УТВЕРЖДЕНО
решением Ученого совета ФМИАТ
от «16» мая 2023 г., протокол № 4/23
Председатель _____ Волков М.А.
(подпись, расшифровка подписи)
«16» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Управление информационной безопасностью
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	5

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

Специализация: «Безопасность открытых информационных систем»
полное наименование

Дата введения в учебный процесс УлГУ: «_01_» 09 2023 г.

Программа актуализирована на заседании кафедры: протокол № 12 от 12.04.2023
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04.2024 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
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
_____ / Андреев А.С. / *(подпись) (Ф.И.О.)* «_11_» 05 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Цель изучения дисциплины:

Изучение методов и средств управления информационной безопасностью.

Задачи освоения дисциплины:

обучить студентов принципам управления информационной безопасностью;

привить студентам навыки реализации мероприятий по управлению информационной безопасностью;

дать студентам представление об устранении рисков информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина относится к обязательным дисциплинам цикла Б1 образовательной программы и читается в 10-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения.

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Информатика»; «Теория информации», «Организационное и правовое обеспечение информационной безопасности», «Основы 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»; «Безопасность операционных систем»; «Разработка и эксплуатация автоматизированных систем в защищённом исполнении.

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

Процесс изучения дисциплины «Управление информационной безопасностью» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-1 – Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**Знать:** значение информации, информационных технологий и информационной безопасности в современном обществе для обеспечения объективных потребностей личности, общества и государства **Уметь:** оценивать роль информации, информационных технологий и информационной безопасности в современном обществе **Владеть:** навыками оценки роли и значения информации, информационных технологий и информационной безопасности в современном обществе
ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	**Знать:** основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации **Уметь:** применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации **Владеть:** навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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

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

Вид учебной работы	Количество часов (форма обучения - очная)			
	Всего по плану	В т.ч. по семестрам		
		6		
Контактная работа обучающихся с преподавателем	80	*80/80		
Аудиторные занятия:	80	*80/80		
Лекции	40	*40/40		
Практические и семинарские занятия	40	*40/40		
Лабораторные работы (лабораторный практикум)				
Самостоятельная работа	28	28		
Форма текущего контроля знаний и контроля сам. работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на лекциях и семинарах; - рефераты на заданные темы		
Курсовая работа				
Всего часов по дисциплине	144	144		
Виды промежуточного контроля (экзамен, зачет)	экзамен	экзамен		
Всего часов по дисциплине	144	144		

* 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. 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 в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
Раздел 1. Стандартизация систем и процессов управления информационной безопасностью							
1. Управление информационной безопасностью. Основные понятия		4	2			2	Тесты Т1, реф. 1, 2
2. Серия стандартов ISO/IEC 27000		4	2			2	Тесты Т2 (5), реф. 3
3. Стандарты на отдельные процессы управления информационной безопасностью		4	2			2	Тесты Т3 (5), реф. 4
4. Отраслевые стандарты в области управления информационной безопасностью		4	2			2	Тесты Т4 (5), реф. 5
Раздел 2. Управление и система управления информационной безопасностью							
5. Анализ рисков информационной безопасности		4	6		6	4	Тесты Т5 (7), реф. 6
6. Система управления информационной безопасностью		4	4			4	Тесты Т6, реф. 7,8
7. Политика информационной безопасности предприятия		6	12		10	4	Тесты Т7 (9), реф. 9,10
8. План защиты информационных ресурсов от несанкционированного доступа		4	4			4	Тесты Т8 (10), реф. 11
9. План обеспечения непрерывной		6	6		2	4	Тесты Т9 (11), реф. 12

работы и восстановления работоспособности информационной системы							
Итого	144	40	40		18	28	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Стандартизация систем и процессов управления информационной безопасностью

Тема 1. Управление информационной безопасностью. Основные понятия

Понятия: системы, системного подхода, процесса, процессного подхода, управления, информационной безопасности. Процессный подход к управлению организации. Управление информационной безопасностью.

Тема 2. Серия стандартов ISO/IEC 27000

Роль стандартов информационной безопасности для решения проблемы ИБ. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Международные стандарты информационной безопасности. Управление информационной безопасностью. Общие критерии безопасности информационных технологий. Основные отечественные стандарты безопасности информационных технологий.

Тема 3. Стандарты на отдельные процессы управления информационной безопасностью ISO/IEC 13335-Методы и средства обеспечения безопасности информационных технологий. ГОСТ Р ИСО/МЭК 13335-1-2006, ГОСТ Р ИСО/МЭК 13335-3-2007, ГОСТ Р ИСО/МЭК 13335-4-2007, ГОСТ Р ИСО/МЭК 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности». ISO/IEC 15408 – Общие критерии и методология оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-1, 2, 3-2008. Международные стандарты ISO серий 9000 (качество) и 14000 (экология). Международные и отечественные стандарты обеспечения непрерывности бизнеса.

Тема 4. Отраслевые стандарты в области управления информационной безопасностью

Стандарты, направленные на минимизацию рисков (ГОСТ Р 53647). Стандарты банковской системы Российской Федерации (СТО БР ИББС). Комплекс документов по обеспечению и поддержанию ИБ организаций банковской системы. Аудит ИБ.

Раздел 2. Управление и система управления информационной безопасностью

Тема 5. Анализ рисков информационной безопасности

Основные понятия управления рисками. Термины и определения. Основные этапы управления рисками (выбор методологии оценки рисков; идентификация активов; анализ угроз и их последствий; выявление уязвимых мест в защите; оценка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска).

Тема 6. Система управления информационной безопасностью

Система управления информационной безопасности организации (СУИБ). Основные функции и компоненты СУИБ организации. Область действия СУИБ. Документальное обеспечение СУИБ. Состав документации СУИБ. Использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СУИБ (СМИБ) организации. Основные этапы создания СУИБ (инвентаризация и категорирование активов; оценка защищенности информационной системы; оценка и обработка информационных рисков; контроль выполнения и эффективности выбранных мер).

Тема 7. Политика информационной безопасности предприятия

Основные понятия политики информационной безопасности (ПИБ) организации. Содер-

жание ПИБ организации. Область применения ПИБ. Понятие ПИБ «в широком» и «в узком» смыслах. «Частные» ПИБ. Стратегии действий на нарушения безопасности.

Тема 8. План защиты информационных ресурсов от несанкционированного доступа

Назначение и основные положения Плана защиты информационных ресурсов от НСД. Обязанности руководителя и сотрудников ОИБ по предупреждению, реагированию и ликвидации последствий нарушений безопасности. Распределение обязанностей между администраторами ИС. Требования безопасности, предъявляемые к пользователям ИС. Основные мероприятия, формальные процедуры и другие технологические процессы по обеспечению ИБ. Выявление попыток НСД. Реагирование на нарушения информационной безопасности. Ликвидация последствий НСД.

Тема 9. План обеспечения непрерывной работы и восстановления работоспособности информационной системы

Понятие управления непрерывности бизнеса. Процесс управление непрерывностью бизнеса (УНБ). Система управления непрерывностью бизнеса (СУНБ). Ключевые компоненты СУНБ. Внедрение управления непрерывностью бизнеса в культуру организации. Программа непрерывного образования и информирования об УНБ. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса. Примерное содержание плана обеспечения непрерывности бизнеса. План восстановления бизнеса.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Стандартизация систем и процессов управления информационной безопасностью

Тема 1. Управление информационной безопасностью. Основные понятия (семинар).

1. Понятия: системы, системного подхода, процесса, процессного подхода, управления, информационной безопасности

2. Процессный подход к управлению организации. Управление информационной безопасностью (ИБ)

Тема 2. Серия стандартов ISO/IEC 27000 (семинар).

1. Роль стандартов информационной безопасности для решения проблемы ИБ.
2. Серия стандартов ISO/IEC 27000 «Информационные технологии.
3. Методы обеспечения безопасности». Международные стандарты информационной безопасности. Управление информационной безопасностью. Общие критерии безопасности информационных технологий.
4. Основные отечественные стандарты безопасности информационных технологий.

Тема 3. Стандарты на отдельные процессы управления информационной безопасностью (семинар).

1. ISO/IEC 13335-Методы и средства обеспечения безопасности информационных технологий.
2. ГОСТ Р ИСО/МЭК 13335-1-2006, ГОСТ Р ИСО/МЭК 13335-3-2007, ГОСТ Р ИСО/МЭК 13335-4-2007, ГОСТ Р ИСО/МЭК 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности».
3. ISO/IEC 15408 – Общие критерии и методология оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-1, 2, 3-2008.
4. Международные стандарты ISO серий 9000 (качество) и 14000 (экология).
5. Международные и отечественные стандарты обеспечения непрерывности бизнеса.

Тема 4. Отраслевые стандарты в области управления информационной безопасностью (семинар).
1. Стандарты, направленные на минимизацию рисков (ГОСТ Р 53647).
2. Стандарты банковской системы Российской Федерации (СТО БР ИББС).
3. Комплекс документов по обеспечению и поддержанию ИБ организаций банковской системы.
4. Аудит ИБ.

Раздел 2. Управление и система управления информационной безопасностью

Тема 5. Анализ рисков информационной безопасности (семинар).
1. Основные понятия управления рисками. Термины и определения.
2. Основные этапы управления рисками
   - 2.1. Выбор методологии оценки рисков
   - 2.2. Идентификация активов
   - 2.3. Анализ угроз и их последствий
   - 2.4. Выявление уязвимых мест в защите
   - 2.5. Оценка рисков
   - 2.6. Выбор защитных мер
   - 2.7. Реализация и проверка выбранных мер
   - **2.8.** Оценка остаточного риска

Тема 6. Система управления информационной безопасностью
1. Система управления информационной безопасности организации (СУИБ).
2. Основные функции и компоненты СУИБ организации.
3. Область действия СУИБ.
4. Документальное обеспечение СУИБ. Состав документации СУИБ.
5. Использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СУИБ (СМИБ) организации.
6. Основные этапы создания СУИБ (инвентаризация и категорирование активов; оценка защищенности информационной системы; оценка и обработка информационных рисков; контроль выполнения и эффективности выбранных мер).

Тема 7. Политика информационной безопасности предприятия
1. Основные понятия политики информационной безопасности (ПИБ) организации.
2. Содержание ПИБ организации.
3. Область применения ПИБ.
4. Понятие ПИБ «в широком» и «в узком» смыслах.
5. «Частные» ПИБ.
6. Стратегии действий на нарушения безопасности.

Тема 8. План защиты информационных ресурсов от несанкционированного доступа
1. Назначение и основные положения Плана защиты информационных ресурсов от НСД.
2. Обязанности руководителя и сотрудников ОИБ по предупреждению, реагированию и ликвидации последствий нарушений безопасности.
3. Распределение обязанностей между администраторами ИС.
4. Требования безопасности, предъявляемые к пользователям ИС.
5. Основные мероприятия, формальные процедуры и другие технологические процессы по обеспечению ИБ.
6. Выявление попыток НСД.
7. Реагирование на нарушения информационной безопасности.
8. Ликвидация последствий НСД.

Тема 9. План обеспечения непрерывной работы и восстановления работоспособности информационной системы

1. Понятие управления непрерывности бизнеса.
2. Процесс управление непрерывностью бизнеса (УНБ).
3. Система управления непрерывностью бизнеса (СУНБ).
4. Ключевые компоненты СУНБ.
5. Внедрение управления непрерывностью бизнеса в культуру организации.
6. Программа непрерывного образования и информирования об УНБ.
7. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса.
8. Примерное содержание плана обеспечения непрерывности бизнеса. План восстановления бизнеса.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторные работы не предусмотрены учебным планом дисциплины.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

8.2. Примерная тематика рефератов:

1. Стратегия национальной безопасности Российской Федерации о месте и роли информационной безопасности.
2. Доктрина информационной безопасности Российской Федерации о проблемах информационной безопасности.
3. Серия стандартов ISO/IEC 27000
4. Стандарты на отдельные процессы управления информационной безопасностью
5. Отраслевые стандарты в области управления информационной безопасностью
6. Анализ рисков информационной безопасности
7. Система управления информационной безопасностью
8. Система управления инцидентами информационной безопасности
9. Политика информационной безопасности предприятия
10. Частные политики информационной безопасности предприятия
11. Структура плана защиты информационных ресурсов предприятия от несанкционированного доступа
12. Структура плана обеспечения непрерывной работы и восстановления работоспособности информационной системы

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 диплом-ных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Понятия: системы, системного подхода, процесса, процессного подхода, управления, информационной безопасности.
2. Процессный подход к управлению организации. Управление информационной безопасностью.
3. Роль стандартов информационной безопасности для решения проблемы ИБ.
4. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности».
5. Методы обеспечения безопасности». Международные стандарты информационной безопасности. Управление информационной безопасностью. Общие критерии безопасности информационных технологий.
6. Основные отечественные стандарты безопасности информационных технологий.
7. ISO/IEC 13335-Методы и средства обеспечения безопасности информационных технологий.
8. ГОСТ Р ИСО/МЭК 13335-1-2006, ГОСТ Р ИСО/МЭК 13335-3-2007, ГОСТ Р ИСО/МЭК 13335-4-2007, ГОСТ Р ИСО/МЭК 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности».
9. ISO/IEC 15408 – Общие критерии и методология оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-1, 2, 3-2008.
10. Международные стандарты ISO серий 9000 (качество) и 14000 (экология).
11. Критерии оценки безопасности информационных систем.
12. Международные и отечественные стандарты обеспечения непрерывности бизнеса.
13. Стандарты, направленные на минимизацию рисков (ГОСТ Р 53647).
14. Стандарты банковской системы Российской Федерации (СТО БР ИББС).
15. Комплекс документов по обеспечению и поддержанию ИБ организаций банковской системы.
16. Аудит ИБ.
17. Основные понятия управления рисками. Термины и определения.
18. Основные этапы управления рисками
19. Система управления информационной безопасности организации (СУИБ).
20. Основные функции и компоненты СУИБ организации.
21. Область действия СУИБ.
22. Документальное обеспечение СУИБ. Состав документации СУИБ.
23. Использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СУИБ (СМИБ) организации.
24. Основные этапы создания СУИБ (инвентаризация и категорирование активов; оценка защищенности информационной системы; оценка и обработка информационных рисков; контроль выполнения и эффективности выбранных мер).
25. Основные понятия политики информационной безопасности (ПИБ) организации.
26. Содержание ПИБ организации.
27. Область применения ПИБ.
28. Понятие ПИБ «в широком» и «в узком» смыслах.
29. «Частные» ПИБ.
30. Стратегии действий на нарушения безопасности.
31. Назначение и основные положения Плана защиты информационных ресурсов от НСД.
32. Обязанности руководителя и сотрудников ОИБ по предупреждению, реагированию и ликвидации последствий нарушений безопасности.

33. Распределение обязанностей между администраторами ИС.
34. Требования безопасности, предъявляемые к пользователям ИС.
35. Основные мероприятия, формальные процедуры и другие технологические процессы по обеспечению ИБ.
36. Выявление попыток НСД.
37. Реагирование на нарушения информационной безопасности.
38. Ликвидация последствий НСД.
39. Понятие управления непрерывности бизнеса.
40. Процесс управление непрерывностью бизнеса (УНБ).
41. Система управления непрерывностью бизнеса (СУНБ).
42. Ключевые компоненты СУНБ.
43. Внедрение управления непрерывностью бизнеса в культуру организации.
44. Программа непрерывного образования и информирования об УНБ.
45. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса.
46. Примерное содержание плана обеспечения непрерывности бизнеса. План восстановления бизнеса.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Стандартизация систем и процессов управления информационной безопасностью **Тема 1.** Управление информационной безопасностью. Основные понятия	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, на семинарах, зачет
Раздел 1. Тема 2. Серия стандартов ISO/IEC 27000	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, на семинарах, зачет
Раздел 1. Тема 3. Стандарты на отдельные процессы управления информационной безопасностью	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, на семинарах, зачет
Раздел 1. Тема 4. Отраслевые стандарты в области управления информационной безопасностью	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, на семинарах, зачет
Раздел 2. Управление и система управления информационной безопасностью Тема 5. Анализ рисков информационной без-	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятием, на семинарах, зачет

опасности			
Раздел 2. Тема 6. Система управления информационной безопасностью	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятием, на семинарах, зачет
Раздел 2. Тема 7. Политика информационной безопасности предприятия	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятием, на семинарах, зачет
Раздел 2. Тема 8. План защиты информационных ресурсов от несанкционированного доступа	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятием, на семинарах, зачет
Раздел 2. Тема 9. План обеспечения непрерывной работы и восстановления работоспособности информационной системы	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятием, на семинарах, зачет

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268

2. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703

дополнительная

1. Шилов, А. К. Управление информационной безопасностью: учебное пособие / Шилов А. К. - Ростов н/Д: Изд-во ЮФУ, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785927527427.html

2. Газизов, А. Р. Управление информационной безопасностью : учебное пособие / А. Р. Газизов, С. Б. Петренкова, Д. В. Фатхи. — Ростов-на-Дону : Донской государственный технический университет, 2019. — 115 с. — ISBN 978-5-7890-1775-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/117771.html

3. Дронова, Г. А. Управление информационной безопасностью : учеб. -метод. пособие / Дронова Г. А. - Новосибирск : Изд-во НГТУ, 2016. - 28 с. - ISBN 978-5-7782-3113-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785778231139.html

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Управление информационной безопасностью» для студентов специалитета по специальности 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл: 329 КБ) — URL: http://lib.ulsu.ru/MegaPro/Download/MObject/4967

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. /  / 04.05.2023 /
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 системы1.

Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

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

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека»

АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Инженер ведущий	Щуренко Ю.В.		04.05.2023
Должность сотрудника УИТТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций: 3/317, 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.	Утверждение РПД и ФОС для набора 2023 года (10.05.01 и 10.05.03). Актуализация РПД и ФОС для наборов 2022 года 10.05.01 и 10.05.03 (без изменений)	Андреев А.С.		12.04.2023 Протокол заседания кафедры № 12
2.	Утверждение РПД и ФОС для набора 2024 года (10.05.03). Актуализация РПД и ФОС для наборов 2023 года 10.05.01 и 10.05.03 (без изменений)	Андреев А.С.		15.04.2024 Протокол заседания кафедры № 10