# Фонд оценочных средств для промежуточной аттестации

по дисциплине

***Защита информации***

Направление подготовки
*02.03.02 Фундаментальная информатика и информационные технологии*

Направленность (профиль)
*Компьютерные науки*

Присваиваемая квалификация
**бакалавр**

Форма обучения
**очная**

Миасс 2026 г.

**02.03.02 Фундаментальная информатика и информационные технологии, Компьютерные науки, Защита информации, 2026, очная**

**Фонд оценочных средств одобрен и рекомендован:**
Проректор по учебной работе утверждено 27.02.26 А.А. Саламатов

Ученым советом Миасского филиала ФГБОУ ВО "ЧелГУ"

Протокол заседания № 8 от 24.02.2026

Председатель Ученого совета Миасского филиала ФГБОУ ВО "ЧелГУ" согласовано Т.В. Малькова

**Заседанием кафедры прикладной математики**

Протокол заседания № 6 от 30.01.2026

Заведующий кафедрой согласовано Е.В. Дутикова

Автор (составитель) И.О. Терентьев

**Структура фонда оценочных средств для промежуточной аттестации по дисциплине соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от 27.09.2022 г. № 573-1 «Об утверждении шаблонов документов».**

# Содержание

# 1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки: *02.03.02 «Фундаментальная информатика и информационные технологии»*
Направленность (профиль): *Компьютерные науки*
Дисциплина: *Защита информации*
Семестр изучения: *7*
Форма промежуточной аттестации: *зачет*

# 2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

## 2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Защита информации» направлено на формирование следующих компетенций:

| Коды компетенций согласно ФГОС (ОПОП ВО) | Содержание компетенций согласно ФГОС (ОПОП ВО) | Индикаторы достижения компетенций согласно ОПОП | Перечень планируемых результатов обучения по дисциплине |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| ОПК-4 | Способен участвовать в разработке технической документации программных продуктов и комплексов с использованием стандартов, норм и правил, а также в управлении проектами создания информационных систем на стадиях жизненного цикла | ОПК-4.1. Демонстрирует знание основных стандартов, норм и правил разработки технической документации, основ управления IT-проектами<br>ОПК-4.2. Способен принимать участие в процессах управления проектами по созданию информационных систем на стадиях жизненного цикла<br>ОПК-4.3. Имеет практический опыт участия в процессах управления IT-проектами | Знать организационнную структуру систем обеспечения информационной безопасности<br><br>Уметь применять сетевые средства защиты<br><br>Владеть навыками обнаружения и защиты от атак и вторжений в сетях |

| | | | |
|---|---|---|---|
| ОПК-5 | Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности | ОПК-5.1. Обладает базовыми знаниями основ установки и администрирования информационных систем и баз данных с учетом информационной безопасности<br>ОПК-5.2. Умеет инсталлировать программное обеспечение информационных систем и баз данных<br>ОПК-5.3. Имеет практический опыт сопровождения программного обеспечения информационных систем и баз данных | Знать<br>средства защиты информации от несанкционированного доступа<br><br>Уметь<br>применять программно-аппаратные средства шифрования<br><br>Владеть<br>навыками обнаружения и предотвращения веб-уязвимостей |

# 3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

## 3.1 Виды оценочных средств

| № п/п | Контролируемые темы/ разделы | Код компетенции/ планируемые результаты обучения | Наименование оценочного средства для текущего контроля | Наименование оценочного средства на промежуточной аттестации |
|---|---|---|---|---|
| 1 | Основы безопасности информационных технологий | ОПК-4<br>Знает организационнную структуру систем обеспечения информационной безопасности<br>Умеет применять сетевые средства защиты<br>Владеет навыками обнаружения и защиты от атак и вторжений в сетях<br>ОПК-5<br>Знает | Тест<br>Собеседование<br>Практическая работа | Вопросы к зачету |
| 2 | Обеспечение безопасности информационных технологий | | Тест<br>Собеседование<br>Практическая работа | Вопросы к зачету |
| 3 | Средства защиты информации от несанкционированного доступа | | Тест<br>Собеседование<br>Практическая работа | Вопросы к зачету |
| 4 | Обеспечение безопасности компьютерных систем и сетей | | Тест<br>Собеседование<br>Практическая работа | Вопросы к зачету |

| | | | | |
|---|---|---|---|---|
| 5 | Обеспечение безопасности веб-ресурсов. | средства защиты информации от несанкционированного доступа<br>Умеет применять программно-аппаратные средства шифрования<br>Владеет навыками обнаружения и предотвращения веб-уязвимостей | Тест<br>Собеседование<br>Практическая работа | Вопросы к зачету |

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе по дисциплине. Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре и являются учебно-методическими материалами ограниченного (конфиденциального) пользования.

### 3.2 Содержание оценочных средств для текущей аттестации

**Тестовые задания по дисциплине «Защита информации» (текущая аттестация)**

**Задания закрытого типа (1–10)**

1. Какая триада определяет основные свойства информационной безопасности?
   а) Скорость, Объём, Надёжность; б) Конфиденциальность, Целостность, Доступность; в) Аутентификация, Авторизация, Учёт; г) Шифрование, Хеширование, Подпись.
1. Какое средство защиты автоматически блокирует вредоносный сетевой трафик в реальном времени?
   а) IDS; б) IPS; в) Firewall; г) Proxy.
2. Какой тип атаки позволяет внедрить и выполнить произвольный код на стороне сервера через непроверенные пользовательские данные?
   а) XSS; б) CSRF; в) SQL Injection; г) Brute Force.
3. Какая технология создаёт защищённый туннель через публичную сеть для безопасного удалённого доступа?
   а) VLAN; б) VPN; в) DMZ; г) NAT.
4. Какой алгоритм хеширования утратил криптографическую стойкость из-за уязвимостей к коллизиям?
   а) SHA-256; б) MD5; в) AES; г) RSA.

5. Что обеспечивает шифрованная файловая система EFS в Windows?
   а) Сетевую аутентификацию; б) Прозрачное шифрование отдельных файлов и папок; в) Защиту от вирусов; г) Мониторинг действий пользователей.
6. Какой принцип разграничения доступа предполагает предоставление пользователям минимально необходимых прав для выполнения задач?
   а) Полного контроля; б) Обязательного контроля; в) Минимальных привилегий; г) Дискреционного контроля.
7. Какое расширение файла обычно указывает на сертификат открытого ключа в формате PEM?
   а) .p12; б) .cer / .pem; в) .dll; г) .log.
8. Какая модель описывает 7 уровней взаимодействия в сети, на каждом из которых могут применяться средства защиты?
   а) TCP/IP; б) OSI; в) DOD; г) ISO 27001.
9. Что является основной целью атаки CSRF (Cross-Site Request Forgery)?
   а) Кража сессионных cookie; б) Принуждение браузера жертвы выполнить нежелательное действие на доверенном сайте; в) Перебор паролей; г) Подмена DNS-записей.

**Задания открытого типа (11–20)**

11. Дайте определения трём базовым свойствам информационной безопасности (CIA). Поясните, почему нарушение любого из них критично для автоматизированной системы.
11. Опишите разницу между симметричным и асимметричным шифрованием. Приведите по одному примеру алгоритма для каждого типа и укажите их основное практическое применение.
12. Что такое SQL-инъекция? Опишите механизм эксплуатации и перечислите не менее трёх мер защиты от данного типа атак.
13. Объясните принцип работы и основное различие между системами IDS и IPS. В каких сценариях целесообразно использовать каждую из них?
14. Что представляет собой модель разграничения доступа к информации? Опишите этапы её разработки для корпоративной информационной системы.
15. Каковы основные задачи подразделения обеспечения информационной безопасности организации? Перечислите не менее четырёх ключевых функций.
16. Опишите механизм работы шифрованной файловой системы EFS. Какую роль играет агент восстановления (Recovery Agent) и где

хранятся ключи шифрования?

17. Какие требования предъявляются к современной парольной политике? Опишите безопасные методы хранения паролей в базе данных (например, использование солей и адаптивных хеш-функций).
18. Что такое виртуальные частные сети (VPN)? Какие основные протоколы (IPsec, SSL/TLS, WireGuard) используются для их построения и какие задачи они решают?
19. Опишите уязвимость XSS (Cross-Site Scripting). В чём разница между Stored, Reflected и DOM-based XSS? Как предотвратить эксплуатацию этой уязвимости?

**Задания на установление соответствия (21–25)**

21. Установите соответствие между свойством ИБ и его определением:

Конфиденциальность | А. Гарантия того, что информация доступна авторизованным пользователям по требованию
Целостность | Б. Свойство информации быть доступной только тем субъектам, которые имеют на это право
Доступность | В. Свойство информации сохранять точность и полноту, не подвергаясь несанкционированным изменениям

21. Установите соответствие между типом атаки и её описанием:

SQL Injection | А. Внедрение вредоносных скриптов на веб-страницы, просматриваемые другими пользователями
XSS | Б. Манипуляция запросами к базе данных через непроверенные входные параметры
CSRF | В. Принуждение авторизованного пользователя выполнить действие без его ведома

22. Установите соответствие между средством защиты и его функцией:

Межсетевой экран (Firewall) | А. Мониторинг трафика и оповещение администратора о подозрительной активности
IDS | Б. Фильтрация входящего и исходящего сетевого трафика на основе заданных правил
IPS | В. Автоматическое блокирование выявленных атак в реальном времени

23. Установите соответствие между криптографическим методом и примером алгоритма:

Симметричное шифрование | А. RSA, ECC
Асимметричное шифрование | Б. AES, ChaCha20
Криптографическое хеширование | В. SHA-256, Argon2

24. Установите соответствие между уровнем модели OSI и применяемым на нём механизмом защиты:

Сетевой уровень | A. TLS/SSL, S/MIME
Транспортный уровень | Б. IPsec, VPN-туннели
Прикладной уровень | В. WAF, OAuth 2.0, цифровые подписи документов

| № задания | Верный ответ | Критерии оценивания |
|---|---|---|
| **Задания закрытого типа (1–10)** | | |
| 1 | б) Конфиденциальность, Целостность, Доступность | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |
| 2 | б) IPS | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |
| 3 | в) SQL Injection | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |
| 4 | б) VPN | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |
| 5 | б) MD5 | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |
| 6 | б) Прозрачное шифрование отдельных файлов и папок | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |
| 7 | в) Минимальных привилегий | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |
| 8 | б) .cer / .pem | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |

| | | |
|---|---|---|
| 9 | б) OSI | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |
| 10 | б) Принуждение браузера жертвы выполнить нежелательное действие на доверенном сайте | **1 балл:** выбран верный вариант. **0 баллов:** выбран неверный вариант. |
| **Задания открытого типа (11–20)** | | |
| 11 | Конфиденциальность: защита от несанкционированного доступа. Целостность: защита от несанкционённого изменения/удаления. Доступность: гарантия работы и доступа к данным по запросу. Нарушение любого свойства ведёт к утечке, порче данных или остановке бизнес-процессов. | **2 балла:** даны точные определения и обоснована критичность. **1 балл:** определения верны, но пояснение поверхностное. **0 баллов:** ответ неверен или отсутствует. |
| 12 | Симметричное: один ключ для шифрования/расшифрования (AES, DES). Быстро, проблема передачи ключа. Асимметричное: пара ключей (открытый/закрытый) (RSA, ECC). Решает проблему обмена ключами, используется для ЭЦП и установления сеансовых ключей. | **2 балла:** корректно описана разница, приведены примеры и области применения. **1 балл:** описана только разница или только примеры. **0 баллов:** ответ неверен. |
| 13 | SQLi: внедрение произвольного SQL-кода через поля ввода. Меры: параметризованные запросы (prepared statements), валидация/санитизация ввода, принцип минимальных привилегий для БД, WAF. | **2 балла:** описан механизм и перечислены ≥3 корректных меры защиты. **1 балл:** описан только механизм или только 1–2 меры. **0 баллов:** ответ неверен. |
| 14 | IDS: только мониторинг и оповещение (passive). | **2 балла:** корректно |

| | | |
|---|---|---|
| | IPS: активное блокирование трафика в реальном времени. IDS используется для анализа и аудита, IPS — для предотвращения атак на периметре или внутри сети. | объяснены принципы и сценарии применения. **1 балл:** объяснено только одно из двух. **0 баллов:** ответ неверен. |
| 15 | Модель разграничения доступа определяет, кто, к каким ресурсам и при каких условиях имеет доступ. Этапы: инвентаризация ресурсов, классификация данных, определение ролей/прав, выбор модели (DAC/MAC/RBAC), документирование и внедрение, аудит. | **2 балла:** дано определение и перечислены ключевые этапы. **1 балл:** указан только один из компонентов. **0 баллов:** ответ неверен. |
| 16 | Задачи: разработка политик ИБ, мониторинг инцидентов, контроль доступа, обучение персонала, аудит и тестирование защищённости, взаимодействие с регуляторами. | **2 балла:** перечислены ≥4 задачи и дано краткое пояснение. **1 балл:** перечислены 1–3 задачи без пояснений. **0 баллов:** ответ неверен. |
| 17 | EFS шифрует файлы на уровне ФС с помощью симметричного ключа (FEK), который сам шифруется открытым ключом пользователя. Агент восстановления хранит отдельный сертификат для экстренного восстановления данных при утере ключей пользователя. | **2 балла:** описан механизм, роль агента и место хранения ключей. **1 балл:** описан только механизм или только роль агента. **0 баллов:** ответ неверен. |
| 18 | Требования: длина ≥12 символов, сложность, регулярная смена, запрет повторного использования. Хранение: адаптивные хеш-функции (Argon2, bcrypt, PBKDF2) + криптографическая соль. Никогда не хранить в открытом виде или с MD5/SHA1. | **2 балла:** перечислены требования и описан безопасный метод хранения. **1 балл:** указано только одно из двух. |

| | | |
|---|---|---|
| | | **0 баллов:** ответ неверен. |
| 19 | VPN: защищённый логический туннель поверх публичной сети. Протоколы: IPsec (сетевой уровень, site-to-site), SSL/TLS (удалённые пользователи), WireGuard (современный, высокопроизводительный). Решают задачи конфиденциальности, целостности и аутентификации трафика. | **2 балла:** дано определение, перечислены протоколы и задачи. **1 балл:** описано только одно из трёх. **0 баллов:** ответ неверен. |
| 20 | XSS: выполнение скриптов в браузере жертвы. Stored: сохраняется на сервере, Reflected: отражается в ответе, DOM-based: обрабатывается на клиенте без отправки на сервер. Защита: экранирование вывода, CSP, валидация ввода, HttpOnly/SameSite для cookie. | **2 балла:** описаны типы и перечислены меры защиты. **1 балл:** описаны только типы или только меры. **0 баллов:** ответ неверен. |
| **Задания на соответствие (21–25)** | | |
| 21 | 1-Б, 2-В, 3-А | **2 балла:** все пары сопоставлены верно. **1 балл:** допущена одна ошибка. **0 баллов:** две и более ошибок. |
| 22 | 1-Б, 2-А, 3-В | **2 балла:** все пары сопоставлены верно. **1 балл:** допущена одна ошибка. **0 баллов:** две и более ошибок. |
| 23 | 1-Б, 2-А, 3-В | **2 балла:** все пары сопоставлены верно. **1 балл:** допущена одна ошибка. **0 баллов:** две и более ошибок. |
| 24 | 1-Б, 2-А, 3-В | **2 балла:** все пары сопоставлены |

| | | |
|---|---|---|
| | | верно.<br>**1 балл:** допущена одна ошибка.<br>**0 баллов:** две и более ошибок. |
| 25 | 1-Б, 2-А, 3-В | **2 балла:** все пары сопоставлены верно.<br>**1 балл:** допущена одна ошибка.<br>**0 баллов:** две и более ошибок. |

| Набрано баллов | Процент выполнения | Оценка по шкале ФОС (Зачёт) | Уровень сформированности ОПК-4, ОПК-5 |
|---|---|---|---|
| 45–50 | 90–100% | **зачтено** | Продвинутый |
| 35–44 | 70–89% | **зачтено** | Базовый |
| 25–34 | 50–69% | **зачтено** | Пороговый |
| 0–24 | <50% | **не зачтено** | Компетенции не сформированы |

## Пример тестового задания

1. Какое свойство компонента (ресурса) АС заключается в том, что он доступен только тем субъектам (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия?
a конфиденциальность
b целостность
c доступность
d неотказуемость
e подотчётность
f достоверность
g аутентичность

2. Какое свойство компонента (ресурса) АС предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права?
a целостность
b конфиденциальность
c доступность
d неотказуемость
e подотчётность

f достоверность
g аутентичность

3. Какое свойство компонента (ресурса) АС означает, что имеющий соответствующие полномочия субъект может без особых проблем получить своевременный доступ к необходимому компоненту системы?
a доступность
b конфиденциальность
c целостность
d неотказуемость
e подотчётность
f достоверность
g аутентичность

**Темы практических работ**

В ходе обучения дисциплине обучающийся должен выполнить набор лабораторных/практических работ.

1. Изучение специальной терминологии, используемой в курсе «Информационная безопасность». Создание личного терминологического словаря.
2. Анализ способов хранения паролей на сайтах. Изучение методов хранения паролей. Поиск потенциально небезопасных сайтов.
3. Безопасность информации в корпоративных информационных системах. Внутренние угрозы.
4. Законодательство в сфере информационной безопасности. Анализ прецедентов.
5. Системы авторизации операционных систем.
6. Изучить работу шифрованной файловой системы EFS: особенности шифрования, файлов и папок, предназначение и работа агента восстановления, способы хранения ключевой информации.
7. Обнаружение и эксплуатация уязвимости SQL Injection: Types of SQL Injection, Different DBMSs, Blind SQL Injection
8. Обнаружение и эксплуатация уязвимости Cross-Site Scripting (XSS) Attacks
9. Обнаружение и эксплуатация уязвимости Cross-Site Request Forgery (CSRF) Attack
10. Обнаружение и эксплуатация уязвимости Command Injection Attacks
11. Обнаружение и эксплуатация уязвимости File Injection Attacks

12. Обнаружение и эксплуатация уязвимости Session Injection Attacks
13. Обнаружение и эксплуатация уязвимости Weak authentication and session management
14. Обнаружение и эксплуатация уязвимости Security Misconfiguration
15. Обнаружение и эксплуатация уязвимости Insufficient Transport Layer Protection

## Вопросы для собеседования

1. Что такое кибербезопасность?
2. Каковы элементы кибербезопасности?
3. Каковы преимущества кибербезопасности?
4. Различия IDS и IPS.
5. Что такое ЦРУ?
6. Что такое брандмауэр?
7. Объяснить трассировку
8. Различия HIDS и NIDS.
9. Объясните SSL
10. Что вы подразумеваете под утечкой данных?
11. Объясните атаку грубой силой. Как это предотвратить?
12. Что такое сканирование портов?
13. Назовите различные уровни модели OSI.
14. Что такое VPN?
15. Кто такие хакеры в черной шляпе?
16. Кто такие белые хакеры?
17. Кто такие серые хакеры?
18. Как сбросить конфигурацию BIOS, защищенную паролем?
19. Что такое MITM-атака?
20. Определите ARP и его рабочий процесс.
21. Объясните ботнет.
22. В чем основное различие между SSL и TLS?
23. Что такое CSRF?
24. Что такое 2FA? Как реализовать это для публичного сайта?
25. Объясните разницу между асимметричным и симметричным шифрованием.
26. Что такое полная форма XSS?
27. Что такое взлом?
28. Что такое сетевой сниффинг?

29. Какое значение имеет мониторинг DNS?
30. Что такое SSH?
31. Достаточно ли протокола SSL для сетевой безопасности?
32. Что такое тестирование черного ящика и тестирование белого ящика?
33. Объясните TCP Трехстороннее рукопожатие.
34. Определите термин остаточный риск. Каковы три способа борьбы с риском?

**Критерии оценивания по видам оценочных средств**

**Критерии оценивания собеседования**

При собеседовании выделяются критерии, по которым оцениваются знания учащихся.

Отметка «отлично» ставится в том случае, если по двум из трех критериев ответ оценивается «отлично» и по одному – на «хорошо».

Отметка «хорошо» – если по двум критериям – не ниже «хорошо» и по одному «удовлетворительно».

Отметка «удовлетворительно» – если по двум критериям не ниже «удовлетворительно» и по одному – «неудовлетворительно».

Отметка «неудовлетворительно» – если по двум и более критериям «неудовлетворительно».

Критерии:

Владение понятийным аппаратом

Владение фактическим материалом по теме

Логичность изложения материала.

**Критерии оценивания теста**

Набранная сумма баллов (процент правильных ответов) - оценка

Менее 60 - неудовлетворительно;

60-75 - удовлетворительно;

76-90 - хорошо;

91-100 - отлично.

**Критерии оценивания практических работ**

Оценка «зачтено» выставляется, если обучающийся свободно ориентируется в терминологии; способен привести примеры; свободно может ответить на дополнительные вопросы. Обучающийся: свободно ориентируется в материале тематики; владеет навыками настройки безопасности; может анализировать информацию и принимать решения;

свободно может ответить на дополнительные вопросы.

Оценка «не зачтено» выставляется, если обучающийся не ориентируется в терминологии; не способен привести примеры; не может ответить на дополнительные вопросы, не владеет навыками настройки безопасности; не может анализировать информацию и принимать решения.

## 4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 4.1 Порядок проведения и содержание оценочных средств промежуточной аттестации

Промежуточная аттестация проводится в форме зачета. Зачет проходит в два этапа.

На первом этапе студент письменно решает одну задачу и отвечает на два вопроса из выбранного случайным образом билета. Во время выполнения можно использовать справочные материалы. Время выполнения – 40 минут.

На втором этапе студент отвечает устно на вопросы из билета. Продолжительность – 10 минут.

Оценочные средства для промежуточной аттестации представлены базой вопросов к зачету.

**База вопросов к зачету**

1. Актуальность проблемы обеспечение безопасности информационных технологий.
2. Основные понятия информационной безопасности. Угрозы информационной безопасности в АС.
3. Виды мер и основные принципы обеспечения информационной безопасности.
4. Правовые основы обеспечения информационной безопасности.
5. Основные защитные механизмы, используемые в СЗИ.
6. Требования к системам и средствам защиты информации от несанкционированного доступа
7. Организационная структура системы обеспечения информационной безопасности.
8. Обязанности конечных пользователей и ответственных за ОИБ в подразделениях.
9. Инструкции по организации парольной и антивирусной защиты.

10. Определение требований к защите ресурсов.
11. Основные задачи подразделения обеспечения информационной безопасности.
12. Концепция информационной безопасности организации.
13. Безопасность информации в корпоративных информационных системах. Внутренние угрозы.
14. Разработка модели разграничения доступа к информации.
15. Управление доступом в компьютерных системах.
16. Задачи контроля и обеспечения безопасности информации.
17. Разрушающие программные воздействия и защита от них.
18. Обеспечение целостности информации.
19. Назначение и возможности СЗИ НСД. Рекомендации по выбору средств защиты от НСД. Аппаратные средства СЗИ НСД.
20. Работа шифрованной файловой системы EFS: особенности шифрования, файлов и папок, предназначение и работа агента восстановления, способы хранения ключевой информации.
21. Системы авторизации операционных систем.
22. Программно-аппаратные средства шифрования.
23. Методы распределения и хранения ключевой и парольной информации
24. Обеспечение безопасности компьютерных систем и сетей
25. Угрозы, уязвимости и атаки в сетях. Сетевые средства защиты.
26. Обеспечение безопасности межсетевого взаимодействия. Удаленные сетевые атаки.
27. Технологии межсетевых экранов.
28. Системы обнаружения атак и вторжений.
29. Виртуальные частные сети.
30. Обеспечение безопасности веб-ресурсов.
31. Уязвимости веб-ресурсов.
32. Обнаружение, эксплуатация и предотвращение веб-уязвимостей (SQL Injection: Types of SQL Injection, Different, DBMSs, Blind SQL Injection, Cross-Site Scripting (XSS) Attacks, Cross-Site Request Forgery (CSRF) Attack, Command Injection Attacks, File Injection Attacks, Session Injection Attacks, Weak authentication and session management, Security Misconfiguration, Insufficient Transport Layer Protection).

## 4.2. Критерии оценивания компетенций в ходе промежуточной аттестации

| Код компетенции | Планируемые результаты обучения по дисциплине | Критерии оценивания | |
|---|---|---|---|
| | | зачтено | Не зачтено |
| ОПК-4 | Знает организационнную структуру систем обеспечения информационной безопасности | Знает организационнную структуру систем обеспечения информационной безопасности | Не знает организационнную структуру систем обеспечения информационной безопасности |
| | Умеет применять сетевые средства защиты | Умеет применять сетевые средства защиты | Не умеет применять сетевые средства защиты |
| | Владеет навыками обнаружения и защиты от атак и вторжений в сетях | Владеет навыками обнаружения и защиты от атак и вторжений в сетях | Не владеет навыками обнаружения и защиты от атак и вторжений в сетях |
| ОПК-5 | Знает средства защиты информации от несанкционированного доступа | Знает средства защиты информации от несанкционированного доступа | Не знает средства защиты информации от несанкционированного доступа |
| | Умеет применять программно-аппаратные средства шифрования | Умеет применять программно-аппаратные средства шифрования | Не умеет применять программно-аппаратные средства шифрования |
| | Владеет навыками обнаружения и предотвращения веб-уязвимостей | Владеет навыками обнаружения и предотвращения веб-уязвимостей | Не владеет навыками обнаружения и предотвращения веб-уязвимостей |

**Критерии оценивания зачета**

Письменный и письменно-устный ответ студента по вопросам дисциплины оценивается положительно с выставлением оценки «зачтено» в следующих случаях:

– студент глубоко и полно владеет содержанием учебного материала; умеет связывать теорию с практикой, решает соответствующие задачи, теоретические выводы подтверждает примерами. Делает выводы логично, четко. Ясно и кратко излагает ответы на поставленные вопросы; умеет обосновывать свои суждения. Дан полный, развёрнутый ответ на поставленный вопрос; показана совокупность осознанных знаний об объекте изучения, утверждения теорем приведены с доказательствами, свободно оперирует понятиями, терминами; в ответе прослеживается чёткая структура, выстроенная в логической последовательности; ответ изложен литературным

грамотным языком и носит самостоятельный характер; все решения задач выполнены верно.
– ответ студента соответствует указанным выше критериям, но содержание ответа имеет отдельные неточности (несущественные ошибки) в изложении теоретического и практического материала, отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой; были допущены неточности в определении понятий, допущены незначительные ошибки в решении задач, допущенные ошибки исправляются студентом после дополнительных вопросов экзаменатора.
– студент обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности и существенные ошибки в определении понятий, формулировке положений, наблюдается нарушение логики изложения; в ответе не присутствуют доказательные выводы; сформированность умений показана слабо, допущены незначительные ошибки в решении задач.
Оценка «не зачтено» за письменный и письменно-устный ответ студента по вопросам дисциплины выставляется в случаях, когда:
– студент имеет разрозненные, бессистемные знания: не умеет выделять главное и второстепенное; допускает ошибки в определении понятий, формулировке теоретических положений, искажает их смысл; беспорядочно и неуверенно излагает материал;
– не умеет соединять теоретические положения с практикой; не умеет применять знания для обоснования и объяснения фактов, не устанавливает межпредметные связи.

### 4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

| Уровень освоения компетенций | Оценка |
|---|---|
| Продвинутый | зачтено |
| Базовый | зачтено |
| Пороговый | зачтено |
| компетенции не сформированы | Не зачтено |

**Уровни формирования компетенций:**

1. Пороговый уровень:
   - предполагает формирование компетенций на начальном уровне: знание базовых терминов, основных понятий кибербезопасности;

- студент способен давать ответы на теоретические вопросы дисциплины, использовать базовые термины; решать основные задачи по защите информации.

2. Базовый уровень:
   - предполагает формирование компетенций на более высоком уровне: понимание организационной структуры систем обеспечения информационной безопасности, защиты информации от несанкционированного доступа;
   - студент способен применять сетевые средства защиты, программно-аппаратные средства шифрования.
3. Продвинутый уровень:
   - предполагает формирование компетенций на высоком уровне, готовность к самостоятельной профессиональной деятельности: формируется знание средств защиты информации от несанкционированного доступа и систем обеспечения информационной безопасности;
   - студент способен самостоятельно применять сетевые средства защиты, программно-аппаратные средства шифрования, владеет навыками обнаружения и защиты от атак и вторжений в сетях, обнаружения и предотвращения веб-уязвимостей