УТВЕРЖДЕНО

решением Учёного совета факультета математики,
информационных и авиационных технологий
от «21» июня 2019 г., протокол № 5/19

Председатель _____ / М.А. Волков

«21» июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	«Защита информации и информационная безопасность»
Факультет	Математики информационных и авиационных технологий
Кафедра	Телекоммуникационных технологий и сетей
Курс	4

Направление (специальность)11.03.02 – «Инфокоммуникационные технологии и системы связи».

код направления (специальности), полное наименование

Направленность (профиль/специализация) «Интернет и гетерогенные сети».

полное наименование

Форма обучения_____очная, _____

(*очная, заочная, очно-заочная (указать только те, которые реализуются)*

Дата введения в учебный процесс УлГУ: «_01_»__сентября__2019___г.

Программа актуализировананазаседании кафедры: протокол №_____ от _____ 20_____г.
Программа актуализировананазаседании кафедры: протокол №_____ от _____ 20_____г.
Программа актуализировананазаседании кафедры: протокол №_____ от _____ 20_____г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Козловский В.Г.	ТТС	к.т.н., доцент

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой телекоммуникационных технологий и сетей, реализующей дисциплину	Заведующий выпускающей кафедрой телекоммуникационных технологий и сетей
_____/ Смагин А.А ____/ *Подпись* *ФИО* «21» июня 2019 г.	(_____/ Смагин А.А ___/ *Подпись* *ФИО* «21» июня 2019 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

Цели освоения дисциплины:

- получение студентами теоретических знаний и практических навыков в области изучения информационной безопасности с учетом тенденций современного развития;
- заложить методически правильные основы знаний, необходимые будущим специалистам-практикам в области информационной безопасности;
- формирование у студента комплексных профессиональных и общекультурных компетенций в области изучения основ информационной безопасности.

Задачи освоения дисциплинызаключаются в обучении студентов:

- На административном уровне рассматриваются политика и программа безопасности, их типовая структура, меры по её выработке и сопровождению.
- На процедурном уровне описываются меры безопасности, имеющие дело с людьми. Формулируются основные принципы, помогающие успеху таких мер.
- Технический уровень, в соответствии с объектным подходом, трактуется как совокупность сервисов. Дается описание каждого сервиса.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП:

Курс входит вариативную часть часть профессионального цикла (Б1.В.ОД.7). Место дисциплины в учебном процессе: 4 курс (7 семестр) по очной форме обучения.

Изучение данной дисциплины базируется на успешно усвоенных базовых понятиях дисциплин математического и естественно-научного цикла и дисциплин профессионального цикла: основы информационных систем; инфокоммуникационные системы и сети; аппаратные средства ЭВМ

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих специальных дисциплин: корпоративные инфокоммуникационные системы; функциональное программирование.

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

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-3 - Владеет методами поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	Знать: механизмы реализации информационной безопасности, современные подходы к построению систем защиты информации, инструментарий информационной безопасности, направления информационной безопасности. Уметь: работать с типовыми средствами защиты информации; анализировать признаки сетевых атак и принимать меры для их нейтрализации, пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ,

	а также в ходе научных исследований Владеть: методами поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности
ПК-6 -Способность оценки параметров безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью	Знать: механизмы реализации информационной безопасности, современные подходы к построению систем защиты информации, инструментарий информационной безопасности, направления информационной безопасности. Уметь: работать с типовыми средствами защиты информации; анализировать признаки сетевых атак и принимать меры для их нейтрализации, пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований Владеть: методами поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности
ПК-15- Способен к администрированию процесса оценки производительности и контроля использования и производительности сетевых устройств , программного обеспечения информационно-коммуникационной системы	Знать: механизмы реализации информационной безопасности, современные подходы к построению систем защиты информации, инструментарий информационной безопасности, направления информационной безопасности. Уметь: работать с типовыми средствами защиты информации; анализировать признаки сетевых атак и принимать меры для их нейтрализации, пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований Владеть: методами поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 4 ЗЕТ

4.2. Объем дисциплиныпо видам учебной работы (144в часах)

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		7
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:	54	54
лекции	18	18
Семинары и практические занятия	18	18
Лабораторныеработы, практикумы	18	18
Самостоятельная работа	54	54
Форма текущего контролязнаний и контролясамостоятельной работы: тестирование, защита лабораторных работ	тестирование, защита лабораторных работ	тестирование, защита лабораторных работ
Виды промежуточной аттестации (экзамен, зачет)	Экзамен 36	Экзамен 36
Всего часов по дисциплине	144	144

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

Форма обучения _____*очная*_____

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия-интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы,практикумы			
1	2	3	4	5	6	7	
Раздел 1. Основные положения защиты информации							
1. Основные понятия в области информационной безопасности.	8	2	2		2	4	тестирование
2. Основные методы защиты информации.	8	2	2		2	4	тестирование
Раздел 2. Правовые основы защиты информации							
3. Юридические аспекты защиты информации.	8	2	2		2	4	тестирование
Раздел 3. Защита от несанкционированного доступа (НСД) в информационных системах							
4. Источники угроз инфор-	8	2	2		2	4	тестирование

мационной безопасности в информационных системах.							
5. Структура системы защиты информации от НСД. Назначение и функции элементов.	8	2	2		2	4	тестирование
6. Технологии межсетевых экранов.	8	2	2		2	4	тестирование
7. Основы криптографии.	8	2	2		2	4	тестирование
Раздел 4. Технические аспекты защиты информационных систем							
8. Обзор типовых средств защиты информации от НСД.	52	4	4	18	4	26	защита лабораторных работ
экзамен	36						
Итого	144	18	18	18	18	54	

5. СОДЕРЖАНИЕ ДИСЦИЛИНЫ (МОДУЛЯ)

Раздел 1. Основные положения защиты информации

Тема 1. Основные понятия в области информационой безопасности.

Цели и задачи курса. Объект и предмет изучения. Базовые понятия и определения. Общие принципы обеспечения защиты информации.

Тема 2. Основные методы защиты информации.

Характеристика уровней защиты информации. Меры защиты. Основные методы реализации программно-технического уровня защиты информационных систем. Модель нарушителя информационных систем.

Раздел 2. Правовые основы защиты информации

Тема 3. Юридические аспекты защиты информации.

Основы законодательства России по вопросам защиты информации, важнейшие законодательные акты в области защиты информации. Законы РФ (“О государственной тайне”, “Об информации, информационных технологиях и о защите информации”, «О персональных данных», «О коммерческой тайне»). Ответственность за нарушения информационной безопасности.

Раздел 3. Защита от НСД в информационных системах

Тема 4. Источники угроз информационной безопасности в информационных системах.

Понятие угрозы. Классификация источников угроз информационной безопасности.Внешние источники угроз. Внутренние источники угроз. Противодействие угрозам.

Тема 5. Структура системы защиты информации от НСД. Назначение и функции элементов.

Концепция защиты СВТ и АС от НСД". Классификация каналов НСД к информации. Основные принципы построения СЗИ от НСД. Характеристика подсистем СЗИ.

Тема 6. Технологии межсетевых экранов.

Основные понятия технологии межсетевых экранов (МЭ). Классификация МЭ. Функции межсетевого экранирования. Фильтрация трафика. Особенности межсетевого экранирования на различных уровнях модели OSI.

Тема 7. Основы криптографии.

Основные понятия криптографии. Требования к криптографическим системам. Симметричные криптосистемы. Виды шифров. Системы с открытым ключом. Электронная подпись. Стойкость шифров.

Раздел 4. Технические аспекты защиты информационных систем

Тема 8. Обзор типовых средств защиты информации от НСД.

Персональные средства аутентификации и защищенного хранения данных - USB-ключи и смарт-карты eToken. Персональное средство криптографической защиты информации «ШИПКА». Электронный замок "Соболь". Система защиты SecretNet. Система защиты конфиденциальной информации и персональных данных SecretDisk.Программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ”.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Основные положения защиты информации

Тема 1. Основные понятия в области информационной безопасности (семинар).

1. Сущность понятий «Информационная безопасность» и «Защита информации».
2. Основные термины и определения информационной безопасности.
3. Информационная безопасность и ее свойства.
4. Основные принципы информационной безопасности.

Тема 2. Основные методы защиты информации (семинар).

1. Уровни защиты информации и их характеристика.
2. Уязвимости в информационных системах.
3. Меры защиты. Административные меры и технические средства.
4. Основные методы и средства защиты информации.
5. Модель действий нарушителя.

Раздел 2. Правовые основы защиты информации

Тема 3.Юридические аспекты защиты информации(семинар).

1. Информация как объект правоотношений (Закон РФ “Об информации, информационных технологиях и о защите информации”).
2. Виды и содержание тайн. Законодательная база охраны государственной тайны (Закон РФ «О государственно тайне»).
3. Виды и содержание тайн. Законодательная база охраны персональных данных (Закон РФ “О персональных данных».
4. Виды и содержание тайн. Правовые основы защиты служебной и профессиональных тайн.
5. Виды и содержание тайн. Правовое регулирование коммерческой тайны (Закон РФ «О коммерческой тайне»).
6. Правовая ответственность за нарушения информационной безопасности.

Раздел 3. Защита от НСД в информационных системах

Тема 4. Источники угроз информационной безопасности в информационных системах (семинар).

1. Понятия угрозы и НСД в информационных системах.
2. Классификация источников угроз информационной безопасности.
3. Внешние источники угроз и защита от них.
4. Внутренние источники угроз и защита от них.

Тема 5. Структура системы защиты информации от НСД. Назначение и функции элементов (семинар).

1. Концепция защиты СВТ и АС от НСД.
2. Классификация каналов НСД к информации.
3. Основные принципы построения СЗИ от НСД.
4. Характеристика основных подсистем СЗИ от НСД.

Тема 6. Технологии межсетевых экранов(семинар).

1. Основные понятия технологии межсетевых экранов.
2. Классификация межсетевых экранов.
3. Функции межсетевого экранирования.
4. Фильтрация трафика.
5. Особенности межсетевого экранирования на различных уровнях модели OSI.

Тема 7. Основы криптографии (семинар).

1. Основные понятия криптографии.
2. Требования к криптографическим системам.
3. Симметричные криптосистемы. Виды шифров.
4. Системы с открытым ключом. Электронная подпись.
5. Стойкость шифров.

Раздел 4. Технические аспекты защиты информационных систем

Тема 8. Обзор типовых средств защиты информации от НСД(семинар).

1. Назначение и возможности персональных средств аутентификации и защищенного хранения данных (USB-ключи и смарт-карты eToken).
2. Назначение и возможности персонального средства криптографической защиты информации «ШИПКА».
3. Назначение и возможности Электронного замка "Соболь".
4. Назначение и возможности системы защиты конфиденциальной информации и персональных данных «SecretDisk».
5. Назначение и возможности системы защиты информации от НСД «SecretNet».
6. Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Раздел 4. Технические аспекты защиты информационных систем

Лабораторная работа № 1.(2 часа).«Восстановление данных с помощью программы Recuva».

Цель: Овладение навыками восстановления файлов после случайного удаления/форматирования, программного сбоя или вирусной атаки. Результат: отчет.

Методические указания: основное внимание должно быть уделено практическому Восстановление данных.

Лабораторная работа № 2.(2 часа). «Сброс паролей в Windows».

Цель: Ознакомление с теоретическими сведениями политик безопасности учетных записей и паролей в Windows, а также овладение навыками их сброса в случаях утери или

компрометации. Результат: отчет.

Методические указания: основное внимание должно быть уделено практическим навыкам.

Лабораторная работа № 3. (2 часа). Назначение, возможности и порядок работы с персональными средствами аутентификации и защищенного 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.

Лабораторная работа № 4. (2 часа). Назначение, возможности и порядок работы с персональным средством криптографической защиты информации «ШИПКА».

Цель: Изучить возможности и научиться работать с персональным средством криптографической защиты информации. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностейперсонального средства криптографической защиты информации.

Лабораторная работа № 5.(3 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".

Лабораторная работа № 6. (3 часа). Назначение и возможности системы защиты конфиденциальной информации и персональных данных «SecretDisk».

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 «SecretDisk».

Лабораторная работа № 7. (3 часа). Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

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

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

Для выполнения указанных выше лабораторных работ необходимо использовать учебно-методическое пособие 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.-**URL^** ftp://10.2.96.134/Text/Amiranov_2016.pdf

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Примерная тематика рефератов:

1. Законодательство Российской Федерации об информационной безопасности.
2. Модель действий нарушителя.
3. Законодательная база охраны государственной тайны.
4. Правовые основы защиты служебной и профессиональных тайн.

5. Правовое регулирование коммерческой тайны.
6. Внешние и внутренние источники угроз информационной безопасности государства.
7. Информационное оружие, его классификации и возможности.
8. Эталонная сетевая модель OSI.
9. Историческая справка возникновения и развития криптографии.
10. Компьютерная система как объект информационной безопасности.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

Примерный перечень вопросов к экзамену:

1. Основные термины и определения информационной безопасности, уровни защиты информации и их характеристика.
2. Информационная безопасность и ее свойства.
3. Основные принципы информационной безопасности.
4. Меры защиты информации. Административные меры и технические средства.
5. Основные методы и средства защиты информации.
6. Модель действий нарушителя.
7. Информация как объект правоотношений. Закон РФ “Об информации, информационных технологиях и о защите информации”.
8. Виды и содержание тайн. Законодательная база охраны государственной тайны. Закон РФ «О государственно тайне».
9. Виды и содержание тайн. Законодательная база охраны персональных данных. Закон РФ “О персональных данных».
10. Виды и содержание тайн. Правовые основы защиты служебной и профессиональных тайн.
11. Виды и содержание тайн. Правовое регулирование коммерческой тайны. Закон РФ «О коммерческой тайне».
12. Правовая ответственность за нарушения информационной безопасности.
13. Понятия угрозы и НСД в информационных системах.
14. Классификация источников угроз информационной безопасности. Внешние источники угроз и защита от них.
15. Классификация источников угроз информационной безопасности. Внутренние источники угроз и защита от них.
16. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
17. Классификация каналов НСД к информации. Основные принципы построения СЗИ от НСД.
18. Система защиты информации от НСД, характеристика основных подсистем.
19. Основные понятия технологии межсетевых экранов. Классификация межсетевых экранов.
20. Функции межсетевого экранирования. Фильтрация трафика.
21. Особенности межсетевого экранирования на различных уровнях модели OSI.
22. Основные понятия криптографии. Требования к криптографическим системам.
23. Симметричные криптосистемы. Виды шифров.
24. Системы с открытым ключом. Электронная подпись.
25. История криптографии. Стойкость шифров.
26. Назначение, возможности и порядок работы с персональными средствами аутентификации и защищенного хранения данных (USB-ключи и смарт-карты eToken).

27. Назначение, возможности и порядок работы с персональным средством криптографической защиты информации «ШИПКА».
28. Назначение, возможности и порядок работы с Электронным замком "Соболь".
29. Назначение и возможности системы защиты конфиденциальной информации и персональных данных «Secret Disk».
30. Назначение и возможности системы защиты информации от НСД «Secret Net».
31. Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Форма обучения _____*очная*_____

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа, подготовка к сдаче зачета, экзамена и др.)***	**Объем в часах**	**Форма контроля (*проверка решения задач, реферата и др.)***
Раздел 1. Основные положения защиты информации			
1. Основные понятия в области информационной безопасности.	проработка учебного материала, подготовка к сдаче зачета	4	тестирование
2. Основные методы защиты информации.	проработка учебного материала, подготовка к сдаче зачета	4	тестирование
Раздел 2. Правовые основы защиты информации			
3. Юридические аспекты защиты информации.	проработка учебного материала, подготовка к сдаче зачета	4	тестирование
Раздел 3. Защита от несанкционированного доступа (НСД) в информационных системах			
4. Источники угроз информационной безопасности в информационных системах.	проработка учебного материала, подготовка к сдаче зачета	4	тестирование
5. Структура систе-	проработка учебного материала, под-	4	тестирование

мы защиты информации от НСД. Назначение и функции элементов.	готовка к сдаче зачета		
6. Технологии межсетевых экранов.	проработка учебного материала, подготовка к сдаче зачета	4	тестирование
7. Основы криптографии.	проработка учебного материала, подготовка к сдаче зачета	4	тестирование
8. Обзор типовых средств защиты информации от НСД.	проработка учебного материала, подготовка к сдаче зачета, отчета по лабораторной работе	26	тестирование

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва :Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр.Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433715
2. 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
3. Хорев, Павел Борисович.
   Методы и средства защиты информации в компьютерных системах : учеб.пособие для вузов по направлению 230100 (654600) "Информатика и вычислительная техника" / Хорев Павел Борисович. - 3-е изд., стер. - Москва : Академия, 2007

дополнительная

1. 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
2. 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
3. Малюк А.А., Защита информации в информационном обществе [Электронный ресурс]: Учебное пособие для вузов. / А.А. Малюк - М. : Горячая линия - Телеком, 2015. - 230 с. - ISBN 978-5-9912-0481-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204811.html

учебно-методическая

1.Андреев, А. С.Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", "Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", "Системный анализ и управление" / А. С. Андреев, С.

М. Бородин, А. М. Иванцов ;УлГУ, ФМиИТ. - Ульяновск :УлГУ, 2015. -**URL^** ftp://10.2.96.134/Text/Andreev2015.pdf
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.-**URL^** ftp://10.2.96.134/Text/Amiranov_2016.pdf

Согласовано:

_____/_____/_____/_____Дол
Должность сотрудника научной библиотеки ФИО подпись дата

б)Программное обеспечение____Windows, MS Office_____

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 / ОООПолитехресурс. - 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

Согласовано:

_____/_____/_____/_____

Должность сотрудника УИТиТФИО подпись дата

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое).*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для предоставления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной инфромационно - образовательной среде, электронно-библиотечной системе.Перечень оборудования, используемого в учебном процессе, указывается в соответствии со сведениями о материально-техническом обеспечении и оснащенности образовательного процесса, размещенными на официальном сайте УлГУ в разделе «Сведения об образовательной организации».

12. 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.

Разработчик _____ доцент кафедры Козловский В.Г.

подпись должностьФИО