

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

Кафедра экономики и управления

УТВЕРЖДАЮ

Руководитель основной профессиональной  
образовательной программы



к.э.н., доцент Карякина И. Е.

## **РАБОЧАЯ ПРОГРАММА**

**Б1.В.ДВ.04.01 «Основы экономической информационной безопасности»**

Уровень высшего образования  
СПЕЦИАЛИТЕТ

Специальность:  
**38.05.01 Экономическая безопасность**

Специализация:  
**Экономико-правовое обеспечение экономической безопасности**

Квалификация:  
экономист

Форма обучения:  
очная

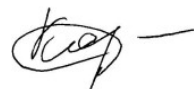
РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск  
2025 г.

Рабочая программа дисциплины Б1.В.ДВ.04.01 «Основы экономической информационной безопасности» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по специальности 38.05.01 Экономическая безопасность», специализация «Экономико-правовое обеспечение экономической безопасности».

Программу составила:

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



Рабочая программа дисциплины Б1.В.ДВ.04.01 «Основы экономической информационной безопасности» утверждена на заседании кафедры экономики и управления, протокол № 10 от 18 июня 2025 г.

Директор Института права, экономики  
и управления



То Кен Сик

## 1 Цель и задачи дисциплины

**Цели** освоения дисциплины: знакомство с базовыми технологиями информационной безопасности на предприятии; с задачами и принципами организации службы информационной безопасности; изучение и классификация несанкционированных действий на взломы информационных систем; рассмотрение базовых сведений о криптографии как средстве защиты информации на предприятии; изучение административных мер и юридических вопросов в области информационной безопасности.

### **Задачи дисциплины:**

- определение целей и принципов защиты информации;
- установление факторов, влияющих на защиту информации;
- изучение современной доктрины информационной безопасности;
- рассмотрение состава защищаемой информации, ее классификацией по видам тайн, материальным носителям, собственникам и владельцам;
- установление структуры угроз защищаемой информации;
- определение места конфиденциального документооборота в организациях различного типа;
- раскрытие принципов, методов и технологии конфиденциального документооборота.

## 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ДВ.04.01 «Основы информационной безопасности» относится к дисциплинам по выбору учебного плана ОПОП по специальности 38.05.01 «Экономическая безопасность».

**Пререквизиты дисциплины:** изучение данной дисциплины базируется на знании следующих дисциплин: Информационные технологии, Информационные системы в экономике, Компьютерное моделирование бизнес-процессов, Экономическая безопасность.

**Постреквизиты дисциплины:** «Экономическая безопасность хозяйствующих субъектов», «Экономическая безопасность».

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

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ПК-18	Способен реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать и использовать в интересах выявления рисков и угроз экономической безопасности, предупреждения, пресечения, раскрытия и расследования преступлений и иных правонарушений в сфере экономики	ПК-18.1 Разрабатывает планы мероприятий, необходимых для проведения финансового расследования; осуществляет сбор, обобщение и закрепление ранее выявленных типологий подозрительной деятельности; ведет базы данных типологий подозрительной деятельности; доводит аналитические материалы до заинтересованных структурных подразделений организации. ПК-18.2 Проверяет соблюдение всех установленных процедур в рамках

		<p>используемых методов.</p> <p>ПК-18.3 Знает методы финансового анализа, источники информации для его проведения, специализированные программные продукты, используемые в профессиональной деятельности.</p>
ПК-39	Способен соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области информационной безопасности	<p>ПК-39.1 Контролирует доступ к документам по профессиональной деятельности; разрабатывает требования к программному обеспечению по управлению рисками, помощь в выборе автоматизированной системы управления рисками; разрабатывает новые алгоритмы и приемы отбора информации из баз данных; апробирует разработанные алгоритмы и приемы отбора информации; определяет порядок обеспечения конфиденциальности информации.</p> <p>ПК-39.2 Использует специализированное программное обеспечение для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне продвинутого пользователя.</p> <p>ПК-39.3 Знает информационную политику организации, основы информационных технологий и информационной безопасности; ключевые риски и средства контроля, связанные с информационными технологиями; требования к обеспечению сохранения коммерческой тайны; основы безопасной работы с компьютерной техникой и информационно-коммуникационными сетями в целях защиты информации</p>

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

##### 4.1 Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет 2 зачетных единиц (72 академических часов).

Очная форма обучения

Вид работы	Трудоемкость, акад. часов	
	7 семестр	всего
<b>Общая трудоемкость</b>	<b>72</b>	<b>72</b>
<b>Контактная работа:</b>	<b>36</b>	<b>36</b>
Лекции (Лек)	18	18
Практическая работа	18	18
Лабораторная работа	-	-
Контактная работа в период теоретического обучения (КонтТО) (Проведение текущих консультаций и индивидуальная работа со студентами)	-	-
Контактная работа в период промежуточной аттестации(КонтПА)	1	1
<b>Промежуточная аттестация</b>	<b>зачет</b>	
<b>Самостоятельная работа:</b>	<b>36</b>	<b>36</b>
- самоподготовка (проработка и повторение материала занятий, учебников и учебных пособий);	12	12
- изучение нормативно-правового законодательства в справочно-правовых системах;	12	12
- подготовка к практическим занятиям.	12	12

Общая трудоемкость дисциплины (модуля) составляет 2 зачетных единиц (72 академических часов).

заочная форма обучения

Вид работы	Трудоемкость, акад. часов	
	7 семестр	всего
<b>Общая трудоемкость</b>	<b>72</b>	<b>72</b>
<b>Контактная работа:</b>	<b>10</b>	<b>10</b>
Лекции (Лек)	4	4
Практическая работа	6	6
Лабораторная работа	-	-
Контактная работа в период теоретического обучения (КонтТО) (Проведение текущих консультаций и индивидуальная работа со студентами)	-	-
Контактная работа в период промежуточной аттестации(КонтПА)	1	1
<b>Промежуточная аттестация</b>	<b>зачет</b>	
<b>Самостоятельная работа:</b>	<b>62</b>	<b>62</b>
- самоподготовка (проработка и повторение материала занятий, учебников и учебных пособий);	12	12
- изучение нормативно-правового законодательства в справочно-правовых системах;	12	12
- подготовка к практическим занятиям.	12	12

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

Очная форма обучения

№	Раздел дисциплины/	Виды учебной работы	Формы текущего
---	--------------------	---------------------	----------------

п/п	темы	(в часах)					контроля успеваемости, промежуточной аттестации
		контактная				Самостоятельна я работа	
		семестр	Лекции	Практические занятия	Лабораторные занятия		
1.	Тема 1. Понятие информационной безопасности, ее роль в национальной безопасности	7	4	4	-	8	практикум, тестирование, опрос, контрольная работа
2.	Тема 2. Терминологические основы информационной безопасности		4	4	-	8	практикум, тестирование, опрос, контрольная работа
3.	Тема 3. Классификация и анализ угроз информационной безопасности		4	4	-	7	практикум, тестирование, опрос, контрольная работа
4.	Тема 4. Атаки на информационную инфраструктуру предприятий		3	3	-	7	практикум, тестирование, опрос, контрольная работа
5.	Тема 5. Задачи и принципы организации службы информационной безопасности предприятия		3	3	-	6	практикум, тестирование, опрос, контрольная работа
	Итого:		18	18		36	

### 4.3 Содержание разделов дисциплины

#### **Тема 1. Понятие информационной безопасности, ее роль в национальной безопасности**

Органы, обеспечивающие национальную безопасность Российской Федерации, цели, задачи. Национальные интересы Российской Федерации в информационной сфере. Приоритетные направления в области защиты информации в Российской Федерации. Тенденции развития информационной политики государств и ведомств. Информационная война, проблемы. Правовое обеспечение защиты информации. Информация с ограниченным доступом, государственная тайна, конфиденциальность, коммерческая тайна, персональные данные.

#### **Тема 2. Терминологические основы информационной безопасности**

Понятие информации и информационной безопасности, информационная война, информационная агрессия, информационное оружие, информационные процессы, информационная система, информационная сфера, виды информации. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации, угрозы - определения, сопоставление. Идентификация, аутентификация, авторизация.

#### **Тема 3. Классификация и анализ угроз информационной безопасности**

Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы: 1) подверженность физическому искажению или уничтожению; 2) возможность несанкционированной

(случайной или злоумышленной) модификации; 3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные.

#### **Тема 4. Атаки на информационную инфраструктуру предприятий**

Типовая атака на систему. Социальная инженерия. Закладки в аппаратном обеспечении. Атаки на средства аутентификации и пароли. Постороннее программное обеспечение. Классификация удаленных атак. Вирусы и их разновидности. Антивирусы. Межсетевые экраны. Удаленные атаки на информационные системы. Атаки на отказ в обслуживании. Атаки на переполнение буфера. Вирусная угроза. Почтовая угроза.

#### **Тема 5. Задачи и принципы организации службы информационной безопасности предприятия**

Определение и цели информационной безопасности. Механизмы информационной безопасности. Инструментарий информационной безопасности. Служба информационной безопасности предприятия. Общие сведения об инвентаризации информационных систем. Классификация информационных объектов и субъектов информационных систем.

### **4.4 Темы и планы практических занятий**

#### **Практическое занятие №1**

Тема **Понятие информационной безопасности, ее роль в национальной безопасности.**

1. Определение и цели информационной безопасности.
2. Механизмы информационной безопасности.
3. Инструментарий информационной безопасности
4. Методы формирования функций защиты.
5. Криптография как способ защиты информации
6. Общие сведения о симметричной криптографии
7. Алгоритмы симметричного шифрования
8. Управление ключами в симметричных системах.

#### **Практическое занятие №2**

Тема **Терминологические основы информационной безопасности.**

1. Анализ терминов и определений информационной безопасности.
2. Основные понятия и методы защиты данных в информационных системах
3. Политика информационной безопасности на предприятии
4. Локальные и удаленные атаки на информационные системы предприятий

#### **Практическое занятие №3**

Тема **Классификация и анализ угроз информационной безопасности.**

1. Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации
2. Характер происхождения угроз: умышленные факторы, естественные факторы.
3. Источники угроз. Предпосылки появления угроз: объективные, субъективные.
4. Автоматизированные средства компьютерной безопасности
5. Антивирусные системы
6. Межсетевые экраны

7. Криптографические средства
8. Основные принципы симметричной криптографии
9. Основные принципы асимметричной криптографии
10. Электронная цифровая подпись.

#### **Практическое занятие №4**

##### **Тема Атаки на информационную инфраструктуру предприятия**

1. Потенциально возможные злоумышленные действия в автоматизированных системах обработки данных.
2. Формирование модели нарушителя.
3. Социальная инженерия, атаки на средства аутентификации, вирусы и троянские программы
4. Атаки на отказ в обслуживании, атаки на поток данных, перехват данных в компьютерной сети
5. Закладки в аппаратном обеспечении информационных систем
6. Общие сведения об инвентаризации информационных систем
7. Общие сведения о контроле физического доступа
8. Системы управления доступом,
9. Биометрические системы аутентификации,
10. Системы видеонаблюдения

#### **Практическое занятие № 5**

##### **Тема Задачи и принципы организации службы информационной безопасности предприятия**

Наименование работы «Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации»

##### Цель работы:

Целью работы является организация поиска в интернете информации по существующим в настоящее время информационным системам предприятий и оценки их с позиции информационной безопасности. Выбор темы, подбор материала, оформление работы, защита учебного проекта является итогом данного вида работы. Период выполнения учебного проекта, сроки рецензирования, сдача и организация его защиты происходят по утвержденному графику. По результатам защиты учебного проекта выставляется общая оценка.

##### Задание:

Проведите исследование по теме, в соответствии с выбранным вариантом. Найти в интернете описание или демоверсию объекта информатизации и написать реферат по плану: полное название информационной системы, описание, характеристика, назначение, архитектура, функциональные возможности, описание модулей, где внедрена, особенности, актуальные угрозы и способы защиты исследуемого объекта информатизации.

##### Тематика (предметные области) информационных систем:

1. Системы маркетинга и продаж
2. Финансовые и учетные системы
3. Производственные системы
4. Системы кадров
5. Автоматизация ЖКХ



6. Продажа авиа/железнодорожных билетов
7. Банковские информационные системы
8. Управление образованием (школой, ВУЗом)
9. Управление социальным обеспечением
10. Управление здравоохранением
11. Управление документооборотом
12. Автоматизация гостиничного бизнеса
13. Учет и регистрация безработных
14. Управление торговлей
15. Управление таможней
16. Управление архивом
17. Автоматизация налоговых служб
18. Автоматизация офиса
19. Автоматизация УВД
20. Библиотечные автоматизированные системы
21. Справочно-правовые системы
22. Экспертные системы

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

1. Определение каналов несанкционированного доступа для личного компьютера (ноутбука)
2. Построение модели нарушителя для информационной системы персональных данных
3. Анализ терминов и определений информационной безопасности. ГОСТы и руководящие документы
4. Оценка безопасности информации на объектах ее обработки.
5. Выявление актуальных угроз информационной безопасности для выбранного объекта информатизации.
6. Построение модели угроз для выбранного объекта информатизации.

### **Тест для самоконтроля по теме**

#### **«Анализ терминов и определений информационной безопасности»**

1. Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.?
2. К каким мерам защиты относится политика безопасности?
  - а) к административным;
  - б) к законодательным;
  - в) к программно-техническим;
  - г) к процедурным.
3. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?
  - а) ACL;
  - б) списки полномочий субъектов;
  - в) атрибутные схемы.

**4. Как называется свойство информации, означающее отсутствие неправомерных, и не предусмотренных ее владельцем изменений?**

- а) целостность;
- б) апеллируемость;
- в) доступность;
- г) конфиденциальность;
- д) аутентичность.

**5. К основным принципам построения системы защиты АИС относятся:**

- а) открытость;
- б) взаимозаменяемость подсистем защиты;
- в) минимизация привилегий;
- г) комплексность;
- д) простота.

**6. Какие из следующих высказываний о модели управления доступом RBAC справедливы?**

- а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей;
- б) роли упорядочены в иерархию;
- в) с каждым объектом доступа ассоциировано несколько ролей ;
- г) для каждой пары «субъект-объект» назначен набор возможных разрешений.

**7. Диспетчер доступа...**

- а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
- б) ... использует атрибутные схемы для представления матрицы доступа;
- в) ... выступает посредником при всех обращениях субъектов к объектам;
- г) ... фиксирует информацию о попытках доступа в системном журнале;

**8. Какие предположения включает неформальная модель нарушителя?**

- а) о возможностях нарушителя;
- б) о категориях лиц, к которым может принадлежать нарушитель;
- в) о привычках нарушителя; г) о предыдущих атаках, осуществленных нарушителем;
- д) об уровне знаний нарушителя.

**9. Что представляет собой доктрина информационной безопасности РФ?**

- а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;
- б) федеральный закон, регулирующий правоотношения в области информационной безопасности;
- в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;
- г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

**10. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?**

- а) политика безопасности верхнего уровня;
- б) политика безопасности среднего уровня;
- в) политика безопасности нижнего уровня;
- г) принцип минимизации привилегий;
- д) защита поддерживающей инфраструктуры.

**11. Какие из перечисленных ниже угроз относятся к классу преднамеренных?**

- а) заражение компьютера вирусами;
- б) физическое разрушение системы в результате пожара;
- в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
- г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
- д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; е) вскрытие шифров криптозащиты информации.

**Тест для самоконтроля по теме**

**«Построение модели нарушителя для информационной системы персональных данных»**

**1. Каким образом проникают в систему макровирусы?**

- а) по электронной почте;
- б) любым способом вместе с зараженными ими файлами;
- в) злоумышленник должен вручную внести вирус в систему;
- г) через Интернет, используя ошибки в сетевых программах;
- д) через съемные носители данных при срабатывании автозагрузки с них.

**2. Какому требованию должен удовлетворять пароль для противодействия атаке по персональному словарию?**

- а) при придумывании пароля не должны использоваться личные данные;
- б) длина пароля должна составлять 12 и более символов;
- в) пароль нельзя открывать никому;
- г) разные сервисы должны защищаться разными паролями;
- д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки препинания и т.д.

**3. Какие недостатки имеют системы обнаружения вторжений, работающие на основе обнаружения аномалий?**

- а) высокий процент ложных срабатываний;
- б) не способны контролировать ситуацию во всей сети;
- в) неспособны анализировать степень проникновения;
- г) работа затруднена при высокой загрузке сети;
- д) снижается эффективность работы сервера, на котором они установлены.

**4. ... — канал между двумя узлами, защищенный за счет шифрования проходящего по нему трафика.**

**5. Как называются вирусы, которые автоматически запускаются в момент старта операционной системы и, таким образом, постоянно функционируют в оперативной памяти?**

- а) резидентные вирусы;
- б) стелс-вирусы;
- в) макровирусы;
- г) полиморфные вирусы;
- д) троянские кони.

**6. К какому классу относятся межсетевые экраны, которые отслеживают текущие соединения и пропускают только такие пакеты, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений?**

- а) Работающие на сетевом уровне;
- б) Работающие на сеансовом уровне;
- в) Работающие на уровне приложений;
- г) Stateless;
- д) Stateful.

**7. Как называются антивирусы, которые работают резидентно, предотвращая заражение файлов?**

- а) детекторы;
- б) фаги;
- в) ревизоры;
- г) вакцины;
- д) фильтры.

**8. Какие вирусы заражают носители данных?**

- а) файловые вирусы;
- б) загрузочные вирусы;
- в) макровирусы;
- г) сетевые черви;
- д) троянские кони.

**9. Как называются VPN, с помощью которых на основе ненадёжной сети создается надежная и защищенная подсеть?**

- а) Внутрикorporативный;
- б) Защищенные;
- в) С удаленным доступом;
- г) Доверительные;
- д) Межкорпоративные.

**10. Какому требованию должен удовлетворять пароль для противодействия фишингу?**

- а) пароль не должен быть производным от слов любого естественного языка;
- б) длина пароля должна составлять 12 и более символов;
- в) пароль нельзя открывать никому;
- г) разные сервисы должны защищаться разными паролями;
- д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки

препинания и т.д.

**11. Что такое VPN?**

- а) система обнаружения вторжений;
- б) протокол обмена ключами;
- в) трансляция сетевых адресов;
- г) виртуальная частная сеть;
- д) протокол защиты передаваемого потока.

**12. Каков основной недостаток обнаружения вирусов путем эвристического сканирования?**

- а) значительная вероятность ложного срабатывания;
- б) крайне медленная работа антивируса;

- в) невозможность обнаружения новых вирусов;
- г) необходимость трудоемкой ручной настройки антивируса.

## **6. Образовательные технологии**

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие средства и формы обучения: мультимедийные лекции, компьютерный 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, изучение нормативно-правового законодательства в справочно-правовых системах, информационный поиск в интернете, выполнение учебных проектов, использование аудио и видео материалов для подготовки к лекционным и практическим занятиям, разработка мультимедийных презентаций, работа с офисным пакетом приложений MSOffice, контроль знаний в тренинго-тестирующей системе.

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

### **Тест для промежуточного контроля**

**1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется**

Выберите один ответ.

- a. Компилятор
- b. Интернет-черви
- c. Вирус

**2. величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется**

Выберите один ответ.

- a. Воздействием (влиянием)
- b. Потерей
- c. Силой

**3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется**

Выберите один ответ.

- a. Троянской программой
- b. Червем
- c. Вирусом

**4. Уровень риска, который считается доступным для достижения желаемого результата, называется**

Выберите один ответ.

- a. Устойчивостью
- b. Терпимостью по отношению к риску
- c. Независимостью

**5. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются**

Выберите один ответ.

- a. Вирусами
- b. Руткитами
- c. Червями

**6. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:**

Выберите один ответ.

- a. Правилами безопасности
- b. Требованием безопасности
- c. Мерами безопасности

**7. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:**

Выберите один ответ.

- a. Управление риском
- b. Предупреждением рисков
- c. Анализом рисков

### **Вопросы для собеседования**

1. Содержание и понятий и определений по безопасности и защите информации.
2. Развитие изменений методологических подходов к организации и обеспечению защиты информации.
3. Классификация других способов и средств защиты информации в развитой период.
4. Комплексность защиты информации и необходимость комплексной защиты.
5. Структуризация понятия комплексной защиты. Тенденция развития систем и процессов обработки информации и вытекающие из них проблемы.
6. Качество информации и краткая характеристика его составляющих.
7. Защита от информации. Раскройте содержание комплексной защиты информации на объекте.
8. Информатизация общества. Государственная политика и основные направления в сфере информатизации.
9. Приведите и охарактеризуйте схему информационного обеспечения деятельности современных объектов (ИОД).
10. Дайте определение информационного кадастра объекта, раскройте его содержание.
11. Приведете и охарактеризуйте схему классификации информации.
12. Унификация структуры информационного потока. Циркуляция информационных потоков, общая схема циркуляции информационных потоков.
13. Задачи обработки информации. Общая структура и содержание унифицированной технологии автоматизированной обработки информации (УТА-ОИ).
14. Содержание основных понятий составляющих концепцию защиты информации в автоматизированных системах (АС).
15. Обеспечение режима секретности при защите информации представленной твердыми копиями
16. Дайте определение АС и раскройте ее специфические особенности.
17. Классификация АС в зависимости от области использования и уровня конфиденциальности.
18. Ведомственная принадлежность АС, степень ущерба при утечке информации.
19. Угроза АС. Источники угроз в различных типах АС.

20. Источники угроз 1-й группы и их краткая характеристика.
21. Источники угроз 2-й группы и их краткая характеристика.
22. Источники угроз 3-й группы и их краткая характеристика.
23. Возможные виды угроз создания людьми.
24. Самостоятельные направления по применению средств защиты информации и их краткая характеристика.
25. Системы защиты информации и требования предъявляемые к ней. Составляющие системы защиты и их краткая характеристика.
26. Охарактеризуйте систему защиты информации от НСД,
27. Виды угроз в каналах систем и связи защита информации в системах связи.
28. Охарактеризуйте систему защиты информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН)
29. Компьютерный вирус. Защита информации от компьютерных вирусов и др. опасных воздействий по каналам распределения программ.
30. Защита юридической значимости электронных документов.
31. Защита несанкционированного копирования программ.
32. Управление государственной системой защиты информации.
33. Организационно-правовое обеспечение безопасности информации.
34. Ответственность за нарушения законодательства в информационной сфере.
35. Что такое информация?
36. Чем отличаются данные от информации?
37. Какая информация является экономической?
38. Охарактеризуйте особенности экономической информации.
39. Что такое программно-аппаратные средства защиты информации?
40. Что такое программные средства защиты информации?
41. Какие механизмы реализуют программно-аппаратные средства защиты информации?
42. Что такое программно-аппаратные средства защиты информации?
43. Что такое программные средства защиты информации?
44. Какие механизмы реализуют программно-аппаратные средства защиты информации?
45. Какие компьютерные угрозы безопасности существуют?
46. Что такое sniffing? Какие методы защиты против него существуют?
47. Что такое IP-spoofing? Какие методы защиты против него существуют?
48. Что такое сетевая разведка? Какие методы защиты против нее существуют?
49. Что такое переполнение буфера? Какие методы защиты против него существуют?
50. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
51. Что такое отказ в обслуживании? Какие методы защиты против него существуют?
52. Что такое фишинг? Какие методы защиты против него существуют?
53. Что такое компьютерный вирус? Какие виды вирусов существуют?
54. Опишите механизм работы вируса. Как вирус может проникнуть на компьютер?
55. Какие существуют механизмы работы антивируса? Опишите их.

### **Темы контрольных работ**

1. Понятие угрозы информационной безопасности.

- 2.Виды угроз информационной безопасности РФ.
- 3.Основные внешние источники угроз информационной безопасности РФ.
- 4.Основные внутренние источники угроз информационной безопасности РФ.
- 5.Методы обеспечения информационной безопасности РФ.
- 6.Ограничение доступа к информации.
- 7.Виды уязвимости информации.
- 8.Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.
- 9.Принципы обеспечения информационной безопасности.
- 10.Особенности обеспечения информационной безопасности в различных сферах общественной жизни.
- 11.Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.
- 12.Ограничение доступа к информации
- 13.Понятие уязвимости информации.
- 14.Виды уязвимости информации.
- 15.Понятие "утечка информации".
- 16.Соотношение форм и видов уязвимости информации.
- 17.Основные функции системы обеспечения информационной безопасности Российской Федерации.
- 18.Категории информации в зависимости от порядка ее предоставления или распространения.
- 19.Специфика объектов информационной защиты.
- 20.Значение защиты информации для субъектов информационных отношений государства, общества, личности.
- 21.Значение защиты информации в политической, военной, экономической и других областях деятельности.
- 22.Информация ограниченного доступа.
- 23.Сведения конфиденциального характера.
- 24.Формы представления конфиденциальной информации.
- 25.Основные средства защиты информации.
- 26.Основные методы защиты информации.
- 27.Требования к системе защиты информации.
- 28.Понятие государственной тайны.
- 29.В каких сферах деятельности РФ предусмотрено отнесение сведений к государственной тайне.
- 30.Основные понятия (категории) в области государственной тайны (допуск к государственной тайне, гриф секретности).
- 31.Что не подлежит отнесению к государственной тайне и засекречиванию.
- 32.Принципы отнесения сведений к государственной тайне и засекречиванию.
- 33.Основные степени секретности сведений, составляющих государственную тайну.
- 34.Принципы отнесения сведений к коммерческой тайне.
- 35.Понятие коммерческой тайны.
- 36.Сведения, которые не могут составлять коммерческую тайну.
- 37.Основные понятия, относящиеся к коммерческой тайне.
- 38.Последствия разглашения сведений, составляющих коммерческую тайну.



- 39.Перечень сведений, составляющих коммерческую тайну фирмы.
- 40.Классификация методов защиты информации.
- 41.Области применения организационных, криптографических и инженерно-технических методов защиты информации.
- 42.Понятие и классификация средств защиты информации.
- 43.Назначение программных, криптографических и технических средств защиты.
- 44.Характеристика и классификация стандартов в области информационной безопасности
- 45.Основные международные и российские стандарты в области информационной безопасности.
- 46.Понятие персональных данных.
- 47.Угрозы информационной безопасности ПДн (источники и характеристика угроз).
- 48.Права субъекта персональных данных.
- 49.Доктрина информационной безопасности РФ (в части защиты общества от деструктивного воздействия информации)
- 50.Понятие «информационная война».
- 51.Информационные войны в информационно-коммуникационном пространстве
- 52.Основные виды информационного оружия.
- 53.Технология ведения информационной войны.
- 54.Методы информационно-психологического воздействия в информационно-коммуникационном пространстве.
- 55.Инструменты деструктивного воздействия на индивидуальное и массовое сознание с помощью информационно-коммуникационных технологий.
- 56.Понятие «информационно-психологическое воздействие»
- 57.Примеры ведения информационных войн.
- 58.Защита от деструктивного воздействия информации.

### **Примерные вопросы к зачету**

1. Теория защиты информации. Основные направления
2. Обеспечение информационной безопасности и направления защиты
3. Требования к системе защиты информации
4. Угрозы информации
5. Виды угроз. Основные нарушения
6. Характер происхождения угроз
7. Источники угроз. Предпосылки появления угроз
8. Система защиты информации
9. Классы каналов несанкционированного получения информации – Причины нарушения целостности информации
10. Методы и модели оценки уязвимости информации
11. Общая модель воздействия на информацию
12. Общая модель процесса нарушения физической целостности информации
13. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных
14. Методологические подходы к оценке уязвимости информации
15. Модель защиты системы с полным перекрытием
16. Рекомендации по использованию моделей оценки уязвимости информации

17. Допущения в моделях оценки уязвимости информации
18. Методы определения требований к защите информации
19. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации
20. Классификация требований к средствам защиты информации
21. Требования к защите, определяемые структурой автоматизированной системы обработки данных
22. Требования к защите, обуславливаемые видом защищаемой информации
23. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации
24. Анализ существующих методик определения требований к защите информации
25. Построение средств защиты информации
26. Средства защиты информации. Антивирусы, средства анализа защищенности, средства обнаружения вторжений
27. Регуляторы в области защиты информации
28. Защита компьютерных сетей на предприятии
29. Виды угроз компьютерных сетей на предприятии
30. Способы защиты компьютерных сетей предприятия
31. Антивирусы как способ защиты компьютерных сетей
32. Автоматизированные средства компьютерной безопасности
33. Электронная цифровая подпись
34. Информационная безопасность предприятия
35. Цифровые сертификаты
36. Виды атак на компьютерные сети предприятия
37. Криптография как способ защиты информации
38. Платежные системы в интернете
39. Безопасность платежей в интернете

## 8 Система оценивания планируемых результатов обучения

Оценка «**зачтено**» выставляется студенту, прочно усвоившему учебный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.

Оценка «**не зачтено**» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания.

Форма контроля	За одну работу		Всего Всего
	Миним. баллов	Макс. баллов	
<b>Текущий контроль:</b>			
- посещение занятий	0,5 баллов	0,5 баллов	9-18
- устный опрос	1 балла	3 баллов	3-10
- компьютерный практикум	2 балла	4 баллов	10-20
- текущее тестирование	2 балла	4 баллов	6-12
- самостоятельная работа	3 балла	5 баллов	6-15

Промежуточная аттестация (зачет)	9 баллов	25 баллов	9-25
Итого за семестр			52-100 баллов

## 9. Учебно-методическое и информационное обеспечение дисциплины

### 9.1 Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567915>
2. Чернова, Е. В. Информационная безопасность человека : учебник для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/566457>
3. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567672>

### 9.2 Дополнительная литература

1. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности»/ В.Ю. Рогозин [и др.].— Электрон. текстовые данные.— Москва: ЮНИТИ-ДАНА, 2025.— 287 с.— Режим доступа: <http://www.iprbookshop.ru/72444.html>
2. Горбенко, А. О. Основы информационной безопасности (введение в профессию) : учебное пособие / А. О. Горбенко. — Санкт-Петербург : Интермедия, 2025. — 335 с. — ISBN 978-5-4383-0136-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/66797.html>
3. Информационная безопасность при управлении техническими системами [Электронный ресурс]: учебное пособие/ С.А. Баркалов [и др.].— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2025.— 528 с.— Режим доступа: <http://www.iprbookshop.ru/68589.html>

### 9.3 Программное обеспечение

#### Операционные системы

- *Альт Линукс*: российская операционная система, обеспечивающая высокий уровень безопасности и соответствие национальным стандартам.
- *РЕД ОС*: отечественная разработка, ориентированная на использование в государственных учреждениях и образовательных организациях.
- *Астра Линукс*: система с повышенными требованиями к безопасности, активно применяемая в различных секторах, включая образование.
- *ОС РОСА ХРОМ*: операционная система предназначена для оснащения рабочих мест пользователей без специальных требований по информационной безопасности.

## **Офисные пакеты**

- *МойОфис*: российский офисный пакет, включающий текстовый редактор, табличный процессор и другие инструменты для работы с документами.
- *P7-Офис*: еще одно отечественное решение, поддерживающее работу с текстами, таблицами и презентациями, полностью совместимое с форматами Microsoft Office.

## **Антивирусное ПО**

- *Kaspersky Lab*: один из ведущих мировых производителей антивирусного ПО, широко используемый в образовательных учреждениях России.
- *Dr.Web*: надежное антивирусное решение с многолетней историей использования в учебных заведениях.

## **Видеоконференции и коллаборация**

- *Сферум*: отечественная платформа для видеоконференций и совместной работы, созданная специально для образовательных нужд.
- *Яндекс.Телемост*: сервис от Яндекса, обеспечивающий надежную видеосвязь и удобные инструменты для онлайн-обучения.
- *TrueConf*: российское решение для видеоконференций, поддерживающее высокое качество связи и широкие функциональные возможности.
- *МТС Линк*: делает коммуникацию со студентами и сотрудниками быстрее, результативнее и выгоднее; позволяет эффективно решить все задачи вуза по онлайн-коммуникациям.

## **СУБД (Системы управления базами данных)**

- *Postgres Pro*: отечественная версия PostgreSQL, адаптированная для использования в России и активно применяемая в образовательных учреждениях.
- *Ред База Данных*: российская система управления базами данных, основанная на Firebird и обеспечивающая высокую надежность и производительность.
- *YDB (ранее Yandex Database)*: масштабируемая база данных от Яндекса, подходящая для различных задач, включая образовательные.

## **Облачное хранилище**

- *Яндекс.Диск*: отечественное облачное хранилище, предлагающее удобный доступ к файлам и интеграцию с другими сервисами Яндекса.
- *Облако Mail.ru*: еще одно популярное российское решение для хранения и обмена файлами, активно используемое в образовании.
- *МойОфис Хранилище*: часть офисного пакета МойОфис, обеспечивающая безопасное хранение и совместную работу с документами.

## **Система управления обучением**

- *Платформа Teachbase*: система дистанционного обучения, которая предназначена для автоматизации процессов обучения за счет своевременного обучения её пользователей и возможности оперативного контроля за подготовкой и переподготовкой пользователей.
- *iSpring Learn*: LMS с полным циклом обучения.
- *GetCourse*: платформа для онлайн-школы, дает возможность создавать тренинги, вести базу.
- *Stepik*: российская образовательная платформа и конструктор бесплатных и платных открытых онлайн-курсов и уроков.

## **Системы управления проектами и совместной работы**

- *Яндекс.Трекер*: российская система для управления задачами и проектами, интегрированная с другими сервисами Яндекса.
- *Сфера*: платформа для управления проектами и задачами, широко используемая в российских компаниях и образовательных учреждениях.
- *Трекер P7-Офис*: часть офисного пакета P7-Офис, предлагающая инструменты для совместной работы и управления проектами.
- *TeamStorm*: платформа для управления командами и процессами разработки.

### Формы и опросы

- *Яндекс.Формы*: российский сервис для создания опросов и анкет, предлагающий удобные инструменты для сбора и анализа данных.
- *Сервисы от 1С: Управление*: специализированные решения для создания и анализа опросов и анкет, используемые в российских организациях.
- *Testograf*: сервис для создания опросов, анкет и тестов для клиентов и сотрудников. Он предоставляет набор инструментов для создания и анализа опросов, а также для управления результатами и отчётами.
- *Univer Online. Анкетирование*: предназначен для сбора и предоставления руководству вуза актуальной информации о качестве образовательного процесса

### Программы для работы с PDF-документами

- *PDF Commander*: российское решение для работы с PDF-файлами, предлагающее широкий функционал для создания, редактирования и просмотра документов.
- *МойОфис Стандартный. Документы*: часть офисного пакета МойОфис, включающая инструменты для работы с PDF-документами.
- *Master PDF*: многофункциональный и простой в использовании редактор файлов в формате PDF.
- *Content AI (ABBYY)*: многофункциональный редактор для решения любых задач с PDF и бумажными документами.

### Почтовые клиенты

- *КриптоАРМ ГОСТ 3*: универсальное приложение для работы с электронными документами со встроенным почтовым клиентом, позволяющим безопасно обмениваться файлами.
- *P7-Офис. Органайзер*: предназначен для управления почтой, деловым расписанием, работы с контактами и планирования задач.
- *RuPost Desktop*: предоставляет полный набор инструментов для организации вашей рабочей жизни. Это включает в себя управление почтой, календарями, контактами, задачами и даже панель быстрых кнопок для удобства.

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

1. Центр дистанционного образования (ЦДО) СахГУ <http://lk.sakhgu.ru/>
2. Официальный сайт Сахалинского государственного университета. <http://www.sakhgu.ru/>
3. Система Антиплагиат ВУЗ <https://xn----7sbaald5acc1auz1bhr.xn--p1ai/>
4. Сайт электронно-библиотечной системы, ООО «Электронное издательство Юрайт» <https://urait.ru/>
5. Справочно-правовая система «Консультант Плюс» <https://www.consultant.ru/>
6. Информационно - правовой портал <https://www.garant.ru/>
7. Сайт научной электронной библиотеки eLIBRARY <https://elibrary.ru/defaultx.asp>
8. Studfiles. <http://www.studfiles.ru/all-vuz/eie/>
9. Единое окно доступа к информационным ресурсам: <http://window.edu.ru/resource/771/40771>
10. Сайт национальной электронной библиотеки <https://нэб.рф>
11. КнигаФонд; ООО «Центр цифровой дистрибуции»: <http://www.knigafund.ru>
12. Электронная библиотека диссертаций; Российская государственная библиотека; <http://www.rsl.ru>; ФГБУ «Российская государственная библиотека»
13. Сайт Университетской библиотеки ONLINE; ООО «Некс-Медиа» (RU); <http://www.biblioclub.ru>
14. ЭБС Издательства «Лань»; ООО «Лань-Тренд»; [www.e.lanbook.com](http://www.e.lanbook.com)

15. Сайт информационной справочной системы Polpred <http://polpred.com/>
16. Сайт электронно-библиотечной системы IPRbooks; ООО «Ай Пи Эр Медиа»; <http://www.iprbookshop.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 2025/2026 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)