




Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### Цели освоения дисциплины:

Целью изучения дисциплины «Безопасность сетей ЭВМ» является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

### Задачи освоения дисциплины:

- изучение типовых угроз безопасности в компьютерных сетях;
- изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
- овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО


Дисциплина «Безопасность сетей ЭВМ» изучается в 9 семестре и относится к базовой части дисциплин блока Б1.Б специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Курс учебной дисциплины тесно увязан с другими учебными дисциплинами, в первую очередь с курсами «Информатика», «Языки программирования», «Технологии и методы программирования», «Организация ЭВМ и вычислительных систем», «Сети и системы передачи информации», «Безопасность операционных систем», «Основы информационной безопасности», «Администрирование сетей ЭВМ», позволяющими понять физическую сущность безопасности сетей ЭВМ.

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

- знание базовых понятий в области информатики и вычислительной техники;
- способность использовать нормативные правовые документы;
- способность анализировать проблемы и процессы;
- способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.


Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Безопасность открытых информационных систем»; «Разработка и эксплуатация защищённых автоматизированных систем»; «Инструментальные средства контроля защищённости информации»; «Сертификация средств защиты информации», а также в ходе всех видов практик.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		


### 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ 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
1	2
ОПК-2 - способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	<p><b>Знать:</b> математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники</p> <p><b>Уметь:</b> применять соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники</p> <p><b>Владеть:</b> навыками корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники</p>
ОПК-3 - способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	<p><b>Знать:</b> языки, системы и инструментальные средства программирования</p> <p><b>Уметь:</b> применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p><b>Владеть:</b> навыками применения языков, систем и инструментальных средств программирования в профессиональной деятельности</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		


1	2
ОПК-4 - способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах	<p><b>Знать:</b> начение информации в развитии современного общества</p> <p><b>Уметь:</b> применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах</p> <p><b>Владеть:</b> навыками понимания значения информации в развитии современного общества, применения достижений современных информационных технологий для поиска информации в компьютерных системах, сетях библиотечных фондах</p>
ОПК-5 - способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	<p><b>Знать:</b> методы научных исследований в работе над междисциплинарными и инновационными проектами</p> <p><b>Уметь:</b> применять методы научных исследований в профессиональной деятельности</p> <p><b>Владеть:</b> навыками применения методов научных исследований</p>
ОПК-6 - способностью применять нормативные правовые акты в профессиональной деятельности	<p><b>Знать:</b> нормативные правовые акты, применяемые в профессиональной деятельности</p> <p><b>Уметь:</b> применять нормативные правовые акты в профессиональной деятельности</p> <p><b>Владеть:</b> навыками применения нормативных правовых актов в профессиональной деятельности</p>
ОПК-7 - способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	<p><b>Знать:</b> приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций</p> <p><b>Уметь:</b> применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций</p> <p><b>Владеть:</b> навыками применения приемов оказания первой помощи, методов защиты производственного персонала и населения в условиях чрезвычайных ситуаций</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

1	2
ОПК-8 - способностью к освоению новых образцов программных, технических средств и информационных технологий	<p><b>Знать:</b> новые образцы программных, технических средств и информационных технологий</p> <p><b>Уметь:</b> осваивать новые образцы программных, технических средств и информационных технологий</p> <p><b>Владеть:</b> навыками применения новых образцов программных, технических средств и информационных технологий</p>
ПК-1 - способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	<p><b>Знать:</b> научно-техническую информацию, нормативные и методические материалы в сфере профессиональной деятельности, в том числе на иностранном языке</p> <p><b>Уметь:</b> изучать, обобщать и систематизировать научно-техническую информацию нормативные и методические материалы в сфере профессиональной деятельности, в том числе на иностранном языке</p> <p><b>Владеть:</b> навыками осуществления поиска, изучения, обобщения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке</p>
ПК-7 - способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	<p><b>Знать:</b> научно-техническую документацию, научно-технические отчеты, обзоры, публикации</p> <p><b>Уметь:</b> разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p> <p><b>Владеть:</b> навыками разработки научно-технической документации, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p>
ПК-18 - способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	<p><b>Знать:</b> типовые управленческие решения при работе с малыми коллективами исполнителей</p> <p><b>Уметь:</b> организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</p> <p><b>Владеть:</b> навыками организации работы малых коллективов исполнителей, выработки и реализации управленческих решений в сфере профессиональной деятельности</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

ПК-19 - способностью разрабатывать предложения по совершенствованию системы управления	<p><b>Знать:</b> основы и составляющие системы управления</p> <p><b>Уметь:</b> разрабатывать предложения по совершенствованию системы управления</p> <p><b>Владеть:</b> Навыками формулирования предложений по совершенствованию системы управления</p>
ПК-21 - способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	<p><b>Знать:</b> документы, регламентирующие работу по обеспечению информационной безопасности автоматизированных систем</p> <p><b>Уметь:</b> разрабатывать проекты документов, регламентирующих работу по обеспечению информационной (ИБ) безопасности (АС)</p> <p><b>Владеть:</b> навыками разработки проектов документов, регламентирующих работу по обеспечению ИБ АС</p>
ПК-25 - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	<p><b>Знать:</b> средства защиты информационно-технологических ресурсов автоматизированной системы и восстановления их работоспособности при возникновении нештатных ситуаций</p> <p><b>Уметь:</b> применять средства защиты информационно-технологических ресурсов автоматизированной системы и восстановления их работоспособности при возникновении нештатных ситуаций</p> <p><b>Владеть:</b> навыками эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы и восстановления их работоспособности при возникновении нештатных ситуаций</p>
ПК-26 - способностью администрировать подсистему информационной безопасности автоматизированной системы	<p><b>Знать:</b> возможности подсистемы информационной безопасности автоматизированной системы</p> <p><b>Уметь:</b> администрировать подсистему информационной безопасности автоматизированной системы</p> <p><b>Владеть:</b> навыками администрирования подсистемы информационной безопасности автоматизированной системы</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

#### 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ


4.1. Объем дисциплины в зачетных единицах (всего) 7.

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

Вид учебной работы	Количество часов (форма обучения <u>дневная</u> )			
	Всего по плану	В т.ч. по семестрам		
		9 семестр		
1	2	3	4	5
Контактная работа обучающихся с преподавателем	90	90/90		
Аудиторные занятия:	90	90/90		
Лекции	36	36/36		
Практические и семинарские занятия				
Лабораторные работы (лабораторный практикум)	54	54/54		
Самостоятельная работа	126	126		
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на семинарах; - вопросы при защите лабораторных работ		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	экзамен	экзамен		
Всего часов по дисциплине:	252	252		

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.




Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

### 4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения дневная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практ. занятия, семинары	Лабораторные работы			
1	2	3	4	5	6	7	8
<b>Раздел 1. Типовые угрозы сетевой безопасности</b>							
1. Сетевые атаки	6	4				2	Тесты Т1
2. Механизмы реализации атак в сетях TCP/IP	6	4				2	Тесты Т2
3. Методы перехвата сетевых соединений в сетях TCP/IP	8	4				4	Тесты Т3
4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак	30	4		6	6	20	Тесты Т4, Лаб. Раб. № 1
<b>Раздел 2. Криптографические методы защиты информации в компьютерных сетях</b>							
5. Криптографические протоколы обеспечения безопасности	26	4		8		14	Тесты Т5, Лаб. Раб. № 2
6. Защита виртуальных частных сетей (VPN)	26	4		8	8	14	Тесты Т6, Лаб. Раб. № 3
7. Разработка защищенных сетевых приложений	26	4		8		14	Тесты Т7, Лаб. Раб. № 4
<b>Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях</b>							
8. Средства защиты локальных сетей при подключении к Интернет	28	4		8		16	Тесты Т8, Лаб. Раб. № 5
9. Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений	60	4		16	16	40	Тесты Т9, Лаб. Раб. № 6,7
<b>Итого:</b>	<b>252</b>	<b>36</b>		<b>54</b>	<b>30</b>	<b>126</b>	



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### Раздел 1. Типовые угрозы сетевой безопасности

#### Тема 1. Сетевые атаки

Стадии проведения сетевой атаки. Классификация сетевых угроз, уязвимостей и атак. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.

#### Тема 2. Механизмы реализации атак в сетях TCP/IP

Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Методы сканирования портов. Методы обнаружения пакетных снифферов. Методы обхода МЭ.

#### Тема 3. Методы перехвата сетевых соединений в сетях TCP/IP

Имперсонация вслепую. Десинхронизация TCP-соединений. Атаки, направленные на сетевую инфраструктуру. Защита от атак.

#### Тема 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак

Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак.

### Раздел 2. Криптографические методы защиты информации в компьютерных сетях

#### Тема 5. Криптографические протоколы обеспечения безопасности

Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

#### Тема 6. Защита виртуальных частных сетей (VPN)

Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и транспортном режимах. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.

#### Тема 7. Разработка защищенных сетевых приложений

Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.


### Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях

#### Тема 8. Средства защиты локальных сетей при подключении к Интернет

Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.

#### Тема 9. Защита серверов и рабочих станций.

Средства и методы предотвращения и обнаружения вторжений. Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

вторжений в общей системе обеспечения сетевой безопасности. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Способы противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell).

## 6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические и семинарские занятия не предусмотрены учебным планом дисциплины.

## 7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

*Цель.* Лабораторный практикум по дисциплине направлен на изучение студентами всех современных подходов для обеспечения информационной безопасности современных операционных систем. Охватывает клиентские операционные системы (на базе Microsoft Windows 10 и Alt Linux), а также серверные операционные системы (на базе Microsoft Server 2026R2 и Alt Linux Server). В соответствии с руководящими документами обучение происходит на сертифицированных версиях операционных систем.

*Методология* основывается на самостоятельном обучении студентов решению стандартных задач на основе технической документации, теоретического материала. Все работы обладают дифференцированной линейно растущей сложностью выполнению и созданы на основе стандартных практических задач современного предприятия. Поиск технической информации, а также подбор необходимого решения производится самостоятельно студентами в открытых источниках и контролируется в ходе лабораторных занятий и процессе демонстрации полученного решения.

*Результат.* Полученные решения демонстрируются студентом для каждого из типа операционных систем. При необходимости демонстрируется ход выполнения работы.


*Требования к оборудованию.* Для выполнения работ студенты используют несколько виртуальных машин с различными версиями операционных систем. Возможно самостоятельное выполнение лабораторных работ вне лаборатории. Компьютер с жестким диском – 100 Gb, ОЗУ: 8 Gb, Windows 10 Pro, BaseAlt (Альт Рабочая станция, Альт сервер), Kali Linux, Oracle Virtual Box, Putty, PGP, Apache, nginx, Statistica, Origin. По желанию студента все виртуальные машины могут быть развернуты на выделенном сервере виртуальных машин в лаборатории. Для моделирования работы сетей используется CISCO Packet Tracer. Сеть лаборатории представляет собой гетерогенную сеть, включающую в себя индивидуальный набор следующего оборудования:

1. Коммутатор L2, L3.
2. Маршрутизатор L3 с функциями VPN.
3. Маршрутизатор Континет КШ 25.
4. Маршрутизатор VipNet Координатор.

Для поддержания работы сетей используется выделенный Коммутатор L3, L3 сконфигурированный для работы независимых сегментов сети.

*Требования к оформлению лабораторной работы.* Все файлы, используемые в лабораторной работе, должны быть представлены в одном каталоге и иметь наименования, описывающие хранимую в файле информацию. Например: ssh\_client\_key.txt – содержит информацию о клиентском ключе для SSH. Должен быть файл read.me с текстовым описанием всех настроек, которые были использованы для выполнения лабораторной работы разбитых на секции. Например:

```
[BaseAlt (Альт Рабочая станция, Альт сервер) Server]
IPv4=10.2.0.1/24
DNS=10.2.0.2
```

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

gateway: 10.2.0.3

; Обозначение комментария

Имена полей должны быть написаны латинскими буквами. Секции могут включать в себя подсекции.

## **Раздел 1. Типовые угрозы сетевой безопасности**

### **Тема 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак**

#### **Лабораторная работа № 1 (6 часов). Строение сетей.**

*Цель.* Изучение базовых механизмов получения информации о конфигурации сети. Получение навыков работы с различными программами, позволяющими определить конфигурацию сети или конфигурацию отдельного устройства в сети. Требуется для выполнения всех последующих лабораторных работ.

*Задача.* Все задачи необходимо выполнить на ОС MS Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер).

- Для каждой из операционных систем установить следующее программное обеспечение:
  - Сканер безопасности Nmap (ZenMap - с графическим режимом)
  - Wireshark
  - Putty
  - whois
  - tranceroute
  - nslookup
- Произвести анализ сайта 80.250.180.133. Обнаружить все открытые порты и протоколы. Составить схему расположения данного ресурса. Установить DNS имена расположенных на указанном IP адресе серверов. ь
- Произвести подключение к серверу 62.76.32.162 по протоколу ssh (стандартный порт).
- Произвести перехват пакетов ssh протокола направляемых к данному серверу при помощи Wireshark. Внимание! Необходимо показать перехват пакетов при получение первого ключа шифрования SSH.
- Для обоих серверов указать номер автономной системы и её владельца.
- Подключиться к WiFi сети университета.
- Вычислить IP адрес шлюза выхода в Интернет.
- Определить протокол шифрования трафика.


## **Раздел 2. Криптографические методы защиты информации в компьютерных сетях**

### **Тема 5. Криптографические протоколы обеспечения безопасности**

#### **Лабораторная работа №2 (8 часов). Удалённый доступ по протоколу SSH.**

*Цель.* Изучение возможностей протокола SSH для получения удалённого доступа к серверу. возможностей протокола SSH для получения удалённого доступа к серверу  
*Задача №1.* Все задачи необходимо выполнить на BaseAlt (Альт Рабочая станция, Альт сервер), с использованием ОС MS Windows в качестве клиентской операционной системы.

- Установить систему openSSH сервер на ОС BaseAlt (Альт Рабочая станция, Альт сервер) и putty на ОС MS Windows.
- Создать ключ серверного шифрования информации.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

- Установить соединение с данным сервером с другого клиента, на котором запущен WireShark. Перехватить ключ серверного шифрования.
- Запретить передачу ключа по открытому каналу.
- Создать ключ клиента.
- Записать ключ клиента на отчуждаемый носитель информации.
- Установить соединение с другой ОС используя ключ клиента. Перехватить трафик и проанализировать полученные пакеты. Объяснить увиденный результат.
- Создать ключи шифрования на клиенте используя puttyGen. Переписать их на отчуждаемый носитель.
- Установить клиентские ключи шифрования для openSSH.
- Произвести соединение с сервером.

*Задача №2.* Все задачи необходимо выполнить на BaseAlt (Альт Рабочая станция, Альт сервер), с использованием ОС MS Windows в качестве клиентской операционной системы.

- Отключить клиентский компьютер на ОС MS Windows от сети Интернет.
- Настроить работы протокола SSH в режиме PORT FORWARDING.
- Создать «проброс» порта из внутренней защищенной сети через сервер до сайта [www.ulsu.ru](http://www.ulsu.ru) и протоколов HTTP и HTTPS.
- Перехватить отправленные пакеты с информацией и продемонстрировать использование шифрования информации.

## **Тема 6. Защита виртуальных частных сетей (VPN)**

### **Лабораторная работа №3 (8 часов). Использование VPN.**

*Цель.* Изучение возможностей программного обеспечения VPN для создания защищенных компьютерных сетей. Получение навыков работы со стандартным программным обеспечением для создания защищенных каналов связи.

*Задача №1.* Создание защищенного межсетевое взаимодействия сетей.


Изменить конфигурацию сети.

1. Скачать на локальный жесткий диск три образа операционных систем: MS Windows 10, MS Windows Server, BaseAlt (Альт Рабочая станция, Альт сервер).
2. Отключиться от общей сети лаборатории и включиться в один из маршрутизаторов MikroTik.
3. Назначить порты маршрутизатора следующим образом: Порты №1,2 – VLAN1; Порты 3,4 – VLAN2;
4. Подключить виртуальные машины клиентских ОС к VLAN1.
5. Подключить виртуальную машину с сервером к VLAN2.
6. Создать ключи доступа и файлы конфигураций для клиентских компьютеров.
7. Установить VPN клиент и применить файлы конфигурации.
8. Передать файл по протоколу SMB в защищенной сети.

*Задача №2.* Использование АПКШ «Континент» для создания защищенной сети.

Изменить конфигурацию сети.

1. Подключить порт 3 к VLAN9.
2. Получить ключи шифрования для АПКШ «Континент» Сервер Доступа.
3. Подключить АПКШ «Континент» к VLAN1.
4. Настроить АПКШ «Континент» Сервер доступа в соответствии с руководством администратора.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

5. Передать файл по протоколу SMB в защищенной сети.

### **Тема 7. Разработка защищенных сетевых приложений**

#### **Лабораторная работа №4 (8 часов). Работа с сертификатами SSL.**

*Цель.* Изучение возможностей центров сертификации (Certificate Authorities). Получение навыков работы с криптографическими ключами. Применение встроенных систем шифрования информации в стандартных приложениях операционных систем.

*Задача.* Для выполнения лабораторной работы используются ОС MS Windows и BaseAlt (Альт Рабочая станция, Альт сервер).

- Необходимо установить и настроить следующее программное обеспечение: OpenSSL
- Выдать сертификат SSL на свое имя: SN - должно содержать вашу ФИО. Также сертификат должен содержать ваш действующий EMAIL адрес.
- Скачать сертификат открытого ключа для Корейко Александра Ивановича.
- Установить сертификат в ОС и настроить электронную почту таким образом, чтобы отправляемые письма содержали вашу электронную подпись и были зашифрованы для получателя Корейко Александр Иванович.
- Установить локальный web сервер (apache, nginx).
- Выдать сертификат для локального веб сервера.
- Продемонстрировать работу по безопасному https соединению.
- Отчет по лабораторной работе должен содержать файл электронного письма в формате SMIME, а также файл сертификата.

### **Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях**

#### **Тема 8. Средства защиты локальных сетей при подключении к Интернет**


#### **Лабораторная работа №5 (8 часов). Моделирование виртуальной сети.**

*Цель.* Ознакомление с методами моделирования сетей. Знакомство с телекоммуникационным оборудованием компании CISCO. Решение практических задач.

*Задание.* Выполняется в программном обеспечении Cisco Packet Tracer

- Ваша фирма переезжает в новый бизнес-центр, где она арендовала 3 помещения, на 1-м, 2-м и 3-м этаже. У вас есть ограниченный набор оборудования:
- 3 коммутатора Cisco 2960
- Маршрутизатор Cisco 1941
- роутер Cisco WRT300N
- Вас попросили разработать схему сети со следующими требованиями:
- Любой компьютер компании может связываться с любым другим компьютером, но при этом, каждое помещение должно быть изолировано.
- На третьем этаже должна быть установлена WiFi точка доступа. Точка должна иметь пароль ulsu30years, должны выдаваться первые 20 адресов. SSID должен быть скрыт.
- На втором этаже установлен WEB сервер. Доступ к нему должны иметь все компьютеры по локальному имени "sharepoint".
- На первом этаже 3 рабочих места, на втором 2 рабочих места и сервер, третий 10 рабочих мест, в том числе 5 беспроводных.



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

- К сетевому оборудованию должен быть предоставлен безопасный доступ по SSH. Для доступа к оборудованию вас попросили создать административную виртуальную сеть "mi6".

### **Тема 9. Защита серверов и рабочих станций.**

#### **Лабораторная работа №6 (8 часов). Обнаружение вторжений.**

*Цель.* Изучение возможностей современного программного обеспечения для обнаружения вторжений. Управление правилами безопасности, анализ журналов событий.

*Задача.* Установка и настройка систем обнаружения вторжений в сети. Проведение атаки на защищенный сегмент сети. Для проведения атаки рекомендуется использовать специализированный дистрибутив ОС – Kali Linux.

- На ОС семейства BaseAlt (Альт Рабочая станция, Альт сервер) следует установить и настроить систему обнаружения вторжений Snort
- При помощи утилит предустановленных в дистрибутив Kali Linux произвести атаку на любой свой компьютер, подключенный к системе обнаружения вторжений Snort.
- Показать, как Snort обнаружил атаку на ваш ресурс.
- Создать правило, обнаруживающие ICMP атаки на ваш ресурс.
- Анализировать журнал событий и продемонстрировать обнаружение атаки.

### **Тема 9. Защита серверов и рабочих станций.**

#### **Лабораторная работа №7 (8 часов). АПКШ «Континент» Обнаружение вторжений**

*Цель.* Изучение возможностей комплекса АПКШ «Континент» для регистрации вторжений в локальную сеть.

*Задача.* Ознакомление с сертифицированными системами обнаружения вторжений в сети. Работа с правилами фильтрации и обнаружения атак.

Изменить конфигурацию сети.


1. Отключить рабочую станцию от локальной сети лаборатории и подключиться к маршрутизатору MikroTik.
2. Настроить порты маршрутизатора №1,2,3 в VLAN1.
3. Настроить порт маршрутизатора №4 в режим MIRRORING («зеркалирование»).
4. Подключить АПКШ «Континент» к порту №4.
5. Настроить АПКШ «Континент» Система обнаружения вторжений в режиме PROMISCUOUS\_MODE.
6. Произвести ICMP атаку в сети.
7. Продемонстрировать результаты работы правил на АПКШ «Континент».

## **8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ**

**8.1** Контрольные работы, курсовые работы и рефераты не предусмотрены учебным планом дисциплины.


## **9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ**

1. Стадии проведения сетевой атаки.
2. Классификация сетевых угроз, уязвимостей и атак.
3. Атаки на реализации сетевых протоколов, отдельные узлы и службы.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		


4. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
5. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.
6. Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP.
7. Методы сканирования портов.
8. Методы обнаружения пакетных сниферов. Методы обхода МЭ.
9. Имперсонация вслепую. Десинхронизация TCP-соединений.
10. Атаки, направленные на сетевую инфраструктуру.
11. Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании.
12. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации.
13. Технические меры защиты от сетевых атак.
14. Протоколы аутентификации на прикладном уровне.
15. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS.
16. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.
17. Назначение, основные возможности, принципы функционирования и варианты реализации VPN.
18. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN.
19. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и транспортном режимах.
20. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.
21. Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.
22. Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности.
23. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ.
24. Достоинства и недостатки МЭ. Построение правил фильтрации.
25. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений.
26. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.
27. Системы обнаружения вторжений (СОВ).
28. Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы.
29. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности.
30. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий.
31. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб.
32. Способы противодействия вторжениям.
33. Системы виртуальных ловушек (Honey Pot и Padded Cell).



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 8. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1	2	3	4
Раздел 1. Типовые угрозы сетевой безопасности Тема 1. Сетевые атаки	Подготовка к лекции, подготовка к сдаче экзамена	2	Тесты перед лекцией, экзамен
Раздел 1. Тема 2. Механизмы реализации атак в сетях TCP/IP	Подготовка к лекции, подготовка к сдаче экзамена	2	Тесты перед лекцией, экзамен
Раздел 1. Тема 3. Методы перехвата сетевых соединений в сетях TCP/IP	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	20	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Криптографические методы защиты информации в компьютерных сетях. Тема 5. Криптографические протоколы обеспечения безопасности	Подготовка к лекции, подготовка к сдаче экзамена	14	Тесты перед лекцией, экзамен
Раздел 2. Тема 6. Защита виртуальных частных сетей (VPN)	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	14	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 7. Разработка защищенных сетевых приложений	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	14	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях Тема 8. Средства защиты локальных сетей при подключении к Интернет	Подготовка к занятию, подготовка рефератов, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	16	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 3. Тема 9. Защита серверов и рабочих станций	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	40	Тесты перед лекцией, тесты на семинаре, экзамен

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Список рекомендуемой литературы:

#### основная

1. Запечников С.В., Основы построения виртуальных частных сетей [Электронный ресурс]: Учебное пособие для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И. - 2-е изд., стереотип. - М.: Горячая линия - Телеком, 2011. - 248 с. - ISBN 978-5-9912-0215-2 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991202152.html>

2. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991204705.html>

2. Бирюков А.А. Информационная безопасность: защита и нападение / Бирюков А. А. - Москва: ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: <https://www.studentlibrary.ru/book/ISBN9785970604359.html>

#### дополнительная

1. Запечников С.В., Основы построения виртуальных частных сетей [Электронный ресурс]: Учебное пособие для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И. - 2-е изд., стереотип. - М.: Горячая линия - Телеком, 2011. - 248 с. - ISBN 978-5-9912-0215-2 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991202152.html>

2. Некоммерческая интернет-версия СПС "КонсультантПлюс":

2.1 Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне». Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_2481/](http://www.consultant.ru/document/cons_doc_LAW_2481/)

2.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации»  
Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/)


2.3 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/](http://www.consultant.ru/document/cons_doc_LAW_208191/)

2.4 Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_112701/](http://www.consultant.ru/document/cons_doc_LAW_112701/)

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.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		


### учебно-методическая

1. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" [Электронный ресурс] : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий, Каф. информ. безопасности и теории управления. - Электрон. текстовые дан. (1 файл : 352 КБ). - Ульяновск : УлГУ, 2017 URL: [http://lib.ulsu.ru/MegaPro/Download/MObject/915/Andreev\\_2017.pdf](http://lib.ulsu.ru/MegaPro/Download/MObject/915/Andreev_2017.pdf)


2. Андреев А. С. 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" [Электронный ресурс] / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. - Электрон. текстовые дан. (1 файл : 14, 7 Мб). - Ульяновск : УлГУ, 2015. Режим доступа <http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf>

3. Клочков А. Е. Методические указания для самостоятельной работы студентов по дисциплине «Безопасность сетей ЭВМ» для студентов специалитета по специальности 10.05.03 очной формы обучения / А. Е. Клочков; УлГУ, ФМиИАТ. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 260 КБ). - Текст : электронный. <http://lib.ulsu.ru/MegaPro/Download/MObject/8740>

Согласовано:

Гл. библиотекарь НБ УлГУ / Полина Н.Ю. /  / 14.06.2019  
Должность сотрудника научной библиотеки      ФИО      подпись      дата



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

#### 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

Должность сотрудника УИиТ

/Клочкова А.В.

ФИО







Подпись

14.06.2019

дата



## ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/вы- пускающей 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

4.2 Объем дисциплины по видам учебной работы (в часах)

Вид учебной работы	Количество часов (форма обучения <u>дневная</u> )			
	Всего по плану	В т.ч. по семестрам		
		5	4	5
1	2	3	4	5
Контактная работа обучающихся с преподавателем	54	54/54*		
Аудиторные занятия:	54	54/54*		
Лекции	18	18/18*		
Практические и семинарские занятия	36	36/36*		
Лабораторные работы (лабораторный практикум)				
Самостоятельная работа	54	54		
Форма текущего контроля знаний и контроля самостоят. работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на семинарах; - рефераты на заданные темы		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	зачет	зачет		
Всего часов по дисциплине	108	108		

\*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.



### **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

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Список рекомендуемой литературы:

#### основная

1. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М.: Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991205252.html>.

2. Судариков С.А., Право интеллектуальной собственности: учебник [Электронный ресурс] / С.А. Судариков. - М.: Проспект, 2014. - 368 с. - ISBN 978-5-392-16752-4 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785392167524.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/](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/](http://www.consultant.ru/document/cons_doc_LAW_191669/)

1.3 Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне».

Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_2481/](http://www.consultant.ru/document/cons_doc_LAW_2481/)

1.4. 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/](http://www.consultant.ru/document/cons_doc_LAW_61798/)

1.5 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](http://www.consultant.ru/document/cons_doc_LAW_61801/)

1.6 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»

Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_48699/](http://www.consultant.ru/document/cons_doc_LAW_48699/)

1.7 Постановление Правительства РФ от 06.02.2010 N 63 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"

Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_97474/](http://www.consultant.ru/document/cons_doc_LAW_97474/)

1.8 Часть четвертая Гражданского кодекса Российской Федерации (231-ФЗ от 18.12.2006) Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_64629/](http://www.consultant.ru/document/cons_doc_LAW_64629/)

2. 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>

#### учебно-методическая

1. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск: УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). URL: <http://edu.ulsu.ru/courses/750/interface/>.

2. **Иванцов А. М.** Методические указания для самостоятельной работы студентов по дисциплине «Организационное и правовое обеспечение информационной безопасности» для студентов специалитета по специальностям 10.05.01 и 10.05.03 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 : 329 КБ). - Текст: электронный.

<http://lib.ulsu.ru/MegaPro/Download/MObject/4967>

Согласовано:

Гл. биб-рь ИБ УлГУ / Полиша И. В. / Б.И. / 14.06.2019  
Должность сотрудника научной библиотеки      ФИО      подпись      дата

## 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](http://window.edu.ru). Режим доступа: <http://window.edu.ru>

6.2. Федеральный портал [Российское образование](http://www.edu.ru). 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  
Должность сотрудника УИиТ

/Клочкова А.В.  
ФИО

  
подпись

14.06.2019  
дата

## ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/вы- пускающей кафедрой	Подпись	Дата
1.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 1	Андреев А.С.		12.05.2021 Протокол заседания кафедры № 12
1.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 2	Андреев А.С.		11.05.2022 Протокол заседания кафедры № 13
2.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 3	Андреев А.С.		12.04.2023 Протокол заседания кафедры № 12

**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. **Znaniium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2021]. - URL: <http://znaniium.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://ebco.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](http://www.edu.ru) : 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  
должность сотрудника УИТиТ

/ Ключкова А.В.  
ФИО

  
подпись

04.05.2021  
дата



**в) Профессиональные базы данных, информационно-справочные системы**

**1. Электронно-библиотечные системы:**

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2022]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2022]. - URL: <https://urait.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2022]. – URL: <https://www.studentlibrary.ru/cgi-bin/mb4x>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2022]. – URL: <https://www.rosmedlib.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2022]. – URL: <https://www.books-up.ru/ru/library/>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2022]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

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

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

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

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

**3. Базы данных периодических изданий:**

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

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

3.3. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД Гребенников. – Москва, [2022]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

**4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2022]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.**

**5. [SMART Imagebase](http://www.ebsco.com) : научно-информационная база данных EBSCO // EBSCOhost**

: [портал]. – URL: <https://ebSCO.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741>. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

**6. Федеральные информационно-образовательные порталы:**

6.1. [Единое окно доступа к образовательным ресурсам](http://window.edu.ru/) : федеральный портал . – URL: <http://window.edu.ru/> . – Текст : электронный.

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

**7. Образовательные ресурсы УлГУ:**

7.1. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

/ Клочкова А.В.  
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 электронная библиотека»** : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

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

**6. Электронная библиотечная система УлГУ** : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.