УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от «_16_» _____06_____ 2020 г., протокол № 5/20

Председатель_____М.А. Волков
(подпись, расшифровка подписи)
«_16_» _____06_____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Информационная безопасность
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

Специальность (направление)**: 09.03.03** «Прикладная информатика»,
профиль «Информационная среда» (Квалификация (степень) - «бакалавр»)
код направления (специальности), полное наименование

полное наименование

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

Дата введения в учебный процесс УлГУ: «_01_»_____09_____2020_г.

Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.

Сведения о разработчиках:

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

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационные технологии»
/_____/ Андреев А.С. / (подпись) (Ф.И.О.) «10» 06 2020 г.	/_____/ Волков М.А. / *Подпись* *(Ф.И.О.)* «_16_»_____06_____2020__г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Цель курса - заложить методически правильные основы знаний в области информационной безопасности, необходимые будущим специалистам в области прикладной информатики.

Информационная безопасность (ИБ)- сравнительно молодая, быстро развивающаяся область информационных технологий (ИТ), для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими ветвями ИТ, базис. Это - первая задача курса, для решения которой привлекается объектно-ориентированный подход.

Успех в области ИБ может принести только комплексный подход. Описание общей структуры и отдельных уровней такого подхода - вторая задача курса. Для ее решения рассматриваются меры законодательного, административного, процедурного и технического уровней.

Предполагается, что большинство понятий, введенных в данном курсе, станет предметом более детального рассмотрения в других, специальных курсах.

Задачи освоения дисциплины:

дать основы: методологии создания систем защиты информации и обеспечения информационной безопасности информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Информационная безопасность» (Б1.Б) изучается в 7 семестре и относится к числу базовых дисциплин блока 1 «Дисциплины (модули)», предназначенного для студентов, обучающихся по направлению подготовки бакалавриата **09.03.03** «Прикладная информатика».

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Информатика и программирование»; «Информационные системы и технологии»; «Проектирование информационных систем»; «Администрирование информационных систем»; «Информационные сети»; «Разработка и стандартизация программных средств и информационных систем»; «Защита в операционных системах»; «Защита в компьютерных сетях».

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: «Информационные ресурсы общества»; «Информатизация общества»; «Экспертные системы»; «Интернет-программирование»; «Интеллектуальные информационные системы»; «Разработка мобильных приложений»; «Открытые технологии разработки программного обеспечения».

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных техно-	**Знать:** Основные требования информационной безопасности в ходе решения стандартных задач профессиональной деятельности **Уметь:** Решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности

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

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 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		
		7		
1	2	3	4	5
Контактная работа обучающихся с преподавателем	54	54/54		
Аудиторные занятия:	54	54/54		
Лекции	18	18/18		
Лабораторные работы (лабораторный практикум)	36	36/36		
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 лабораторных работах; - вопросы перед лекциями; - рефераты на заданные темы		

Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	Зачёт	Зачёт		
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 и разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практические занятия, семинары	Лабораторные работы			
1	2	3	4	5	6	7	8
Раздел 1. Основные положения защиты информации							
1	2	3	4	5	6	7	8
1. Основные понятия в области защиты информации	4	2				2	Тесты Т1, рефераты (№ 1,2,6)
2. Источники угроз информационной безопасности в информационных системах	20	2		8		10	Тесты Т2, Реферат № 3), лаб. раб. 1
3. Правовой режим защиты государственной тайны	4	2				2	Тесты Т3, реферат (№ 8)
4. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации	4	2				2	Тесты Т4, реферат (№ 9)
5. Законодательство Российской Федерации по вопросам защиты персональных данных	4	2				2	Тесты Т5, рефераты (№ 2,10,11)
6. Юридические аспекты защиты информации	4	2				2	Тесты Т6, реферат (№ 5)

Раздел 2. Основные методы и средства обеспечения информационной безопасности							
7. Основные понятия криптографической защиты информации	4	2				2	Тесты Т7, реферат (№ 14), лаб. раб. № 2,3,4
8. Идентификация, аутентификация и контроль доступа к информации	28	2		12		14	Тесты Т8, реферат (№ 13)
9. Методы и средства защиты информации от утечки по техническим каналам	36	2		16		18	Тесты Т9, рефераты (№ 12, 15), лаб. раб. № 5,6,7,8
Итого:	108	18	-	36		54	

5. СОДЕРЖАНИЕ КУРСА (МОДУЛЯ)

Раздел 1. Основные положения защиты информации

Тема 1. Основные понятия в области защиты информации.

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

Тема 2. Источники угроз информационной безопасности в информационных системах.

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

Тема 3. Правовой режим защиты государственной тайны.

Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны.

Тема 4. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации.

Понятие коммерческой, профессиональной тайн и служебной информации по российскому законодательству. Коммерческая, профессиональная тайны. Служебная тайна. Правовые режимы тайн. Юридическая ответственность за нарушения правовых режимов информации ограниченного доступа (дисциплинарная, гражданско-правовая, административная, уголовная).

Тема 5. Законодательство Российской Федерации по вопросам защиты персональных данных.

Основные мероприятия по вопросам защиты информации и документы, разрабатываемые на предприятии в соответствии с Федеральным законом РФ «О персональных данных».

Тема 6. Юридические аспекты защиты информации.

Основы законодательства России в области защиты информации: Закон РФ “О государственной тайне”, Закон РФ “Об информации, информационных технологиях и о

защите информации", Закон РФ «О персональных данных», Закон РФ «О коммерческой тайне». Ответственность за нарушения информационной безопасности.

Раздел 2. Основные методы и средства обеспечения информационной безопасности

Тема 7. 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. Обобщенные схемы симметричной и ассимметричной криптосистем.

Тема 8. Идентификация, аутентификация и контроль доступа к информации.

Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Пароли, сертификаты и электронные подписи. Методы аутентификации. Разграничение доступа по виду, характеру, назначению, степени важности и конфиденциальности информации.

Тема 9. Методы и средства защиты информации от утечки по техническим каналам.

Основные методы и средства защиты информации от утечки в электромагнитном и акустическом (виброакустическом) каналах (экранирование, зашумление и фильтрация опасных сигналов). Средства противодействия перехвату «информации по техническим каналам.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 1. Основные положения защиты информации

Тема 2. Источники угроз информационной безопасности в информационных системах.

Лабораторная работа № 1. (8 часов). «Выработка концептуальных основ деятельности по обеспечению информационной безопасности предприятия».

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

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

Раздел 2. Основные методы и средства обеспечения информационной безопасности

Тема 8. Идентификация, аутентификация и контроль доступа к информации

Лабораторная работа № 2. «Электронный замок "Соболь". (4 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 № 3. (4 часа). «Назначение и возможности Программно-аппаратного комплекса 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 Программно-аппаратного комплекса средств защиты информации от НСД.

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

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

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

Тема 9. Методы и средства защиты информации от утечки по техническим каналам.

Лабораторная работа № 5 (2 часа). «Защита каналов передачи информации генератором шума «Гром-ЗИ-4».

Цель работы: Ознакомление с техническими характеристиками генератора шума «Гром-ЗИ-4», изучение правил его эксплуатации и получение практических навыков работы с генератором шума Гром-ЗИ-4».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с генератором шума Гром-ЗИ-4».

Лабораторная работа № 6 (6 часов). «Изучение методов поиска и локализации специальных технических средств с использованием прибора ST-032 Пиранья».

Цель работы: изучить возможности прибора ST-032 «Пиранья» и научиться осуществлять поиск и локализацию специальных технических средств несанкционированного получения информации.

Методические указания: основное внимание должно быть уделено практической эксплуатации в ходе поиска и локализации специальных технических средств несанкционированного получения информации.

Лабораторная работа № 7 (4часа). «Исследование акустического зашумления помещения».

Цель работы: Исследование возможностей генератора шума SI-3010, получение практических навыков в работе по акустическому зашумлению помещения.

Методические указания: основное внимание должно быть уделено практическим навыкам в работе по акустическому зашумлению помещения.

Лабораторная работа № 8 **(4 часа). «**Обнаружение радиоизлучающих устройств с использованием сканирующего радиоприемника AR-3000A».

Цель работы: Ознакомление с техническими характеристиками изделия AR-3000A, изучение правил эксплуатации изделия, получение практических навыков работы с изделием.

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. Интересы личности (общества, государства) в информационной сфере.
3. Угрозы информационной безопасности Российской Федерации.
4. Информационная система как объект информационной безопасности.
5. Юридические аспекты защиты информации.

6. Законодательство РФ об информационной безопасности.
7. Требования Федерального закона РФ «Об информации, информационных технологиях и о защите информации».
8. Требования Федерального закона РФ «О государственной тайне».
9. Требования Федерального закона РФ «О коммерческой тайне».
10. Законодательство РФ в области защиты персональных данных.
11. Проблемы защиты персональных данных.
12. Основные каналы утечки информации при обработке на компьютерах.
13. Программные и аппаратные средства защиты информации от несанкционированного доступа.
14. Криптография в современном мире.
15. Основные методы защиты информации от утечки по техническим каналам.

8.2.1 Правила оформления рефератов

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

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЁТУ

1. Базовые понятия и определения информационной безопасности
2. Основные принципы организации защиты информации
3. Угрозы информационной безопасности и их проявления
4. Классификация источников угроз информационной безопасности
5. Модель действий нарушителя
6. Назначение и возможности сканирующего радиоприемника AR-3000A
7. Порядок отнесения сведений к государственной тайне.
8. Система защиты сведений, составляющих государственную тайну.
9. Информация как объект правоотношений (Закон РФ “Об информации, информационных технологиях и о защите информации”)
10. Виды и содержание тайн государства
11. Законодательная база охраны государственной тайны (Закон РФ «О государственно тайне»)
12. Законодательная база охраны персональных данных (Закон РФ “О персональных данных»
13. Правовые основы защиты служебной и профессиональных тайн
14. Правовое регулирование коммерческой тайны закон РФ «О коммерческой тайне»
15. Основные понятия криптографии. История криптографии. Пример простейшего шифра
16. Симметричные и асимметричные криптографические системы
17. Основы идентификации и аутентификации
18. Классификация протоколов аутентификации
19. Первоочередные мероприятия по созданию системы защиты персональных данных на предприятии.
20. Методы пассивной и активной защиты

21. Технические средства обнаружения утечки информации по акустическому (виброакустическому) каналу

22. Средства противодействия перехвату «информации по акустовибрационному каналу

23. Назначение и возможности Электронного замка "Соболь".

24. Назначение и возможности Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

25. Назначение и возможности системы защиты от НСД «Dallas Lock»

26. Назначение и возможности имитатора многофункционального «ИМФ-2»

27. Назначение и возможности прибора ST-032 «Пиранья»

28. Назначение и возможности генератора шума «Гром-ЗИ-4

29. Назначение и возможности генератора шума SI-3010

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1	2	3	4
Раздел 1. Основные положения защиты информации. Тема 1. Основные понятия в области защиты информации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты и вопросы перед лекцией, зачёт
Раздел 1. Тема 2. Источники угроз информационной безопасности в информационных системах	Подготовка к лекции, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче зачёта	10	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, зачёт
Раздел 1. Тема 3. Правовой режим защиты государственной тайны.	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты и вопросы перед лекцией, зачёт
Раздел 1. Тема 4. Правовые режимы защиты коммерческой, профессиональной тайн и служебной информации.	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты и вопросы перед лекцией, зачёт
Раздел 1. Тема 5. Законодательство Российской Федерации по вопросам защиты персональных данных.	Подготовка к лекции, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче зачёта	2	Тесты и вопросы перед лекцией, зачёт
Раздел 1. Тема 6. Юридические аспекты защиты информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче зачёта	6	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, зачёт
Раздел 2. Основные методы и средства обеспече-	Подготовка к лекции, семинару, подготовка рефе-	2	Тесты и вопросы перед лекцией, зачёт

ния информационной безопасности. Тема 7. Основные понятия криптографической защиты информации	ратов, подготовка к лабораторным работам, подготовка к сдаче зачёта		
Раздел 2. Тема 8. Идентификация, аутентификация и контроль доступа к информации	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче зачёта	14	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, зачёт
Раздел 2. Тема 9. Методы и средства защиты информации от утечки по техническим каналам	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче зачёта	18	Тесты и вопросы перед лекцией, вопросы и тесты на лабораторной работе, 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

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

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

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

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

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

1.3 Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации"

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

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

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

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

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

учебно-методическая

1. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", «Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", «Системный анализ и управление» / А.С. Андреев, С.М. Бородин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54с. http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf

2. Иванцов А. М.

Методические указания для самостоятельной работы студентов по дисциплине «Информационная безопасность» для студентов бакалавриата по направлению 09.03.03 «Прикладная информатика» 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 : 341 КБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/4259

Согласовано:
Гл. библ-рь ИБ УлГУ / Полина К.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

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://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 : 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. УИТиТ	/ Клочкова А.В. /		05.06.2020
должность сотрудника УИТиТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer;
- электронный замок "Соболь" – 3 комплекта;
- система защиты от НСД «Dallas Lock». 4 комплекта;
- программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ” – 1 комплект;
- имитатор многофункциональный имитатор «ИМФ-2»;
- прибор ST-032 «Пиранья»;
- генератор шума «Гром-ЗИ-4;
- генератор шума SI-3010;
- сканирующий радиоприемник AR-3000A.

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

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

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

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

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

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

Разработчик: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО