

УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий

от «16» 06 2020 г., протокол № 120
Председатель М.А. Волков
(подпись, расшифровка подписи)
«16» 06 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Программно-аппаратные средства обеспечения информационной безопасности
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

Специальность: 10.05.03 "Информационная безопасность автоматизированных систем"
(код специальности (направления), полное наименование)

Специализация: "Безопасность открытых информационных систем"
полное наименование

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

Дата введения в учебный процесс УлГУ: «01» 09 2020 г.

Программа актуализирована на заседании кафедры: протокол № 12 от 12.05.2021 г.

Программа актуализирована на заседании кафедры: протокол № 13 от 11.05.2022 г.

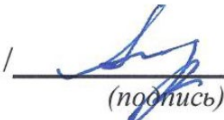
Программа актуализирована на заседании кафедры: протокол № 12 от 12.04.2023 г.

Сведения о разработчиках:


ФИО	Кафедра	Должность, ученая степень, звание
Иванцов Андрей Михайлович	ИБ и ТУ	Кандидат технических наук, доцент

СОГЛАСОВАНО

Заведующий выпускающей кафедрой
«Информационная безопасность и теория
управления»

/  / Андреев А.С. /
(подпись) (Ф.И.О.)

«10» 06 2020 г.

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

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Основной целью освоения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» является формирование у студентов знаний о спектре программно-аппаратных средств обеспечения информационной безопасности, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач по настройке, выбору и эксплуатации программно-аппаратных средств защиты информации.

Задачи освоения дисциплины:

Основные задачи дисциплины – дать знания:

- о методах и средствах защиты информации в компьютерных системах;
- о защитных механизмах, реализованных в средствах защиты информационных систем;
- о современных программно-аппаратных средствах защиты информации;
- о применении средств криптографической защиты информации и средств защиты информации от НСД для решения задач обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО


Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» изучается в 8 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 «Физика», «Электроника и схемотехника», «Безопасность операционных систем», «Основы информационной безопасности», «Техническая защита информации», «Системы и сети передачи информации», позволяющими понять физическую сущность возникновения технических каналов утечки информации, возможности современных средств технической разведки, методы и способы защиты от утечки по техническим каналам.

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

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


Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Безопасность сетей ЭВМ»; «Разработка и эксплуатация защищённых автоматизированных систем»; «Безопасность открытых информационных систем»; «Инструментальные средства контроля защищенности информации»; «Сертификация средств защиты информации».

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 - Способность корректно применять при решении профессиональных задач соответствующий математический аппарат, в том числе с использованием вычислительной техники	<p>Знать: математический аппарат, используемый для при решения профессиональных задач в том числе с использованием вычислительной техники</p> <p>Уметь: анализировать явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> <p>Владеть: соответствующим математическим аппаратом для решения профессиональных задач</p>
ОПК-3 - Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности	<p>Знать: основные языки, системы и инструментальные средства программирования, используемые в профессиональной деятельности</p> <p>Уметь: применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>Владеть: навыками применения языков, систем и инструментальных средств программирования для решения профессиональных задач</p>
ОПК-5 - Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	<p>Знать: основные методы научных исследований, используемых в профессиональной деятельности</p> <p>Уметь: применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами</p> <p>Владеть: навыками применения методов научных исследований в профессиональной деятельности</p>
ОПК-6 - Способность применять нормативные правовые акты в профессиональной деятельности	<p>Знать: основные нормативные правовые акты в профессиональной деятельности</p> <p>Уметь: применять нормативные правовые акты в профессиональной деятельности</p> <p>Владеть: навыками применения нормативных и правовых актов</p>

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

1	2
ОПК-7 - Способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	<p>Знать: основные приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций</p> <p>Уметь: применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций</p> <p>Владеть: навыками применения приемов оказания первой помощи, методов защиты производственного персонала и населения в условиях чрезвычайных ситуаций</p>
ОПК-8 - Способность к освоению новых образцов программных, технических средств и информационных технологий	<p>Знать: основные характеристики новых образцов технических средств и информационных технологий</p> <p>Уметь: осваивать новые образцы технических средств и информационных технологий</p> <p>Владеть: навыками освоения новых образцов технических средств и информационных технологий</p>
ПК-1 - Способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	<p>Знать: основные методы поиска, изучения, обобщения и систематизации научно-технической информации</p> <p>Уметь: осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке</p> <p>Владеть: навыками поиска, изучения, обобщения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке</p>
ПК-2 - Способность создавать и исследовать модели автоматизированных систем	<p>Знать: методы создания и исследования моделей автоматизированных систем</p> <p>Уметь: создавать и исследовать модели автоматизированных систем</p> <p>Владеть: навыками создания и исследования моделей автоматизированных систем</p>

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

1	2
ПК-3 - Способность проводить анализ защищенности автоматизированных систем	<p>Знать: основы анализа защищенности автоматизированных систем</p> <p>Уметь: проводить анализ защищенности автоматизированных систем</p> <p>Владеть: навыками проведения анализа защищенности автоматизированных систем</p>
ПК-4 - Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	<p>Знать: сущность модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>Уметь: разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>Владеть: навыками разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p>
ПК-19 - Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	<p>Знать: основные процессы и процедуры совершенствования системы управления информационной безопасностью автоматизированной системы</p> <p>Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем</p> <p>Владеть: навыками разработки предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем</p>
ПК-20 - Способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	<p>Знать: основные требования к информационной безопасности автоматизированных систем</p> <p>Уметь: организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности</p> <p>Владеть: навыками организации, разработки, внедрения, эксплуатации и сопровождения автоматизированной системы с учетом требований информационной безопасности</p>

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


1	2
ПК-25 - Способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	<p>Знать: основы эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы и восстановления их работоспособности при возникновении нештатных ситуаций</p> <p>Уметь: обеспечивать эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций</p> <p>Владеть: навыками обеспечения эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы и восстановления их работоспособности при возникновении нештатных ситуаций</p>
ПК-26 - Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	<p>Знать: основы инструментального мониторинга защищенности информации в автоматизированной системе; типовые каналы утечки информации в автоматизированной системе</p> <p>Уметь: проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации</p> <p>Владеть: навыками проведения инструментального мониторинга защищенности информации в автоматизированной системе; навыками выявления каналов утечки информации в автоматизированной системе</p>

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 <u>дневная</u>)			
	Всего по плану	В т.ч. по семестрам		
		8 семестр		
1	2	3	4	5
Контактная работа обучающихся с преподавателем	90	90/90		
Аудиторные занятия:	90	90/90		
Лекции	36	36/36		

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

1	2	3	4	5
Практические и семинарские занятия	36	36/36		
Лабораторные работы (лабораторный практикум)	18	18/18		
Самостоятельная работа	54	54		
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 - 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.

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					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практ. занятия, семинары	Лабораторные работы			
1	2	3	4	5	6	7	8
Раздел 1. Основные принципы и методы создания программно-аппаратных средств обеспечения информационной безопасности							
1. Предмет и задачи дисциплины «Программно-аппаратные средства информационной безопасности» (ПАСОИБ).	4	2				2	Тесты Т1, реферат 11
2. Анализ угроз информационной безопасности	4	2				2	Тесты Т2, реферат 12
3. Механизмы защиты. Политика безопасности в информационных системах	8	2	2			4	Тесты Т3, реф. 13, 14
4. Основные принципы в работе программно-аппаратных средств обеспечения информационной безопасности	6	2	2			2	Тесты Т4, реф. 13, 14
5. Типовая структура и основные функции программно-аппаратных средств обеспечения информационной безопасности	6	2	2			2	Тесты Т5, реферат 15
6. Методы разграничения доступа и управления доступом	4	2				2	Тесты Т6, реферат 16
7. Методы обеспечения идентификации и аутентификации	6	2	2			2	Тесты Т7, реферат 17
8. Методы и средства хранения ключевой информации	12	2	2	4	4	4	Тесты Т8, реферат 5
Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа							

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

1	2	3	4	5	6	7	8
9. Защита от незаконного копирования и использования программ	6	2	2			2	Тесты Т9, реферат 1
10. Защита от разрушающих программных воздействий и изучения кода программ	6	2	2			2	Тесты Т10, реф. 2, 7
11. Основные подходы к защите данных от НСД	6	2	2			2	Тесты Т11, реф. 18, 3
12. Определение факта доступа к файлам. Доступ к данным со стороны процесса	10	2	4			4	Тесты Т12, реферат 16
13. Особенности защиты данных от изменения	10	2	4			4	Тесты Т13, реферат 8
14. Основные средства криптографической защиты	16	2	2	6	6	6	Тесты Т14, реферат 19
15. ПАСОИБ в сетях передачи данных	22	2	4	8	8	8	Тесты Т15, реф. 4, 9
16. Управление безопасностью сети	6	2	2			2	Тесты Т16, реферат 10
17. Сертификация СЗИ	12	4	4			4	Тесты Т17, реферат 20
Итого:	144	36	36	18	18	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности

Тема 1. Предмет и задачи дисциплины «Программно-аппаратные средства информационной безопасности» (ПАСОИБ).

Основные понятия и определения в создании ПАСОИБ. Предмет и задачи дисциплины. Нормативно-правовая база создания и использования ПАСОИБ.

Тема 2. Анализ угроз информационной безопасности.


Понятие доступа, субъект и объект доступа. Классификация угроз информационной безопасности. Каналы утечки информации. Угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами. Модель нарушителя.

Тема 3. Механизмы защиты. Политика безопасности в компьютерных системах.

Требования к защищенности. Оценка защищенности Модели управления доступом. Функции ядра безопасности. Способы защиты конфиденциальности, целостности и доступности в КС. Классификация функциональных требований по защите информации. Требования к защищенности ИС на уровне защиты объектов, защиты линий, защиты БД, защиты подсистем управления. Политика безопасности.

Тема 4. Основные принципы в создании программно-аппаратных средств обеспечения информационной безопасности.

Классификация ПАСОИБ. Функциональные возможности ПАСОИБ. Принципы разработки ПАСОИБ. Концепция диспетчера доступа. Функционирование диспетчера доступа при управлении доступом к защищаемым ресурсам. Порядок проектирования

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

ПАСОИБ. Модель системы защиты информации (СЗИ).

Тема 5. Типовая структура и основные программно–аппаратных средств обеспечения информационной безопасности

Структура ПАСОИБ. Компоненты и подсистемы. Типовые функции ПАСОИБ. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСОИБ. Перспективы развития ПАСОИБ. Принципы действия и технологические особенности ПАСОИБ, реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем.

Тема 6. Методы разграничения доступа и управления доступом

Методы ограничения доступа и управления доступом. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Идентификация и аутентификация. Парольные системы. Дискреционное управление доступом. Мандатное управление доступом. Ролевое управление доступом.

Тема 7. Методы обеспечения идентификации и аутентификации

Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами. Симметричные методы аутентификации. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Авторизация. Контроль и управление доступом средствами операционной системы и программно-аппаратными техническими средствами.

Тема 8. Методы и средства хранения ключевой информации

Информация, используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи. Классификация средств хранения ключей и идентифицирующей информации. Организация хранения ключей. Магнитные диски прямого доступа. Средство TouchMemory. Типовые решения в организации ключевых систем. Открытое распределение ключей. Метод управляемых векторов. Персональные средства аутентификации и защищенного хранения данных.

Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа

Тема 9. Защита от незаконного копирования и использования программ.


Классификация аппаратных и программных компонентов защиты программ. Структура ПО. Способы встраивания средств защиты в ПО. Способы определения факта незаконного копирования и использования программ. Способы защиты от незаконного копирования и использования программ. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.

Тема 10. Защита от разрушающих программных воздействий и изучения кода программ.

Способы изучения кода программ. Обратное проектирование ПО. Способы защиты программ от изучения кода. Основные принципы обеспечения безопасности программ. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.

Тема 11. Основные подходы к защите данных от НСД.

Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам в различных ОС. Защита сетевого файлового ресурса. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Характеристики программно-аппаратных

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

средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ

Тема 12. Определение факта доступа к файлам. Доступ к данным со стороны процесса.

Способы определения факта доступа. Журналы доступа. Критерии информативности журналов доступа. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа. Понятие электронного замка. Принципы построения и функционирования электронных замков. Механизмы контроля аппаратной конфигурации ПЭВМ.

Тема 13. Особенности защиты данных от изменения.

Защита массивов информации от изменения. Имитозащита. Криптографическая постановка защиты от изменения данных. Подходы к решению задачи защиты данных от изменения. Подход на основе формирования имитоприставки. Подход на основе формирования хэш-функции, требования к построению и способы реализации. Формирование электронной подписи (ЭП). Особенности защиты документов и исполняемых файлов. Проблема самоконтроля исполняемых модулей. Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаления программ и файлов.

Тема 14. Методы криптографической защиты.

Классификация методов криптографического преобразования. Нормативно-правовая база. Требования к программно-аппаратным комплексам шифрования. Необходимые и достаточные функции аппаратного средства криптозащиты. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.

Тема 15. ПАСОИБ в сетях передачи данных.

Классификация программно-аппаратных средств защиты информации в сетях передачи данных. Принципы построения и функционирования межсетевых экранов в сетях передачи данных. Программно-аппаратные средства межсетевого экранирования. Основные принципы защиты информации при передаче по каналам связи. Программно-аппаратные средства защиты информации при передаче по каналам связи. Основные принципы обнаружения сетевых атак. Основные принципы защиты от сетевых атак. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак.

Тема 16. Управление безопасностью сети.

Основные принципы управления безопасностью сети. Программно-аппаратные средства управления безопасностью сети. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи


Тема 17. Сертификация СЗИ.

Система сертификации СЗИ. Задачи сертификации ПАСОИБ на соответствие требованиям информационной безопасности. Нормативно-правовая база сертификации ПАСОИБ на соответствие требованиям информационной безопасности. Технология сертификации ПАСОИБ на соответствие требованиям информационной безопасности.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

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

Раздел 1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности

Тема 3. Механизмы защиты. Политика безопасности в компьютерных системах (семинар).

1. Модели управления доступом.
2. Способы защиты конфиденциальности, целостности и доступности в КС.
3. Требования к защищенности ИС на уровне защиты объектов, защиты линий, защиты БД, защиты подсистем управления.
4. Политика безопасности.

Тема 4. Основные принципы в создании в создании программно-аппаратных средств обеспечения информационной безопасности (семинар).

1. Принципы разработки ПАСОИБ.
2. Функционирование диспетчера доступа при управлении доступом к защищаемым ресурсам.
3. Проектирование ПАСОИБ.
4. Модель системы защиты информации (СЗИ).

Тема 5. Типовая структура и основные функции программно-аппаратных средств обеспечения информационной безопасности (семинар).

1. Структура ПАСОИБ. Компоненты и подсистемы.
2. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСОИБ.
3. Принципы действия и технологические особенности ПАСОИБ, реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем.

Тема 7. Методы обеспечения идентификации и аутентификации (семинар).

1. Локальная и удаленная идентификация.
2. Способы хранения идентифицирующей информации.
3. Связь с ключевыми системами.
4. Контроль и управление доступом средствами операционной системы и программно-аппаратными техническими средствами.

Тема 8. Методы и средства хранения ключевой информации (семинар).

1. Информация, используемая для контроля доступа: ключи и пароли.
2. Злоумышленник и ключи.
3. Организация хранения ключей.
4. Персональные средства аутентификации и защищенного хранения данных.

Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа

Тема 9. Защита незаконного копирования и использования программ (семинар).


1. Способы встраивания средств защиты в ПО.
2. Способы определения факта незаконного копирования и использования программ.
3. Способы защиты от незаконного копирования и использования программ.

Тема 10. Защита от разрушающих программных воздействий и изучения кода программ (семинар).

1. Способы изучения кода программ. Обратное проектирование ПО.
2. Способы защиты программ от изучения кода.
3. Защита от разрушающих программных воздействий.

Тема 11. Основные подходы к защите данных от НСД (семинар).

1. Оценка надежности систем ограничения доступа – сведение к задаче оценки

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

стойкости.

2. Организация доступа к файлам в различных ОС.
3. Защита сетевого файлового ресурса.

Тема 12. Определение факта доступа к файлам. Доступ к данным со стороны процесса (семинар).

1. Способы определения факта доступа. Журналы доступа.
2. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
3. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя.
4. Принципы построения и функционирования электронных замков.
5. Механизмы контроля аппаратной конфигурации ПЭВМ.

Тема 13. Особенности защиты данных от изменения (семинар).

1. Подходы к решению задачи защиты данных от изменения.
2. Подход на основе формирования имитоприставки (МАС), способы построения МАС.
3. Подход на основе формирования хэш-функции, требования к построению и способы реализации. Формирование электронной подписи (ЭЦП).
4. Особенности защиты документов и исполняемых файлов.
5. Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаления программ и файлов.

Тема 14. Методы криптографической защиты (семинар).

1. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования.
2. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.

Тема 15. ПАСОИБ в сетях передачи данных. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак (семинар).

1. Принципы построения и функционирования межсетевых экранов в сетях передачи данных.
2. Основные принципы защиты информации при передаче по каналам связи.
3. Программно-аппаратные средства защиты информации при передаче по каналам связи.
4. Основные принципы обнаружения сетевых атак.
5. Основные принципы защиты от сетевых атак.

Тема 16. Управление безопасностью сети (семинар).


1. Основные принципы управления безопасностью сети.
2. Программно-аппаратные средства управления безопасностью сети.
3. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи

Тема 17. Сертификация СЗИ.

1. Система сертификации СЗИ.
2. Технология сертификации ПАСОИБ на соответствие требованиям информационной безопасности.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности

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

Тема 8. Методы и средства хранения ключевой информации

Лабораторная работа № 2 (4 часа). «Настройка усиленной аутентификации с использованием СЗИ от НСД Dallas Lock на базе eToken».

Цель работы: Настройка и использование «eToken» для аутентификации и получение практических навыков работы с персональным средством аутентификации и защищенного хранения данных».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с персональным средством аутентификации и защищенного хранения данных».

Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа

Тема 12. Определение факта доступа к файлам. Доступ к данным со стороны процесса.

Лабораторная работа № 2 (6 часа). «Использование электронного замка ПАК Соболев».

Цель работы: Использование «ПАК Соболев» для контроля аппаратной конфигурации ПЭВМ, получение практических навыков работы с электронным замком».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с электронным замком».

Тема 13. Особенности защиты данных от изменения.

Лабораторная работа № 3 (6 часа). «Использование СЗИ Dallas Lock».

Цель работы: Использование СЗИ «Dallas Lock» для защиты от несанкционированного изменения, установки или удаления программ и файлов, получение практических навыков работы с СЗИ от НСД».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с СЗИ от НСД».

Лабораторная работа № 4 (6 часа). «Использование СЗИ от НСД Secret Disk».

Цель работы: Использование СЗИ «Secret Net» для защиты от несанкционированного изменения, установки или удаления программ и файлов, получение практических навыков работы с СЗИ от НСД».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с СЗИ от НСД».

Тема 14. Методы криптографической защиты.

Лабораторная работа № 5 (4 часа). «Использование персонального средства криптографической защиты информации ШИПКА».

Цель работы: Получение практических навыков работы со средством криптографической защиты информации».


Методические указания: основное внимание должно быть уделено практическим навыкам работы с электронным замком».

Тема 15. ПАСОИБ в сетях передачи данных. Межсетевые экраны. Средства экранирования. Обнаружение сетевых атак.

Лабораторная работа № 6 (8 часа). «Использование программно-аппаратных комплексов VipNet».

Цель работы: Организация меж сетевого взаимодействия защищенных сетей ViPNet. Получение практических навыков работы со средством криптографической защиты информации».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с электронным замком».

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

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Контрольные работы не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика рефератов:


1. Защита от незаконного копирования программ
2. Защита от незаконного использования программ
3. Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
4. Программно-аппаратные средства защиты информации в сетях передачи данных
5. Методы и средства хранения ключевой информации
6. Защита от разрушающих программных воздействий.
7. Защита от изучения кода программ.
8. Защита данных от изменения.
9. Способы и средства обнаружения сетевых атак.
10. Программно-аппаратные средства управления безопасностью сети.
11. Классификация программно-аппаратных средств обеспечения информационной безопасности
12. Классификация угроз информационной безопасности
13. Основные принципы и механизмы защиты информации
14. Политики безопасности в информационных системах
15. Типовая структура и основные функции программно-аппаратных средств обеспечения информационной безопасности
16. Основные методы разграничения доступа и управления доступом
17. Основные методы обеспечения идентификации и аутентификации
18. Основные подходы к защите данных от НСД
19. Методы и средства криптографической защиты
20. Сертификация средств защиты информации

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. Рацевев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

8.3 Примерная тематика курсовых работ:

1. Разработка подсистемы аутентификации мобильного (веб-приложения) предприятия.
2. Сравнительный анализ методов, используемых в типовых системах контроля и управления доступом (СКУД) предприятий.
3. Анализ акустических каналов утечки информации.
4. Анализ эффективности использования физических средств защиты.
5. Принципы обнаружения и локализации радиозакладок.
6. Сравнительный анализ характеристик средств обнаружения радиозакладок.
7. Разработка диспетчера доступа для реляционных СУБД.
8. Реализация защиты информации от утечки через ПЭМИН.
9. Предотвращение утечки информации по цепям электропитания и заземления.
10. Способы увеличения дальности скрытного наблюдения в оптическом видимом и инфракрасном диапазонах.


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

8.3.1 Правила оформления курсовых работ

Требования к курсовым работам для студентов отражены 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. Основные понятия и определения в создании программно-аппаратных средств обеспечения информационной безопасности (ПАСОИБ). Нормативно-правовая база создания ПАСОИБ.
2. Понятие доступа, субъект и объект доступа. Классификация угроз безопасности. Каналы утечки информации. Угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами.
3. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности.
4. Модели управления доступом. Функции ядра безопасности. Способы защиты конфиденциальности, целостности и доступности в КС.
5. Классификация функциональных требований по защите информации. Требования к защищенности ИС на уровне защиты объектов, защиты линий, защиты БД, защиты подсистем управления. Политика безопасности.
6. Классификация ПАСОИБ. Функциональные возможности ПАСОИБ. Принципы разработки ПАСОИБ. Порядок проектирования ПАСОИБ.
7. Концепция диспетчера доступа. Функционирование диспетчера доступа при управлении доступом к защищаемым ресурсам.
8. Структура ПАСОИБ. Компоненты и подсистемы. Типовые функции ПАСОИБ. Обязательные требования по обеспечению ИБ, предъявляемые к ПАСОИБ.
9. Принципы действия и технологические особенности ПАСОИБ, реализующих отдельные функциональные требования по защите информации и данных, их взаимодействие с общесистемными компонентами вычислительных систем.
10. Методы ограничения доступа и управления доступом. Идентификация и аутентификация. Парольные системы. Управление доступом.
11. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами.
12. Классификация средств хранения ключей и идентифицирующей информации. Организация хранения ключей. Типовые решения в организации ключевых систем.
13. Способы изучения кода программ. Обратное проектирование ПО. Способы защиты программ от изучения кода. Основные принципы обеспечения безопасности программ.
14. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.
15. Классификация программно-аппаратных средств защиты от несанкционирован-

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


ного доступа к информации, хранимой в ПЭВМ. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ

16. Способы определения факта доступа. Журналы доступа. Критерии информативности журналов доступа. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
17. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
18. Понятие электронного замка. Принципы построения и функционирования электронных замков. Механизмы контроля аппаратной конфигурации ПЭВМ.
19. Подходы к решению задачи защиты данных от изменения. Особенности защиты документов и исполняемых файлов.
20. Классификация методов криптографического преобразования. Нормативно-правовая база. Требования к программно-аппаратным комплексам шифрования. Необходимые и достаточные функции аппаратного средства криптозащиты.
21. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носители алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.
22. Классификация программно-аппаратных средств защиты информации в сетях передачи данных. Принципы построения и функционирования межсетевых экранов в сетях передачи данных. Программно-аппаратные средства межсетевого экранирования.
23. Основные принципы защиты информации при передаче по каналам связи. Программно-аппаратные средства защиты информации при передаче по каналам связи. Основные принципы обнаружения сетевых атак. Основные принципы защиты от сетевых атак.
24. Основные принципы управления безопасностью сети. Программно-аппаратные средства управления безопасностью сети. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи
25. Основные принципы сертификации СЗИ.
26. Назначение, возможности и использование системы защиты от НСД «Secret Disk».
27. Назначение, возможности и порядок работы с персональными средствами аутентификации и защищённого хранения данных (USB-ключи и смарт-карты eToken).
28. Назначение, возможности и порядок работы с персональным средством криптографической защиты информации «ШИПКА».
29. Назначение, возможности и порядок работы с Электронным замком "Соболь".
30. Назначение, возможности и порядок работы с СЗИ «Dallas Lock».
31. Назначение, возможности и порядок работы с программно-аппаратным комплексом VipNet».
32. Состав и основные функции программно-аппаратного комплекса VipNet».


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

9. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1	2	3	4
Раздел 1. Основные принципы и методы создания программно-аппаратных средств обеспечения информационной безопасности. Тема 1. Предмет и задачи дисциплины «Программно-аппаратные средства информационной безопасности» (ПАСОИБ)	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, экзамен
Раздел 1. Тема 2. Анализ угроз информационной безопасности	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, экзамен
Раздел 1. Тема 3. Механизмы защиты. Политика безопасности в компьютерных системах	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 4. Основные принципы в работе ПАСОИБ	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 5. Типовая структура и основные функции ПАСОИБ	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, экзамен
Раздел 1. Тема 6. Методы разграничения доступа и управления доступом	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 7. Методы обеспечения идентификации и аутентификации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 1. Тема 8. Методы и средства хранения ключевой информации	Подготовка к занятию, подготовка рефератов, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен

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

1	2	3	4
Раздел 2. Программно-аппаратные средства защиты информации от несанкционированного доступа. Тема 9. Защита от незаконного копирования и использования программ	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 10. Защита от разрушающих программных воздействий и изучения кода программ	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 11. Основные подходы к защите данных от НСД	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 12. Определение факта доступа к файлам. Доступ к данным со стороны процесса	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 2. Тема 13. Особенности защиты данных от изменения	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	4	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 2. Тема 14. Основные средства криптографической защиты	Подготовка к занятию, подготовка рефератов, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	6	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 2. Тема 15. ПАСОИБ в сетях передачи данных.	Подготовка к занятию, подготовка рефератов, подготовка к семинару, лабораторным работам, подготовка к сдаче экзамена	8	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, экзамен
Раздел 2. Тема 16. Управление безопасностью сети	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты на семинаре, экзамен
Раздел 2. Тема 17. Сертификация СЗИ	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	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. 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. Свиначев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: учеб. пособие / Свиначев 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. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. - 586 с. - ISBN 978-5-9912-0424-8 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991204248.html>

дополнительная

1. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс] / Бузов Г.А. - М.: Горячая линия - Телеком, 2010. - 240 с. - ISBN 978-5-9912-0121-6 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991201216.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/

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/

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/


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/

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: <http://gostexpert.ru/gost/gost-27002-2012>

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


2. Андреев А. С. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", "Математическое обеспечение и администрирование информационных систем",

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

"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. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» для студентов специалитета по специальности 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2020. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 356 КБ). - Текст : электронный. <http://lib.ulsu.ru/MegaPro/Download/MObject/7919>

Согласовано:

Гл. библиотекарь НБ УлГУ / Полина Н.Ю. /  / 05.06.2020
Должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2020]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2020]. - URL: <https://www.biblio-online.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2020]. – URL: http://www.studentlibrary.ru/catalogue/switch_kit/x2019-128.html. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2020]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Znanium.com : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2020]. - URL: <http://znanium.com>. – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.


1.6. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: <http://web.a.ebscohost.com/ehost/search/advanced?vid=1&sid=e3ddfb99-a1a7-46dd-a6eb-2185f3e0876a%40sessionmgr4008>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва: КонсультантПлюс, [2020].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2020]. – 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, [2020]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст: электронный

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

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2020]. – 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, [2020]. – 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** : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://www.edu.ru>. – Текст : электронный.


7. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2020]. - Режим доступа: <https://dvs.rsl.ru>.

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

9. Образовательные ресурсы УлГУ:

9.1. 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.

9.2. Образовательный портал УлГУ. – URL: <http://edu.ulsu.ru>. – Режим доступа : для зарегистр. пользователей. – Текст : электронный.

Согласовано:
Зам. нач. УИиТ /Клочкова А.В. /  05.06.2020
Должность сотрудника УИиТ ФИО подпись дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:




Аудитории для проведения лекций , семинарских, лабораторных занятий: 3/317, 2/246.

Аудитория 2/246 укомплектована специализированной мебелью, учебной доской, имеются мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

Используемые технические средства:

- система защиты конфиденциальной информации и персональных данных «Secret Disk;
- электронный замок "Соболь";
- персональные средства аутентификации и защищённого хранения данных - USB-ключи и смарт-карты eToken;
- система защиты от НСД «Dallas Lock»;
- персональное средство криптографической защиты информации «ШИПКА»;
- программно-аппаратный комплекс VipNet».

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
2.	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
3.	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

Приложение 1

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2021]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

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

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

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

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

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

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

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

1.9. Русский язык как иностранный : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2021]. – URL: <https://ros-edu.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2021].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2021]. – URL: <https://dlib.eastview.com/browse/udb/12>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2021]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

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

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

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

6. Федеральные информационно-образовательные порталы:

6.1. **Единое окно доступа к образовательным ресурсам** : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://window.edu.ru/>. – Текст : электронный.

6.2. [Российское образование](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

/ Клочкова 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 : 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.