УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» 06 2019 г., протокол № 5/19
Председатель _____ М.А. Волков
(подпись, расшифровка подписи)
«24» 06 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Основы информационной безопасности
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	3

Специальность: 10.05.01 "Компьютерная безопасность"
код направления (специальности), полное наименование

Специализация: "Математические методы защиты информации"
полное наименование

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

Дата введения в учебный процесс УлГУ: «01» 09 2019 г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.

Сведения о разработчиках:

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

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
_____ / Андреев А.С. / (подпись) (Ф.И.О.) «15» 06 2019 г.	_____ / Андреев А.С. / (подпись) (Ф.И.О.) «15» 06 2019 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина имеет целью:

обучить студентов принципам обеспечения информационной безопасности, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем;

содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Названная дисциплина является базовой для изучения других дисциплин специальности «Компьютерная безопасность», а также будет использована при выполнении курсовых и дипломных работ.

Задачи освоения дисциплины: дать основы: методологии создания систем защиты информации; методов, средств и приемов ведения информационных войн; обеспечения информационной безопасности компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Основы информационной безопасности» изучается в 5 семестре и относится к числу базовой части дисциплин блока Б1, предназначенного для студентов, обучающихся по специальности 10.05.01 – «Компьютерная безопасность».

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Информатика»; «Гуманитарные аспекты информационной безопасности», «Теория информации», «Организационное и правовое обеспечение информационной безопасности».

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

знание базовых понятий в области информатики и теории информации;

способность использовать нормативные правовые документы;

способность анализировать социально-значимые 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: «Компьютерные сети»; «Модели безопасности компьютерных систем»; «Защита в операционных системах»; «Основы построения защищенных компьютерных сетей»; «Защита программ и данных»; «Техническая защита информации»; «Криптографические методы защиты информации»; «Криптографические протоколы».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
1	2
ОК-5 - способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	**Знать:** Роль и место информационной безопасности в системе национальной безопасности страны; содержание информационной войны, методы и средства её ведения **Уметь:** Пользоваться современной научно-технической информацией по исследуемым проблемам и задачам **Владеть:** Профессиональной терминологией в области информационной безопасности
ОПК-7 - способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	**Знать:** Сущность и понятие информации, информационной безопасности и характеристику ее составляющих **Уметь:** Анализировать и оценивать угрозы информационной безопасности объекта **Владеть:** Навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; навыками применения типовых технических средств защиты информации
ПК-13 - способность организовывать работу малых коллективов исполнителей, на-ходить и принимать управленческие ре-шения в сфере профессиональной деятельности	**Знать:** Методы и технологии управления в сфере профессиональной деятельности **Уметь:** Принимать управленческие решения и оценивать их эффективность **Владеть:** Навыками выбора, обо-снования, реализации и контроля результатов управленческого решения

1	2
ПК-15 - способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	**Знать:** Основные средства и методы обеспечения информационной безопасности **Уметь:** Анализировать и оценивать угрозы информационной безопасности компьютерных систем **Владеть:** Навыками формулирования предложений и рекомендаций по совершенствованию системы управления ИБ компьютерной системы
ПК-16 - разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем	**Знать:** Основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности **Уметь:** Применять действующую законодательную базу в области обеспечения ИБ при разработке проектов нормативных, правовых и методических материалов, регламентирующих работу по обеспечению ИБ предприятия **Владеть:** Навыками работы с нормативными правовыми актами по обеспечению ИБ компьютерных систем

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3.

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

Вид учебной работы	Количество часов (форма обучения дневная)			
	Всего по плану	В т.ч. по семестрам		
		5		
Контактная работа обучающихся с преподавателем	54	54/54		
Аудиторные занятия:	54	54/54		
Лекции	36	36/36		
Практические и сем. занятия				
Лабораторные работы (лаб. 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 лаб. работ - рефераты на заданные темы		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	Зачет	Зачет		
Всего часов по дисциплине:	108	108		

В случае необходимости использования в учебном процессе частично/исключительно

дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

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

Форма обучения _____дневная_____

Название разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практ. занятия, семинары	Лабораторные работы			
1	2	3	4	5	6	7	8
Раздел 1. Информационная безопасность в системе национальной безопасности РФ							
1. Понятие национальной безопасности.	4	2				2	Тесты Т1, реф. 1, 3, 8
2. Национальные интересы России в инф. сфере.	4	2				2	Тесты Т2, реф. 2, 9
3. Угрозы информационной безопасности РФ.	12	2		6	6	4	Тесты Т3, реф. 4, 5; лаб. раб. 1
4. Источники угроз информационной безопасности РФ.	4	2				2	Тесты Т4, реф. 7,10
Раздел 2. Информационная война, методы и средства ее ведения							
5. Информационная безопасность и инф. противоборство	4	2				2	Тесты Т5, реф. № 11
6. Приемы информационного воздействия в инф. войне.	4	2				2	Тесты Т6, реф. № 6
7. Типовая стратегия информационной войны.	4	2				2	Тесты Т7, реф. № 12
Раздел 3. Защита от несанкционированного доступа (НСД) в информационных системах							
8. Классификация автоматизированных систем и требования по защите информации.	4	2				2	Тесты Т8, реф. № 13
9. Структура системы защиты информации от НСД. Назначение и функции элементов.	4	2				2	Тесты Т9, реф. № 14
10. Модели управления доступом.	6	2				4	Тесты Т10, реф. 15

1	2	3	4	5	6	7	8
Раздел 4. Основные методы обеспечения информационной безопасности							
11. Основные понятия криптографической защиты информации.	4	2				2	Тесты Т11, реф. № 16
12. Симметричные криптографические системы.	4	2				2	Тесты Т12, реф. № 17
13. Асимметричные криптографические системы.	4	2				2	Тесты Т13, реф. № 18
14. Идентификация и аутентификация.	4	2				2	Тесты Т14, реф. № 19
15. Разграничение и контроль доступа к информации.	4	2				2	Тесты Т15, реф. № 20
16. Технологии межсетевых экранов.	6	2				4	Тесты Т16, реф. № 21
17. Виртуальные частные сети (VPN).	4	2				2	Тесты Т17, реф. № 22
18. Методы обнаружения вторжений (атак).	6	2				4	Тесты Т18, реф. № 23
Раздел 5. Средства защиты информации от несанкционированного доступа							
19 Перс. средства аутентификации данных - USB-ключи и смарт-карты eToken.	4			2	2	2	лаб. раб. 2
20. Система защиты от НСД «Dallas Lock».	6			4	4	2	лаб. раб. 3
21. Электронный замок "Соболь".	4			2	2	2	лаб. раб. 4
22. Система защиты конф. информации и персональных данных «Secret Disk».	4			2	2	2	лаб. раб. 5
23 Программно - аппаратный комплекс средств защиты информации от НСД “Аккорд»	4			2	2	2	лаб. раб. 6
Итого:	108	36		18	18	54	

5. СОДЕРЖАНИЕ КУРСА

Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации

Тема 1. Понятие национальной безопасности.

Сущность и содержание национальной безопасности. Основные задачи в области обеспечения национальной безопасности. Объект и субъект безопасности. Виды безопасности: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.

Тема 2. Национальные интересы России в информационной сфере.

Место и роль России в глобальном информационном пространстве. Национальные интересы России в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

Тема 3. Виды угроз информационной безопасности Российской Федерации.

Проблемы обеспечения информационной безопасности. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в её продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Классификация угроз безопасности информационных и телекоммуникационных средств и систем. Модель действий нарушителя.

Тема 4. Источники угроз информационной безопасности РФ.

Внешние источники угроз. Внутренние источники угроз. Классификация источников угроз и уязвимостей информационной безопасности.

Раздел 2. Информационная война, методы и средства её ведения

Тема 5. Информационная безопасность и информационное противоборство.

Понятие информационной войны (ИВ). Проблемы ИВ. Субъекты информационного противоборства (ИП). Цель ИП. Составные части и методы ИП.

Тема 6. Приемы информационного воздействия в ИВ. ИВ как целенаправленное информационное воздействие информационных систем. Способы перепрограммирования информационных систем. Проблема начала информационной войны.

Тема 7. Типовая стратегия информационной войны.

Обобщенный алгоритм информационной войны. Основные аспекты информационной войны. Последствия информационной войны.

Раздел 3. Защита от несанкционированного доступа (НСД) к информации

Тема 8. Классификация автоматизированных систем и требования по защите информации.

Документы Гостехкомиссии при Президенте РФ. Концепции защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности. Требования к информационным системам по обеспечению безопасности информации.

Тема 9. Структура системы защиты информации от НСД. Назначение и функции элементов.

Направления защиты от НСД. Основные способы НСД. Принципы защиты информации от НСД. Структура системы защиты информации от НСД, назначение и функции элементов.

Тема 10. Модели управления доступом.

Правила разграничения доступа. Мандатная и дискреционная модели управления доступом. Ролевая и атрибутные модели.

Раздел 4. Основные методы обеспечения информационной безопасности

Тема 11. Основные понятия криптографической защиты информации.

В данной лекции определяются предмет и задачи криптографии, формулируются основополагающие определения и требования к криптографическим системам защиты информации, дается историческая справка об основных этапах развития криптографии как науки. Рассматривается пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы.

Тема 12. Симметричные криптографические системы.

Обобщенная схема симметричной криптосистемы. Алгоритм шифрования DES. Стандарт шифрования ГОСТ Р34.12-2015. Особенности применения алгоритмов симметричного шифрования.

Тема 13. Асимметричные криптографические системы.

Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом. Функция хэширования. Электронная подпись.

Тема 14. Идентификация и аутентификация.

Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Пароли, сертификаты и электронные подписи. Методы аутентификации.

Тема 15. Разграничение и контроль доступа к информации.

Разграничение доступа по виду, характеру, назначению, степени важности и секретности информации; по способам ее обработки: считать, записать, внести изменения, выполнить команду; по условному номеру терминала; по времени обработки и др. Разделение привилегий на доступ к инф.

Тема 16. Технологии межсетевых экранов.

Технология межсетевых экранов (МЭ) - одна из самых первых технологий защиты корпоративных сетей от внешних угроз. Показано, что МЭ способствует реализации политики безопасности, определяет разрешенные службы, типы доступа к ним и является реализацией этой политики в терминах сетевой конфигурации, хостов, маршрутизаторов и других мер защиты. Функции МЭ

Тема 17. Виртуальные частные сети.

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

Тема 18. Методы обнаружения вторжений (атак).

Краткая история вторжений (атак) на интрасети. Основные понятия. Классификация систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений.

Раздел 5. Средства защиты информации от несанкционированного доступа

Тема 19. Персональные средства аутентификации и защищённого хранения данных - USB-ключи и смарт-карты eToken.

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

Тема 20. Система защиты от НСД «Dallas Lock». Назначение, возможности, установка и порядок работы с системой защиты от НСД.

Тема 21. Электронный замок "Соболь".

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

Тема 22. Система защиты конф. информации и персональных данных «Secret Disk».

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

Тема 23. Программно-аппаратный комплекс (ПАК) средств защиты информации от НСД “Аккорд–АМДЗ”.

Назначение, возможности, установка и использование ПАК средств защиты информации от НСД “Аккорд–АМДЗ”.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом дисциплины.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации

Тема 3. Виды угроз информационной безопасности Российской Федерации.

Лабораторная работа № 1. (6 часов). «Выработка концептуальных основ деятельности по обеспечению информационной безопасности предприятия».

Цель: Анализ информационных активов, используемых компанией и выработка концептуальных основ деятельности по обеспечению корпоративной инф. безопасности. Результат: отчет.

Методические указания: основное внимание должно быть уделено практическому выявлению угроз и базовых уязвимостей конкретных информационных активов предприятия, а также выбору методов и средств противодействия имеющимся угрозам информационной безопасности.

Раздел 5. Средства защиты информации от несанкционированного доступа

Тема 19. Персональные средства аутентификации и защищенного хранения данных - USB-ключи и смарт-карты eToken.

Лабораторная работа № 2. (2 часа). Назначение, возможности и порядок работы с персональными средствами аутентификации и защищённого хранения данных (USB-ключи и смарт-карты eToken).

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

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

Тема 20. Система защиты от НСД «Dallas Lock».

Лабораторная работа № 3. (4 часа). Назначение и возможности системы защиты от НСД **«Dallas Lock».**

Цель: Изучить возможности и научиться работать с системой защиты. Результат: отчет.

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

Тема 21. Электронный замок "Соболь".

Лабораторная работа № 4. (2 часа). Назначение, возможности и порядок работы с Электронным замком "Соболь".

Цель: Изучить возможности и научиться работать с электронным замком "Соболь". Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке, установке и практическому освоению возможностей электронного замка "Соболь".

Тема 22. Система защиты конфиденциальной информации и персональных данных «Secret Disk».

Лабораторная работа № 5. (2 часа). Назначение и возможности системы защиты конфиденциальной информации и персональных данных «Secret Disk».

Цель: Изучить возможности и научиться работать с системой защиты конфиденциальной информации и персональных данных. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей «Secret Disk».

Тема 23. Программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ”.

Лабораторная работа № 6. (2 часа). Назначение и возможности Программно-аппаратного комплекса (ПАК) средств защиты информации от НСД “Аккорд–АМДЗ”.

Цель: Изучить возможности и научиться работать с комплексом средств защиты от НСД. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке, установке и практическому освоению возможностей ПАК средств защиты информации от НСД.

Все лабораторные работы проводятся в интерактивной форме, а именно используются: диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами, группами студентов; элементы деловых игр, «мозговой штурм» или дискуссии по рассматриваемым вопросам.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

8.2 Примерная тематика рефератов:

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Виды защищаемой информации.
3. Интересы личности (общества, государства) в информационной сфере.
4. Угрозы информационной безопасности Российской Федерации.
5. Внешние и внутренние источники угроз информационной безопасности государства.
6. Информационное оружие, его классификация и возможности.
7. Компьютерная система как объект информационной безопасности.
8. Понятие национальной безопасности.
9. Национальные интересы России в информационной сфере.
10. Источники угроз информационной безопасности Российской Федерации.
11. Информационная безопасность и информационное противоборство.
12. Типовая стратегия информационной войны.
13. Классификация автоматизированных систем и требования по защите информации.
14. Структура системы защиты информации от НСД. Назначение и функции элементов.
15. Модели управления доступом.
16. Основные понятия криптографической защиты информации.
17. Симметричные криптографические системы. Достоинства и недостатки.
18. Асимметричные криптографические системы. Достоинства и недостатки.
19. Основные методы обеспечения инф. безопасности. Идентификация и аутентификация.
20. Основные методы обеспечения информационной безопасности. Разграничение и контроль доступа к информации.
21. Основные методы обеспечения информационной безопасности. Межсетевые экраны.
22. Виртуальные частные сети (VPN).
23. Методы обнаружения вторжений (атак).

8.2.1 Правила оформления рефератов

Объём реферата 7-10 листов печатного текста. К оформлению рефератов предъявляются такие же требования, как и к курсовым работам для студентов 3 курса, описанные в учебно-методическом пособии: Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЁТУ

1. Понятие национальной безопасности РФ. Основные задачи в области обеспечения национальной безопасности.
2. Основные элементы национальной безопасности Российской Федерации.
3. Классификация видов национальной безопасности Российской Федерации.
4. Информационная безопасность. Основные принципы и составляющие Государственной политики обеспечения информационной безопасности Российской Федерации.
5. Место и роль России в глобальном информационном пространстве. Интересы личности в информационной сфере.
6. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
7. Проблемы обеспечения информационной безопасности.
8. Понятие угрозы информации. Угрозы конфиденциальности, целостности и доступности.
9. Классификация угроз информации.
10. Модель действий нарушителя.
11. Источники угроз информационной безопасности РФ. Внешние источники угроз.
12. Источники угроз информационной безопасности РФ. Внутренние источники угроз.
13. Классификация источников угроз и уязвимостей информационной безопасности.
14. Понятие информационной войны. Проблемы информационных войн.
15. Субъекты и цели информационного противоборства. Составные части и методы информационного противоборства.
16. Информационное оружие, его классификация и возможности.
17. Информационная война как целенаправленное информационное воздействие информационных систем.
18. Приемы информационного воздействия в информационной войне. Способы перепрограммирования информационных систем.
19. Типовая стратегия информационной войны. Основные аспекты и последствия информационной войны.
20. Документы Гостехкомиссии при Президенте Российской Федерации. Концепции защиты автоматизированных систем и средств вычислительной техники.
21. Документы Гостехкомиссии при Президенте Российской Федерации. Классификация информационных систем по уровню их защищенности.
22. Документы Гостехкомиссии при Президенте Российской Федерации. Требования к информационным системам по обеспечению безопасности информации.
23. Направления защиты от несанкционированного доступа (НСД). Основные способы НСД. Принципы защиты информации от НСД.
24. Структура системы защиты информации от НСД, назначение и функции элементов.
25. Правила разграничения доступа к информации. Мандатная модель управления доступом.
26. Правила разграничения доступа к информации. Дискреционная модель управления доступом.

27. Основные понятия криптографической защиты информации. Историческая справка об основных этапах развития криптографии как науки.
28. Основные требования к криптографическим системам защиты информации. Пример простейшего шифра.
29. Обобщенная схема симметричной криптосистемы. Стандарт шифрования «Магма». Особенности применения алгоритмов симметричного шифрования.
30. Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом. Функция хэширования.
31. Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом. Электронная подпись.
32. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации.
33. Пароли, сертификаты и цифровые подписи. Методы аутентификации.
34. Понятие разграничения доступа. Разграничение доступа по виду, характеру, назначению, степени важности и секретности информации.
35. Технология межсетевых экранов (МЭ). Виды МЭ.
36. Технология межсетевых экранов (МЭ). Функции МЭ.
37. Основные понятия и функции виртуальных частных сетей (VPN).
38. Варианты построения виртуальных защищенных каналов. Средства обеспечения безопасности виртуальных частных сетей (VPN).
39. Назначение, возможности и порядок работы с персональными средствами аутентификации и защищённого хранения данных (USB-ключи и смарт-карты eToken).
40. Назначение, возможности установка и порядок работы с системой защиты от НСД «Dallas Lock».
41. Назначение, возможности и порядок работы с Электронным замком "Соболь".
42. Назначение, возможности и использование системы защиты от НСД «Secret Disk».
43. Назначение, возможности и использование программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1	2	3	4
Раздел 1. Информационная безопасность в системе национальной безопасности РФ. Тема 1. Понятие национальной безопасности	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 1. Тема 2. Национальные интересы России в информационной сфере	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 1. Тема 3. Угрозы информационной безопасности РФ	Подготовка к лекции, подготовка рефератов, подготовка к лаб. работе, под. к сдаче экзамена	4	Тесты перед лекцией, вопросы во время лаб. работ, зачёт

1	2	3	4
Раздел 1. Тема 4. Источники угроз информационной безопасности РФ	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 2. Инф. война, методы и средства ее ведения. Тема 5. Инф. безопасность и инф. противоборство	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 2. Тема 6. Приемы информационного воздействия в инф. войне	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 2. Тема 7. Типовая стратегия информационной войны	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 3. Защита от НСД в информационных системах. Тема 8. Классификация автоматизированных систем и требования по защите информации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 3. Тема 9. Структура СЗИ от НСД. Назначение и функции элементов	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 3. Тема 10. Модели управления доступом	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, зачёт
Раздел 4. Основные методы обеспечения информационной безопасности. Тема 11. Основные понятия криптографической защиты информации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 4. Тема 12. Симметричные криптографические системы	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 4. Тема 13. Асимметричные криптографические системы	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 4. Тема 14. Идентификация и аутентификация	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 4. Тема 15. Разграничение и контроль доступа к информации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт
Раздел 4. Тема 16. Технологии межсетевых экранов	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, зачёт
Раздел 4. Тема 17. Виртуальные частные сети (VPN)	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, зачёт

1	2	3	4
Раздел 4. Тема 18. Методы обнаружения вторжений (атак)	Подготовка к лекции, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, зачёт
Раздел 5. Средства защиты информации от несанкционированного доступа. Тема 19 Персональные средства аутентификации данных - USB-ключи и смарт-карты eToken	Подготовка к лабораторным работам, подготовка к сдаче экзамена	2	Тесты перед лекцией, вопросы во время лабораторных работ, зачёт
Раздел 5. Тема 20. Система защиты от НСД «Dallas Lock».	Подготовка к лаб. работам, подготовка к сдаче экзамена	4	Тесты перед лекцией, вопросы во время лаб. работ, зачёт
Раздел 5. Тема 21. Электронный замок "Соболь".	Подготовка к лабораторным работам, подготовка к сдаче экзамена	2	Тесты перед лекцией, вопросы во время лаб. работ, зачёт
Раздел 5. Тема 22. Система защиты конфиденциальной информации и персональных данных «Secret Disk».	Подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	2	Тесты перед лекцией, вопросы во время лабораторных работ, зачёт
Раздел 5. Тема 23. Программно - аппа- ратный комплекс средств защиты информации от НСД “Аккорд»	Подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	2	Тесты перед лекцией, вопросы во время лабораторных работ, зачёт

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

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

2. Новиков В.К., Информационное оружие - оружие современных и будущих войн [Электронный ресурс] / Новиков В.К. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2013. - 262 с. - ISBN 978-5-9912-0166-7 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201667.html

3. Долозов Н.Л., Программные средства защиты информации: конспект лекций [Электронный ресурс] / Долозов Н.Л. - Новосибирск: Изд-во НГТУ, 2015. - 63 с. - ISBN 978-5-7782-2753-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778227538.html

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

1.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")

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

1.3 Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации"
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

1.4 Закон РФ 2010 года N 390-ФЗ «О безопасности» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/

1.5 Федеральный закон от 27.07.2006 N152-ФЗ "О персональных данных" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

1.6 Федеральный закон от 29.07.2004 N98-ФЗ "О коммерческой тайне" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

2. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. - Воронеж: ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html.

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

3.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспе-чения 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;

3.2 ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — Режим доступа https://gostexpert.ru/gost/gost-28147-89

4. Андрианов В.В., Обеспечение информационной безопасности бизнеса [Электронный ресурс] / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. - 2-е изд., перераб. и доп. - М.: ЦИПСиР, 2011. - 373 с. - ISBN 978-5-9614-1364-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785961413649.html.

5. Туманов С.А., Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" [Электронный ресурс]: / Туманов С.А. - Новосибирск: Изд-во НГТУ, 2016. - 56 с. - ISBN 978-5-7782-2826-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778228269.html.

учебно-методическая

1. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", "Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", "Системный анализ и управление" / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. - Ульяновск : УлГУ, 2015.- URL: http://lib.ulsu.ru/MegaPro/Download/MObject/297

2. Лабораторный практикум по математическим методам защиты информации: учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев; УлГУ, ФМИиАТ. - Ульяновск: УлГУ, 2016. 54 с. **URL:**
http://lib.ulsu.ru/MegaPro/Download/MObject/270

3. **Иванцов** А. М.

Методические указания для самостоятельной работы студентов по дисциплине «Основы 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 : 406 КБ). - Текст: электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/4966

Согласовано:

Гл. библ-рь ИБ УлГУ Полякова И.Ю. 14.06.2019

Должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

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

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

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

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

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

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

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

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

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

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

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

6. Федеральные информационно-образовательные порталы:

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

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

7. Образовательные ресурсы УлГУ:

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

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

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

Согласовано:

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

Должность сотрудника УИиТ ФИО подпись дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer;
- система защиты конфиденциальной информации и персональных данных «Secret Disk. Базовый комплект с USB-ключом – 4 комплекта;
- электронный замок "Соболь" – 3 комплекта;
- персональные средства аутентификации и защищённого хранения данных - USB-ключи и смарт-карты eToken – 3 комплекта;
- система защиты от НСД «Dallas Lock». 4 комплекта;
- программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ” – 1 комплект.

Аудитория для проведения занятий - 2/24б.

Аудитория 2/24б укомплектована специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

– для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

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

Разработчик: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО

ЛИСТ ИЗМЕНЕНИЙ

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

Приложение 1

4.2 Объем дисциплины по видам учебной работы (в часах)

Вид учебной работы	Количество часов (форма обучения дневная)			
	Всего по плану	В т.ч. по семестрам		
		5		
Контактная работа обучающихся с преподавателем	54	54/54*		
Аудиторные занятия:	54	54/54*		
Лекции	36	36/36*		
Практические и сем. занятия				
Лабораторные работы (лаб. 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 лаб. работ - 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.

Приложение 2

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

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

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

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

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

Приложение 3

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

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

2. Новиков В.К., Информационное оружие - оружие современных и будущих войн [Электронный ресурс] / Новиков В.К. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2013. - 262 с. - ISBN 978-5-9912-0166-7 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201667.html

3. Долозов Н.Л., Программные средства защиты информации: конспект лекций [Электронный ресурс] / Долозов Н.Л. - Новосибирск: Изд-во НГТУ, 2015. - 63 с. - ISBN 978-5-7782-2753-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778227538.html

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

1.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

1.3 Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации"
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

1.4 Закон РФ 2010 года N 390-ФЗ «О безопасности» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/

1.5 Федеральный закон от 27.07.2006 N152-ФЗ "О персональных данных" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

1.6 Федеральный закон от 29.07.2004 N98-ФЗ "О коммерческой тайне" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

2. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. - Воронеж: ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html.

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

3.1 ГОСТ Р ИСО/МЭК 27002-2012 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;

3.2 ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — Режим доступа https://gostexpert.ru/gost/gost-28147-89

4. Андрианов В.В., Обеспечение информационной безопасности бизнеса [Электронный ресурс] / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. - 2-е изд., перераб. и доп. - М.: ЦИПСиР, 2011. - 373 с. - ISBN 978-5-9614-1364-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785961413649.html.

5. Туманов С.А., Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" [Электронный ресурс]: / Туманов С.А. - Новосибирск: Изд-во НГТУ, 2016. - 56 с. - ISBN 978-5-7782-2826-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778228269.html.

учебно-методическая

1. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", "Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", "Системный анализ и управление" / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. - Ульяновск : УлГУ, 2015.- URL: http://lib.ulsu.ru/MegaPro/Download/MObject/297

2. Лабораторный практикум по математическим методам защиты информации: учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев; УлГУ, ФМИиАТ. - Ульяновск: УлГУ, 2016. 54 с. **URL:** http://lib.ulsu.ru/MegaPro/Download/MObject/270

3. **Иванцов** А. М.
Методические указания для самостоятельной работы студентов по дисциплине «Основы 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 : 406 КБ). - Текст : электронный.
http://lib.ulsu.ru/MegaPro/Download/MObject/4966

Согласовано:
Гл. библ-рь ИБ УлГУ / Полина И. Ю / [подпись] / 14.06.2019
Должность сотрудника научной библиотеки / ФИО / подпись / дата

Приложение 4

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

б) Программное обеспечение

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

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

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

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

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

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

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

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

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

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

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

6. Федеральные информационно-образовательные порталы:

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

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

7. Образовательные ресурсы УлГУ:

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

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

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

Согласовано:

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

Должность сотрудника УИТиТ ФИО подпись дата