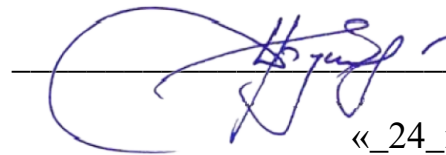


Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной  
образовательной программы



Буинцев Д.Н.

«\_24\_» сентября 2024 г

**РАБОЧАЯ ПРОГРАММА**

Дисциплины

*Б1.В.ДВ.01.01 Защита конфиденциальной информации в организации*

Уровень высшего образования

**БАКАЛАВРИАТ**

Направление подготовки

*10.03.01 Информационная безопасность*

профиль

*Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)*

Квалификация

*Бакалавр*

Форма обучения

***очная***

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск  
2024

Рабочая программа дисциплины Б1.В.ДВ.01.01 Защита конфиденциальной информации в организации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

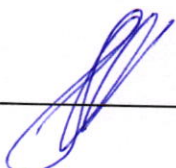
Программу составил(и):

О.С. Корнева, доцент кафедры информатики,  
кандидат педагогических наук



Рабочая программа дисциплины Б1.В.ДВ.01.01 Защита конфиденциальной информации в организации утверждена на заседании кафедры информатики, протокол № 8 от 19.03.2024 г.

Исполняющий обязанности  
заведующего кафедрой информатики



Осипов Г.С.

## 1. Цель и задачи дисциплины

### Цель дисциплины

Целью дисциплины «Защита конфиденциальной информации в организации» является обучение приемам и методам работы с конфиденциальной информацией в организациях; владение навыками применения комплексного подхода к обеспечению информационной безопасности конфиденциальных документов.

### Задачи дисциплины

- Изучение правил и нормативных документов реализации политики информационной безопасности по защите и обработке конфиденциальных документов.
- Развитие знаний и умений в области документооборота при обращении с конфиденциальной информацией, анализировать возможные пути утечки информации и принимать меры по их устранению.
- Формирование компетенций в области сбора и анализа исходных данных для проектирования средств обеспечения информационной безопасности.
- Обеспечение условий для активизации познавательной деятельности студентов и формирования у них практического опыта работы с системами защиты конфиденциальной информации.

## 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ДВ.01.01 Защита конфиденциальной информации организации относится к дисциплинам по выбору блока 1 «Дисциплины (модули)» учебного плана направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)».

**Пререквизиты дисциплины:** «Основы информационной безопасности», «Системы электронного документооборота», «Организационно и правовое обеспечение информационной безопасности»

**Постреквизиты дисциплины:** «Защита персональных данных в организации», «Программно-аппаратные средства защиты информации», «Комплексное обеспечение защиты информации объекта информатизации», «Выполнение и защита выпускной квалификационной работы».

## 3. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС–2	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ПКС-2.1 Знать способы решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации. ПКС-2.2 Уметь решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации ПКС-2.3 Иметь навыки решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации
ПКС–3	Способен осуществлять управление средствами	ПКС-3.1 Знать программно-аппаратные средства защиты информации, современные подходы к

	защиты информации, в том числе осуществляющими непрерывный мониторинг защищенности автоматизированных систем	разработке и эксплуатации автоматизированных систем, средства управления и защиты автоматизированных систем. ПКС-3.2 Уметь применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска), в том числе средства, осуществляющие непрерывный мониторинг защищенности автоматизированных систем. ПКС-3.3 Владеть навыками выбора программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.
--	--	---

#### 4. Структура и содержание дисциплины (модуля)

##### 4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет **4** зачетных единиц (**144** академических часа).

Вид работы	Очная форма Трудоемкость, акад. часов	
	6 семестр	всего
<b>Общая трудоемкость</b>	<b>144</b>	<b>144</b>
<b>Контактная работа:</b>	<b>68</b>	<b>68</b>
Лекции (Лек)	30	30
Лабораторные работы (Лаб)	32	32
Контактная работа в период теоретического обучения (КонтТО) (Проведение текущих консультаций и индивидуальная работа со студентами)	5	5
Контактная работа в период промежуточной аттестации(КонтПА)	1	1
<b>Промежуточная аттестация (зачет)</b>	<b>26</b>	<b>26</b>
<b>Самостоятельная работа:</b>	<b>50</b>	<b>50</b>
- самоподготовка (проработка и повторение материала занятий, учебников и учебных пособий);	25	25
- подготовка к лабораторным занятиям;	25	25

##### 4.2.Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

№ п/п	Раздел дисциплины/ темы	Виды учебной работы (в часах)					Формы текущего контроля успеваемости, промежуточной аттестации
		контактная				Самостоятельная работа	
		семестр	Лекции	Практические занятия	Лабораторные занятия		
1.	Тема 1. Введение в	6	8		8	12	Лабораторный

	организацию конфиденциального делопроизводства и защиты коммерческой тайны						практикум, контрольные вопросы, проверка домашнего задания
2.	Тема 2 Жизненный цикл конфиденциального документа		8		8	12	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
3.	Тема 3 Программные средства защиты конфиденциальной информации		8		8	12	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
4.	Тема 4 Технические средства защиты конфиденциальной информации		6		8	14	Лабораторный практикум, контрольные вопросы, проверка домашнего задания
	<i>Зачет</i>						
	<b>Итого:</b>		<b>30</b>		<b>32</b>	<b>50</b>	

### 4.3. Содержание разделов дисциплины

#### **Тема 1. Введение в организацию конфиденциального делопроизводства и защиты коммерческой тайны**

Законодательная сторона защиты конфиденциальной информации в организации. Иерархия законодательных органов, порядок создания законов и подзаконных актов, область действия по времени и месту. Охраняемые сведения, понятия тайны и ее виды применительно к различным организациям. Основные законы, связанные с конфиденциальным делопроизводством. Организация конфиденциального делопроизводства. Особенности организации конфиденциального делопроизводства с использованием электронного документооборота. ФСБ, ФСТЭК, Роскомнадзор, Роспатент и другие организации, являющиеся регуляторами по отношению к вопросам конфиденциального делопроизводства.

#### **Тема 2. Жизненный цикл конфиденциального документа**

Путь конфиденциального делопроизводства от создания до уничтожения. Составление номенклатур, формирование и оформление конфиденциальных дел. Подготовка конфиденциальных документов для архивного хранения и уничтожения. ГОСТ Р 51275-2006 Защиты информации. Защита конфиденциальной информации при ее передаче по сети. Система защищенного электронного документооборота. Основные задачи, решаемые системами электронного документооборота. Электронно-цифровая подпись.

#### **Тема 3 Программные средства защиты конфиденциальной информации**

Антивирусная защита. Межсетевые экраны как средство защиты от несанкционированного доступа. Криптографические средства. Сканеры уязвимостей. Системы обнаружения атак. Парольная защита. Идентификация и аутентификация. Модели разграничения доступа к информационным системам и ресурсам. Виды электронной подписи и принципы использования. Удостоверяющие центры и сертификат ключа. Квалифицированный сертификат.

#### **Тема 4 Технические средства защиты конфиденциальной информации**

Общетехнические средства контроля физического доступа к конфиденциальной информации. Разрешительная система доступа к конфиденциальной информации. Санкционированный и несанкционированный доступ. Электронные ключи и замки. Биометрические системы аутентификации. Система видеонаблюдения. Система охраны

периметра.

## **4.4 Темы и планы лабораторных занятий**

### **Тема 1. Введение в организацию конфиденциального делопроизводства и защиты коммерческой тайны**

Вопросы:

1. Законодательная сторона защиты конфиденциальной информации в организации.
2. Иерархия законодательных органов, порядок создания законов и подзаконных актов, область действия по времени и месту.
3. Охраняемые сведения, понятия тайны и ее виды применительно к различным организациям.
4. Основные законы, связанные с конфиденциальным делопроизводством.
5. Организация конфиденциального делопроизводства.
6. Особенности организации конфиденциального делопроизводства с использованием электронного документооборота.
7. ФСБ, ФСТЭК, Роскомнадзор, Роспатент и другие организации, являющиеся регуляторами по отношению к вопросам конфиденциального делопроизводства.

### **Тема 2. Жизненный цикл конфиденциального документа**

Вопросы:

1. Путь конфиденциального делопроизводства от создания до уничтожения.
2. Составление номенклатур, формирование и оформление конфиденциальных дел.
3. Подготовка конфиденциальных документов для архивного хранения и уничтожения.
4. ГОСТ Р 51275-2006 защиты информации.
5. Защита конфиденциальной информации при ее передаче по сети.
6. Система защищенного электронного документооборота.
7. Основные задачи, решаемые системами электронного документооборота.
8. Электронно-цифровая подпись.

### **Тема 3 Программные средства защиты конфиденциальной информации**

Вопросы:

1. Антивирусная защита.
2. Межсетевые экраны как средство защиты от несанкционированного доступа.
3. Криптографические средства.
4. Сканеры уязвимостей.
5. Системы обнаружения атак.
6. Парольная защита.
7. Идентификация и аутентификация.
8. Модели разграничения доступа к информационным системам и ресурсам.
9. Виды электронной подписи и принципы использования.
10. Удостоверяющие центры и сертификат ключа.
11. Квалифицированный сертификат.

### **Тема 4 Технические средства защиты конфиденциальной информации**

Вопросы:

1. Общетехнические средства контроля физического доступа к конфиденциальной информации.
2. Разрешительная система доступа к конфиденциальной информации.
3. Санкционированный и несанкционированный доступ.

4. Электронные ключи и замки.
5. Биометрические системы аутентификации.
6. Система видеонаблюдения.
7. Система охраны периметра.

## **5. Темы дисциплины (модуля) для самостоятельного изучения**

### **Вопросы для самостоятельного изучения**

1. Создание и защита электронного документооборота на современном предприятии.
2. Проектирование системы электронного документооборота с применением защиты информации.
3. Электронные системы документооборота и делопроизводства.
4. Автоматизация делопроизводства средствами программ ЭДО и организация работы защиты информации.
5. Использование Internet для организации электронного документооборота и способы защиты информации.
6. Проблемы документационного обеспечения управления и использование электронной цифровой подписи с ее защитой.
7. Организация работы по защите автоматизированных систем документационного обеспечения управления.
8. Анализ современных систем автоматизации делопроизводства в организации и электронного документооборота, особенности их классификации.
9. Проблемы автоматизации электронного документооборота.
10. Автоматизация бизнес-процессов с помощью систем электронного документооборота.
11. Процесс внедрения различных информационных систем на предприятии для электронного документооборота
12. Применение информационной системы электронного документооборота и защита информации
13. Проблемы внедрения средств электронного документооборота и защиты данных
14. Основные преимущества электронного документооборота и анализ электронных систем документирования управленческой деятельности в организации
15. Электронный документооборот на предприятии и защита персональных данных
16. Проблема внедрения использования безбумажного документооборота в государственном и муниципальном управлении и вопросы конфиденциальности информации
17. Проблемы внедрения новых информационных технологий в делопроизводство и особенности защиты информации в делопроизводстве
18. Управление документооборотом и защитой данных
19. Организация документооборота с защитой персональных данных за рубежом
20. Понятие электронного документа
21. Электронные архивы российских предприятий
22. Система контроля доступа к электронному документообороту
23. Комплексная автоматизированная система учета конфиденциальных документов на предприятии
24. Разработка требований по организационной защите электронного документооборота, передаваемого и получаемого по сети Internet
25. Обоснование и разработка мер организационной защиты документооборота при взаимодействии сотрудников предприятий со сторонними организациями
26. Архивные документы в системе электронного документооборота

27. Основы управления электронным документооборотом
28. Проектирование системы электронного документооборота
29. Системы управления электронным документооборотом

## **6. Образовательные технологии**

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие средства и формы обучения: мультимедийные лекции, лабораторный практикум, информационное моделирование, учебные проекты, имитация профессиональной деятельности.

При организации самостоятельной работы студентов используются средства и формы обучения: работа с учебной и научной литературой в электронных библиотеках, информационный поиск в интернете, выполнение учебных проектов, использование аудио и видео материалов для подготовки к лекционным и практическим занятиям, контроль знаний в тренинго-тестирующей системе.

## **7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)**

### **Тестовые задания**

- 1) К правовым методам, обеспечивающим информационную безопасность, относятся:
  - а) Разработка аппаратных средств обеспечения правовых данных
  - б) Разработка и установка во всех компьютерных правовых сетях журналов учета
  - в) действий
  - г) Разработка и конкретизация правовых нормативных актов обеспечения безопасности
- 2) Основными источниками угроз информационной безопасности являются:
  - а) Хищение жестких дисков, подключение к сети, инсайдерство
  - б) Перехват данных, хищение данных, изменение архитектуры системы
  - в) Хищение данных, подкуп системных администраторов, нарушение регламента работы
- 3) Виды информационной безопасности:
  - а) Персональная, корпоративная, государственная
  - б) Клиентская, серверная, сетевая
  - в) Локальная, глобальная, смешанная
- 4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
  - а) Несанкционированного доступа, воздействия в сети
  - б) Инсайдерства в организации
  - в) Чрезвычайных ситуаций
- 5) Основные объекты информационной безопасности:
  - а) Компьютерные сети, базы данных
  - б) Информационные системы, психологическое состояние пользователей
  - в) Бизнес-ориентированные, коммерческие системы
- 6) Основными рисками информационной безопасности являются:
  - а) Искажение, уменьшение объема, перекодировка информации
  - б) Техническое вмешательство, выведение из строя оборудования сети
  - в) Потеря, искажение, утечка информации
- 7) К основным принципам обеспечения информационной безопасности относится:
  - а) Экономической эффективности системы безопасности
  - б) Многоплатформенной реализации системы
  - в) Усиления защищенности всех звеньев системы
- 8) Основными субъектами информационной безопасности являются:



- а) руководители, менеджеры, администраторы компаний
  - б) органы права, государства, бизнеса
  - в) сетевые базы данных, брандмауэр
- 9) К основным функциям системы безопасности относят:
- а) Установление регламента, аудит системы, выявление рисков
  - б) Установка новых офисных приложений, смена хостинг-компаний
  - в) Внедрение аутентификации, проверки контактных данных пользователей
- 10) Принципом информационной безопасности является принцип недопущения:
- а) Неоправданных ограничений при работе в сети (системе)
  - б) Рисков безопасности сети, системы
  - в) Презумпции секретности
- 11) Принципом политики информационной безопасности является принцип:
- а) Невозможности миновать защитные средства сети (системы)
  - б) Усиления основного звена сети, системы
  - в) Полного блокирования доступа при риск-ситуациях
- 12) Принципом политики информационной безопасности является принцип:
- а) Усиления защищенности самого незащищенного звена сети (системы)
  - б) Перехода в безопасное состояние работы сети, системы
  - в) Полного доступа пользователей ко всем ресурсам сети, системы
- 13) Принципом политики информационной безопасности является принцип:
- а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
  - б) Одноуровневой защиты сети, системы
  - в) Совместимых, однотипных программно-технических средств сети, системы
- 14) К основным типам средств воздействия на компьютерную сеть относится:
- а) Компьютерный сбой
  - б) Логические закладки («мины»)
  - в) Аварийное отключение питания
- 15) Когда получен спам по e-mail с приложенным файлом, следует:
- а) Прочитать приложение, если оно не содержит ничего ценного – удалить
  - б) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
  - в) Удалить письмо с приложением, не раскрывая (не читая) его
- 16) Принцип Кирхгофа:
- а) Секретность ключа определена секретностью открытого сообщения
  - б) Секретность информации определена скоростью передачи данных
  - в) Секретность закрытого сообщения определяется секретностью ключа
- 17) ЭЦП – это:
- а) Электронно-цифровой преобразователь
  - б) Электронно-цифровая подпись
  - в) Электронно-цифровой процессор
- 18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- а) Покупка нелегального ПО
  - б) Ошибки эксплуатации и неумышленного изменения режима работы системы
  - в) Сознательного внедрения сетевых вирусов
- 19) Наиболее распространены угрозы информационной безопасности сети:
- а) Распределенный доступ клиент, отказ оборудования
  - б) Моральный износ сети, инсайдерство
  - в) Сбой (отказ) оборудования, нелегальное копирование данных
- 20) Наиболее распространены средства воздействия на сеть офиса:
- а) Слабый трафик, информационный обман, вирусы в интернет
  - б) Вирусы в сети, логические мины (закладки), информационный перехват
  - в) Компьютерные сбои, изменение администрирования, топологии
- 21) Утечкой информации в системе называется ситуация, характеризующаяся:
- а) Потерей данных в системе
  - б) Изменением формы информации

- в) Изменением содержания информации
- 22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
  - а) Целостность
  - б) Доступность
  - в) Актуальность
- 23) Угроза информационной системе (компьютерной сети) – это:
  - а) Вероятное событие
  - б) Детерминированное (всегда определенное) событие
  - в) Событие, происходящее периодически
- 24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
  - а) Регламентированной
  - б) Правовой
  - в) Защищаемой
- 25) Разновидностями угроз безопасности (сети, системы) являются:
  - а) Программные, технические, организационные, технологические
  - б) Серверные, клиентские, спутниковые, наземные
  - в) Личные, корпоративные, социальные, национальные
- 26) Полную ответственность за защищенность компьютерной сети несет:
  - а) Владелец сети
  - б) Администратор сети
  - в) Пользователь сети
- 27) Политика безопасности в системе (сети) – это комплекс:
  - а) Руководств, требований обеспечения необходимого уровня безопасности
  - б) Инструкций, алгоритмов поведения пользователя в сети
  - в) Нормы информационного права, соблюдаемые в сети
- 28) Наиболее важным при реализации защитных мер политики безопасности является:
  - а) Аудит, анализ затрат на проведение защитных мер
  - б) Аудит, анализ безопасности
  - в) Аудит, анализ уязвимостей, риск-ситуаций

### **Примерный перечень вопросов к зачету (6 семестр)**

1. Законодательная сторона защиты конфиденциальной информации в организации.
2. Иерархия законодательных органов, порядок создания законов и подзаконных актов, область действия по времени и месту.
3. Охраняемые сведения, понятия тайны и ее виды применительно к различным организациям.
4. Основные законы, связанные с конфиденциальным делопроизводством.
5. Организация конфиденциального делопроизводства.
6. Особенности организации конфиденциального делопроизводства с использованием электронного документооборота.
7. ФСБ, ФСТЭК, Роскомнадзор, Роспатент и другие организации, являющиеся регуляторами по отношению к вопросам конфиденциального делопроизводства.
8. Путь конфиденциального делопроизводства от создания до уничтожения.
9. Составление номенклатур, формирование и оформление конфиденциальных дел.
10. Подготовка конфиденциальных документов для архивного хранения и уничтожения.
11. ГОСТ Р 51275-2006 защиты информации.
12. Защита конфиденциальной информации при ее передаче по сети.
13. Система защищенного электронного документооборота.
14. Основные задачи, решаемые системами электронного документооборота.
15. Электронно-цифровая подпись.

16. Антивирусная защита.
17. Межсетевые экраны как средство защиты от несанкционированного доступа.
18. Криптографические средства.
19. Сканеры уязвимостей.
20. Системы обнаружения атак.
21. Парольная защита.
22. Идентификация и аутентификация.
23. Модели разграничения доступа к информационным системам и ресурсам.
24. Виды электронной подписи и принципы использования.
25. Удостоверяющие центры и сертификат ключа.
26. Квалифицированный сертификат.
27. Общетеchnические средства контроля физического доступа к конфиденциальной информации.
28. Разрешительная система доступа к конфиденциальной информации.
29. Санкционированный и несанкционированный доступ.
30. Электронные ключи и замки.
31. Биометрические системы аутентификации.
32. Система видеонаблюдения.
33. Система охраны периметра.

## 8. Система оценивания планируемых результатов обучения

Критерии оценивания зачета:

- оценка **«зачтено»** выставляется студенту, который твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике.
- оценка **«не зачтено»** выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, допускающему в ответе или в решении задач грубые ошибки.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
Текущее тестирование	1	3	3	9
Промежуточная аттестация (экзамен)			12	43
<b>Итого за семестр</b>			<b>52</b>	<b>100</b>

## 9. Учебно-методическое и информационное обеспечение дисциплины

### 9.1. Основная литература

1. Кришталюк, А. Н. Конфиденциальное делопроизводство и защита коммерческой тайны : курс лекций / А. Н. Кришталюк. — Орел : Межрегиональная Академия безопасности и выживания (МАБИБ), 2014. — 199 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/33427.html>
2. Минин, О. В. Защита конфиденциальной информации при электронном документообороте : учебное пособие / О. В. Минин, И. В. Минин. — Новосибирск : Новосибирский государственный технический университет, 2011. — 20 с. — ISBN 978-5-7782-1829-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/44918.html>

3. Учебно-методическое пособие по выполнению лабораторных работ по дисциплине Методы и средства защиты компьютерной информации / составители А. Г. Симонян, И. А. Денисов. — Москва : Московский технический университет связи и информатики, 2016. — 55 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/61497.html>

## 9.2 Дополнительная литература

1. Учебно-методическое пособие по дисциплине Методы и средства защиты компьютерной информации / составители А. Г. Симонян. — Москва : Московский технический университет связи и информатики, 2016. — 32 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/61498.html>

2. Кирпичников, А. П. Криптографические методы защиты компьютерной информации : учебное пособие / А. П. Кирпичников, З. М. Хайбуллина. — Казань : Казанский национальный исследовательский технологический университет, 2016. — 100 с. — ISBN 978-5-7882-2052-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/79313.html>

3. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87992.html>

## 9.3 Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Professional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 1000-1499 Node 2 year Educational Renewal License (лицензия 2022-190513-020932-503-526), срок пользования с 2019-05-13 по 2021-04-13
10. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
11. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
12. Межсетевой экран для OS Linux Netfilter
13. Антивирусная программа Dr.Web
14. Антивирус Касперского
15. Пакет анализа сетевого трафика Wireshark
16. Система обнаружения атак Snort
17. «Антиплагиат. ВУЗ». Лицензионный договор №194 от 22.03. 2018 года;
18. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
19. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20

## **9.4 Профессиональные базы данных и информационные справочные системы современных информационных технологий**

1. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки (<https://github.com/>)
2. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.nt.ru>)
3. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
4. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
5. Интернет-университет информационных технологий ([www.intuit.ru](http://www.intuit.ru))
6. Онлайн среда разработки приложений ([ideone.com](http://ideone.com))
7. Журнал «КомпьютерПресс» ([www.compress.ru](http://www.compress.ru))
8. Издательство «Открытые системы» ([www.osp.ru](http://www.osp.ru))
9. Издание о высоких технологиях ([www.cnews.ru](http://www.cnews.ru))
10. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
11. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
12. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
13. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
14. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

## **10 Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

### ***Для слепых и слабовидящих:***

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

### ***Для глухих и слабослышащих:***

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

### ***Для лиц с нарушениями опорно-двигательного аппарата:***

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме

на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

***Для слепых и слабовидящих:***

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

***Для глухих и слабослышащих:***

- в печатной форме;
- в форме электронного документа.

***Для обучающихся с нарушениями опорно-двигательного аппарата:***

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

***для слепых и слабовидящих:***

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

***для глухих и слабослышащих:***

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

***для обучающихся с нарушениями опорно-двигательного аппарата:***

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

## **11 Материально-техническое обеспечение дисциплины (модуля)**

Для проведения всех видов занятий (лекционных и практических) используются специально оборудованные кабинеты и аудитории, соответствующие действующим противопожарным правилам, средства для видеопросмотра, класс компьютерной техники. Для ведения занятий в достаточном количестве имеются компьютеры и офисная техника, учебники и учебные пособия в фондах университетской библиотеки. Имеется доступ к нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета.

Для самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями, справочно-правовой системой и возможностью доступа в глобальную сеть. Компьютерный класс оснащён аудиовизуальной техникой для показа лекционного материала и презентаций студенческих работ.

***К рабочей программе прилагаются:***

**Приложение 1** – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

**Приложение 2** – Методические указания для обучающихся по освоению дисциплины (модуля).

УТВЕРЖДЕНО  
Протокол заседания кафедры

наименование

№ \_\_\_\_\_ от «\_\_\_\_» \_\_\_\_\_ 20\_\_\_\_ г.

**ЛИСТ ИЗМЕНЕНИЙ**

в рабочей программе (модуле) дисциплины \_\_\_\_\_  
(название дисциплины)  
по направлению подготовки (специальности) \_\_\_\_\_

на 20\_\_ / 20\_\_ учебный год

1. В \_\_\_\_\_ вносятся следующие изменения:  
(элемент рабочей программы)

- 1.1. ....;
- 1.2. ....;
- ...
- 1.9. ....

2. В \_\_\_\_\_ вносятся следующие изменения:  
(элемент рабочей программы)

- 2.1. ....;
- 2.2. ....;
- ...
- 2.9. ....

3. В \_\_\_\_\_ вносятся следующие изменения:  
(элемент рабочей программы)

- 3.1. ....;
- 3.2. ....;
- ...
- 3.9. ....

Составитель \_\_\_\_\_ Фамилия И.О.  
(подпись, расшифровка подписи)

" \_\_\_\_\_ " \_\_\_\_\_ 20\_\_\_\_ г.

Зав. кафедрой \_\_\_\_\_ Фамилия И.О.  
(подпись, расшифровка подписи)