

Федеральное государственное образовательное бюджетное учреждение  
высшего образования  
**«Финансовый университет при Правительстве  
Российской Федерации»  
(Финансовый университет)**

**Владикавказский филиал Финуниверситета**

УТВЕРЖДАЮ  
Заместитель директора  
по учебно-методической работе  
Владикавказского филиала  
Финуниверситета  
З. Айлар З.К. Айларова  
«31» августа 2026 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

по дисциплине

**«ОП.11 ИНФОРМАЦИОННАЯ  
БЕЗОПАСНОСТЬ»**

по специальности 09.02.13 Интеграция решений с применением  
технологий искусственного интеллекта

Владикавказ 2026

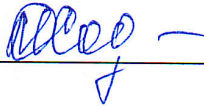
Фонд оценочных средств по дисциплине разработан на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.13 Интеграция решений с применением технологий искусственного интеллекта.

Составитель:

Теблосева Анжела Викторовна, преподаватель.

Фонд оценочных средств рассмотрен и рекомендован к утверждению на заседании предметной (цикловой) комиссии математики и информатики.

Протокол от «28» 08 2026 г. № 1

Председатель предметной (цикловой)  
комиссии математики и информатики  М.К. Ходова

1. Паспорт фонда оценочных средств  
по дисциплине «ОП.11 Информационная безопасность» 09.02.13 Интеграция  
решений с применением технологий искусственного интеллекта

| Результаты обучения<br>(знания, умения)                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Общие и<br>профессиональные<br>компетенции | Наименован<br>ие темы                                                               | Наименование оценочного<br>средства                                                                                                                                                                                                          |                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                            |                                                                                     | Текущий контроль<br>успеваемости                                                                                                                                                                                                             | Промежуточ<br>ная<br>аттестация                                                                      |
| <b>Освоенные знания:</b><br>-структура базовых угроз и источников риска;<br>-алгоритмы идентификации угроз в нормативных документах;<br>-классификацию угроз по источникам и способам реализации; - методы построения моделей угроз.<br><b>Освоенные умения:</b><br>-распознавать базовые угрозы ИБ в профессиональном контексте;<br>-выделять этапы анализа угроз и составлять план действий;<br>-анализировать архитектуру системы на предмет уязвимостей;<br>-составлять модель угроз для ИС с элементами ИИ. | ОК. 01                                     | Тема 1.1.<br>Введение в информационную безопасность                                 | Вопросы для устного (письменного) опроса по теме «Введение в информационную безопасность»<br><br>Практическое занятие – решение ситуационных задач.                                                                                          | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | ОК. 01<br>ОК. 02                           | Тема 1.2.<br>Классификация угроз и уязвимости автоматизированных систем             | Вопросы для устного (письменного) опроса по теме «Классификация угроз и уязвимости автоматизированных систем»<br><br>Практическое занятие – решение ситуационных задач.<br><br>Тест по разделу «Основы информационной безопасности и угрозы» | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |
| <b>Освоенные знания:</b><br>- номенклатуру источников правовой информации (152-ФЗ, приказы ФСТЭК;<br>- форматы оформления локальных нормативных актов;                                                                                                                                                                                                                                                                                                                                                           | ОК.03                                      | Тема 2.1.<br>Правовое обеспечение информационной безопасности и защита персональных | Вопросы для устного (письменного) опроса по теме «Правовое обеспечение информационной безопасности и защита                                                                                                                                  | Вопросы и практико-ориентированные задания для промежуточной аттестации                              |

|                                                                                                                                                                                                                                                                             |                                  |                                                                              |                                                                                                                                                                                                                                                 |                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| содержание 152-ФЗ, законов «О безопасности», «Об информации»; основы правовой ответственности в информационной сфере;                                                                                                                                                       |                                  | х данных                                                                     | персональных данных»<br><br>Практическое занятие – решение ситуационных задач.                                                                                                                                                                  | (дифференцированного зачета)                                                                         |
| <b>Освоенные умения:</b><br>- находить и анализировать нормативные акты в области защиты информации; оформлять результаты правового анализа;<br>- составлять правовые документы (политики, положения); определять актуальность нормативной базы для конкретной организации; | ОК.02<br>ОК.09                   | Тема 2.2.<br>Инженерно-техническая защита информации и безопасность объектов | Вопросы для устного (письменного) опроса по теме «Инженерно-техническая защита информации и безопасность объектов»<br><br>Практическое занятие – решение ситуационных задач .                                                                   | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |
|                                                                                                                                                                                                                                                                             | ОК.01<br>ОК.02<br>ОК.03<br>ОК.09 | Тема 2.3.<br>Криптографические методы защиты информации                      | Вопросы для устного (письменного) опроса по теме «Криптографические методы защиты информации»<br><br>Практическое занятие – решение ситуационных задач.<br><br>Тест по разделу «Организационно-правовые и технические основы защиты информации» | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |
| <b>Освоенные знания:</b><br>- принципы работы фаерволов, IDS/IPS, VPN-протоколов; методы анализа сетевого трафика;<br>- типовые уязвимости веб-приложений и способы их эксплуатации; методы защиты от инъекций, XSS, небезопасной аутентификации;                           | ОК 01,<br>ОК.03<br>ОК.09         | Тема 3.1.<br>Сетевые угрозы и методы обеспечения безопасности сетей          | Вопросы для устного (письменного) опроса по теме «Сетевые угрозы и методы обеспечения безопасности сетей»<br><br>Практическое занятие – решение ситуационных задач.                                                                             | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                  |                                                                            |                                                                                                                                                                                                                              |                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <p>- профессиональную терминологию в области сетевых протоколов, атак, средств защиты; особенности произношения и написания англоязычных аббревиатур (DoS, IDS, PKI, XSS).</p> <p><b>Освоенные умения:</b><br/>-применять сетевые сканеры и анализаторы трафика; настраивать правила межсетевого экрана и VPN;<br/>- выявлять уязвимости по методике OWASP Top 10; использовать специализированные инструменты тестирования;<br/>- участвовать в обсуждении настроек сетевого оборудования на профессиональном языке; писать простые отчёты по результатам аудита безопасности.</p> | <p>ОК 01<br/>ОК.09</p>           | <p>Тема 3.2.<br/>Безопасность беспроводных сетей и мобильных устройств</p> | <p>Вопросы для устного (письменного) опроса по теме «Безопасность беспроводных сетей и мобильных устройств»</p> <p>Практическое занятие – решение ситуационных задач.</p>                                                    | <p>Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета)</p> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>ОК.02<br/>ОК.03<br/>ОК.09</p> | <p>Тема 3.3.<br/>Безопасность приложений и веб-ресурсов</p>                | <p>Вопросы для устного (письменного) опроса по теме «Безопасность приложений и веб-ресурсов»</p> <p>Практическое занятие – решение ситуационных задач.</p> <p>Тест по разделу «Безопасность компьютерных сетей и систем»</p> | <p>Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета)</p> |
| <p><b>Освоенные знания:</b><br/>-этапы процесса управления рисками; шкалы оценки вероятности и ущерба;<br/>-структуру политики ИБ и стандартов (ISO 27001, ГОСТ; порядок документирования процедур реагирования;<br/>-основные этапы разработки и реализации проектов в сфере ИБ;<br/>-правила подготовки</p>                                                                                                                                                                                                                                                                       | <p>ОК.03</p>                     | <p>Тема 4.1.<br/>Управление рисками информационной безопасности</p>        | <p>Вопросы для устного (письменного) опроса по теме «Управление рисками информационной безопасности»</p> <p>Практическое занятие – решение ситуационных задач.</p>                                                           | <p>Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета)</p> |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                         |                                                                            |                                                                                                                                                                                                                                                    |                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <p>презентаций и проектной документации;<br/>-сновы правового регулирования ИИ в РФ и мире;<br/>-принципы дифференциальной приватности и объяснимости ИИ.</p> <p><b>Освоенные умения:</b><br/>-проводить качественную оценку рисков;<br/>-выбирать меры обработки рисков (снижение, принятие, передача)<br/>-разрабатывать регламенты реагирования на инциденты;<br/>-планировать действия по ликвидации последствий сбоев;<br/>-презентовать идеи по улучшению системы защиты информации;<br/>-оценивать жизнеспособность проектных решений в области ИБ;<br/>-выявлять этические и правовые риски внедрения ИИ-решений;<br/>-формулировать требования к прозрачности моделей.</p> <p><b>Освоенные знания:</b><br/>-действующие стандарты в области ИБ (серии 27000, 56545, 56546);<br/>-правила интерпретации терминологии в нормативных документах;<br/>-лексический минимум для описания вредоносного ПО,</p> | ОК.02<br>ОК.03          | Тема 4.2.<br>Организация режима информационной безопасности на предприятии | Вопросы для устного (письменного) опроса по теме «Организация режима информационной безопасности на предприятии»<br><br>Практическое занятие – решение ситуационных задач.                                                                         | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ОК.01<br>ОК.02<br>ОК.09 | Тема 4.3.<br>Специфика защиты систем искусственного интеллекта             | Вопросы для устного (письменного) опроса по теме «Специфика защиты систем искусственного интеллекта»<br><br>Практическое занятие – решение ситуационных задач.<br><br>Тест по разделу «Управление информационной безопасностью и защита систем ИИ» | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ОК.01<br>ОК.02<br>ОК.09 | Тема 5.1<br>Вредоносное программное обеспечение и методы защиты            | Вопросы для устного (письменного) опроса по теме Вредоносное программное обеспечение и методы защиты»<br><br>Практическое занятие – решение ситуационных задач.                                                                                    | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |

|                                                                                                                                                                                                                                                                                                                                                                                                              |                         |                                                                   |                                                                                                                                                                                                                                                               |                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <p>методов анализа и защиты;<br/>-правила работы с англоязычными базами уязвимостей (CVE, NVD).</p> <p><b>Освоенные умения:</b><br/>– работать с профессиональными тезаурусами и базами стандартов;<br/>-сравнивать требования ГОСТ, ФСТЭК, ISO;<br/>-анализировать отчёты об инцидентах и угрозах (в т.ч. международные источники);<br/>-строить связные сообщения о методах защиты от вредоносного ПО.</p> | ОК.01<br>ОК.02          | Тема 5.2.<br>Резервное копирование и восстановление данных        | Вопросы для устного (письменного) опроса по теме «Резервное копирование и восстановление данных»                                                                                                                                                              | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |
|                                                                                                                                                                                                                                                                                                                                                                                                              | ОК.01<br>ОК.02<br>ОК.03 | Тема 5.3.<br>Терминологическая база и стандартизация в области ИБ | <p>Вопросы для устного (письменного) опроса по теме «Терминологическая база и стандартизация в области ИБ»</p> <p>Практическое занятие – решение ситуационных задач.</p> <p>Тест по разделу «Специальные вопросы обеспечения информационной безопасности»</p> | Вопросы и практико-ориентированные задания для промежуточной аттестации (дифференцированного зачета) |

## 2. Комплект оценочных средств

### 1.Задания для текущего контроля успеваемости

#### **1.1. Вопросы для устного (письменного) опроса по темам. (ОК.01, ОК.02, ОК.03, ОК.09)**

#### Раздел 1. Основы информационной безопасности и угрозы (ОК 01, ОК 02)

##### Тема 1.1. Введение в информационную безопасность

1. Понятие информации, информационной безопасности. Основные составляющие ИБ: конфиденциальность, целостность, доступность.
2. Национальные интересы в информационной сфере. Место ИБ в системе национальной безопасности.
3. Нормативно-правовое регулирование в области ИБ: Конституция РФ, законы «О безопасности», «Об информации, информационных технологиях и о защите информации».
4. Понятие угрозы информационной безопасности. Классификация угроз (природные, техногенные, антропогенные). Источники угроз.

##### Тема 1.2. Классификация угроз и уязвимости автоматизированных систем

- 1.Детальная классификация угроз: по природе возникновения, по степени преднамеренности, по положению источника.
2. Понятие уязвимости. Классификация уязвимостей (программные, технические, организационные, человеческий фактор).
3. Анализ угроз и уязвимостей, характерных для систем, обрабатывающих большие данные и использующих технологии искусственного интеллекта (отравление данных, искажение модели, состязательные атаки).
4. Понятие угрозы информационной безопасности.

#### Раздел 2. Организационно-правовые и технические основы защиты информации.

(ОК 01, ОК 02, ОК 03, ОК 09)

##### Тема 2.1. Правовое обеспечение информационной безопасности и защита персональных данных.

1. Законодательство РФ в области защиты информации. Ответственность за правонарушения в информационной сфере.
2. Правовой режим защиты государственной тайны, коммерческой тайны, конфиденциальной информации.

3. Федеральный закон «О персональных данных» №152-ФЗ. Принципы и условия обработки персональных данных. Права субъектов персональных данных.

4. Хранение и уничтожение персональных данных.

## Тема 2.2. Инженерно-техническая защита информации и безопасность объектов

1. Основные понятия и концепция инженерно-технической защиты
2. Физическая защита объектов информатизации. Средства охраны, контроля доступа, видеонаблюдения.
3. Технические каналы утечки информации (акустические, визуально-оптические, электромагнитные). Методы и средства их перекрытия.
4. Угрозы безопасности информации и технические каналы утечки.

## Тема 2.3. Криптографические методы защиты информации

1. Основные понятия криптографии: шифрование, дешифрование, ключ. Симметричные и асимметричные криптосистемы.
2. Электронная подпись (ЭП): понятие, назначение, виды. Правовое регулирование ЭП.
3. Хэш-функции. Управление ключами. Инфраструктура открытых ключей (PKI).
4. Основные криптосистемы с открытым ключом
5. Прикладные аспекты и реализация криптографических методов
6. Применение средств криптографической защиты информации (СКЗИ)
7. Разработка внутренних документов по защите информации

## Раздел 3. Безопасность компьютерных сетей и систем (ОК 01, ОК 02, ОК 03, ОК 09)

### Тема 3.1. Сетевые угрозы и методы обеспечения безопасности сетей

1. Основные угрозы безопасности компьютерных сетей: перехват данных, анализ трафика, подмена узлов, атаки типа «отказ в обслуживании» (DoS/DDoS).
2. Межсетевые экраны (Firewalls): принципы работы, типы (фильтрующие, прокси-серверы, stateful inspection).
3. VPN (Virtual Private Network): протоколы, назначение, схемы построения защищенных каналов связи.
4. Системы обнаружения и предотвращения вторжений (IDS/IPS).

### Тема 3.2. Безопасность беспроводных сетей и мобильных устройств

1. Особенности обеспечения безопасности в сетях Wi-Fi. Протоколы защиты: WEP, WPA/WPA2/WPA3. Угрозы для беспроводных сетей.
2. Основные угрозы для мобильных устройств и платформ. Вредоносное ПО для мобильных устройств.
3. Правила безопасной работы в публичных сетях Wi-Fi. Меры защиты мобильных устройств.

#### Тема 3.3. Безопасность приложений и веб-ресурсов

1. Основные уязвимости веб-приложений (OWASP Top 10): инъекции SQL, межсайтовый скриптинг (XSS), небезопасная аутентификация и др.
2. Безопасность баз данных. Защита от SQL-инъекций.
3. Безопасность облачных вычислений и хранения данных. Модели разделения ответственности.

### Раздел 4. Управление информационной безопасностью и защита систем ИИ. (ОК 01, ОК 02, ОК 03, ОК 09)

#### Тема 4.1. Управление рисками информационной безопасности.

1. Понятие и основные этапы управления рисками ИБ: идентификация, оценка, обработка рисков.
2. Методы оценки рисков (качественные и количественные). Шкалы ущерба и вероятности.
3. Выбор мер по обработке рисков (снижение, принятие, избегание, передача). Остаточный риск.
4. Документирование процедур оценки рисков.

#### Тема 4.2. Организация режима информационной безопасности на предприятии.

1. Политика информационной безопасности как основной документ. Структура и содержание политики ИБ.
2. Стандарты и методологии в области ИБ (ISO/IEC 27000, ГОСТ Р ИСО/МЭК 27001).
3. Реагирование на инциденты ИБ. План действий в случае нарушения безопасности. Компьютерная криминалистика (форензика).

#### Тема 4.3. Специфика защиты систем искусственного интеллекта.

1. Классификация уязвимостей систем ИИ: атаки на этапе обучения (отравление данных), атаки на этапе эксплуатации (состязательные примеры), атаки, направленные на кражу модели.

2. Методы защиты: валидация и очистка данных, состязательное обучение, дифференциальная приватность.
3. Этические аспекты применения ИИ. Прозрачность и объяснимость моделей ИИ. Правовое регулирование в сфере ИИ.

Раздел 5. Специальные вопросы обеспечения информационной безопасности.  
(ОК 01, ОК 02, ОК 03, ОК 09)

Тема 5.1 Вредоносное программное обеспечение и методы защиты.

1. Классификация вредоносного ПО: вирусы, черви, трояны, программы-шпионы, программы-вымогатели (шифровальщики).
2. Современные угрозы: АРТ-атаки (целевые атаки), полиморфизм, стелс-технологии.
3. Признаки заражения компьютерных систем. Анализ поведения программ.
4. Методы и средства антивирусной защиты: сигнатурный и эвристический анализ, проактивная защита. Политика использования антивирусных средств.

Тема 5.2. Резервное копирование и восстановление данных.

1. Цели и задачи резервного копирования как элемента обеспечения доступности и целостности информации.
2. Типы резервного копирования: полное, инкрементальное, дифференциальное.
3. Схемы ротации носителей.
4. Программно-аппаратные средства резервного копирования. Хранение резервных копий (on-premise, облако).
5. Политика резервного копирования и восстановления. План Disaster Recovery (DRP).

Тема 5.3. Терминологическая база и стандартизация в области ИБ

1. Основные термины и определения в области информационной безопасности. Работа с профессиональным тезаурусом.
2. Анализ разночтений в терминологии различных нормативных документов (ГОСТ, ФСТЭК, международные стандарты).
3. Обзор действующих стандартов в области ИБ: серии ГОСТ Р ИСО/МЭК 27000, ГОСТ Р 56545, ГОСТ Р 56546.

## **Критерии оценки ответов студента в процессе устного (письменного) опроса**

Оценка «отлично» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания вопросов программного материала.

Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе некоторые неточности.

Оценка «удовлетворительно» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом показавшему владение основными понятиями, выносимых на рассмотрение вопросов, необходимыми для дальнейшего обучения и способность применять полученные знания по образцу в стандартной ситуации.

Оценки «неудовлетворительно» заслуживает студент, который не знает большей части основного содержания выносимых на рассмотрение вопросов дисциплины (темы), допускает грубые ошибки в формулировках основных понятий.

### **1.2. Вопросы компьютерного тестирования (ОК.01, ОК.02, ОК.03, ОК.09)**

## **РАЗДЕЛ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УГРОЗЫ**

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

#### **Вопрос 1.**

Какие три принципа составляют базовую триаду информационной безопасности (CIA)?

- А) Анонимность, подлинность, надежность
- Б) Конфиденциальность, целостность, доступность
- В) Аутентичность, авторизация, аудит
- Г) Безопасность, приватность, устойчивость

#### **Вопрос 2.**

Установите соответствие между типом угрозы и ее примером.

#### **1. Природная угроза**

А) Отказ системы охлаждения из-за перегрузки электросети

#### **2. Техногенная угроза**

Б) Наводнение, разрушившее дата-центр

#### **3. Антропогенная угроза**

В) Ошибка администратора при настройке прав доступа

Вопрос 3.

Какие из перечисленных нормативных актов составляют основу правового регулирования ИБ в РФ? (Выберите 3 верных ответа)

- А) Конституция РФ
- Б) Федеральный закон «О безопасности»
- В) Трудовой кодекс РФ
- Г) Федеральный закон «Об информации, информационных технологиях и о защите информации»
- Д) Федеральный закон «О рекламе»

Вопрос 4.

Что из перечисленного относится к организационным уязвимостям информационной системы?

Тип: Одиночный выбор

Варианты ответов:

- А) Ошибка в коде веб-приложения
- Б) Отсутствие утвержденного регламента резервного копирования
- В) Неисправность сетевого коммутатора
- Г) Использование устаревшей версии ОС

Вопрос 5.

Какие угрозы специфичны для систем, использующих технологии искусственного интеллекта и большие данные? (Выберите 3 верных ответа)

- А) Отравление обучающих данных (data poisoning)
- Б) Состязательные атаки на этапе эксплуатации модели
- В) Физическое хищение серверных стоек
- Г) Кража или реверс-инжиниринг модели ИИ
- Д) Перегрев процессора при вычислениях

Вопрос 6.

Уязвимость информационной системы всегда является следствием умышленных действий злоумышленника.

- А) Верно
- Б) Неверно

## РАЗДЕЛ 2. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ И ТЕХНИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Вопрос 1.

Какой принцип обработки персональных данных НЕ закреплен в Федеральном законе №152-ФЗ?

- А) Обработка ограничивается достижением конкретных, заранее определенных целей
- Б) Содержание и объем обрабатываемых данных должны соответствовать

заявленным целям

В) Обработка данных может осуществляться бессрочно без уведомления субъекта

Г) Хранение данных осуществляется в форме, позволяющей определить субъекта ПДн

Вопрос 2.

Установите соответствие между видом информации ограниченного доступа и регулирующим ее законом.

1. Государственная тайна

А) Федеральный закон «О коммерческой тайне»

2. Коммерческая тайна

Б) Закон РФ «О государственной тайне»

3. Персональные данные

В) Федеральный закон «О персональных данных»

Вопрос 3.

Оператор обязан уничтожить персональные данные по достижении целей обработки или при отзыве согласия субъекта, если иное не предусмотрено законом.

А) Верно

Б) Неверно

Вопрос 4.

Какой из перечисленных каналов НЕ является техническим каналом утечки информации?

А) Акустический (виброакустический)

Б) Электромагнитный

В) Визуально-оптический

Г) Социальная инженерия

Вопрос 5.

Какие средства относятся к системе контроля и управления доступом (СКУД)? (Выберите 3 верных ответа)

А) Биометрические считыватели

Б) Турникеты и шлюзовые кабины

В) Генераторы белого шума

Г) Электронные пропуска и контроллеры

Д) Источники бесперебойного питания

Вопрос 6.

Экранирование помещений и использование сетевых фильтров применяется для защиты от электромагнитного излучения и наводок.

А) Верно

Б) Неверно

Вопрос 7.

В чем основное отличие симметричной криптосистемы от асимметричной?

- А) В симметричной используется один ключ для шифрования и дешифрования, в асимметричной пара ключей
- Б) Асимметричная система работает значительно быстрее симметричной
- В) Симметричная система применяется только для создания электронной подписи
- Г) Асимметричная система не требует управления ключами

Вопрос 8.

Для чего в криптографии применяются хэш-функции?

- А) Для сжатия больших объемов данных
- Б) Для обеспечения конфиденциальности передаваемой информации
- В) Для контроля целостности данных и создания цифровых подписей
- Г) Для генерации сертификатов открытых ключей

Вопрос 9.

Какие компоненты входят в инфраструктуру открытых ключей (PKI)?

(Выберите 3 верных ответа)

- А) Центр сертификации (CA)
- Б) Репозиторий сертификатов и списков отзыва (CRL)
- В) Антивирусный шлюз
- Г) Регистрационный центр (RA)
- Д) Межсетевой экран

### РАЗДЕЛ 3. БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ И СИСТЕМ

Вопрос 1.

Какой тип межсетевого экрана анализирует состояние соединений и принимает решения на основе контекста сессии?

- А) Фильтрующий пакетный экран (Packet Filter)
- Б) Прокси-сервер прикладного уровня
- В) Экран с проверкой состояния (Stateful Inspection)
- Г) Шлюз сетевого уровня

Вопрос 2.

Установите соответствие между системой сетевой безопасности и ее основной функцией.

1. IDS (Система обнаружения вторжений)

3. VPN

2. IPS (Система предотвращения вторжений)

- А) Пассивный мониторинг трафика и оповещение об аномалиях
- Б) Создание защищенного туннеля

для передачи данных через  
публичные сети  
В) Активное блокирование  
подозрительного трафика в  
реальном времени

Вопрос 3.

Какие протоколы используются для построения защищенных VPN-каналов? (Выберите 3 верных ответа)

- А) IPsec
- Б) OpenVPN
- В) FTP
- Г) L2TP
- Д) HTTP

Вопрос 4

Какой протокол защиты беспроводной сети считается наиболее устаревшим и криптографически нестойким?

- А) WPA3
- Б) WPA2-PSK
- В) WEP
- Г) WPA-Enterprise

Вопрос 5.

Какие меры повышают безопасность мобильного устройства? (Выберите 4 верных ответа)

- А) Регулярное обновление операционной системы и приложений
- Б) Отключение автоматического подключения к открытым точкам Wi-Fi
- В) Установка приложений исключительно из официальных магазинов
- Г) Использование простых PIN-кодов для быстрого разблокирования
- Д) Включение функции удаленного стирания данных при потере

Вопрос 6.

Подключение к публичной сети Wi-Fi без использования VPN или HTTPS-соединений делает передаваемые данные доступными для анализа злоумышленником в той же сети.

- А) Верно
- Б) Неверно

Вопрос 7.

Что представляет собой атака типа «SQL-инъекция»?

- А) Внедрение вредоносного JavaScript в браузер пользователя
- Б) Подмена DNS-записей для перенаправления на фишинговый сайт
- В) Внедрение произвольных SQL-команд через поля ввода для доступа к базе данных
- Г) Перебор учетных данных через форму авторизации

Вопрос 8.

Какие уязвимости входят в топ OWASP Top 10? (Выберите 3 верных ответа)

- А) Небезопасная десериализация
- Б) Отсутствие контроля доступа на уровне объектов

- В) Межсайтовый скриптинг (XSS)
- Г) Использование устаревших аппаратных драйверов
- Д) Сбой питания сервера

Вопрос 9.

В модели разделения ответственности облачных сервисов (IaaS, PaaS, SaaS) провайдер всегда отвечает за физическую безопасность дата-центра и сетевой инфраструктуры.

- А) Верно
- Б) Неверно

#### РАЗДЕЛ 4. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И ЗАЩИТА СИСТЕМ ИИ

Вопрос 1.

Установите соответствие между стратегией обработки риска и примером ее применения.

- 1. Снижение риска
- 2. Принятие риска
- 3. Передача риска
- 4. Избегание риска

- А) Отказ от использования уязвимого стороннего сервиса
- Б) Внедрение многофакторной аутентификации
- В) Оформление страховой полиса от киберинцидентов
- Г) Осознанное решение не применять меры из-за низкой вероятности и ущерба

Вопрос 2.

Что такое «остаточный риск» в процессе управления информационной безопасностью?

- А) Риск, который возникает после реализации всех мер защиты
- Б) Риск, оставшийся после применения мер по обработке первоначального риска
- В) Риск, который руководство решило полностью игнорировать
- Г) Совокупность всех идентифицированных угроз до оценки

Вопрос 3.

Какие методы относятся к качественной оценке рисков ИБ? (Выберите 2 верных ответа)

- А) Построение матрицы вероятности и ущерба на основе экспертных суждений
- Б) Расчет SLE, ARO и ALE в денежном выражении
- В) Ранжирование рисков по шкалам «Высокий/Средний/Низкий»
- Г) Монте-Карло моделирование финансовых потерь

Вопрос 4.

Какой документ является основополагающим для системы менеджмента

информационной безопасности в организации?

- А) Штатное расписание
- Б) Политика информационной безопасности
- В) Инструкция по охране труда
- Г) График отпусков ИТ-отдела

Вопрос 5.

Какие этапы включает жизненный цикл реагирования на инциденты ИБ?  
(Выберите 4 верных ответа)

- А) Подготовка и превентивные меры
- Б) Обнаружение и анализ
- В) Соккрытие инцидента от руководства до полного восстановления
- Г) Сдерживание, ликвидация и восстановление
- Д) Анализ извлеченных уроков и совершенствование процедур

Вопрос 6.

Стандарт ISO/IEC 27001 содержит требования к системе менеджмента информационной безопасности (СМИБ) и предназначен для сертификации организаций.

- А) Верно
- Б) Неверно

Вопрос 7.

Что подразумевается под «отравлением данных» (data poisoning) в контексте систем ИИ?

- А) Физическое повреждение серверов, хранящих датасеты
- Б) Внесение злоумышленником искаженных примеров в обучающую выборку для ухудшения или изменения поведения модели
- В) Шифрование весов нейронной сети для предотвращения кражи
- Г) Удаление резервных копий модели из облачного хранилища

Вопрос 8

Дифференциальная приватность позволяет использовать данные для обучения моделей ИИ, гарантируя, что выводы не раскроют информацию о конкретных индивидуумах в наборе данных.

- А) Верно
- Б) Неверно

Вопрос 9.

Какие методы применяются для защиты моделей машинного обучения на этапе эксплуатации? (Выберите 3 верных ответа)

- А) Состязательное обучение (adversarial training)
- Б) Валидация и фильтрация входных данных
- В) Отключение логирования запросов к модели
- Г) Регуляризация и проверка устойчивости к состязательным примерам
- Д) Публикация обучающих данных в открытом доступе

## РАЗДЕЛ 5. СПЕЦИАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вопрос 1.

Установите соответствие между типом вредоносного ПО и его характеристикой.

1. Червь
2. Троянская программа
3. Программа-вымогатель

- А) Маскируется под легитимное ПО, открывает злоумышленнику удаленный доступ
- Б) Самостоятельно распространяется по сети без прикрепления к файлам
- В) Шифрует файлы пользователя и требует перечисления средств за ключ расшифровки

Вопрос 2.

Что отличает АРТ-атаки (Advanced Persistent Threat) от массовых вредоносных рассылок?

- А) Они носят кратковременный характер и нацелены на получение быстрой финансовой выгоды
- Б) Они осуществляются случайными пользователями без специальной подготовки
- В) Они характеризуются длительным скрытым присутствием в инфраструктуре и высокой целевой направленностью
- Г) Они используют только известные сигнатуры вирусов

Вопрос 3.

Какие методы анализа используются современными средствами антивирусной защиты? (Выберите 3 верных ответа)

- А) Сигнатурный анализ
- Б) Эвристический анализ
- В) Случайное удаление системных файлов
- Г) Проактивная (поведенческая) защита
- Д) Физическая изоляция компьютера от сети на постоянной основе

Вопрос 4.

При каком типе резервного копирования архивируются только те данные, которые изменились с момента последнего резервного копирования любого типа?

- А) Полное резервное копирование
- Б) Дифференциальное резервное копирование

- В) Инкрементальное резервное копирование
- Г) Зеркальное копирование

Вопрос 5.

Установите соответствие между схемой ротации носителей и ее описанием.

1. Схема «Грандфатер-Отец-Сын»
2. Схема Tower of Hanoi

- А) Использует математический алгоритм для минимизации количества перезаписей носителей при сохранении глубокой истории
- Б) Классическая иерархическая схема с ежедневными, еженедельными и ежемесячными копиями

Вопрос 6.

Что обязательно должен содержать план аварийного восстановления (Disaster Recovery Plan, DRP)? (Выберите 3 верных ответа)

- А) Приоритетность восстановления критических информационных систем
- Б) Перечень ответственных лиц и их контактные данные
- В) Маркетинговый план продвижения услуг после простоя
- Г) Пошаговые процедуры восстановления данных и инфраструктуры
- Д) График плановых отпусков сотрудников

Вопрос 7.

Какая серия международных стандартов является базовой для систем менеджмента информационной безопасности?

- А) ISO 9000
- Б) ISO/IEC 27000
- В) ISO 14000
- Г) ISO 45001

Вопрос 8

В нормативной базе РФ термины «информационная безопасность» и «защита информации» имеют абсолютно идентичное смысловое значение и могут использоваться как полные синонимы во всех официальных документах.

- А) Верно
- Б) Неверно

Вопрос 9

Какие стандарты регулируют вопросы защиты информации и ИБ на территории РФ? (Выберите 3 верных ответа)

- А) ГОСТ Р ИСО/МЭК 27001
- Б) ГОСТ Р 56545 (методика оценки угроз)
- В) ГОСТ Р 56546 (управление рисками ИБ)
- Г) ГОСТ 7.32 (отчет о научно-исследовательской работе)
- Д) ГОСТ Р 52872 (доступность веб-ресурсов).

### **Критерии оценки знаний студентов при проведении тестирования**

Оценка «отлично» выставляется при условии правильного ответа студента не менее чем на 86 % тестовых заданий;

Оценка «хорошо» выставляется при условии правильного ответа студента на 70-85 % тестовых заданий;

Оценка «удовлетворительно» выставляется при условии правильного ответа студента на 50-69 % тестовых заданий;

Оценки «неудовлетворительно» заслуживает студент при условии правильного ответа студента менее чем на 50 % тестовых заданий.

### **1.3. Практические ситуационные задания (ОК.01, ОК.02, ОК.03, ОК.09)**

#### **Раздел 1. Основы информационной безопасности и угрозы**

#### **Практическое занятие №1 (Тема 1.1). Правовой анализ и идентификация базовых угроз информационной безопасности**

##### **Задание:**

1. Изучите выдержки из ФЗ «О безопасности», ФЗ «Об информации, информационных технологиях и о защите информации» и ФЗ «О персональных данных».
2. Проанализируйте ситуацию: *«Сотрудник отдела продаж скопировал базу данных клиентов (ФИО, номера телефонов, адреса) на личный USB-накопитель для работы дома. Устройство было утеряно в общественном транспорте».*
3. Выполните:
  - Определите, какие принципы ИБ (конфиденциальность, целостность, доступность) были нарушены.
  - Классифицируйте угрозу по источнику (природная, техногенная, антропогенная), преднамеренности и положению источника.
  - Укажите, статьи каких нормативных актов нарушены (ссылки на конкретные статьи).
  - Предложите 3 организационные и 2 технические меры для предотвращения подобных инцидентов.

#### **Практическое занятие №2 (Тема 1.2). Разработка модели угроз и уязвимостей для информационной системы с элементами ИИ**

##### **Задание:**

1. Изучите предложенную архитектуру гипотетической системы: Веб-интерфейс → API-шлюз → ML-модель (классификатор) → База данных (SQL).
2. Идентифицируйте и оформите в виде таблицы модель угроз:

| Актив       | Угроза                             | Источник угрозы         | Уязвимость (программная/техническая/организационная) |
|-------------|------------------------------------|-------------------------|------------------------------------------------------|
| База данных | SQL-инъекция                       | Злоумышленник (внешний) | Отсутствие валидации ввода на стороне API            |
| ML-Модель   | Отравление данных (Data Poisoning) | ...                     | ...                                                  |

3. Укажите не менее 5 активов и 8-10 соответствующих угроз (обязательно включив специфичные для ИИ: *состязательные атаки, кража модели*).

## Раздел 2. Организационно-правовые и технические основы защиты информации

### Практическое занятие №3 (Тема 2.1). Разработка организационно-распорядительной документации по защите персональных данных

Задание:

На основе 152-ФЗ разработайте фрагмент локального нормативного акта организации — «Политики обработки персональных данных». В документе должны быть отражены следующие разделы:

1. Цели сбора ПДн.
2. Перечень обрабатываемых категорий ПДн.
3. Принципы и условия обработки.
4. Сроки хранения и порядок уничтожения ПДн при достижении целей.
5. Права субъектов ПДн.

Результат: Текстовый документ (1-2 стр.).

### Практическое занятие №4 (Тема 2.2). Исследование и классификация средств инженерно-технической защиты информации

Задание:

1. Ознакомьтесь с виртуальным стендом или планом этажа организации.
2. Определите, какие объекты информатизации требуют физической защиты.
3. Заполните таблицу, предложив средства защиты для каждого объекта:

| Объект защиты              | Угроза                           | Средство ИТЗИ (СКУД, видеонаблюдение, охрана) |
|----------------------------|----------------------------------|-----------------------------------------------|
| Серверная комната          | НСД (несанкционированный доступ) | ...                                           |
| Рабочая станция бухгалтера | ...                              | ...                                           |

4. Перечислите технические каналы утечки информации (акустические, визуальные, электромагнитные) и предложите методы их перекрытия для серверной комнаты.

### **Практическое занятие №5 (Тема 2.3). Применение средств криптографической защиты информации (СКЗИ)**

Задание:

Вам необходимо зашифровать конфиденциальный файл и подписать его электронной подписью (УКЭП) в тестовой среде (или на бумаге — выполнить моделирование).

1. Опишите пошаговый алгоритм шифрования файла с использованием симметричного алгоритма (например, AES).
2. Опишите процесс генерации ключевой пары (асимметричное шифрование) и подписания файла.
3. Смоделируйте ситуацию: получив файл, ваш коллега должен его расшифровать и проверить подпись.
4. *Вопрос:* В чем отличие УКЭП от ПЭП?

### **Раздел 3. Безопасность компьютерных сетей и систем**

#### **Практическое занятие №6 (Тема 3.1). Конфигурирование межсетевого экрана для защиты периметра сети**

Задание:

На основе предложенной сетевой топологии (или симулятора Cisco Packet Tracer):

1. Сформулируйте правила фильтрации трафика для корпоративного межсетевого экрана (Firewall).
2. Необходимо разрешить доступ сотрудникам к Интернету, но запретить доступ к социальным сетям.

3. Настроить DMZ-зону для веб-сервера (разрешить входящий HTTPS, запретить доступ к внутренней сети).
4. *Вопрос:* В чем отличие Stateful Inspection от простого пакетного фильтра?

### **Практическое занятие №7 (Тема 3.2). Аудит безопасности беспроводной сети**

Задание:

Используя анализатор Wi-Fi (например, Wireshark или мобильное приложение):

1. Определите, какие точки доступа доступны в радиусе действия.
2. Идентифицируйте, какой протокол шифрования используется (WEP, WPA2, WPA3) и оцените его надежность.
3. Смоделируйте угрозы: *Подмена MAC-адреса, Злоумышленник создает точку доступа с тем же SSID (Evil Twin).*
4. Предложите меры защиты для корпоративной Wi-Fi сети.

### **Практическое занятие №8 (Тема 3.3). Выявление и анализ уязвимостей веб-приложений**

Задание:

На тестовом сайте (или в среде виртуальной машины DVWA):

1. Проанализируйте страницу авторизации на наличие уязвимости SQL-инъекции.
2. Составьте инъекцию для обхода пароля.
3. В поле ввода комментария вставьте скрипт XSS: `<script>alert("Test")</script>`. Опишите последствия, если бы это был рабочий сайт.
4. Предложите методы защиты от XSS и SQL-инъекций (санитизация входных данных, параметризация запросов).

## **Раздел 4. Управление информационной безопасностью и защита систем ИИ**

### **Практическое занятие №9 (Тема 4.1). Проведение качественной оценки и обработки рисков информационной безопасности**

Задание:

Вам необходимо оценить риски для информационной системы кредитной организации.

1. Идентифицируйте 3 ключевых актива.
2. Постройте матрицу рисков (Вероятность: Низкая/Средняя/Высокая; Ущерб: Низкий/Средний/Высокий).

3. Для каждого выявленного риска выберите стратегию обработки: *Снижение, Принятие, Передача (страхование), Избегание*. Обоснуйте выбор.
4. Определите понятие "Остаточный риск".

### **Практическое занятие №10 (Тема 4.2). Разработка регламентов реагирования на инциденты информационной безопасности**

Задание:

Разработайте фрагмент регламента реагирования на инцидент «Вирус-шифровальщик на рабочей станции бухгалтера». В регламенте опишите 4 этапа:

1. Обнаружение: по каким признакам сотрудник/администратор поймет, что произошел инцидент?
2. Сдерживание: что нужно сделать немедленно (отключить от сети, отключить питание)?
3. Восстановление: порядок действий (переустановка ОС, восстановление данных из бэкапа).
4. Анализ: какие уроки извлечены для предотвращения в будущем.

### **Практическое занятие №11 (Тема 4.3). Анализ уязвимостей модели машинного обучения**

Задание (на основе готового датасета, например, распознавание цифр MNIST):

1. Обучите простую модель (нейросеть) на датасете.
2. Продемонстрируйте, как изменение одного пикселя в изображении может привести к неверной классификации (*состязательная атака*).
3. Опишите понятия «Дифференциальная приватность» и объясните, как она защищает данные пользователей при обучении модели.
4. *Этический кейс*: Стоит ли внедрять систему распознавания лиц в публичных местах, если она имеет погрешность в 5% для определенных расовых групп? Почему?

### **Практическое занятие №12 (Тема 4.3). Искажение входных данных (состязательный шум)**

Задание:

1. Возьмите любое изображение.
2. Наложите на него едва заметный шум.
3. Покажите, как меняется ответ модели распознавания (если есть доступ к инструментам) или смоделируйте ситуацию на бумаге.
4. Предложите метод защиты от таких атак (*состязательное обучение*).

## **Раздел 5. Специальные вопросы обеспечения информационной безопасности**

### **Практическое занятие №13 (Тема 5.1). Анализ вредоносного ПО и методов защиты**

**Задание:**

1. Заполните таблицу классификации вредоносного ПО (Вирусы, Черви, Трояны, Вымогатели, Шпионы).
2. Изучите лог антивируса или описание инцидента АРТ-атаки. Определите: что такое АРТ-атака, чем она отличается от массовой рассылки вирусов.
3. Сравните методы: *Сигнатурный анализ vs Эвристический vs Проактивная защита*. В чем преимущества каждого?

### **Практическое занятие №14 (Тема 5.2). Разработка политики резервного копирования**

**Задание:**

Для сервера с базой данных (объем 500 ГБ) разработайте политику резервного копирования:

1. Выберите схему (полное + инкрементальное или дифференциальное). Обоснуйте выбор.
2. Назначьте расписание для каждого типа копирования.
3. Рассчитайте необходимое дисковое пространство на 30 дней.
4. Выберите схему ротации носителей («Грандфатер-Отец-Сын»).

### **Практическое занятие №15 (Тема 5.3). Анализ угроз облачных технологий**

**Задание:**

1. Проанализируйте модели ответственности IaaS, PaaS, SaaS в облаке.
2. Определите: кто (провайдер или клиент) отвечает за настройку прав доступа к базе данных в модели PaaS?
3. Перечислите 5 основных угроз для облачных сред (по версии OWASP или CSA).
4. Предложите меры защиты конфиденциальных данных в облачном хранилище (шифрование, управление ключами).

### **Практическое занятие №16 (Тема 5.3). Анализ угроз мобильных технологий**

**Задание:**

1. Изучите механизм разрешений в Android/iOS.
2. Проанализируйте приложение (например, фонарик), которое запрашивает доступ к контактам и СМС. К какой угрозе это относится?

3. Опишите, как работает система MDM (Mobile Device Management) для защиты корпоративных устройств.
4. *Ситуация:* Сотрудник подключился к общедоступной сети Wi-Fi кафе. Какие угрозы для его устройства и корпоративных данных существуют?

### **Практическое занятие №17 (Тема 5.3). Анализ специализированных векторов атак и методов защиты**

Задание:

1. Опишите, как работает атака Man-in-the-Middle (MITM) на примере ARP-spoofing.
2. Как защититься от MITM (HTTPS, шифрование, статические ARP-записи)?
3. Изучите механизм атаки Phishing. Составьте памятку для сотрудников по распознаванию фишинговых писем (не менее 5 пунктов).

### **Практическое занятие №18 (Тема 5.3). Изучение сложных технических атак и методов защиты (Микроархитектурные уязвимости)**

Задание:

1. Изучите атаки типа Spectre и Meltdown.
2. Объясните, в чем принципиальная сложность защиты от таких атак (аппаратный уровень).
3. Укажите, какие меры были приняты производителями CPU для минимизации рисков.
4. Предложите организационные меры, которые могут снизить риск эксплуатации данных уязвимостей.

### **Практическое занятие №19 (Тема 5.3). Анализ реальных кибератак и прогнозирование будущих угроз**

Задание:

1. Проанализируйте кейс реальной атаки (например, WannaCry, SolarWinds или атака на Colonial Pipeline).
2. Опишите этапы атаки (Initial Access → Execution → Exfiltration).
3. Какие уязвимости были использованы? Какие меры защиты помогли бы предотвратить или минимизировать ущерб?
4. Спрогнозируйте 2-3 тренда развития угроз на ближайшие 2-3 года в контексте развития ИИ.

#### **Критерии оценки выполнения практических ситуационных заданий**

Оценка «отлично» выставляется студенту, если практическое ситуационное задание выполнено в полном объеме с соблюдением необходимой последовательности действий; итогом решения задания явилось получение

правильных результатов и выводов; в ходе решения задания верно и аккуратно выполнены все вычисления и записи.

Оценка «хорошо» выставляется студенту, если практическое ситуационное задание выполнено правильно с учетом мелких погрешностей или недочетов.

Оценка «удовлетворительно» выставляется студенту, если практическое ситуационное задание выполнено правильно не менее чем наполовину, допущены некоторые погрешности или одна грубая ошибка.

Оценки «неудовлетворительно» заслуживает студент, если при решении практического ситуационного задания допущены две (и более) грубые ошибки, или задание не решено полностью.

#### **1.4. Задания для самостоятельной работы** (ОК.01, ОК.02, ОК.03, ОК.09)

Задание по теме 3.1 Сетевые угрозы и методы обеспечения безопасности сетей (2 часа): Организация защищенного канала связи с использованием VPN

Задание:

1. Изучите протоколы IPsec, OpenVPN, WireGuard.
2. Выберите подходящий протокол для подключения удаленного сотрудника к корпоративной сети.
3. Составьте схему VPN-туннеля и опишите этапы его настройки.

Задание по теме 4.2 Организация режима информационной безопасности на предприятии (2 часа): Обеспечение непрерывности бизнеса и восстановление после сбоев

Задание:

1. Изучите понятия RPO и RTO.
2. Предложите план аварийного восстановления для небольшой компании (5 серверов).
3. Опишите, как тестировать план DRP.

Задание по теме 5.3 Терминологическая база и стандартизация в области ИБ (2 часа): Специализированные атаки и методы противодействия

Задание:

1. Самостоятельно изучите виды атак по сторонним каналам (Side-channel attacks) — например, атака по времени выполнения операции (Timing attack) или анализ питания (Power analysis).
2. Подготовьте краткий доклад (5-7 минут) о том, как злоумышленники могут извлечь ключ шифрования, измеряя время работы алгоритма, и как этому противодействовать.

### **Критерии оценки выполнения заданий для самостоятельной работы**

Оценка «отлично» выставляется студенту, если задание выполнено в полном объеме с соблюдением необходимой последовательности действий; итогом решения задания явилось получение правильных результатов и выводов; в ходе решения задания верно и аккуратно выполнены все вычисления и записи.

Оценка «хорошо» выставляется студенту, если задание выполнено правильно с учетом мелких погрешностей или недочетов.

Оценка «удовлетворительно» выставляется студенту, если задание выполнено правильно не менее чем наполовину, допущены некоторые погрешности или одна грубая ошибка.

Оценки «неудовлетворительно» заслуживает студент, если при решении задания допущены две (и более) грубые ошибки, или задание не решено полностью.

## **2. Вопросы и задания для промежуточной аттестации**

### **2.1. Вопросы и задания для устного (письменного) зачета по дисциплине**

#### **Вопросы для устного (письменного) зачета по дисциплине (ОК.01, ОК.02, ОК.03, ОК.09)**

1. Понятие информации и информационной безопасности. Основные принципы обеспечения ИБ.
2. Триада информационной безопасности: конфиденциальность, целостность, доступность — содержание и примеры нарушений.
3. Национальные интересы Российской Федерации в информационной сфере.
4. Место информационной безопасности в системе национальной безопасности РФ.
5. Конституция РФ как основа правового регулирования в области информационной безопасности.
6. Федеральный закон «О безопасности»: основные положения, касающиеся информационной сферы.
7. Федеральный закон «Об информации, информационных технологиях и о защите информации»: предмет регулирования и ключевые нормы.
8. Понятие угрозы информационной безопасности. Классификация угроз по источникам возникновения.
9. Природные, техногенные и антропогенные угрозы: характеристики и примеры.
10. Детальная классификация угроз: по степени преднамеренности, положению источника, способу реализации.
11. Понятие уязвимости информационной системы. Отличие уязвимости от угрозы и риска.
12. Классификация уязвимостей: программные, технические, организационные, человеческий фактор.
13. Специфические угрозы для систем, обрабатывающих большие данные и использующих технологии ИИ.
14. Атаки на системы искусственного интеллекта: отравление данных, искажение модели, состязательные примеры.
15. Законодательство РФ в области защиты информации: система нормативных правовых актов.
16. Виды ответственности за правонарушения в информационной сфере: административная, уголовная, гражданско-правовая, дисциплинарная.
17. Правовой режим государственной тайны: основания отнесения сведений к государственной тайне, степени секретности.
18. Коммерческая тайна: понятие, условия защиты, меры по обеспечению конфиденциальности.
19. Конфиденциальная информация: виды, правовое регулирование, особенности защиты.
20. Федеральный закон №152-ФЗ «О персональных данных»: предмет регулирования, основные понятия.

21. Принципы обработки персональных данных по 152-ФЗ.
22. Условия обработки персональных данных: согласие субъекта, договор, законные основания.
23. Права субъекта персональных данных и гарантии их реализации.
24. Требования к хранению и уничтожению персональных данных.
25. Понятие и концепция инженерно-технической защиты информации.
26. Физическая защита объектов информатизации: средства охраны, контроля доступа, видеонаблюдения.
27. Технические каналы утечки информации: акустические, визуально-оптические, электромагнитные.
28. Методы и средства перекрытия технических каналов утечки информации.
29. Основные понятия криптографии: шифрование, дешифрование, криптоключ, криптостойкость.
30. Симметричные криптосистемы: принципы работы, преимущества, недостатки, примеры алгоритмов.
31. Асимметричные криптосистемы: принципы работы, преимущества, недостатки, примеры алгоритмов.
32. Электронная подпись: понятие, назначение, виды (ПЭП, НЭП, УКЭП).
33. Правовое регулирование электронной подписи в Российской Федерации.
34. Хэш-функции: назначение, требования, примеры применения.
35. Управление ключами: жизненный цикл ключа, требования к хранению и замене.
36. Инфраструктура открытых ключей (PKI): компоненты, назначение, принципы функционирования.
37. Применение средств криптографической защиты информации (СКЗИ) в организациях.
38. Основные угрозы безопасности компьютерных сетей: перехват данных, анализ трафика, подмена узлов.
39. Атаки типа «отказ в обслуживании» (DoS/DDoS): механизмы реализации и методы защиты.
40. Межсетевые экраны (Firewalls): принципы работы, типы (фильтрующие, прокси, stateful inspection).
41. VPN (Virtual Private Network): назначение, протоколы (IPsec, OpenVPN, L2TP), схемы построения.
42. Системы обнаружения и предотвращения вторжений (IDS/IPS): отличия, принципы работы, места размещения.
43. Особенности обеспечения безопасности в беспроводных сетях Wi-Fi.
44. Протоколы защиты беспроводных сетей: WEP, WPA, WPA2, WPA3 — сравнительная характеристика.
45. Угрозы для беспроводных сетей: несанкционированный доступ, Evil Twin, перехват трафика.
46. Основные угрозы для мобильных устройств и платформ: вредоносное ПО, фишинг, уязвимости ОС.
47. Правила безопасной работы в публичных сетях Wi-Fi.
48. Меры защиты мобильных устройств в корпоративной среде.
49. Основные уязвимости веб-приложений по методике OWASP Top 10.

50. SQL-инъекции: механизм атаки, примеры, методы защиты.
51. Межсайтовый скриптинг (XSS): виды атак, последствия, способы предотвращения.
52. Проблемы небезопасной аутентификации и управления сессиями в веб-приложениях.
53. Защита баз данных от несанкционированного доступа и инъекций.
54. Безопасность облачных вычислений: модель разделения ответственности (IaaS, PaaS, SaaS).
55. Понятие и основные этапы управления рисками информационной безопасности.
56. Идентификация и оценка рисков ИБ: качественные и количественные методы.
57. Шкалы ущерба и вероятности при оценке рисков информационной безопасности.
58. Стратегии обработки рисков: снижение, принятие, избегание, передача.
59. Понятие остаточного риска и порядок его документирования.
60. Политика информационной безопасности организации: назначение, структура, содержание.
61. Стандарты и методологии в области ИБ: серия ISO/IEC 27000, ГОСТ Р ИСО/МЭК 27001.
62. Реагирование на инциденты ИБ: этапы, роли, документирование.
63. Компьютерная криминалистика (форензика): цели, методы, сохранение цифровых доказательств.
64. Классификация уязвимостей систем искусственного интеллекта по этапам жизненного цикла.
65. Методы защиты моделей машинного обучения: валидация данных, состязательное обучение.
66. Дифференциальная приватность: понятие, назначение, применение в системах ИИ.
67. Этические аспекты применения искусственного интеллекта: прозрачность, объяснимость, справедливость.
68. Правовое регулирование в сфере искусственного интеллекта в РФ и за рубежом.
69. Классификация вредоносного программного обеспечения: вирусы, черви, трояны, шпионы, вымогатели.
70. Современные угрозы: АРТ-атаки, полиморфизм, стелс-технологии.
71. Признаки заражения компьютерных систем вредоносным ПО.
72. Методы антивирусной защиты: сигнатурный анализ, эвристический анализ, проактивная защита.
73. Политика использования антивирусных средств в организации.
74. Цели и задачи резервного копирования в контексте обеспечения доступности и целостности информации.
75. Типы резервного копирования: полное, инкрементальное, дифференциальное — сравнительная характеристика.
76. Схемы ротации носителей резервного копирования: принципы и примеры применения.

77. Программно-аппаратные средства резервного копирования: локальные и облачные решения.
78. Политика резервного копирования и восстановления: основные положения.
79. План аварийного восстановления (Disaster Recovery Plan, DRP): структура, метрики RTO/RPO.
80. Основные термины и определения в области информационной безопасности.
81. Анализ разночтений в терминологии нормативных документов: ГОСТ, ФСТЭК, международные стандарты.
82. Обзор стандартов в области ИБ: серии ГОСТ Р ИСО/МЭК 27000, ГОСТ Р 56545, ГОСТ Р 56546.
83. Анализ угроз безопасности облачных и мобильных технологий.
84. Специализированные атаки и методы противодействия: атаки по сторонним каналам, микроархитектурные уязвимости.
85. Анализ реальных инцидентов информационной безопасности: тренды и прогнозирование угроз.

## **2.2. Задания для устного (письменного) зачета по дисциплине (ОК.01, ОК.02, ОК.03, ОК.09)**

### **Задание 1.**

**Ситуация:** Сотрудник компании по неосторожности переслал файл с персональными данными клиентов на личную электронную почту. Файл был перехвачен злоумышленниками.

**Задание:** Определите, какие принципы информационной безопасности нарушены. Какие статьи Федерального закона №152-ФЗ применены к данной ситуации? Предложите три организационные и две технические меры для предотвращения подобных инцидентов в будущем.

### **Задание 2.**

**Ситуация:** При анализе сетевого трафика обнаружена аномальная активность: с внутренней рабочей станции устанавливаются соединения на подозрительные внешние порты в нерабочее время.

**Задание:** Определите возможные причины аномалии. Составьте алгоритм расследования инцидента. Какие средства мониторинга и анализа трафика целесообразно использовать?

### **Задание 3.**

**Ситуация:** Сотрудник службы технической поддержки по телефону сообщил злоумышленнику, выдававшему себя за руководителя, пароль от учетной записи другого сотрудника.

**Задание:** Определите тип атаки. Разработайте регламент идентификации и аутентификации сотрудников при обращении в службу поддержки. Предложите меры обучения персонала противодействию социальной

инженерии.

#### Задание 4.

**Ситуация:** Вам звонит мужчина, представляется Иваном из IT-отдела. Голос взволнованный: «В нашей сети вирус, он шифрует диски! Я вижу, что ваш компьютер уже в зоне риска. Срочно назовите ваш логин и пароль от доменной учетной записи, чтобы я вывел вас из-под удара. Если не сделаете это за 2 минуты, все файлы будут утеряны».

**Вопрос:** Как отличить реального администратора от злоумышленника? Ваши действия?

#### Задание 5.

**Ситуация:** Вы получаете электронное письмо с ящика, похожего на корпоративный (например, seo@comp-account.ru вместо seo@comp-account.ru). В письме срочное требование от генерального директора: «Вышлите список всех паролей от CRM и бухгалтерии на этот адрес, через 10 минут у меня встреча с аудиторами».

**Вопрос:** Какие признаки говорят о подделке? Должны ли пароли передаваться по электронной почте?

#### Задание 6.

**Ситуация:** На парковке офиса вы находите флешку с наклейкой «Зарплата ведомость Q4 2023». У вас есть ноутбук с доступом к внутренней сети.

**Вопрос:** Можно ли вставлять найденный носитель в рабочий компьютер? Обоснуйте риск.

#### Задание 7.

**Ситуация:** Бухгалтер распечатала платежные поручения с реквизитами организации на общем принтере (на этаже 100 человек). За документами никто не пришел, они пролежали в лотке 3 часа.

**Вопрос:** К какому классу инцидентов это относится? Предложите решение.

#### Задание 8.

**Ситуация:** Сотрудник компании по неосторожности переслал файл с персональными данными клиентов на личную электронную почту. Файл был перехвачен злоумышленниками.

**Вопрос:** Определите, какие принципы информационной безопасности нарушены. Какие статьи Федерального закона №152-ФЗ применены к данной ситуации?

#### Задание 9.

**Ситуация:** Сотрудница салона сотовой связи за денежное вознаграждение скопировала персональные данные 11 клиентов (паспортные данные, номера телефонов) и передала их неустановленному лицу через

мессенджер.

**Вопрос:** Определите, какие принципы обработки ПДн нарушены. Предложите меры, которые должен был принять работодатель для предотвращения злоупотреблений со стороны персонала.

Задание 10.

**Ситуация:** Жительница города опубликовала в открытой группе «ВКонтакте» фотографию, фамилию, имя и номера телефонов другой гражданки без её согласия.

**Вопрос:** Какое право субъекта ПДн нарушено? Предложите механизмы, которые позволяют операторам соцсетей или гражданам оперативно реагировать на подобные публикации.

Задание 11.

**Ситуация:** Злоумышленник организовал «офис» в своей квартире, получал через мессенджеры файлы с фотографиями паспортов граждан РФ и передавал их третьим лицам для регистрации сим-карт. В его компьютере обнаружено около 3000 паспортных фото.

**Вопрос:** Какие статьи УК РФ квалифицируют данное деяние? Предложите технические и организационные меры для банков и операторов связи по проверке подлинности предоставляемых данных.

Задание 12.

**Ситуация:** Сотрудник отдела кадров, работая удалённо в кафе, подключился к общедоступной Wi-Fi сети без VPN и отправил по электронной почте отчёт с паспортными данными сотрудников. Злоумышленники перехватили трафик.

**Вопрос:** Определите нарушенный принцип обработки ПДн. Какие требования ст. 19 152-ФЗ нарушены?

Задание 13.

**Ситуация:** Менеджер компании, отвечая на запрос контрагента, по ошибке отправил файл с персональными данными клиентов на адрес электронной почты, очень похожий на нужный (с опечаткой в одной букве). Файл оказался у конкурентов.

**Вопрос:** Какие принципы обработки данных нарушены? Какие статьи 152-ФЗ регламентируют обязанность оператора уведомлять субъектов об утечке? Предложите организационные меры по контролю за исходящей корреспонденцией.

Задание 14.

**Ситуация:** Сотрудник транспортной компании потерял в общественном транспорте служебный ноутбук, на жёстком диске которого в незашифрованном виде хранились базы данных с полной информацией о клиентах (ФИО, адреса, паспортные данные).

**Вопрос:** Какие требования к хранению ПДн нарушены? Предложите

технические и организационные меры.

#### Задание 14.

**Ситуация:** В отделе продаж использовался общий доступ к корпоративной CRM-системе через один логин и простой пароль «123456». Уволенный сотрудник, знавший пароль, после увольнения зашёл в систему и скачал базу клиентов для конкурентов. В организации не была настроена двухфакторная аутентификация (2FA).

**Вопрос:** Определите нарушенные принципы разграничения доступа. Какие меры ответственности могут быть применены к организации за недостаточную защиту?

#### Критерии оценки устного (письменного) зачета по дисциплине

Оценка «отлично» выставляется, если ответ студента полный, логичный, структурированный и исчерпывающий. Студент демонстрирует глубокое понимание теоретического материала, свободно и корректно оперирует профессиональной терминологией. Практическое задание выполнено в полном объеме.

Оценка «хорошо» выставляется, если ответ студента достаточно полный и логичный, демонстрирует уверенное владение теоретическим материалом. Допускаются незначительные шероховатости в формулировках или мелкие неточности в терминологии. Практическое задание выполнено, предложенное решение в целом верное и охватывает основные аспекты задачи, но содержит незначительные недочеты в аргументации или выборе оптимальных инструментов.

Оценка «удовлетворительно» выставляется, если ответ студента фрагментарный, демонстрирует поверхностное понимание теоретического материала и неуверенное владение базовой терминологией. Логика изложения нарушена. Практическое задание выполнено с существенными недочетами: предложенное решение охватывает лишь часть задачи, студент испытывает трудности с обоснованием выбора методов и не видит взаимосвязи между этапами работы.

Оценка «неудовлетворительно» выставляется, если ответ студента не соответствует поставленным вопросам, демонстрирует отсутствие понимания теоретического материала и неумение применять его на практике. Студент не владеет базовой профессиональной терминологией. Практическое задание не выполнено или содержит грубые ошибки.