


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



**УТВЕРЖДЕНО**

решением Ученого совета ФМИАТ

от «17» мая 2022 г., протокол № 4/22

Председатель Волков М.А.

(подпись, расшифровка подписи)

«17» мая 2022 г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Сертификация средств защиты информации
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

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 2022 г.

Программа актуализирована на заседании кафедры: протокол № 13 от 11 мая 2022 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
Перцева Ирина Анатольевна	ИБ иТУ	Доцент, к.ф.-м.н.

СОГЛАСОВАНО

Заведующий выпускающей кафедрой  
«Информационная безопасность и теория  
управления»

 / Андреев А.С. /  
*(подпись) (Ф.И.О.)*

« 11 » 05 2022 г.

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

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### Цели освоения дисциплины:

Учебная дисциплина «Сертификация средств защиты информации» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью освоения дисциплины «Сертификация средств защиты информации» является формирование у студентов знаний по основам организации сертификации средств защиты информации по требованиям безопасности информации, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач сертификации по требованиям безопасности информации с учетом требований системного подхода.

### Задачи освоения дисциплины:

Основные задачи дисциплины – дать знания:

- по основам сертификации по требованиям безопасности информации;
- по основам проведения сертификационных испытаний;
- по программным средствам сертификационных испытаний и анализа безопасности программного кода;
- по методическому обеспечению сертификации по требованиям безопасности информации.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО


Дисциплина «Сертификация средств защиты информации» изучается в 8 семестре и относится к вариативной части дисциплин блока Б1 специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Курс учебной дисциплины тесно связан с другими учебными дисциплинами, в первую очередь с курсами «Криптографические методы защиты информации», «Безопасность операционных систем», «Безопасность вычислительных сетей», позволяющими понять физическую сущность процесса сертификации по требованиям безопасности информации.

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

- знание базовых понятий в области 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: «Разработка и эксплуатация автоматизированных систем в защищенном исполнении», «Аттестация объектов информатизации», при прохождении технологической, преддипломной практик, выполнении научно-исследовательской работы.

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

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
1	2
ПК-1 - Способен организовать работы по выполнению в информационной системе требований защиты информации ограниченного доступа	<p><b>Знать:</b> Источники и классификацию угроз информационной безопасности Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Нормативные правовые акты в области защиты информации</p> <p><b>Уметь:</b> Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации Организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты Организовывать процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях</p> <p><b>Владеть:</b> Навыками организации применения защищенных протоколов, межсетевых экранов и средств обнаружения вторжений для защиты информации в сетях Навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем</p>
ПК-2 - Способен осуществлять тестирование систем защиты информации автоматизированных систем	<p><b>Знает:</b> Принципы построения и функционирования систем и сетей передачи информации Эталонную модель взаимодействия открытых систем Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах</p> <p><b>Умеет:</b> Применять действующую нормативную базу в области обеспечения безопасности информации Контролировать безотказное функционирование технических средств защиты информации</p> <p><b>Владеет:</b> Навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем</p>
ПК-3 - Способен раз-	<b>Знать:</b>

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


рабатывать проектные решения по защите информации в автоматизированных системах	<p>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</p> <p>Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов</p> <p>Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем</p> <p>Принципы формирования политики информационной безопасности в автоматизированных системах</p> <p><b>Уметь:</b></p> <p>Применять действующую нормативную базу в области обеспечения защиты информации</p> <p>Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты</p> <p>Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе</p> <p><b>Владеть:</b></p> <p>Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации</p> <p>Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах</p>
---	---

#### 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 2.

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

Вид учебной работы	Количество часов (форма обучения <u>очная</u> )	
	Всего по плану	В т.ч. по семестрам
		8 семестр
Контактная работа обучающихся с преподавателем	54/54*	54/54*
Аудиторные занятия:	54/54*	54/54*
Лекции	18/18*	18/18*
Практические и семинарские занятия	-	-
Лабораторные работы (лабораторный практикум)	36/36*	36/36*
Самостоятельная работа	18	18
Форма текущего контроля знаний и контроля самостоятельной работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не		- вопросы при защите лабораторных работ - рефераты на заданные темы

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


Вид учебной работы	Количество часов (форма обучения <u>очная</u> )	
	Всего по плану	В т.ч. по семестрам 8 семестр
менее 2 видов)		
Курсовая работа	---	---
Виды промежуточной аттестации (экзамен, зачет)	зачет	зачет
Всего часов по дисциплине:	72	72

\* 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 очная

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			
<b>Раздел 1. Основы сертификации средств защиты информации по требованиям безопасности информации</b>							
1. Виды и системы сертификации	8	2			2	2	Тесты Т1, реферат № 1)
2. Участники и порядок сертификации по требованиям защиты информации	8	2			2	2	Тесты Т2, реферат (№ 2,3)
3. Руководящие документы ФСТЭК России	6	2			2	2	Тесты Т3, реферат (№ 5,10)
<b>Раздел 2. Порядок проведения сертификации средств защиты информации</b>							
4. Сертификация средств вычислительной техники (СВТ) по требованиям защищенности от НСД к информации	14	2		8	2	2	Тесты Т4, реферат (№ 7,9)
5. Сертификация программного обеспечения по требованиям безопасности информации	10	2			2	2	Тесты Т5, реферат (№ 3,7)

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

6. Сертификация по требованиям безопасности информации по «Общим критериям»	18	2		8	2	2	Тесты Т6, реферат (№ 2,6)
<b>Раздел 3. Методы и средства проведения сертификационных испытаний</b>							
7. Применение автоматизированных средств	16	2		8	2	2	Тесты Т7, реферат (№ 1,2), лаб. раб № 1,2
8. Порядок проведения сертификационных испытаний	10	2		4	2	2	Тесты Т8, реферат (№ 3), лаб. раб № 3
9. Проверка производства сертифицированных средств защиты информации	14	2		8	2	2	Тесты Т9, реферат (№ 4,8), лаб. раб № 4,5,6
Итого:	108	18		36	18	18	

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### Раздел 1. Основы сертификации средств защиты информации по требованиям безопасности информации

#### Тема 1. Виды и системы сертификации

Назначение сертификации по требованиям защиты информации. Законодательно-правовые основы сертификации. Обязательность сертификации. Ответственность разработчиков средств защиты информации за сертификацию программных, аппаратно-программных и аппаратных средств.

#### Тема 2. Участники и порядок сертификации по требованиям защиты информации

Особенности систем сертификации ФСТЭК России, Минобороны России, ФСБ России, СВР России. Виды сертификационных испытаний средств защиты информации и автоматизированных систем в защищенном исполнении. Инструментальная база сертификационных испытаний.

#### Тема 3. Руководящие документы ФСТЭК России

Классификация АС. Показатели защищенности от несанкционированного доступа. Классификация по уровню контроля отсутствия недеklarированных возможностей. Сертификация по стандарту ГОСТ ИСО/МЭК 15408.

### Раздел 2. Порядок проведения сертификации средств защиты информации


#### Тема 4. Сертификация средств вычислительной техники (СВТ) по требованиям защищенности от НСД к информации

Показатели защищенности СВТ. Порядок проведения сертификационных испытаний на соответствие классам защищенности СВТ. Отчетность по результатам испытаний.

#### Тема 5. Сертификация программного обеспечения по требованиям безопасности информации

Выбор требуемого класса защищенности и уровня контроля отсутствия НДВ. Сертификация ПО в информационных системах, обрабатывающих персональные данные. Сертификация на соответствие техническим условиям.

#### Тема 6. Сертификация по требованиям безопасности информации по «Общим

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

критериям»

Определение системы оценки. Оценочные уровни доверия. Функции безопасности объекта оценки (ОО). Разработка задания по безопасности (ЗБ). Разработка профиля защиты (ПЗ).

### **Раздел 3. Методы и средства проведения сертификационных испытаний**

#### **Тема 7. Применение автоматизированных средств**

Программное средство сертификационных испытаний на отсутствие НДВ «АК-ВС». Программа фиксации и контроля исходного состояния ПО «ФИКС». Средство для проведения инспекционного контроля «ПИК-Эшелон». Статический анализ программного кода. Динамический анализ программного кода.

#### **Тема 8. Порядок проведения сертификационных испытаний**

Порядок оформления заявки регулятору на сертификацию средств защиты информации. Порядок оформления решения о проведении сертификации средств защиты информации. Оформление акта отбора образца. Перечень документации, представляемой в испытательную лабораторию. Порядок получения сертификата соответствия, приложений к сертификату. Применение знака соответствия.

#### **Тема 9. Проверка производства сертифицированных средств защиты информации**

Исходные данные для проведения предварительной проверки производства (ППП). Порядок работы комиссии по ППП. Разработка акта ППП. Утверждение акта ППП у регулятора. Инспекционный контроль.

## **6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ**

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Семинарские занятия не предусмотрены учебным планом дисциплины.

## **7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)**

### **Раздел 2. Порядок проведения сертификации средств защиты информации**

**Тема 4.** Сертификация средств вычислительной техники (СВТ) по требованиям защищенности от НСД к информации

Лабораторная работа № 1 (4 часа). «Проведение проверки реализации дискреционного и мандатного принципов контроля доступа».

Цель работы: Получение практических навыков проверки реализации дискреционного и мандатного принципов контроля доступа.

Методические указания: основное внимание должно быть уделено практическим навыкам по проверке реализации дискреционного и мандатного принципов контроля доступа.

Лабораторная работа № 2 (4 часа). «Проведение испытаний экспертно-документальным методом и методом функционального тестирования».

Цель работы: Получение практических навыков по проведению испытаний экспертно-документальным методом и методом функционального тестирования.


Методические указания: основное внимание должно быть уделено практическим навыкам по проведению испытаний экспертно-документальным методом и методом функционального тестирования.

### **Раздел 3. Методы и средства проведения сертификационных испытаний**

**Тема 6.** Сертификация по требованиям безопасности информации по «Общим критериям»

Лабораторная работа № 3 (4 часа). «Разработка ЗБ».

Цель работы: Получение практических навыков по разработке ЗБ в соответствии с

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

ГОСТ ИСО/МЭК 15408.

Методические указания: основное внимание должно быть уделено практическим навыкам по разработке ЗБ.

Лабораторная работа № 4 (4 часа). «Разработка ПЗ».

Цель работы: Получение практических навыков по разработке ПЗ в соответствии с ГОСТ ИСО/МЭК 15408.

Методические указания: основное внимание должно быть уделено практическим навыкам по разработке ПЗ.

**Тема 7.** Применение автоматизированных средств

Лабораторная работа № 5 (4 часа). «Работа с программным средством сертификационных испытаний на отсутствие НДВ «АК-ВС».

Цель работы: с программным средством сертификационных испытаний на отсутствие НДВ «АК-ВС» изучение правил его эксплуатации в соответствии с руководством».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с «АК-ВС».

Лабораторная работа № 6. (2 часа). «Ознакомление с программой фиксации и контроля исходного состояния ПО «ФИКС».

Цель работы: Получение практических навыков в работе с программой фиксации и контроля исходного состояния ПО «ФИКС».

Методические указания: основное внимание должно быть уделено практическим навыкам работы с программой «ФИКС».

Лабораторная работа № 7. (2 часа). «Ознакомление со средством для проведения инспекционного контроля «ПИК-Эшелон».

Цель работы: Получение практических навыков в работе со средством для проведения инспекционного контроля «ПИК-Эшелон».

Методические указания: основное внимание должно быть уделено практическим навыкам работы со средством для проведения инспекционного контроля «ПИК-Эшелон».

**Тема 8.** Порядок проведения сертификационных испытаний

Лабораторная работа № 8 (4 часа). «Оформление пакета документов для сертификации средств защиты информации».

Цель работы: Получить навыки оформления документов для сертификации средств защиты информации.

Методические указания: основное внимание должно быть уделено практическим навыкам оформления документов для сертификации средств защиты информации.

**Тема 9.** Проверка производства сертифицированных средств защиты информации

Лабораторная работа № 9 (4 часа). «Оформление пакета документов для предварительной проверки производства программных средств защиты информации».


Цель работы: Получить навыки оформления документов для предварительной проверки программных производства средств защиты информации.

Методические указания: основное внимание должно быть уделено практическим навыкам оформления документов для предварительной проверки производства программных средств защиты информации.

Лабораторная работа № 10 (4 часа). «Оформление пакета документов для предварительной проверки производства аппаратно-программных средств защиты информации».

Цель работы: Получить навыки оформления документов для предварительной проверки аппаратно-программных производства средств защиты информации.



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

Методические указания: основное внимание должно быть уделено практическим навыкам оформления документов для предварительной проверки производства аппаратно-программных средств защиты информации.

Все лабораторные работы проводятся в интерактивной форме, а именно используются:

диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами, группами студентов;

элементы деловых игр, «мозговой штурм» или дискуссии по рассматриваемым вопросам.

## **8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ**

**8.1** Контрольные работы не предусмотрены учебным планом дисциплины.

### **8.2 Примерная тематика рефератов:**

1. Особенности сертификации АС в защищенном исполнении
2. Особенности сертификации межсетевых экранов (МЭ)
3. Виды и системы сертификации
4. Аппаратно-программные средства проведения сертификационных испытаний
5. Принципы работы с программой Miranda IM
6. Выявление уязвимостей программного кода
7. Аудит безопасности программных систем
8. Принципы работы средства контроля «ФИКС»
9. Принципы работы средств автоматизации процесса тестирования «Ревизор»
10. Принципы работы средств для анализа памяти ПЭВМ типа «Terrier»

#### **8.2.1 Правила оформления рефератов**


1. Объем 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. Рацев. – 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).

#### **8.3 Примерная тематика курсовых работ:**

Данный вид работы не предусмотрен учебным планом дисциплины.

## **9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ**


1. Законодательно-правовые основы сертификации
2. Обязательность сертификации
3. Особенности систем сертификации различных регуляторов
4. Виды сертификационных испытаний средств защиты информации и автоматизированных систем в защищенном исполнении
5. Инструментальная база сертификационных испытаний
6. Классификация АС
7. Показатели защищенности от несанкционированного доступа
8. Классификация по уровню контроля отсутствия недеklarированных возможностей
9. Показатели защищенности АС
10. Сертификация по стандарту ГОСТ ИСО/МЭК 15408

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


11. Показатели защищенности СВТ
12. Порядок проведения сертификационных испытаний на соответствие классам защищенности СВТ
13. Выбор требуемого класса защищенности и уровня контроля отсутствия НДВ
14. Статический анализ программного кода
15. Динамический анализ программного кода
16. Основные факторы обеспечения защиты информации от угроз утечки информации
17. Классификация направлений и методов инженерно-технической защиты информации
18. Порядок проведения сертификационных испытаний
19. Проверка производства сертифицированных средств защиты информации
20. Принципы работы изделия «АК-ВС»
21. Порядок разработки ЗБ
22. Порядок разработки ПЗ

### 10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Основы сертификации средств защиты информации по требованиям безопасности информации Тема 1. Виды и системы сертификации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед лекцией, зачет
Раздел 1. Тема 2. Участники и порядок сертификации по требованиям защиты информации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед лекцией, зачет
Раздел 1. Тема 3. Руководящие документы ФСТЭК России	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед лекцией, зачет
Раздел 2. Порядок проведения сертификации средств защиты информации Тема 4. Сертификация средств вычислительной техники (СВТ) по требованиям защищенности от НСД к информации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед лекцией, зачет
Раздел 2. Тема 5. Сертификация программного обеспечения по требованиям безопасности информации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед лекцией, зачет
Раздел 2. Тема 6. Сертификация по требованиям безопасности информации по «Общим критериям»	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед лекцией, эзачет
Раздел 3. Методы и средства проведения сертификационных испытаний Тема 7. Применение автоматизированных средств	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче зачета	2	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, зачет

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

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 3. Тема 8. Порядок проведения сертификационных испытаний	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче зачета	2	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, зачет
Раздел 3. Тема 9. Проверка производства сертифицированных средств защиты информации	Подготовка к занятию, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче зачета	2	Тесты перед лекцией, тесты на семинаре, вопросы на лабораторной работе, зачет

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

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Список рекомендуемой литературы:

#### основная

1. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991204705.html>

2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образова-тельная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/467370>

#### дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

2.1 Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне». Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_2481/](http://www.consultant.ru/document/cons_doc_LAW_2481/)

2.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации». - URL : [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/)

2.3 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации").- URL : [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_208191/](http://www.consultant.ru/document/cons_doc_LAW_208191/)

2.4 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - URL : [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_147084/](http://www.consultant.ru/document/cons_doc_LAW_147084/)


3. Нерсисянц, А. А. Защита информации : учебное пособие / А. А. Нерсисянц. — Ростов-на-Дону : Северо-Кавказский филиал Московского технического университета связи и информатики, 2010. — 61 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/61295.html>


4. Гродзенский, Я. С. Информационная безопасность : учебное пособие / Гродзенский Я. С. - Москва : РГ-Пресс, 2020. - 144 с. - ISBN 978-5-9988-0845-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785998808456.html>

#### учебно-методическая

1. Методические указания для самостоятельной работы студентов по дисциплине «Сертификация средств защиты информации» для студентов специалитета по специальности 10.05.03 очной формы обучения / А. С. Корсунский; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2020. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 295 КБ). - URL : <http://lib.ulsu.ru/MegaPro/Download/MObject/8173>

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. /  / 04.05.2022 /  
должность сотрудника научной библиотеки ФИО подпись дата

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

## 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. 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.

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

– 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** : федеральный портал . – URL: <http://window.edu.ru/> . – Текст : электронный.

6.2. **Российское образование** : 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

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

## 12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций – 3/316, 2/26, 3/420, семинарских, лабораторных занятий: 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

\_\_\_\_\_  
должность

доцент

Перцева Ирина Анатольевна  
ФИО