

**УТВЕРЖДЕНО**

решением Ученого совета факультета математики,  
информационных и авиационных технологий

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

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

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

Специализация: "Безопасность открытых информационных систем"  
*полное наименование*


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

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

Программа актуализирована на заседании кафедры: протокол № 12 от 12.05.2021 г.  
Программа актуализирована на заседании кафедры: протокол № 13 от 11.05.2022 г.  
Программа актуализирована на заседании кафедры: протокол № 12 от 12.04.2023 г.  
Сведения о разработчиках:

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

<b>СОГЛАСОВАНО</b>
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
  (подпись) / <u>Андреев А.С.</u> / (Ф.И.О.)
« <u>10</u> » <u>06</u> 20 <u>20</u> г.

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

## 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

Дисциплина относится к базовой части цикла Б1.Б образовательной программы и читается в 6-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»; «Защита интеллектуальной собственности», «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»; «Безопасность операционных систем»; «Разработка и эксплуатация защищённых автоматизированных систем»; «Криптографические методы защиты информации»; «Криптографические протоколы».


## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ 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
ОК-6 – способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Знать: социальные, культурные и иные различия при работе в коллективе Уметь: работать в коллективе, толерантно воспринимая социальные, культурные и иные различия Владеть: Навыками работы в коллективе
ОПК-1 – способностью анализировать физические явления и процессы, применять	Знать: соответствующий математический аппарат для

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


соответствующий математический аппарат для формализации и решения профессиональных задач	<p>формализации и решения профессиональных задач</p> <p>Уметь:</p> <p>применять математический аппарат для формализации и решения профессиональных задач</p> <p>Владеть:</p> <p>Навыками применения математического аппарата для формализации и решения профессиональных задач</p>
ОПК-2 – способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	<p>Знать:</p> <p>соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники</p> <p>Уметь:</p> <p>Применять соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники</p> <p>Владеть:</p> <p>Навыками применения соответствующего математического аппарата, в том числе с использованием вычислительной техники</p>
ОПК-5 – способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ОПК-6 – способностью применять нормативные правовые акты в профессиональной деятельности	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>

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


ПК-1 - способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-7 – способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-8 – способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-11 – способностью разрабатывать политику информационной безопасности автоматизированной системы	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-12 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>

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

ПК-13 – способностью участвовать в проектировании средств защиты информации автоматизированной системы	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-14 – способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-18 – способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-21 – способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>

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

ПК-22 – способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-24 – способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-25 – способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>
ПК-28 – способностью управлять информационной безопасностью автоматизированной системы	<p>Знать:</p> <p>требования и основные характеристики информационной безопасности;</p> <p>Уметь:</p> <p>эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах</p> <p>Владеть:</p> <p>терминологией теории информационной безопасности</p>

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


#### 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	54	*54/54		
Аудиторные занятия:	54	*54/54		
Лекции	18	*18/18		
Практические и семинарские занятия	36	*36/36		
Лабораторные работы (лабораторный практикум)				
Самостоятельная работа	54	54		
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.


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

### 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			
1	2	3	4	5	6	7	8
<b>Раздел 1. Стандартизация систем и процессов управления информационной безопасностью</b>							
1. Управление информационной безопасностью. Основные понятия		2	2			4	Тесты Т1, реф. 1, 2
2. Серия стандартов ISO/IEC 27000 2/5		2	2			4	Тесты Т2 (5), реф. 3
3. Стандарты на отдельные процессы управления информационной безопасностью		2	2			4	Тесты Т3 (5), реф. 4
4. Отраслевые стандарты в области управления информационной безопасностью		2	2			4	Тесты Т4 (5), реф. 5
<b>Раздел 2. Управление и система управления информационной безопасностью</b>							
5. Анализ рисков информационной безопасности 2/7		2	6		6	8	Тесты Т5 (7), реф. 6
6. Система управления информационной безопасностью 2/6		2	4			6	Тесты Т6, реф. 7,8
7. Политика информационной безопасности предприятия 2/9		2	10		10	12	Тесты Т7 (9), реф. 9,10
8. План защиты информационных ресурсов от несанкционированного доступа 2/10		2	4			6	Тесты Т8 (10), реф. 11
9. План обеспече-		2	4		2	6	Тесты Т9 (11),



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

ния непрерывной работы и восстановления работоспособности информационной системы 2/11							реф. 12
Итого	108	18	36		18	54	

## 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).

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

### **Тема 7. Политика информационной безопасности предприятия**

Основные понятия политики информационной безопасности (ПИБ) организации. Содержание 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.

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

**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.

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

## 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 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](ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf).

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

## 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.

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


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
<b>Раздел 1. Стандартизация систем и процессов управления информационной безопасностью</b> Тема 1. Управление информационной безопасностью. Основные понятия	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятием, на семинарах, зачет
<b>Раздел 1. Тема 2.</b> Серия стандартов ISO/IEC 27000	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятием, на семинарах, зачет
<b>Раздел 1. Тема 3.</b> Стандарты на отдельные процессы управления информационной безопасностью	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятием, на семинарах, зачет
<b>Раздел 1. Тема 4.</b> Отраслевые стандарты в области управления информационной безопасностью	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, на семинарах, зачет
<b>Раздел 2. Управление и система управления информационной безопасностью</b> Тема 5. Анализ рисков информационной без-	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	8	Тесты перед занятием, на семинарах, зачет

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

опасности			
<b>Раздел 2. Тема 6.</b> Система управления информационной безопасностью	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	6	Тесты перед занятием, на семинарах, зачет
<b>Раздел 2. Тема 7.</b> Политика информационной безопасности предприятия	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	12	Тесты перед занятием, на семинарах, зачет
<b>Раздел 2. Тема 8.</b> План защиты информационных ресурсов от несанкционированного доступа	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	6	Тесты перед занятием, на семинарах, зачет
<b>Раздел 2. Тема 9.</b> План обеспечения непрерывной работы и восстановления работоспособности информационной системы	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	6	Тесты перед занятием, на семинарах, зачет

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

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Список рекомендуемой литературы

#### основная

1. Курило, А. П. Основы управления информационной безопасностью: учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Вып. 1. - Москва: Горячая линия - Телеком, 2013. - 244 с. (Серия "Вопросы управления информационной безопасностью"). - ISBN 978-5-9912-0271-8. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL:

<https://www.studentlibrary.ru/book/ISBN9785991202718.html>

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://www.biblio-online.ru/bcode/449285>

#### 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. 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>

#### учебно-методическая

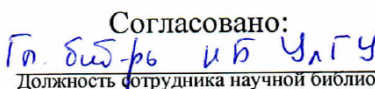
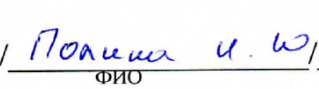
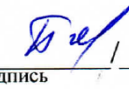
1. Дронова, Г. А. Управление информационной безопасностью: учеб. -метод. пособие / Дронова Г. А. - Новосибирск: Изд-во НГТУ, 2016. - 28 с. - ISBN 978-5-7782-3113-9. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL:

<https://www.studentlibrary.ru/book/ISBN9785778231139>.

2. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск: УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). URL: <http://edu.ulsu.ru/courses/750/interface/>.

3. **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). - Текст: электронный.


<http://lib.ulsu.ru/MegaPro/Download/MObject/4967>

Согласовано:  
 /  /  / 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.



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

## 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](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://ebco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741>. – Режим доступа : для авториз. пользователей. – Изображение: электронные.

### 6. Федеральные информационно-образовательные порталы:

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

6.2. **Российское образование** : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://www.edu.ru>. – Текст : электронный.

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

**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 зарегистрир. пользователей. – Текст: электронный.

Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

Клочкова А.В.  
ФИО

 05.06.2020  
подпись дата

**12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:**

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

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

**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:

  
подпись




доцент кафедры

должность

Иванцов Андрей Михайлович

ФИО

## ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/вы- пускающей кафедрой	Подпись	Дата
1.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 1	Андреев А.С.		12.05.2021 Протокол заседания кафедры № 12
2.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 2	Андреев А.С.		11.05.2022 Протокол заседания кафедры № 13
3.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 3	Андреев А.С.		12.04.2023 Протокол заседания кафедры № 12

**в) Профессиональные базы данных, информационно-справочные системы**

**1. Электронно-библиотечные системы:**

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

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

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

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

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

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

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

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

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

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

**3. Базы данных периодических изданий:**

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

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

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

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

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

**6. Федеральные информационно-образовательные порталы:**

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



**в) Профессиональные базы данных, информационно-справочные системы****1. Электронно-библиотечные системы:**

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2022]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2022]. - URL: <https://urait.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2022]. – URL: <https://www.studentlibrary.ru/cgi-bin/mb4x>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2022]. – URL: <https://www.rosmedlib.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2022]. – URL: <https://www.books-up.ru/ru/library/>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2022]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2022]. - URL: <http://znanium.com>. – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

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

1.9. База данных «Русский как иностранный» : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2022]. – URL: <https://ros-edu.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

**2. КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2022].

**3. Базы данных периодических изданий:**

3.1. База данных периодических изданий EastView : электронные журналы / ООО ИВИС. - Москва, [2022]. – URL: <https://dlib.eastview.com/browse/udb/12>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2022]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД Гребенников. – Москва, [2022]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

**4. Федеральная государственная информационная система «Национальная электронная библиотека»** : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2022]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

**5. SMART Imagebase** : научно-информационная база данных EBSCO // EBSCOhost

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

**6. Федеральные информационно-образовательные порталы:**

6.1. [Единое окно доступа к образовательным ресурсам](http://window.edu.ru/) : федеральный портал . – URL: <http://window.edu.ru/> . – Текст : электронный.

6.2. [Российское образование](http://www.edu.ru) : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: <http://www.edu.ru>. – Текст : электронный.

**7. Образовательные ресурсы УлГУ:**

7.1. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

/ Клочкова А.В.  
ФИО

  
подпись

/  
дата

**в) Профессиональные базы данных, информационно-справочные системы**

**1. Электронно-библиотечные системы:**

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

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

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

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

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

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

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

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

**3. Базы данных периодических изданий:**

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

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

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

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

**6. Электронная библиотечная система УлГУ** : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.