знать:** Основные требования информационной безопасности в ходе решения стандартных задач профессиональной деятельности **Уметь:** Решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности **Владеть:** Методологией настройки информационных систем в процессе

безопасности	защиты информации
ПК-7 - способность настраивать, эксплуатировать и сопровождать информационные системы и сервисы	**Знать:** Основные современные информационные системы и сервисы в области защиты информации **Уметь:** Настраивать, эксплуатировать и сопровождать типовые средства защиты информации от несанкционированного доступа **Владеть:** Навыками администрирования основных подсистем информационной безопасности объекта защиты
ПК-8 - способность проводить тестирование компонентов программного обеспечения ИС	**Знать:** Основные требования информационной безопасности в ходе тестирования программного обеспечения ИС **Уметь:** Проводить тестирование компонентов программного обеспечения ИС учетом основных требований информационной безопасности **Владеть:** Методологией тестирования компонентов программного обеспечения ИС в процессе защиты информации

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	48	48/48		
Аудиторные занятия:	48	48/48		
Лекции	12	12/12		
Практические и семинарские занятия	12	12/12		
Лабораторные работы (лабораторный практикум)	24	24/24		
Самостоятельная работа	96	96		
Форма текущего контроля знаний и контроля		Тестирование на семинарах и лабораторных		

самостоятельной работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		работах; - вопросы и тесты перед лекциями; - рефераты на заданные темы		
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	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		лекции	Практич. занятия, семинар	Лабораторные работы			
1	2	3	4	5	6	7	8
Раздел 1. Атаки на интрасети							
1. Классификация вторжений. Типовые удаленные атаки.	4	2	2			2	Тесты Т1, рефераты (№ 1,7,8,9)
2. Основные методы, используемые нарушителями для проникновения в интрасети.	10	2	2			2	Тесты Т2, рефераты (№ 2,3)
Раздел 2. Основные методы и средства защиты интрасетей от вторжений							
3. Многоуровневая защита интрасетей.	12	2	2	4		20	Тесты Т3, рефераты (№ 10, 11), лаб. раб. 1

4. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.	24	2	2	4		20	Тесты Т4, рефераты (№ 4,5,12), лаб. раб. 2
5. Системы обнаружения вторжений.	20	2	2	10		28	Тесты Т5, рефераты (№ 2, 13), лаб. раб. № 3, 4
6. Виртуальные частные сети.	14	2	2	8		24	Тесты Т6, рефераты (№ 6,14), лаб. раб. 5
Итого:	144	12	12	24		96	

5. СОДЕРЖАНИЕ КУРСА (МОДУЛЯ)

Раздел 1. Атаки на интрасети

Тема 1. 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 2. 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 и средства защиты интрасетей от вторжений

Тема 3. 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 4. 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 5. Системы обнаружения вторжений.

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

Тема 6. Виртуальные частные сети.

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

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 1. 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).
4. Проблемы безопасности интрасетей.

Тема 2. 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 3. Многоуровневая защита интрасетей (семинар).

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

Тема 4. 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 5. Системы обнаружения вторжений (семинар).

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

Тема 6. 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 и средства защиты интрасетей от вторжений

Тема 3. Многоуровневая защита интрасетей.

Лабораторная работа № 1. **(4 часа).** «Разработка Политики 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 4. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

Лабораторная работа № **2 (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.

Тема 5. Системы обнаружения вторжений.

Лабораторная работа № 3 **(2 часа).** Назначение и возможности системы обнаружения вторжений «**Dallas Lock**».

Цель: изучить возможности и научиться работать с СОВ «Dallas Lock». Результат: отчет.

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

Лабораторная работа № 4 **(8 часов).** Назначение и возможности Детектора атак АПКШ «Континент».

Тема 6. Виртуальные частные сети (VPN).

Лабораторная работа № 5 **(8 часов)**. Назначение и возможности ПАК «ViPNet».

Цель: Изучить возможности и научиться работать с ПАК «ViPNet». Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей ПАК «ViPNet» по построению витрувльныз частных сетей.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика рефератов:

1. Обнаружение вторжений. Краткий исторический обзор.
2. Основные методы обнаружения вторжений.
3. Атаки на сети с использованием сетевых протоколов.
4. Эталонная сетевая модель OSI.
5. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.
6. Виртуальные частные сети (VPN).
7. Типовые удаленные атаки на интрасети.
8. Классификация вторжений (атак).
9. Роль администрирования интрасетей для защиты их от вторжений.
10. Политики безопасности интрасети организации.
11. Сетевой аудит.
12. Технология межсетевых экранов.
13. Классификация систем обнаружения вторжений.
14. 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. 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.
7. Классические методы**,** используемые нарушителями для проникновения в интрасети. Метод «подбор пароля».
8. Классические методы**,** используемые нарушителями для проникновения в интрасети. Метод «грубой силы».
9. Классические методы**,** используемые нарушителями для проникновения в интрасети. Метод «зашифровать и сравнить».
10. Классические методы**,** используемые нарушителями для проникновения в интрасети. Социальная инженерия.
11. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод «перехват данных».
12. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод «мониторинг в системе X Window».
13. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод «подмена системных утилит».
14. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов "Летучая смерть".
15. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов «SYN-бомбардировка».
16. 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.
17. Классификация межсетевых экранов**.**
18. Функции межсетевых экранов**.**
19. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Экранирующий маршрутизатор.
20. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Шлюз сеансового уровня.
21. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Экранирующий маршрутизатор.
22. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Шлюз прикладного уровня.

23. Классификация систем обнаружения вторжений.
24. Интеллектуальное и поведенческое обнаружение вторжений.
25. Роль хоста-бастиона при обнаружении вторжений.
26. Виртуальные частные сети (VPN). Основные понятия и функции VPN.
27. Варианты построения виртуальных защищенных каналов.
28. Средства обеспечения безопасности виртуальных частных сетей (VPN).
29. Назначение и возможности ПАК «ViPNet».
29. Назначение и возможности АПКШ «Континент».
30. Назначение и возможности Детектора атак АПКШ «Континент».

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. Классификация вторжений. Типовые удаленные атаки	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, вопросы и тесты на семинаре, экзамен
Раздел 1. Тема 2. Основные методы, используемые нарушителями для проникновения в интрасети	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты и вопросы на семинаре, экзамен
Раздел 2. Основные методы и средства защиты интрасетей от вторжений. Тема 3. Многоуровневая защита интрасетей	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	20	Тесты перед лекцией, тесты и вопросы на семинаре, вопросы на лабораторной работе экзамен
Раздел 2. Тема 4. 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	20	Тесты перед лекцией, тесты и вопросы на семинаре, вопросы на лабораторной работе экзамен
Раздел 2. Тема 5. Системы обнаружения вторжений	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	28	Тесты перед лекцией, тесты и вопросы на семинаре, экзамен
Раздел 2. Тема 6. Виртуальные частные сети	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	24	Тесты перед лекцией, тесты и вопросы на семинаре, 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. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/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 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 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. Бо-

родин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54с. - Режим доступа: **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, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл: 368 КБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/4973

Согласовано:
Гл. библ-рь ИБ УлГУ / Попова И.Ю / Подпись / 14.06.2019
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** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов, [2019]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://www.biblio-online.ru.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: https://e.lanbook.com.

1.5**. Znanium.com** [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://znanium.com.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва: КонсультантПлюс, [2019].

3**. База данных периодических изданий** [Электронный ресурс]: электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://нэб.рф.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://dvs.rsl.ru.

6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

8. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

Согласовано:
Зам. нач. УИиТ /Клочкова А.В. / 14.06.2019
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»;
- генератор шума «Гром-ЗИ-4;
- генератор шума SI-3010;
- 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: подпись доцент кафедры должность Иванцов Андрей Михайлович ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой	Подпись	Дата
1	Внесение изменений в п.п. 4.2 Объем дисциплины по видам учебной работы п. «Общая трудоемкость дисциплины» с оформлением приложения 1	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
2	Внесение изменений в п. 13 «Специальные условия для обучающихся с ограниченными возможностями здоровья» с оформлением приложения 2	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
3	Внесение изменений в п/п а) Список рекомендуемой литературы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 3	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14
4	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 4	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14

Приложение 1

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	48	48/48*		
Аудиторные занятия:	48	48/48*		
Лекции	12	12/12*		
Практические и семинарские занятия	12	12/12*		
Лабораторные работы (лабораторный практикум)	24	24/24*		
Самостоятельная работа	96	96		
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; - рефераты на заданные темы		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	экзамен 36	экзамен 36		
Всего часов по дисциплине:	180 с экзаменом	180 с экзаменом		

*Количество часов работы ППС с обучающимися в дистанционном формате с применением электронного обучения

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.

Приложение 2

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

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

Приложение 3

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. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/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 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 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. - Режим доступа: **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, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл: 368 КБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/4973

Согласовано:

Гл. библ-рь ИБ УлГУ / Полина И.Ю / Подпись / 14.06.2019

Должность сотрудника научной библиотеки / ФИО / подпись / дата

http://lib.ulsu.ru/MegaPro/Download/MObject/4973

Приложение 4

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов, [2019]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://www.biblio-online.ru.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: https://e.lanbook.com.

1.5**. Znanium.com** [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://znanium.com.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва: КонсультантПлюс, [2019].

3**. База данных периодических изданий** [Электронный ресурс]: электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://нэб.рф.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://dvs.rsl.ru.

6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

8. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

Согласовано:

Зам. нач. УИиТ /Клочкова А.В. / 14.06.2019

Должность сотрудника УИТиТ ФИО подпись дата