Федеральное государственное бюджетное образовательное учреждение высшего образования

**РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА и ГОСУДАРСТВЕННОЙ СЛУЖБЫ при ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ**

Факультет среднего профессионального образования

УТВЕРЖДЕНА
решением цикловой (методической) комиссии общепрофессиональных дисциплин и профессиональных модулей специальностей 09.02.07 Информатика и вычислительная техника
Протокол от 31.10.2025 № 2

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## ОП.06. Основы информационной безопасности

Специальность – 09.02.12 Техническая эксплуатация и сопровождение информационных систем

Профиль – на базе основного общего образования

Квалификация – специалист по технической эксплуатации и сопровождению информационных систем

Форма обучения – очная

Год набора – 2026

Санкт-Петербург 2025 год

**Автор-составитель:** Вилков Владислав Евгеньевич, преподаватель ФСПО СЗИУ РАНХиГС.

**СОДЕРЖАНИЕ**

## 1 Общие положения

### 1.1 Область применения программы

Рабочая программа учебной дисциплины «Основы информационной безопасности» является частью основной профессиональной образовательной программы по специальности СПО 09.02.12 «Техническая эксплуатация и сопровождение информационных систем».

### 1.2 Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Основы информационной безопасности» является частью профессиональной подготовки, входит в общепрофессиональный цикл дисциплин. Базируется на таких дисциплинах, как «Информатика», «Операционные системы и среды», «Основы алгоритмизации и программирования» является основополагающей для такой дисциплины, как «Разработка информационных систем».

Дисциплина изучается на 2 курсе в 3 семестре.

### 1.3 Цели и задачи учебной дисциплины

Цель дисциплины «Основы информационной безопасности»: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Задачи дисциплины:

– овладение понятийным аппаратом информационной безопасности (освоение ключевых терминов и определений, понимание исторического контекста и эволюции информационной безопасности, осознание актуальности современных угроз и рисков);

– формирование знаний в области нормативно-правового регулирования (изучение действующих законов, стандартов и регламентов в сфере информационной безопасности, включая международные стандарты ISO 27001, GDPR и др., освоение принципов разработки политик и процедур безопасности);

– освоение основ криптографии (понимание принципов работы симметричных и асимметричных алгоритмов шифрования, хэширования и цифровых подписей, знакомство со стеганографией и практическими аспектами применения криптографических методов);

– приобретение навыков защиты сетевой инфраструктуры (изучение базовых принципов сетевой безопасности, методов противодействия атакам типа DDoS, MITM и др., практическое освоение технологий VPN и межсетевых экранов);

– развитие компетенций в области безопасности приложений (изучение типичных уязвимостей веб-приложений согласно OWASP Top Ten, освоение практик безопасного программирования, навыков тестирования на проникновение и анализа уязвимостей);

– овладение методами защиты данных (понимание принципов шифрования данных в покое и в транзите, освоение процедур резервного копирования и восстановления данных, управление доступом к информации);

– изучение особенностей безопасности облачных технологий (освоение моделей облачных услуг — IaaS, PaaS, SaaS — и связанных с ними аспектов безопасности, практическое исследование механизмов защиты в облачных средах);

– формирование навыков реагирования на инциденты безопасности (освоение процедур анализа и управления инцидентами, основ цифровой криминалистики и форензики, методов восстановления после инцидентов, знакомство с аспектами кибербезопасности, промышленного шпионажа и OSINT);

– осознание роли человеческого фактора в информационной безопасности (изучение методов социальной инженерии, психологических аспектов атак, разработка и внедрение политик информационной безопасности для персонала);

– ориентация в перспективных направлениях информационной безопасности (анализ современных тенденций и новых технологий — AI, ML, блокчейн — в сфере безопасности, осмысление этических аспектов информационной безопасности).

**1.4 Планируемые результаты обучения по дисциплине**

**Перечень компетенций**

| ***Код ОК,*** ***ПК*** | **Уметь** | **Знать** | **Владеть навыками** |
|---|---|---|---|
| ОК.01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, | актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; | - |

| ***Код ОК,*** ***ПК*** | **Уметь** | **Знать** | **Владеть навыками** |
|---|---|---|---|
| | необходимую для решения задачи и/или проблемы; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) | алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности | |
| ОК.02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности | определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать | номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств. | - |

| ***Код ОК,*** ***ПК*** | **Уметь** | **Знать** | **Владеть навыками** |
|---|---|---|---|
| | современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач | | |
| ОК.09 Пользоваться профессиональной документацией на государственном и иностранном языках | понимать тексты на базовые профессиональные темы | лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности | - |
| ПК 1.7 Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем | - идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС - осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС - разрабатывать документы в рамках технической поддержки процессов создания (модификации) и сопровождения ИС - настраивать СУБД в рамках технической поддержки процессов создания (модификации) и сопровождения ИС | - основы ИБ организации - модель угроз информационной безопасности ИС организации заказчика - процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика - основы администрирования СУБД - основы системного администрирования - Коммуникационное оборудование - сетевые протоколы - Основы современных операционных систем - устройство и функционирование современных ИС - основы архитектуры мультиарендного | - распознавание инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС - передача информации об инцидентах в службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС - информирование заинтересованных лиц заказчика и в своей организации об инцидентах ИБ, связанных с работой ИС, для принятия управленческих решений, минимизирующих |

| ***Код ОК,*** ***ПК*** | **Уметь** | **Знать** | **Владеть навыками** |
|---|---|---|---|
| | | программного обеспечения | ущерб от инцидента ИБ, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС - временное блокирование доступа к ИС (при необходимости) при обнаружении инцидентов ИБ в рамках технической поддержки процессов создания (модификации) и сопровождения ИС |

В результате освоения учебной дисциплины студент должен:

| | |
|---|---|
| иметь практический опыт | – работы с криптографическими средствами защиты информации;<br>– настройке и администрированию систем безопасности;<br>– выявления и предотвращения информационных угроз;<br>– применения методов аутентификации и авторизации;<br>– работы с системами обнаружения вторжений;<br>– проведения аудита безопасности информационных систем;<br>– реагирования на инциденты информационной безопасности;<br>– разработки политик безопасности;<br>– настройке средств шифрования данных;<br>– работы с системами резервного копирования. |
| уметь | – выявлять задачи и проблемы в профессиональном или социальном контексте;<br>– анализировать задачи и проблемы, выделяя их составные элементы;<br>– определять этапы решения задачи;<br>– находить и эффективно использовать информацию, необходимую для решения задачи или проблемы;<br>– составлять план действий для решения задачи;<br>– определять требуемые ресурсы для реализации плана;<br>– применять актуальные методы работы в профессиональной и смежных областях;<br>– реализовывать намеченный план;<br>– оценивать результаты и последствия своих действий (самостоятельно или с помощью наставника);<br>– формулировать задачи для информационного поиска;<br>– выбирать необходимые источники информации;<br>– планировать процесс поиска информации;<br>– структурировать полученные данные;<br>– выделять наиболее значимые элементы в массиве информации;<br>– оценивать практическую ценность результатов поиска; |

| | |
|---|---|
| | – оформлять результаты информационного поиска;<br>– использовать информационные технологии для решения профессиональных задач;<br>– работать с современным программным обеспечением;<br>– применять цифровые инструменты для решения профессиональных задач;<br>– понимать тексты на базовые профессиональные темы;<br>– обеспечивать шифрование и конфиденциальность данных;<br>– анализировать требования к безопасности информационных систем;<br>– разрабатывать и внедрять меры безопасности;<br>– реализовывать технические решения по защите данных (хэширование паролей, сессионные токены, двухфакторная аутентификация). |
| знать | – актуальный профессиональный и социальный контекст профессиональной деятельности;<br>– основные источники информации и ресурсы, необходимые для решения задач и проблем в профессиональной и/или социальной сфере;<br>– алгоритмы выполнения работ в профессиональной области и смежных сферах;<br>– методы работы в профессиональной сфере и смежных областях;<br>– структуру плана, необходимого для решения профессиональных задач;<br>– порядок оценки результатов решения задач в профессиональной деятельности;<br>– номенклатуру информационных источников, используемых в профессиональной деятельности;<br>– приёмы структурирования информации;<br>– формат оформления результатов информационного поиска, а также современные средства и устройства информатизации;<br>– порядок применения современных средств информатизации и программного обеспечения (в том числе цифровых инструментов) в профессиональной деятельности;<br>– профессиональную лексику, необходимую для описания предметов, средств и процессов в своей сфере деятельности;<br>– принципы обеспечения безопасности хранения данных;<br>– методы защиты баз данных от внешних угроз;<br>– основы криптографии и методы шифрования данных;<br>– стандарты и протоколы безопасности (включая SSL/TLS, SSH, Kerberos, HTTPS, OAuth, OpenID Connect);<br>– методы аутентификации и авторизации пользователей (использование паролей, сертификатов, биометрических данных);<br>– законодательные и нормативные акты в сфере информационной безопасности (GDPR, HIPAA, PCI DSS и др.);<br>– отраслевую нормативную техническую документацию и ключевые источники информации для профессиональной деятельности;<br>– современный отечественный и зарубежный опыт в профессиональной сфере;<br>– принципы и методы обеспечения безопасности информационных систем;<br>– современные технологии и методы в области безопасности информационных систем;<br>– источники угроз информационной безопасности и способы их предотвращения;<br>– основные угрозы безопасности мобильных приложений;<br>– стандартные криптографические алгоритмы для шифрования данных;<br>– принципы обеспечения безопасности передачи данных по сети;<br>– основы безопасности приложений и ИТ-инфраструктуры;<br>– методы анализа уязвимостей и мониторинга безопасности; |

| | |
|---|---|
| | – ключевые принципы и методы защиты ИТ-инфраструктуры и веб-приложений;<br>– типовые уязвимости и угрозы безопасности, а также способы их обнаружения и предотвращения;<br>– инструменты и технологии обеспечения безопасности ИТ-инфраструктуры и веб-приложений (брандмауэры, системы обнаружения вторжений, антивирусные программы). |

## 2 Структура и содержание дисциплины

### 2.1 Объем учебной дисциплины и виды работ

| Виды учебной работы | Объем учебной работы, час. |
|---|---|
| Учебная нагрузка обучающихся всего, в том числе: | 60 |
| лекции | 12 |
| практические занятия | 40 |
| курсовая работа | - |
| самостоятельная работа обучающихся | - |
| консультации | 2 |
| промежуточная аттестация | 6 |
| Форма промежуточной аттестации | Экзамен |

### 2.2 Тематический план и содержание дисциплины

| № п/п | Наименование тем (разделов) | Содержание тем (разделов) | Распределение часов | | | Формируемые компетенции | Формы текущего контроля |
|---|---|---|---|---|---|---|---|
| | | | Л | ПР | СРС | | |
| | **Раздел 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** | | | | | | |
| 1 | Тема 1.1. Введение в информационную безопасность | **Содержание учебного материала**<br>Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности | 2 | - | - | ОК.01, ОК.02, ОК.09 | О |
| 2 | Тема 1.2. Управление безопасностью информации | **Содержание учебного материала**<br>Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.) | 2 | - | - | ОК.01, ПК 1.7, | О |
| 3 | Тема 1.3. Криптография | **Содержание учебного материала**<br>Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение | 1 | 12 | - | ОК.02, ПК 1.7, | О,Т,ПЗ, |

| № п/п | Наименование тем (разделов) | Содержание тем (разделов) | Распределение часов | | | Формируемые компетенции | Формы текущего контроля |
|---|---|---|---|---|---|---|---|
| | | | Л | ПР | СРС | | |
| | | криптографии в приложениях. Стеганография. **Практические занятия:** Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения. | | | | | |
| 4 | Тема 1.4. Защита сетевой инфраструктуры | **Содержание учебного материала** Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов **Практические занятия:** Организация защиты от атак Организация работы VPN и межсетевого экрана | 1 | 6 | - | ОК.01, | О,Т,ПЗ |
| 5 | Тема 1.5. Безопасность приложений | **Содержание учебного материала** Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей. **Практические занятия:** Тестирование на проникновение и анализ уязвимостей. | 1 | 6 | - | ОК.02, ОК.09, ПК 1.7 | О,Т,ПЗ |
| 6 | Тема 1.6. Защита данных | **Содержание учебного материала** Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным **Практические занятия:** Выполнение резервного копирования и восстановления данных. Управление доступом к данным | 1 | 4 | - | ПК 1.7 | О,Т,ПЗ |
| 7 | Тема 1.7. Безопасность облачных технологий | **Содержание учебного материала** Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности **Практические занятия:** Изучение модели облачных услуг и их безопасности | 1 | 4 | - | ОК.01, ОК.09, ПК 1.7 | О,Т,ПЗ |

| № п/п | Наименование тем (разделов) | Содержание тем (разделов) | Распределение часов | | | Формируемые компетенции | Формы текущего контроля |
|---|---|---|---|---|---|---|---|
| | | | Л | ПР | СРС | | |
| 8 | Тема 1.8. Инциденты безопасности | **Содержание учебного материала** Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика **Практические занятия:** Работа с инцидентами. | 1 | 4 | - | ОК.01, ПК 1.7 | О,Т,ПЗ |
| 9 | Тема 1.9. Социальная инженерия и человеческий фактор | **Содержание учебного материала** Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности **Практические занятия:** Разработка политики информационной безопасности | 1 | 4 | - | ОК.09, ПК 1.7 | О,Т,ПЗ |
| 10 | Тема 1.10. Будущее информационной безопасности | **Содержание учебного материала** Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности | 1 | - | - | ОК.01, ОК.02, ПК 1.7 | О |
| | | Итого часов: | 12 | 40 | - | | |

### 2.3. Регламент распределения видов работ по дисциплине с ДОТ

Данная дисциплина реализуется с применением дистанционных образовательных технологий (ДОТ). Распределение видов учебной работы, форматов текущего контроля представлены в Таблице 2.3.

Таблица 2.3. — Распределение видов учебной работы и текущей аттестации

| **Вид учебной работы** | **Формат проведения** |
|---|---|
| Лекционные занятия | Частично с применением ДОТ |
| Практические занятия | Частично с применением ДОТ |
| Текущий контроль | Частично с применением ДОТ |
| Промежуточная аттестация | Контактная аудиторная работа |
| **Формы текущего контроля** | **Формат проведения** |

| | |
|---|---|
| Тестирование | Частично с применением ДОТ |
| Опрос | Контактная аудиторная работа |
| Практические задания | Частично с применением ДОТ |

Доступ к системе дистанционных образовательных программ осуществляется каждым обучающимся самостоятельно с любого устройства на портале: https://sziu-de.ranepa.ru, в соответствии с их индивидуальным паролем и логином к личному кабинету/ профилю.

Текущий контроль, проводимый в системе дистанционного обучения, оцениваются как в системе дистанционного обучения, так и преподавателем вне системы.

Доступ к материалам лекций предоставляется в течение всего семестра по мере прохождения освоения программы. Доступ к каждому виду работ и количество попыток на выполнение задания предоставляется ограниченное время согласно регламенту дисциплины, опубликованному в системе дистанционного обучения. Преподаватель оценивает выполненные обучающимися работы не позднее 14 рабочих дней после окончания срока выполнения.

## 3 Материалы текущего контроля успеваемости и промежуточной аттестации обучающихся

### 3.1 Формы и методы текущего контроля успеваемости и промежуточной аттестации обучающихся

Формы текущего контроля успеваемости:

**Опрос (О**) позволяет выявить правильность ответа по содержанию, его последовательность, самостоятельность суждений и выводов, степень развития логического мышления.

| Оценка | Критерии оценивания |
|---|---|
| **«Отлично»** | Ответ правильный по содержанию, логически выстроен и последователен. Студент демонстрирует самостоятельность суждений и выводов, свободно оперирует терминами, раскрывает суть понятий и их взаимосвязи. Проявляется высокий уровень развития логического мышления: студент способен анализировать, сопоставлять, приводить примеры и аргументировать позицию. |

| | |
|---|---|
| **«Хорошо»** | Ответ в целом правильный и достаточно последовательный, отражает понимание основных положений темы. Студент владеет терминологией, но может испытывать небольшие затруднения при раскрытии сложных взаимосвязей или аргументации. Допускаются незначительные неточности, которые студент способен исправить самостоятельно после наводящих вопросов. |
| **«Удовлетворительно»** | Ответ содержит основные сведения по теме, но отличается недостаточной последовательностью, фрагментарностью или слабой аргументацией. Студент знает базовые понятия, но испытывает трудности в раскрытии их взаимосвязей и применении на практике. Для устранения пробелов требуется руководство преподавателя. |
| **«Неудовлетворительно»** | Ответ неправильный или крайне неполный, отсутствует логическая структура, наблюдается путаница в терминах и понятиях. Студент не способен самостоятельно сформулировать выводы, не демонстрирует понимания сути темы. Требуется повторное изучение основных разделов дисциплины под руководством преподавателя. |

**Тестирование (Т)** – задания, с вариантами ответов.

| Оценка | Критерии оценивания |
|---|---|
| **«Отлично»** | Студент правильно ответил на 90–100 % вопросов теста. Ответы демонстрируют уверенное владение материалом, отсутствие ошибок в базовых и усложнённых заданиях. |
| **«Хорошо»** | Студент правильно ответил на 75–89 % вопросов. Допускаются отдельные неточности, не искажающие суть понятий; в целом материал усвоен, но есть пробелы в отдельных темах. |
| **«Удовлетворительно»** | Студент правильно ответил на 50–74 % вопросов. Усвоены базовые понятия, но имеются существенные пробелы; допускаются ошибки в применении правил и интерпретации условий заданий. |

| | |
|---|---|
| **«Неудовлетворительно»** | Студент правильно ответил менее чем на 50 % вопросов либо не представил тест на проверку. Проявлены значительные пробелы в знаниях, непонимание ключевых тем дисциплины. |

**Практическое задание (ПЗ)** используется для закрепления теоретических знаний и отработки навыков и умений, способности применять знания при решении конкретных задач.

| Оценка | Критерии оценивания |
|---|---|
| **«Отлично»** | Студент демонстрирует глубокое знание материала и свободно выполняет задание. Понимает взаимосвязь основных понятий темы, обосновывает выбранные методы решения, корректно интерпретирует результаты. Работа выполнена полностью, без ошибок, с соблюдением всех требований к оформлению и срокам сдачи. |
| **«Хорошо»** | Студент полностью знает материал и успешно выполняет предусмотренные задания. Допускает незначительные ошибки (неточность фактов, небольшие погрешности в расчётах или оформлении, стилистические неточности), которые не влияют на общий результат и могут быть быстро исправлены самостоятельно. |
| **«Удовлетворительно»** | Студент владеет основным материалом в объёме, необходимом для дальнейшего изучения дисциплины, и справляется с выполнением задания. Допускает погрешности в решении или оформлении, но обладает необходимыми знаниями для их устранения под руководством преподавателя. Работа в целом соответствует требованиям, но нуждается в доработке. |
| **«Неудовлетворительно»** | Студент имеет существенные пробелы в знании основного материала, не справляется с выполнением задания или допускает серьёзные ошибки, искажающие результат. Нуждается в повторении основных разделов курса под руководством преподавателя; работа не соответствует требованиям либо сдана с грубыми нарушениями сроков и формата. |

**Формы текущего контроля**

| № п/п | Название темы | Формы текущего контроля успеваемости |
|---|---|---|
| 1 | Тема 1.1. Введение в информационную безопасность | О |
| 2 | Тема 1.2. Управление безопасностью информации | О |
| 3 | Тема 1.3. Криптография | Т, ПЗ, О |
| 4 | Тема 1.4. Защита сетевой инфраструктуры | Т, ПЗ, О |
| 5 | Тема 1.5. Безопасность приложений | Т, ПЗ, О |
| 6 | Тема 1.6. Защита данных | Т, ПЗ, О |
| 7 | Тема 1.7. Безопасность облачных технологий | Т, ПЗ, О |
| 8 | Тема 1.8. Инциденты безопасности | Т, ПЗ, О |
| 9 | Тема 1.9. Социальная инженерия и человеческий фактор | Т, ПЗ, О |
| 10 | Тема 1.10. Будущее информационной безопасности | О |

Примечание. В столбце «Форма текущего контроля успеваемости, промежуточной аттестации» перечисляются все используемые в учебном процессе по данной дисциплине формы контроля освоения материала. (Т – тестирование; ПЗ – практическое задание, О - опрос).

### 3.2 Оценочные средства текущего контроля успеваемости обучающихся

**Вопросы к устному опросу:**

***Тема 1.6. Защита данных***

1. Объясните разницу между шифрованием данных «в покое» (*data at rest*) и «в транзите» (*data in transit*). Приведите по одному конкретному примеру технологий или протоколов, применяемых для каждого типа шифрования, и поясните, почему для этих сценариев требуются разные подходы.

2. Перечислите ключевые принципы стратегии резервного копирования данных (например, правило 3-2-1) и подробно раскройте каждый из них. Объясните, почему соблюдение этих принципов критически важно для обеспечения устойчивости бизнеса к инцидентам потери данных.

3. Опишите последовательность действий при планировании процедуры восстановления данных после сбоя. Укажите, какие факторы необходимо учитывать при определении допустимого времени восстановления (*RTO*) и допустимой потери данных (*RPO*), и как эти показатели влияют на выбор стратегии резервного копирования.

4. Расскажите о моделях управления доступом к данным (DAC, MAC, RBAC, ABAC). Сравните их основные особенности, приведите пример сценария, где каждая из них будет

наиболее эффективна, и объясните, почему организация может выбрать ту или иную модель в зависимости от своих потребностей в безопасности.

5. Перечислите типичные угрозы для конфиденциальности и целостности данных при их хранении и передаче. Для каждой угрозы укажите не менее одного технического или организационного метода защиты, который позволяет снизить риски её реализации, и кратко поясните принцип работы этого метода.

### *Тема 1.7. Безопасность облачных технологий*

1. Перечислите ключевые особенности обеспечения безопасности в облачных средах, отличающие их от традиционных локальных инфраструктур. Объясните, как распределённая природа облаков и мультитенантность влияют на подходы к защите данных и какие новые риски они порождают.

2. Сравните модели облачных услуг IaaS, PaaS и SaaS с точки зрения распределения ответственности за безопасность между провайдером и клиентом. Для каждой модели укажите, за какие аспекты безопасности отвечает поставщик услуг, а за какие — потребитель, и приведите по одному конкретному примеру уязвимости, характерной для каждой модели.

3. Опишите основные механизмы изоляции данных в мультитенантных облачных средах. Перечислите не менее трёх технических решений или протоколов, обеспечивающих разделение ресурсов между клиентами, и объясните, как они предотвращают перехват данных или несанкционированный доступ между разными арендаторами.

4. Расскажите о роли шифрования в обеспечении безопасности облачных сервисов. Укажите, какие типы данных следует шифровать в облаке, какие алгоритмы и ключи рекомендуется использовать, и в чём заключаются особенности управления ключами шифрования в облачной среде по сравнению с локальной инфраструктурой.

5. Перечислите основные рекомендации по безопасному использованию облачных сервисов с точки зрения конечных пользователей и администраторов. Укажите не менее пяти конкретных действий или настроек (например, многофакторная аутентификация, мониторинг логов, настройка политик доступа), объясните, как каждое из них повышает защищённость, и приведите пример сценария, где отсутствие такой меры может привести к инциденту безопасности.

## Примеры практических заданий

***Тема 1.1. Введение в информационную безопасность***

***1. Анализ актуальных угроз***

***Задание:*** на основе открытых источников (отчёты компаний-вендоров, новостные публикации за последний год) составьте перечень из 5–7 наиболее распространённых угроз ИБ в корпоративной среде. Для каждой угрозы укажите:

- краткое описание механизма реализации;
- потенциальный ущерб;
- пример реального инцидента (с указанием года и организации).
- Результаты оформите в виде таблицы.

***2. Исторический обзор***

***Задание:*** подготовьте краткую хронологию (10–12 ключевых событий) развития ИБ с 1970-х годов до настоящего времени. Для каждого события укажите год, название/описание и его значение для отрасли. Представьте результат в виде временной шкалы (можно в графическом редакторе или таблице).

***Тема 1.2. Управление безопасностью информации***

***1. Анализ нормативно-правовой базы***

***Задание:*** сравните требования к защите персональных данных в РФ (ФЗ-152) и ЕС (GDPR) по следующим критериям:

- определение персональных данных;
- обязанности оператора;
- штрафы за нарушения;
- сроки уведомления о инцидентах.
- Результаты представьте в сравнительной таблице.

***2. Оценка рисков по методике ISO 27001***

***Задание:*** для условного предприятия (выберите сферу деятельности самостоятельно) проведите упрощённую оценку рисков:

- выделите 3–4 ключевых информационных актива;
- для каждого актива определите 2–3 угрозы и уязвимости;
- оцените вероятность и воздействие по 5-балльной шкале;
- рассчитайте уровень риска (вероятность × воздействие).

Оформите результаты в виде матрицы рисков.

***Тема 1.3. Криптография***

***1. Шифрование данных***

***Задание:*** используя инструмент OpenSSL (или аналогичный), выполните:

- генерацию пары ключей (RSA, 2048 бит);
- шифрование текстового файла открытым ключом;
- расшифрование закрытым ключом.
- Опишите последовательность команд и приведите скриншоты результатов.

***2. Анализ алгоритмов хэширования***

***Задание:*** для строк «Hello, World!» и «Hello, world!» рассчитайте хэши SHA-256 и MD5. Сравните результаты, объясните, почему они различаются. Приведите код (на любом языке программирования) или команды консоли для расчёта.

**Примеры тестовых заданий**

***Часть 1. Задания с выбором одного правильного ответа***

***1.*** Что такое DDoS-атака?

а) Кража данных через уязвимость в ПО

б) Перегрузка ресурса множеством запросов с целью нарушения его работы

в) Внедрение вредоносного кода в веб-приложение

г) Перехват сетевого трафика

***Часть 2. Задания на установление соответствия***

2. Установите соответствие между угрозой и её описанием:

Угроза:

1. Фишинг
2. Вредоносное ПО
3. SQL-инъекция
4. Эксплойт

Описание:

А) Неавторизованный доступ к системе через уязвимость

Б) Отправка поддельных писем для кражи данных

В) Программы, наносящие вред системе (вирусы, трояны)

Г) Внедрение вредоносного кода в запросы к БД

***Часть 3. Задания на последовательность действий***

3. Установите правильную последовательность этапов реагирования на инцидент ИБ:

а) Локализация угрозы

б) Уведомление заинтересованных сторон

в) Выявление инцидента

г) Восстановление систем

д) Анализ причин и предотвращение повторений

***Часть 4. Ситуационные задачи***

4. В компании произошёл инцидент: злоумышленники получили доступ к базе данных клиентов. Какие шаги необходимо предпринять в первую очередь? Опишите план действий по этапам (не менее 4 шагов).

### 3.3 Оценочные средства по дисциплине для промежуточной аттестации

**Вопросы для подготовки к экзамену**

1. Дайте определение информационной безопасности (ИБ). Перечислите и раскройте три основных принципа ИБ (триада CIA).

2. Охарактеризуйте этапы развития ИБ: от первых систем до современности.

3. Что такое угроза ИБ? Приведите классификацию угроз по источникам возникновения.

4. Перечислите 5–7 актуальных угроз ИБ в корпоративной среде (2024–2025 гг.) и кратко опишите механизмы их реализации.

5. В чём заключается понятие «риск ИБ»? Как соотносятся угрозы, уязвимости и риски?

6. Перечислите ключевые нормативно-правовые акты РФ в области ИБ (не менее 4). Укажите их сферу регулирования.

7. Что регулирует GDPR? Назовите 3–4 основных требования этого регламента.

8. Опишите структуру политики ИБ организации. Какие разделы она должна включать?

9. Изложите методику оценки рисков ИБ по стандарту ISO 27001 (этапы, критерии, инструменты).

10. В чём заключается принцип «соответствия стандартам»? Приведите примеры сертификатов ИБ и их значение.

11. Объясните разницу между симметричным и асимметричным шифрованием. Приведите примеры алгоритмов.

12. Что такое хеш-функция? Назовите 2–3 алгоритма хеширования и области их применения.

13. Опишите принцип работы VPN. Какие протоколы VPN считаются наиболее безопасными?

14. Что такое MITM-атака? Перечислите способы защиты от неё.

15. Как межсетевой экран (firewall) обеспечивает защиту сети? Опишите типы правил фильтрации.

16. Перечислите основные компоненты сетевой безопасности (не менее 5).

17. Что такое DDoS-атака? Опишите 3–4 метода её реализации и способы противодействия.

18. Как настроить правила iptables для блокировки подозрительного трафика? Приведите примеры команд.

19. В чём отличие DMZ-зоны от внутренней сети? Как она повышает безопасность?

20. Что такое IDS/IPS? Чем отличаются эти системы?

21. Перечислите 5 уязвимостей из OWASP Top 10 2023 и кратко опишите каждую.

22. Что такое SQL-инъекция? Приведите пример кода с уязвимостью и способ её устранения.

23. Опишите принципы безопасного программирования (не менее 5 правил).

24. Что включает тестирование на проникновение (penetration testing)? Перечислите этапы.

25. Как обнаружить XSS-уязвимость? Приведите пример вредоносного скрипта и метод защиты.

26. В чём разница между шифрованием «в покое» и «в транзите»? Приведите примеры технологий для каждого случая.

27. Опишите стратегию 3-2-1 для резервного копирования. Почему она считается надёжной?

28. Что такое RBAC? Приведите пример матрицы доступа для компании из 3 ролей.

29. Как реализовать шифрование диска в Linux/Windows? Назовите инструменты.

30. Что такое токенизация данных? В каких сценариях она применяется?

31. Сравните модели IaaS, PaaS и SaaS по уровню ответственности за безопасность.

32. Перечислите 4–5 ключевых рисков безопасности в облаке.

33. Что такое CSPM? Как он помогает управлять облачной безопасностью?

34. Опишите принцип «безопасности как кода» (Security as Code) в облачных средах.

35. Как обеспечить шифрование данных в облачном хранилище? Приведите примеры сервисов.

36. Перечислите этапы жизненного цикла инцидента ИБ (от обнаружения до закрытия).

37. Что такое цифровая криминалистика? Опишите порядок сбора цифровых улик.

38. Как составить отчёт о инциденте (IR Report)? Какие разделы он должен включать?

39. Что такое OSINT? Приведите 3 примера источников OSINT для расследования инцидентов.

40. Опишите сценарий реагирования на утечку данных (действия в первые 24 часа).

41. Перечислите 5 техник социальной инженерии и приведите примеры их применения.

42. Как обучить сотрудников распознавать фишинговые письма? Назовите 4–5 признаков фишинга.

43. Что такое «красная команда» (Red Team)? Как она тестирует устойчивость к социальной инженерии?

44. Опишите структуру программы повышения осведомлённости по ИБ (security awareness program).

45. Как разработать политику парольной безопасности? Приведите требования к паролям

46. Как ИИ и ML применяются в ИБ? Приведите 3 примера использования.

47. В чём заключаются риски безопасности блокчейна? Как их минимизировать?

48. Что такое квантовая криптография? Почему она считается перспективной?

49. Опишите этические проблемы использования ИИ в кибербезопасности (не менее 3).

50. Какие новые угрозы могут появиться в связи с развитием IoT и 6G? Предложите способы защиты.

## 4. Методические указания для обучающихся по освоению дисциплины

Приступая к изучению дисциплины «Основы информационной безопасности», студент должен ознакомиться с содержанием данной «Рабочей учебной программы дисциплины» с тем, чтобы иметь четкое представление о своей работе.

В первую очередь необходимо уяснить цель и задачи изучаемой дисциплины, оценить объем материала, познакомиться с предложенной и подобрать основную и дополнительную

литературу, выявить наиболее важные проблемы, стоящие по вопросам изучаемой дисциплины.

Выполнение заданий осуществляется в соответствии с учебным планом и программой. Они должны выполняться в соответствии с методическими рекомендациями, выданными преподавателем, и представлены в установленные преподавателем сроки.

Работая с учебниками и учебными пособиями, целесообразно законспектировать тот материал, который не сообщался студентам на лекциях.

На занятиях лекционного и практического характера студентам для работы требуется: тетрадь для записи лекций и заданий.

Для успешного овладения программой дисциплины необходимо выполнять следующие требования:

- посещать все лекционные и практические занятия;
- все рассматриваемые на лекциях и практических занятиях темы и вопросы обязательно фиксировать в тетради;
- в случае пропуска занятий по каким-либо причинам необходимо обязательно самостоятельно изучать соответствующий материал в Moodle, фиксируя записи в тетради, а также выполнять практические задания.

Подготовка к зачету с оценкой осуществляется по представленным в списке основной и дополнительной литературе. Рекомендуемые литература и интернет-ресурсы будут полезны при выполнении практических заданий и для подготовки к тестированиям.

Методические рекомендации по составлению конспекта

Конспект — сложный способ изложения содержания книги или статьи в логической последовательности. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта. Выделите главное, составьте план, представляющий собой перечень заголовков, подзаголовков, вопросов, последовательно раскрываемых затем в конспекте.

Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

При оформлении конспекта необходимо стремиться к емкости каждого предложения.

Методические рекомендации по составлению опорного конспекта

Опорный конспект — вид внеаудиторной самостоятельной работы студента по созданию краткой информационной структуры, обобщающей и отражающей суть материала лекции, темы учебника.

Опорный конспект — это наилучшая форма подготовки к ответу на вопросы.

Основная цель опорного конспекта — облегчить запоминание. Этапы составления опорного конспекта:

1. Изучить материалы темы, выбрать главное и второстепенное;

2. Установить логическую связь между элементами темы;

3. Представить характеристику элементов в краткой форме;

4. Выбрать опорные сигналы для акцентирования главной информации и отобразить в структуре работы.

Методические рекомендации по прохождению тестирования

Тестирование — это исследовательский метод, который позволяет выявить уровень знаний, умений и навыков, способностей, а также их соответствие определенным нормам усвоения, путем выполнения испытуемым ряда специальных заданий.

Следует понимать, что тестовые задания могут быть представлены в различных формах:

− задания закрытой формы, в которых обучающийся выбирает один или несколько правильных ответов из заданного набора:

− задания на дополнение (открытые задания), требующие самостоятельного получения ответов:

− задания на установления соответствия (с множественным выбором), выполнение которых связано с выявлением соответствия между элементами нескольких множеств:

− задания на установление правильной последовательности, в которых от учащегося требует указать порядок действий или процессов и другие. Этапы подготовки к тестированию:

1. Внимательно прочитайте материал по конспекту, составленному на учебном занятии. Прочитайте тот же материал по учебнику, учебному пособию.

2. Постарайтесь разобраться с непонятным, в частности новыми терминами и конструкциями.

3. Ответьте на контрольные вопросы для самопроверки, имеющиеся в учебнике, конспекте и т. д.

4. Кратко перескажите содержание изученного материала «своими словами».

5. Выучите определения основных понятий, условные обозначения, формулы и конструкции.

Подготовка к практическим занятиям

В ходе подготовки к практическим занятиям необходимо изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях, ознакомиться с программным обеспечением. Следует дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой.

Заканчивать подготовку следует закреплением материала с использованием соответствующих программных продуктов.

Все практические задания, предусмотренные рабочей программой, представлены в фонде оценочных средств по дисциплине.

Критерии оценивания выполненных практических работ:

- правильность выполнения работы (отсутствие фактических, логических и других ошибок);
- полнота выполнения работы;
- своевременность выполнения;
- правильность оформления отчета.

За задания, выполненные позже установленного срока или с нарушениями требований к оформлению, оценка на балл снижается.

Порядок организации самостоятельной работы студентов

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Целью самостоятельной работы студентов является: овладение практическими знаниями, профессиональными умениями и навыками деятельности по специальности, опытом творческой, исследовательской деятельности.

Самостоятельная работа студентов предполагает:

- самостоятельный поиск ответов и необходимой информации в рамках изучаемых тем;
- выполнение заданий для самостоятельной работы, в том числе тестов;
- изучение теоретического и лекционного материала, а также основной и дополнительной литературы при подготовке к практическим занятиям.

## 5 Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

**Основная литература**

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 202507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547 (дата обращения: 16.11.2025).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950 (дата обращения: 16.11.2025).

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 16.11.2025)

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082 (дата обращения: 16.11.2025)

**Дополнительная литература**

1. Вострецова, Е. В. Основы информационной безопасности : учебное пособие / Е. В. Вострецова. — 2019. — УДК 004.056.5(075.8), ББК 32.972.53я73, В78.

2. Галатенко, В. А. Основы информационной безопасности : учебное пособие для вузов / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий, 2020. — 264 с. — (Основы информационных технологий). — ISBN 978-5-9556-0224-2.

3. Шаньгин, В. Ф. Комплексная защита информации в компьютерных системах : учебное пособие / В. Ф. Шаньгин. — Москва : Логос, 2021. — 528 с. — ISBN 978-5-98704-662-4.

4. Ярочкин, В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. — 4-е изд. — Москва : Академический Проект, 2023. — 544 с. — (Gaudeamus). — ISBN 978-5-8291-4121-6.

**Интернет-ресурсы**

1. Электронно-библиотечная система «Лань» — (дата обращения: 16.11.2025).
2. КонсультантПлюс — (дата обращения: 16.11.2025).
3. Официальный интернет-портал правовой информации — (дата обращения: 16.11.2025).

4. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) — (дата обращения: 16.11.2025).

5. Сайт Федеральной службы безопасности Российской Федерации (ФСБ России) — (дата обращения: 16.11.2025).

**Нормативно-техническая документация:**

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. Федеральный закон от 21.07.1993 № 5485-1 «О государственной тайне».

5. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

7. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ.

8. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (глава 13 «Административные правонарушения в области связи и информации»).

9. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

10. Приказ ФСО России от 07.08.2009 № 487 «Об утверждении Положения о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации».

11. ГОСТ Р 50922–96 «Защита информации. Основные термины и определения».

12. ГОСТ Р 50.1.053–2005 «Информационные технологии. Основные термины и определения в области технической защиты информации».

13. ГОСТ Р ИСО/МЭК 15408–1–2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

14. ГОСТ Р ИСО/МЭК 15408–2–2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

15. ГОСТ Р ИСО/МЭК 15408–3–2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности».

16. ГОСТ Р ИСО/МЭК 27001 «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования».

17. ГОСТ Р ИСО/МЭК 27002 «Информационные технологии. Практические правила управления информационной безопасностью».

## 6 Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

***Для реализации дисциплины необходимы:***

Лаборатория компьютерных сетей и информационной безопасности, включающая:

− рабочие станции (персональные компьютеры) с характеристиками не ниже: процессор — Intel Core i5 (или аналогичный AMD), ОЗУ — 16 ГБ, SSD — не менее 256 ГБ;

− коммутационное оборудование (коммутаторы, маршрутизаторы) для построения сетевых топологий;

− средства защиты информации (межсетевые экраны, средства криптографической защиты);

− серверную стойку с серверами для развёртывания сетевых сервисов и хранения данных;

− проекционное оборудование (проектор/интерактивная доска) для демонстрации материалов;

− сетевое подключение со скоростью не менее 100 Мбит/с.

***Программное обеспечение***

Операционные системы: Windows 10/11, Linux (Ubuntu, CentOS, Astra, Alt)

Средства виртуализации: Oracle VM VirtualBox, VMware Workstation

Диагностическое и тестовое ПО: Wireshark (анализ сетевого трафика) Nmap (сканирование сетей и портов), Metasploit Framework (тестирование на проникновение), OpenVAS (сканер уязвимостей), Kali Linux (дистрибутив для тестирования безопасности).

Системное ПО: антивирусные решения (Kaspersky Endpoint Security, Dr.WEB, ESET NOD32), средства резервного копирования (Acronis True Image, Veeam Backup), утилиты для мониторинга системы (HWMonitor, AIDA64), инструменты для работы с дисками и разделами (GParted, DiskGenius).

Офисные пакеты: Microsoft Office 365, LibreOffice

Системы управления базами данных: PostgreSQL, MySQL/MariaDB, Microsoft SQL Server (Express-версия), MongoDB (для работы с NoSQL-данными).

***Электронно-библиотечные системы (ЭБС)***

1. ЭБС «BOOK.RU». — URL: https://book.ru/
2. ЭБС «Znanium». — URL: https://znanium.ru/
3. ЭБС «Айбукс». — URL: https://ibooks.ru/
4. ЭБС «Лань». — URL: https://e.lanbook.com/
5. ЭБС «Юрайт». — URL: https://urait.ru/
6. Электронные каталоги библиотеки СЗИУ РАНХиГС. — URL: https://sziu-lib.ranepa.ru/