Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»
Финансово-экономический колледж

УТВЕРЖДАЮ
Директор
_____ Р. А. Сычев
«__» _____ 2026г.

Рабочая программа дисциплины
Основы информационной безопасности

Специальность
09.02.12 ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И СОПРОВОЖДЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Форма обучения	очная
Часов по учебному	48
в том числе:	
аудиторные занятия	40
самостоятельная работа	8

Ростов-на-Дону
2026 г.

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	10			
Вид занятий	УП	РП	УП	РП
Лекции	20	20	20	20
Практические	20	20	20	20
Итого ауд.	40	40	40	40
Контактная работа	40	40	40	40
Сам. работа	8	8	8	8
Итого	48	48	48	48

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.12 ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И СОПРОВОЖДЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ (приказ Министерство просвещения Российской Федерации от 10.03.2025 г. № 184)

Рабочая программа составлена по образовательной программе 09.02.12 ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И СОПРОВОЖДЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ для набора 2026 года
программа среднего профессионального образования

Учебный план утвержден учёным советом вуза от 03.03.2026 протокол № 9

Программу составил(и): Преп., Ленц С.С

Председатель ЦМК: Ламин В. А.

Рассмотрено на заседании ЦМК от 06.03.2026 протокол № 7

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	ОП
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Операционные системы и среды
2.1.2	Математический аппарат в отрасли информационных технологий
2.1.3	Базы данных
2.1.4	Архитектура аппаратных средств и основы сетевых технологий
2.1.5	Основы алгоритмизации и программирования
2.1.6	Тестирование и эксплуатация информационных систем
2.1.7	Проектирование и разработка информационных систем
2.1.8	Настройка и обеспечение работоспособности программных и аппаратных средств устройств инфокоммуникационных систем
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Автоматизация процессов тестирования программного обеспечения
2.2.2	Демонстрационный экзамен

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

3.1 Знать

ОК 01.: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте

алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах

структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности

ОК 02.: Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

номенклатуру информационных источников, применяемых в профессиональной деятельности

приемы структурирования информации; формат оформления результатов поиска информации

современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности

ОК 09.: Пользоваться профессиональной документацией на государственном и иностранном языках

лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

правила построения простых и сложных предложений на профессиональные темы

основные общеупотребительные глаголы (бытовая и профессиональная лексика)

3.2 Уметь

ОК 01.: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части

определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы

составлять план действия; определять необходимые ресурсы; реализовывать составленный план; оценивать результат и последствия своих действий

ОК 02.: Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

определять задачи для поиска информации; определять необходимые источники информации

планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации

оформлять результаты поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение и цифровые средства

ОК 09.: Пользоваться профессиональной документацией на государственном и иностранном языках

понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые)

понимать тексты на базовые профессиональные темы

участвовать в диалогах на знакомые общие и профессиональные темы

3.3 Владеть

ОК 01.: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

навыками распознавания и анализа профессиональных проблем

навыками поиска информации и планирования действий

навыками реализации плана и оценки результатов

ОК 02.: Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

навыками определения цели поиска

навыками структурирования и анализа информации

навыками применения ИТ для решения профессиональных задач

ОК 09.: Пользоваться профессиональной документацией на государственном и иностранном языках

навыками понимания профессиональной речи

навыками чтения профессиональных текстов

навыками устной профессиональной коммуникации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1. Введение в информационную безопасность					
1.1	Тема 1.1. Основные понятия, история, угрозы ИБ /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
	Раздел 2. Управление безопасностью и криптография					

2.1	Тема 2.1. Нормативно-правовое регулирование ИБ. Политики безопасности /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
2.2	Тема 2.2. Основы криптографии (симметричное, асимметричное, хэширование, цифровая подпись, стеганография) /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
2.3	Тема 2.3. Практическая работа с алгоритмами шифрования /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
2.4	Тема 2.4. Практическая работа с цифровой подписью и стеганографией /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
2.5	Тема 2.5. Самостоятельная работа: изучение ФЗ-152 и настройка шифрования на домашнем ПК /Ср/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
	Раздел 3. Сетевая безопасность					
3.1	Тема 3.1. Сетевые атаки (DDoS, MITM, ARP-spoofing). Межсетевые экраны /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
3.2	Тема 3.2. VPN, IDS/IPS. Анализ трафика /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
3.3	Тема 3.3. Безопасность беспроводных сетей (Wi-Fi) /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
3.4	Тема 3.4. Практическая работа: настройка брандмауэра /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
3.5	Тема 3.5. Практическая работа: настройка VPN и анализ трафика /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
3.6	Тема 3.6. Практическая работа: анализ безопасности Wi-Fi /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
3.7	Тема 3.7. Самостоятельная работа: настройка брандмауэра и анализ сетевых атак /Ср/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
	Раздел 4. Безопасность приложений и защита данных					
4.1	Тема 4.1. Уязвимости веб-приложений (OWASP Top 10) /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	

4.2	Тема 4.2. Тестирование на проникновение, шифрование данных и резервное копирование /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
4.3	Тема 4.3. Практическая работа: эксплуатация уязвимостей веб-приложений /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
4.4	Тема 4.4. Практическая работа: сканирование уязвимостей с помощью OWASP ZAP /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
4.5	Тема 4.5. Практическая работа: резервное копирование и шифрование данных /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
4.6	Тема 4.6. Самостоятельная работа: анализ уязвимости OWASP и скрипт резервного копирования /Ср/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
	Раздел 5. Инциденты, социальная инженерия и кибергигиена					
5.1	Тема 5.1. Реагирование на инциденты. Цифровая криминалистика (форензика) /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
5.2	Тема 5.2. Социальная инженерия. Кибергигиена. Этические аспекты /Лек/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
5.3	Тема 5.3. Практическая работа: анализ логов и расследование инцидента /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
5.4	Тема 5.4. Самостоятельная работа: известные инциденты ИБ и проверка кибергигиены /Ср/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	
5.5	Тема 5.5. Практическая работа: разбор фишинга и разработка памятки Дифференцированный зачет /Пр/	5	2	ОК 01. ОК 02. ОК 09.	Л1.1Л2.1.Э1 Э2 Э3	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация проходит в форме дифференцированного зачета. Перечень вопросов к дифференцированному зачету:

1.Дайте определение информационной безопасности. Назовите основные составляющие (триада CIA).
2.Перечислите основные виды угроз информационной безопасности.
3.Что такое политика информационной безопасности? Какие разделы она включает?
4.Назовите основные нормативно-правовые акты РФ в области ИБ (ФЗ-149, ФЗ-152, Приказы ФСТЭК).
5.Что такое модель угроз? Для чего она разрабатывается?
6.Цели и задачи стандарта ISO/IEC 27001.
7.Что такое криптография? Назовите основные задачи криптографии.
8.Отличие симметричного шифрования от асимметричного. Примеры алгоритмов.
9.Что такое хэш-функция? Где применяется? Примеры алгоритмов (MD5, SHA).
10.Что такое цифровая подпись? Как работает и для чего используется?
11.Что такое стеганография? Примеры.
12.Какие сетевые атаки вы знаете? Принцип DDoS-атаки и способы защиты.
13.Что такое MITM-атака (man-in-the-middle)? Как защититься?
14.Назначение и принцип работы межсетевого экрана (брандмауэра). Типы.
15.Что такое VPN? Какие протоколы VPN знаете? Для чего используется VPN?
16.Системы обнаружения вторжений (IDS/IPS): разница, примеры.
17.Уязвимости беспроводных сетей Wi-Fi. Как защитить Wi-Fi?
18.Что такое OWASP Top 10? Приведите 3–4 примера уязвимостей веб-приложений.
19.Что такое SQL-инъекция? Как выполняется и как защититься?
20.Что такое XSS (межсайтовый скриптинг)? Типы XSS, методы защиты.
21.Что такое тестирование на проникновение (пентест)? Этапы.
22.Инструменты для анализа защищённости веб-приложений (Burp Suite, OWASP ZAP, Nikto).
23.Шифрование данных в покое и в транзите. Примеры технологий.
24.Стратегии резервного копирования: полное, инкрементное, дифференциальное.
25.Что такое инцидент информационной безопасности? Жизненный цикл реагирования.
26.Что такое цифровая криминалистика (форензика)? Задачи.
27.Что такое социальная инженерия? Примеры атак (фишинг, претекстинг, кви-про-кво).
28.Основные правила цифровой гигиены для ИТ-специалиста.
29.Этические аспекты информационной безопасности.
30.Современные тенденции в области ИБ (AI, ML, блокчейн). Новые угрозы.
31.История развития информационной безопасности.
32.Сравнительный анализ симметричных и асимметричных криптоалгоритмов.
33.Анализ уязвимостей OWASP Top 10 на примере реальных веб-приложений.
34.Методы защиты от DDoS-атак.
35.Социальная инженерия: методы и противодействие.
36.Правовые аспекты защиты персональных данных в РФ (ФЗ-152).
37.Облачная безопасность: риски и средства защиты.
38.Роль цифровой криминалистики в расследовании инцидентов.
39.Этические хакеры (пентестеры): функции, инструменты, ответственность.
40.Сравнение алгоритмов хэширования (MD5, SHA-1, SHA-256).
41.Безопасность мобильных устройств и приложений.
42.Тенденции развития информационной безопасности с использованием AI и ML.

Критерии оценивания

5 баллов – полный и правильный ответ на все вопросы билета с логическим обоснованием аргументов, в ответе нет ошибок.

4 балла – вопросы билета раскрыты полностью, но обоснования и доказательства недостаточны; допущены 2–3 несущественные ошибки, исправленные по требованию преподавателя.

3 балла – правильный ответ на вопросы билета, но допущено более одной ошибки по изложению фактов или более 2–3 недочётов в ответе.

2 балла – допущены существенные ошибки, показавшие, что обучающийся не обладает обязательными умениями по данной теме в полной мере.

5.2. Фонд оценочных средств для проведения текущего контроля

Представлен в Приложении 1 к рабочей программе дисциплины.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ				
6.1. Рекомендуемая литература				
6.1.1. Основная литература				
	Авторы,	Заглавие	Издательство,	Колич-во
Л1.1	Щербак А. В.	Информационная безопасность : учебник для СПО	М. : Юрайт, 2026. — 2-е изд. — 252 с.	https://web5.urait.ru/bcode/588374 неограниченный доступ зарегистрированным пользователям
6.1.2. Дополнительная литература				
	Авторы,	Заглавие	Издательство,	Колич-во
Л2.1	Полякова Т. А., Стрельцов А. А., Чубукова С. Г. и др. (под ред. Т. А. Поляковой, А. А. Стрельцова)	Организационное и правовое обеспечение информационной безопасности : учебник для СПО	М. : Юрайт, 2025. — 2-е изд., перераб. и доп. — 357 с	https://web5.urait.ru/bcode/561717[reference:5] неограниченный доступ зарегистрированным пользователям
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	База данных угроз ФСТЭК России https://bdu.fstec.ru			
Э2	Портал «Информационная безопасность России			
Э3	Red Soft – документация по Red OS, установка ПО https://redsoft.ru			
6.3. Перечень программного обеспечения				
6.3.1	Офисный пакет Red OS			
6.3.2	Офисный пакет LibreOffice			
6.4 Перечень информационных справочных систем				
6.4.1	ИСС «КонсультантПлюс»			
6.4.2	ИСС «Гарант»			

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ
Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ОП.06 Основы информационной безопасности

1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

УУД, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОК.01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам			
Знать: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	**Получение систематических знаний** о сущности информационной безопасности, угрозах, нормативной базе, методах защиты информации	**Уровень знаний** основных понятий ИБ, классификации угроз, криптографических алгоритмов, сетевых атак, уязвимостей веб-приложений	**Т(1-42)**
Уметь: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы составлять план действия; определять необходимые ресурсы; реализовывать составленный план; оценивать результат и последствия своих действий	**Сформировать систематическое умение** идентифицировать инциденты ИБ, настраивать средства защиты (брандмауэр, VPN, антивирус), применять криптографию	**Уровень умения** выполнять практические действия по защите информации, анализировать логи, выявлять уязвимости	**Т(1-42)** **ПЗ(1-10)**
Владеть: навыками распознавания и анализа профессиональных проблем навыками поиска информации и планирования действий навыками реализации плана и оценки результатов	**Сформировать систематическое владение** методами анализа угроз, настройки защиты, реагирования на инциденты,	**Уровень владения** навыками применения антивирусной защиты, шифрования, управления	**Т(1-42)** **ПЗ(1-10)**

навыками поиска информации и планирования действий навыками реализации плана и оценки результатов	составления отчётности	доступом, расследования инцидентов	
ОК.02: Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности			
Знать: номенклатуру информационных источников, применяемых в профессиональной деятельности приемы структурирования информации; формат оформления результатов поиска информации современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности	**Получение систематических знаний** о базах данных угроз (ФСТЭК, CVE), порталах (Infosec, OWASP), инструментах анализа (Wireshark, ZAP)	**Уровень знаний** источников профессиональной информации и средств их применения	**Т(1-42)**
Уметь: определять задачи для поиска информации; определять необходимые источники информации планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации оформлять результаты поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение и цифровые средства	**Сформировать систематическое умение** использовать OWASP ZAP, Wireshark, OpenSSL, GPG для поиска уязвимостей, анализа трафика, шифрования данных	**Уровень умения** работать с профессиональными базами данных, составлять отчёты по результатам сканирования и анализа	**Т(1-42)** **ПЗ(1-10)**
Владеть: навыками определения цели поиска навыками структурирования и анализа информации навыками применения ИТ для решения профессиональных задач	**Сформировать систематическое владение** навыками поиска информации об уязвимостях, анализа защищённости, оформления результатов в виде отчётов и рекомендаций	**Уровень владения** инструментарием поиска и анализа информации для выявления инцидентов ИБ	**Т(1-42)** **ПЗ(1-10)**
ОК.09: Пользоваться профессиональной документацией на государственном и иностранном языках			
Знать: лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	**Получение систематических знаний** англоязычных терминов в области ИБ (security, threat,	**Уровень знаний** профессиональной лексики для чтения документации (man-страницы, руководства к	**Т(1-42)**

правила построения простых и сложных предложений на профессиональные темы основные общеупотребительные глаголы (бытовая и профессиональная лексика)	encryption, firewall, vulnerability, incident)	OpenSSL, Wireshark)	
Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые) понимать тексты на базовые профессиональные темы участвовать в диалогах на знакомые общие и профессиональные темы	**Сформировать систематическое умение** читать и понимать команды на английском (gpg --verify, iptables -L), следовать инструкциям из официальной документации	**Уровень умения** работать с документацией на государственном и иностранном языках при настройке средств защиты	**Т(1-42)** **ПЗ(1-10)**
Владеть: навыками понимания профессиональной речи навыками чтения профессиональных текстов навыками устной профессиональной коммуникации	**Сформировать систематическое владение** навыками самостоятельного изучения технической документации на русском и английском языке для решения задач ИБ	**Уровень владения** профессиональной терминологией для общения со службой ИБ и составления отчётов	**Т(1-42)** **ПЗ(1-10)**

Т – тестовые задания, ПЗ – практические задания.

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тестовые задания:

1. Что понимается под информационной безопасностью в рамках классической триады CIA?
    a. защита информации от несанкционированного копирования и распространения
    b. обеспечение конфиденциальности, целостности и доступности информации
    c. предотвращение любых технических сбоев в работе информационных систем
    d. комплекс мер по шифрованию всех данных, передаваемых по сети
2. К какому виду угроз информационной безопасности относится нарушение целостности данных?
    a. угрозы конфиденциальности
    b. угрозы доступности
    c. угрозы целостности
    d. угрозы аутентичности
3. Какой раздел обязательно входит в политику информационной безопасности организации?
    a. описание архитектуры локальной сети
    b. правила использования съёмных носителей и доступа в Интернет
    c. список всех установленных программных продуктов
    d. детальный план эвакуации при пожаре
4. Какой федеральный закон регулирует защиту персональных данных в Российской Федерации?

a. ФЗ-149 «Об информации, информационных технологиях и о защите информации»
b. ФЗ-152 «О персональных данных»
c. ФЗ-63 «Об электронной подписи»
d. ФЗ-187 «О безопасности критической информационной инфраструктуры»

5. Для чего разрабатывается модель угроз информационной безопасности?
   a. для расчёта бюджета на закупку антивирусного программного обеспечения
   b. для определения актуальных угроз и уязвимостей, а также оценки рисков
   c. для создания резервных копий всех данных организации
   d. для разработки дизайна пользовательского интерфейса информационной системы
6. Какова основная цель стандарта ISO/IEC 27001?
   a. описание алгоритмов симметричного шифрования
   b. установление требований к системе менеджмента информационной безопасности (СМИБ)
   c. классификация вредоносного программного обеспечения
   d. стандартизация форматов цифровых сертификатов
7. Какая задача **не** относится к основным задачам криптографии?
   a. обеспечение конфиденциальности
   b. обеспечение целостности
   c. обеспечение аутентификации
   d. обеспечение высокой скорости передачи данных по каналу связи
8. В чём главное отличие симметричного шифрования от асимметричного?
   a. симметричное шифрование использует два разных ключа, асимметричное — один
   b. симметричное шифрование использует один и тот же ключ для шифрования и расшифрования, асимметричное — пару ключей (открытый и закрытый)
   c. симметричное шифрование применяется только для текстовых данных, асимметричное — для любых
   d. симметричное шифрование всегда медленнее асимметричного
9. Для чего применяется хэш-функция MD5 или SHA-256?
   a. для обратимого шифрования коротких сообщений
   b. для проверки целостности данных и создания цифровых отпечатков
   c. для генерации псевдослучайных чисел
   d. для сжатия файлов без потерь
10. Какое свойство обеспечивает цифровая подпись?
    a. конфиденциальность передаваемого сообщения
    b. неотказуемость (невозможность отказа от авторства) и целостность
    c. увеличение скорости передачи данных
    d. анонимность отправителя
11. Что из перечисленного является примером стеганографии?
    a. шифрование письма с помощью алгоритма AES
    b. скрытие текстового сообщения внутри изображения формата JPEG
    c. подписание документа электронной подписью
    d. проверка пароля по его хэш-сумме
12. Каков принцип DDoS-атаки?
    a. перехват трафика между клиентом и сервером
    b. подбор пароля методом перебора по словарю
    c. отправка огромного количества запросов с множества хостов для исчерпания ресурсов сервера
    d. внедрение вредоносного SQL-кода в поле ввода веб-формы
13. Какой метод наиболее эффективен для защиты от MITM-атак (человек посередине)?
    a. использование сложных паролей
    b. применение шифрования и проверки подлинности сертификатов (TLS/SSL)
    c. регулярное обновление антивирусных баз
    d. отключение межсетевого экрана
14. Какую функцию выполняет межсетевой экран (брандмауэр) с фильтрацией пакетов?

a. анализирует заголовки пакетов и принимает решение о пропуске или блокировке на основе заданных правил
b. шифрует весь исходящий трафик
c. обнаруживает и удаляет вирусы в почтовых вложениях
d. создаёт резервные копии сетевых настроек

15. Для чего в первую очередь используется технология VPN?
    a. для ускорения загрузки веб-страниц
    b. для создания защищённого канала связи через небезопасную сеть (например, Интернет)
    c. для фильтрации спама в электронной почте
    d. для управления правами доступа в локальной сети
16. Чем IDS (система обнаружения вторжений) отличается от IPS (система предотвращения вторжений)?
    a. IDS только сигнализирует о подозрительной активности, IPS может блокировать её в реальном времени
    b. IDS работает на сетевом уровне, IPS — на прикладном
    c. IDS использует сигнатурный анализ, IPS — только аномальный
    d. принципиальных отличий нет, это синонимы
17. Какая уязвимость характерна для протокола WPA2 в сетях Wi-Fi?
    a. отсутствие шифрования передаваемых данных
    b. уязвимость KRACK, позволяющая переустановить ключ шифрования
    c. обязательное использование короткого вектора инициализации
    d. невозможность скрыть SSID точки доступа
18. Какая уязвимость **не** входит в OWASP Top 10?
    a. SQL-инъекция
    b. межсайтовый скриптинг (XSS)
    c. небезопасная десериализация
    d. переполнение буфера в ядре операционной системы
19. Какой символ в SQL-запросе часто используется для начала однострочного комментария при эксплуатации SQL-инъекции?
    a. # (решётка)
    b. -- (два дефиса)
    c. // (два слеша)
    d. %% (два процента)
20. Какой тип XSS-атаки подразумевает сохранение вредоносного скрипта на сервере (например, в базе данных) и его последующее выполнение у всех посетителей страницы?
    a. отражённая XSS (Reflected XSS)
    b. хранимая XSS (Stored XSS)
    c. DOM-based XSS
    d. слепая XSS (Blind XSS)
21. С какого этапа обычно начинается тестирование на проникновение (пентест)?
    a. эксплуатация уязвимостей
    b. составление отчёта
    c. сбор информации и разведка (reconnaissance)
    d. закрепление в системе
22. Какой из инструментов предназначен для анализа защищённости веб-приложений?
    a. Wireshark
    b. OWASP ZAP
    c. Nmap
    d. Metasploit
23. Что означает «шифрование данных в покое»?
    a. шифрование трафика во время передачи по сети
    b. шифрование файлов, хранящихся на жёстком диске или в базе данных
    c. шифрование только метаданных файловой системы
    d. шифрование данных с использованием аппаратных модулей HSM
24. Чем инкрементное резервное копирование отличается от дифференциального?

a. инкрементное копирует все данные каждый раз, дифференциальное — только изменения с момента последнего полного копирования
b. инкрементное копирует только изменения с момента последнего копирования (любого), дифференциальное — изменения с момента последнего **полного** копирования
c. дифференциальное копирование всегда требует больше места, чем инкрементное
d. это одно и то же, разные названия

25. С какой фазы начинается жизненный цикл реагирования на инцидент ИБ?
    a. сдерживание (containment)
    b. ликвидация последствий (eradication)
    c. обнаружение и анализ (detection and analysis)
    d. подготовка (preparation)
26. Что является одной из главных задач цифровой криминалистики (форензики)?
    a. предотвращение взлома системы в реальном времени
    b. сбор, сохранение и анализ цифровых доказательств без их изменения
    c. автоматическое восстановление удалённых файлов
    d. настройка политик брандмауэра
27. Какой из примеров относится к атаке социальной инженерии?
    a. подбор пароля с помощью гибридной атаки
    b. отправка фишингового письма с просьбой срочно подтвердить учётные данные
    c. эксплуатация уязвимости нулевого дня в веб-сервере
    d. сканирование портов целевого хоста
28. Что **не** является правилом цифровой гигиены для ИТ-специалиста?
    a. регулярно обновлять операционную систему и программное обеспечение
    b. использовать двухфакторную аутентификацию
    c. записывать все пароли в незашифрованный текстовый файл на рабочем столе
    d. проверять подлинность ссылок перед переходом
29. Какой этический принцип запрещает специалисту по ИБ использовать полученные знания для несанкционированного доступа к чужим системам?
    a. принцип ответственности
    b. принцип законности
    c. принцип конфиденциальности
    d. принцип доступности
30. Какая современная технология активно используется для выявления аномалий и новых угроз в информационной безопасности?
    a. машинное обучение (ML) и искусственный интеллект (AI)
    b. классическое сигнатурное антивирусное сканирование
    c. одностороннее хэширование MD5
    d. симметричное шифрование AES-256
31. С какого периода принято отсчитывать историю современной информационной безопасности?
    a. с изобретения письменности
    b. с появления первых мэйнфреймов и многопользовательских систем в 1960-х – 1970-х годах
    c. с момента создания сети Интернет в 1990-х годах
    d. с принятия Федерального закона «О персональных данных» в 2006 году
32. Какой из криптоалгоритмов является асимметричным?
    a. AES
    b. Blowfish
    c. RSA
    d. ChaCha20
33. Какую уязвимость OWASP Top 10 позволяет эксплуатировать атака вида ' OR '1'='1?
    a. небезопасная десериализация
    b. включение сторонних файлов (LFI/RFI)
    c. SQL-инъекция
    d. подделка межсайтовых запросов (CSRF)

34. Какой метод **не** помогает защититься от DDoS-атак?
    a. использование CDN и сервисов фильтрации трафика (Cloudflare, Qrator)
    b. настройка rate limiting на веб-сервере
    c. отключение межсетевого экрана для ускорения обработки пакетов
    d. применение синхронизированных cookie (SYN cookie)
35. Какой приём используется в претекстинге (одном из видов социальной инженерии)?
    a. рассылка писем от имени банка с вредоносным вложением
    b. создание вымышленной легенды для получения доверия жертвы и выведывания информации
    c. перехват SMS с кодом подтверждения
    d. внедрение кейлоггера на компьютер жертвы
36. Какая информация относится к персональным данным согласно ФЗ-152?
    a. только паспортные данные и ИНН
    b. любая информация, прямо или косвенно относящаяся к определённому физическому лицу
    c. сведения о юридическом лице из ЕГРЮЛ
    d. общедоступная информация из открытых реестров
37. Какой риск связан с использованием публичных облачных сервисов (модель «разделяемой ответственности»)?
    a. провайдер полностью отвечает за безопасность данных клиента и его приложений
    b. клиент несёт ответственность за безопасность своих данных и настройку доступа в своей части облачной инфраструктуры
    c. облачные сервисы не подвержены DDoS-атакам
    d. данные в облаке всегда шифруются провайдером без возможности отключения
38. Что является первоочередным действием при сборе цифровых доказательств (форензика)?
    a. выключить компьютер для предотвращения дальнейших изменений
    b. создать побитовую копию (образ) носителя информации
    c. удалить все подозрительные файлы и очистить логи
    d. сразу сообщить об инциденте в СМИ
39. Какую функцию выполняют этичные хакеры (пентестеры)?
    a. взламывают системы для личной выгоды или развлечения
    b. легально, с разрешения владельца, ищут уязвимости для их последующего устранения
    c. разрабатывают вредоносное программное обеспечение на заказ
    d. администрируют почтовые серверы компаний
40. Какой из алгоритмов хэширования считается криптостойким на сегодняшний день?
    a. MD5
    b. SHA-1
    c. SHA-256
    d. CRC32
41. Какой механизм рекомендуется для защиты данных в мобильных приложениях?
    a. хранение токенов доступа в открытом виде в SharedPreferences
    b. использование безопасного хранилища (Keystore / Keychain) и проверка SSL-сертификатов
    c. отказ от шифрования для повышения производительности
    d. передача данных по протоколу HTTP без шифрования
42. Как AI и ML помогают в сфере информационной безопасности?
    a. полностью заменяют необходимость в специалистах SOC
    b. позволяют выявлять аномалии и новые угрозы на основе поведенческого анализа, сокращая время реакции
    c. используются исключительно для взлома паролей
    d. гарантируют 100% защиту от всех видов атак

Критерии оценивания:

- 5 баллов выставляется, если правильные ответы даны на 85-100% тестовых заданий

- 4 балла выставляется студенту, если правильные ответы даны на 65-84% тестовых заданий

- 3 балла выставляется студенту, если правильные ответы даны на 50-64% тестовых заданий

- 2 балла выставляется студенту, если правильные ответы даны на менее 50% тестовых заданий

Практические задания:

№ 1

Тема: Работа с алгоритмами шифрования (AES, RSA, хэширование)

Цель: Научиться применять симметричное (AES) и асимметричное (RSA) шифрование, вычислять хэш-функции.

Теоретические вопросы:

1. Принцип работы симметричного шифрования (AES, DES).
2. Принцип работы асимметричного шифрования (RSA).
3. Понятие хэш-функции (MD5, SHA-256), области применения.

Оборудование и ПО:

ПК с ОС Red OS Murom, Python 3 (библиотеки cryptography, hashlib), OpenSSL.

Задания:

1. Сгенерировать 256-битный ключ AES и вектор инициализации (IV).
2. Зашифровать текстовый файл secret.txt алгоритмом AES-CBC.
3. Расшифровать полученный файл и сравнить с исходным.
4. Сгенерировать пару RSA-ключей (2048 бит).
5. Зашифровать короткое сообщение открытым ключом, расшифровать закрытым.
6. Вычислить SHA-256 хэш от исходного файла и записать в отчёт.

Порядок выполнения (Python + библиотека cryptography):

```
python
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.backends import default_backend
import os

key = os.urandom(32)
iv = os.urandom(16)
cipher = Cipher(algorithms.AES(key), modes.CBC(iv), backend=default_backend())
encryptor = cipher.encryptor()
with open('secret.txt', 'rb') as f:
    plain = f.read()
    pad_len = 16 - (len(plain) % 16)
    plain += bytes([pad_len]) * pad_len
    ct = encryptor.update(plain) + encryptor.finalize()
with open('secret.enc', 'wb') as f:
    f.write(ct)

# расшифрование
decryptor = cipher.decryptor()
dec = decryptor.update(ct) + decryptor.finalize()
# удалить дополнение
dec = dec[:-dec[-1]]
```

Отчёт:

Предоставить скриншоты кода, результаты шифрования/расшифрования, хэш-сумму, выводы.

№ 2

Тема: Создание и проверка цифровой подписи (GnuPG / OpenSSL)

Цель: Научиться генерировать ключевую пару GPG, подписывать файлы и проверять подпись.

Теоретические вопросы:

1. Что такое цифровая подпись? Отличие от шифрования.
2. Применение GPG и OpenSSL.
3. Понятие открытого и закрытого ключа.

Оборудование и ПО:

Red OS Murom, GnuPG (установлен по умолчанию), OpenSSL.

Задания:

1. Сгенерировать ключевую пару GPG (алгоритм RSA, 2048 бит).
2. Экспортировать публичный ключ в файл mypubkey.gpg.
3. Подписать текстовый файл document.txt своей подписью (создать отдельную подпись).
4. Проверить подпись с помощью публичного ключа.
5. Импортировать публичный ключ одногруппника и проверить его подпись на другом файле.

Порядок выполнения (команды в терминале):

```
bash
gpg --full-generate-key              # создать ключ
gpg --list-keys                      # посмотреть ключи
gpg --output mypubkey.gpg --export user@example.com
gpg --sign document.txt              # создаст document.txt.gpg
gpg --verify document.txt.gpg
gpg --import friend_key.gpg
gpg --verify friend_doc.gpg
```

Отчёт:

Привести команды, скриншоты ключей, результаты проверки подписи, выводы.

№ 3

Тема: Настройка правил брандмауэра (iptables/nftables)

Цель: Получить навыки фильтрации сетевого трафика, блокировки портов и IP-адресов.

Теоретические вопросы:

1. Принцип работы межсетевого экрана.
2. Цепочки INPUT, OUTPUT, FORWARD.
3. Типы правил (ACCEPT, DROP, REJECT).

Оборудование и ПО:

Red OS Murom (с правами sudo), виртуальная машина для тестирования (опционально).

Задания:

1. Просмотреть текущие правила (nft list ruleset или iptables -L).
2. Запретить все входящие соединения, кроме SSH (порт 22) с IP-адреса 192.168.1.100.
3. Разрешить все исходящие соединения.
4. Заблокировать доступ к порту 80 (HTTP) для всех.
5. Сохранить правила (iptables-save).

Порядок выполнения:

```
bash
sudo iptables -P INPUT DROP
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.1.100 -j ACCEPT
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A OUTPUT -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j DROP
sudo iptables-save > /etc/iptables/rules.v4
```

Проверка: telnet 192.168.1.100 80 – должно быть отказано; ssh с разрешённого IP – доступно.

Отчёт:

Скриншоты списка правил, результаты тестирования (nmap, telnet), выводы.

№ 4

Тема: Анализ безопасности Wi-Fi. Настройка защищённой точки доступа

Цель: Научиться оценивать уязвимости беспроводных сетей, настраивать WPA3.

Теоретические вопросы:

1. Уязвимости WEP, WPA2 (KRACK).
2. Протокол WPA3, 802.1X.
3. Инструменты: aircrack-ng, iw, nmcli.

Оборудование и ПО:

Ноутбук с Wi-Fi-адаптером, поддерживающим режим монитора (или учебный роутер), Red OS Murom.

Задания:

1. Сканировать доступные Wi-Fi сети командой iw dev wlan0 scan.
2. Определить тип шифрования своей домашней/учебной сети.
3. Настроить точку доступа (на роутере или на ПК с hostapd) с WPA3-Personal.
4. Подключиться к ней с другого устройства.
5. Проанализировать защищённость: попытаться захватить handshake (без реального взлома, только для отчёта).

Порядок выполнения (пример настройки hostapd):

bash

sudo apt install hostapd dnsmasq

sudo nano /etc/hostapd/hostapd.conf

Содержимое:

text

interface=wlan0

driver=nl80211

ssid=MySecureWiFi

hw_mode=g

channel=6

wpa=2

wpa_key_mgmt=SAE

wpa_passphrase=VeryStrongPassword123

rsn_pairwise=CCMP

Запуск: sudo hostapd /etc/hostapd/hostapd.conf

Отчёт:

Результаты сканирования (SSID, каналы, шифрование), конфигурационный файл hostapd, скриншоты подключения клиента, выводы.

№ 5

Тема: Установка и настройка VPN-сервера (OpenVPN). Анализ трафика в Wireshark

Цель: Научиться разворачивать VPN-сервер, подключать клиента, перехватывать и анализировать инкапсулированный трафик.

Теоретические вопросы:

1. Принцип работы VPN.
2. Протоколы OpenVPN, IPsec, WireGuard.
3. Использование Wireshark для анализа пакетов.

Оборудование и ПО:

Две виртуальные машины (сервер и клиент) с Red OS Murom, OpenVPN, Wireshark.

Задания:

1. Установить OpenVPN на сервер.
2. Сгенерировать сертификаты с помощью easy-rsa.
3. Настроить серверную конфигурацию (server.conf).
4. Настроить клиента (client.ovpn).
5. Подключить клиента к серверу.
6. Запустить Wireshark на интерфейсе tun0, выполнить ping между клиентом и сервером.
7. Проанализировать заголовки пакетов (отличие от обычного трафика).

Порядок выполнения (сокращённо):

bash
# на сервере
sudo dnf install openvpn easy-rsa
make-cadir ~/openvpn-ca
cd ~/openvpn-ca
./easyrsa init-pki
./easyrsa build-ca
./easyrsa gen-req server nopass
./easyrsa sign-req server server
# ... создать клиентские ключи
# скопировать keys в /etc/openvpn/server/
sudo systemctl start openvpn-server@server

На клиенте: импортировать client.ovpn, подключиться через sudo openvpn --config client.ovpn.

Отчёт:

Схема сети, команды генерации ключей, конфигурационные файлы, скриншоты Wireshark, выводы.

№ 6

Тема: Анализ уязвимостей веб-приложений (OWASP Top 10, SQL-инъекции, XSS) на стенде DVWA

Цель: Научиться выявлять и эксплуатировать SQL-инъекции и XSS на тестовом стенде, применять защиту.

Теоретические вопросы:

1. Что такое OWASP Top 10.
2. Принцип SQL-инъекции (union, time-based).
3. Типы XSS (хранимая, отражённая, DOM-based).
4. Методы защиты: подготовленные запросы, экранирование вывода.

Оборудование и ПО:

Docker, контейнер DVWA (Damn Vulnerable Web Application), браузер, Burp Suite или OWASP ZAP (по желанию).

Задания:

1. Запустить DVWA в контейнере Docker.
2. Установить уровень безопасности Low.
3. На странице SQL Injection (User ID) ввести ' OR '1'='1 – получить всех пользователей.
4. Выполнить union-запрос для получения данных из другой таблицы (например, ' UNION SELECT user,password FROM users --).
5. На странице XSS (Reflected) вставить скрипт <script>alert('XSS')</script>.
6. Переключить защиту на уровень High (или Impossible) и показать, что инъекции перестали работать.

Порядок выполнения:

bash
docker pull vulnerables/web-dvwa
docker run --rm -p 80:80 vulnerables/web-dvwa

Открыть http://localhost, логин admin / password.

Отчёт:

Скриншоты успешной SQL-инъекции и XSS, листинг защищённого кода (например, PDO с подготовленными запросами), выводы.

№ 7

Тема: Сканирование уязвимостей с помощью OWASP ZAP. Составление отчёта

Цель: Научиться пользоваться сканером безопасности веб-приложений OWASP ZAP, анализировать результаты и составлять отчёт.

Теоретические вопросы:

1. Принцип работы сканеров уязвимостей (активное/пассивное сканирование).
2. Основные функции OWASP ZAP (перехват прокси, spider, active scan).

3. Интерпретация отчёта (уровни риска: High, Medium, Low, Informational).

Оборудование и ПО:

OWASP ZAP (Java-версия), DVWA или другой тестовый стенд.

Задания:

1. Запустить OWASP ZAP, настроить прокси в браузере (localhost:8080).
2. Обойти spider-ом тестовое приложение DVWA.
3. Выполнить активное сканирование (Active Scan) выбранного URL.
4. Проанализировать найденные уязвимости (SQLi, XSS и др.).
5. Экспортировать отчёт в формате HTML.
6. В отчёте указать рекомендации по устранению критических уязвимостей.

Отчёт:

Приложить HTML-отчёт ZAP (или скриншоты его основных разделов), список уязвимостей с рисками, краткие рекомендации.

№ 8

Тема: Настройка резервного копирования (rsync, Windows Backup) и шифрование данных (GPG)

Цель: Научиться настраивать резервное копирование, шифровать файлы перед передачей, проверять восстановление.

Теоретические вопросы:

1. Стратегии резервного копирования (полное, инкрементное, дифференциальное).
2. Утилиты: rsync, tar, Windows Backup.
3. Шифрование данных в покое и при передаче (GPG, OpenSSL).

Оборудование и ПО:

Red OS Murom или Windows, GPG, rsync.

Задания:

1. Создать каталог ~/important_data с несколькими файлами.
2. Выполнить резервное копирование с помощью rsync -av на внешний диск или в другую директорию.
3. Зашифровать резервную копию (например, tar czf - important_data | gpg --symmetric --cipher-algo AES256 > backup.tar.gz.gpg).
4. Расшифровать и восстановить данные в другой каталог.
5. Написать простой bash-скрипт для автоматического резервного копирования с ротацией (хранить 5 последних копий).

Порядок выполнения:

bash

```
mkdir ~/backup
rsync -av ~/important_data/ ~/backup/
tar czf - important_data | gpg -c --cipher-algo AES256 > backup.tar.gz.gpg
gpg -d backup.tar.gz.gpg | tar xzf - -C ~/restore/
```

Скрипт backup.sh:

bash

```
#!/bin/bash
rsync -av ~/important_data/ /mnt/backup/$(date +%Y%m%d)/
find /mnt/backup/ -type d -mtime +5 -exec rm -rf {} \;
```

Отчёт:

Команды и их вывод, содержимое скрипта, проверка восстановления, выводы.

№ 9

Тема: Анализ логов безопасности (Windows Event Log, syslog). Выявление аномалий

Цель: Научиться анализировать системные журналы, выявлять признаки атак (брутфорс, несанкционированный доступ).

Теоретические вопросы:

1. Жизненный цикл инцидента ИБ.
2. Источники логов: Event Log (Windows), syslog (Linux), журналы брандмауэра.

3. Ключевые события: 4624 (успешный вход), 4625 (неудачный вход), 5156 (сетевое соединение).

Оборудование и ПО:

Лабораторный стенд с Windows/Linux, файлы логов (предоставлены преподавателем или сгенерированы).

Задания:

1. Сгенерировать события: 5 неудачных попыток входа с одного IP.
2. Используя wevtutil (Windows) или grep /var/log/auth.log (Linux), найти эти события.
3. Проанализировать предоставленный преподавателем лог-файл (содержит брутфорс, подозрительные соединения).
4. Выявить временные метки, IP-адреса атакующего, затронутые учётные записи.
5. Составить краткий отчёт об инциденте: время, тип атаки, рекомендации.

Отчёт:

Таблица с обнаруженными событиями, анализ частоты неудачных входов, вывод о наличии атаки, меры блокировки (fail2ban, брандмауэр).

№ 10

Тема: Разбор фишингового письма. Разработка памятки по противодействию социальной инженерии

Цель: Научиться распознавать признаки фишинга, разрабатывать рекомендации для сотрудников.

Теоретические вопросы:

1. Методы социальной инженерии: фишинг, претекстинг, кви-про-кво, вишинг.
2. Признаки фишингового письма (неправильный домен отправителя, орфографические ошибки, угроза срочности, подозрительные ссылки).
3. Правила цифровой гигиены.

Оборудование и ПО:

Образцы фишинговых писем (предоставлены преподавателем или найдены в открытых источниках, например, phishing.org).

Задания:

1. Получить от преподавателя 2–3 примера фишинговых писем (скриншоты или текст).
2. Провести анализ каждого письма по пунктам:
   - Адрес отправителя (проверить на подделку).
   - Тема письма, приветствие.
   - Наличие ссылок (проверить реальный домен, не сокращая).
   - Наличие вложений (опасные расширения .exe, .zip, .js).
   - Запрос личных данных или пароля.
3. Определить, является ли письмо фишинговым.
4. Написать памятку для сотрудников (5–7 пунктов) «Как распознать фишинг и не стать жертвой».
5. Придумать и описать сценарий атаки по телефону (вишинг) и способ защиты.

Отчёт:

Разбор каждого письма (таблица признаков), итоговое заключение, текст памятки, описание сценария фишинга.

Критерии оценивания:

- 5 баллов выставляется, если правильные ответы даны на 85-100% практических заданий

- 4 балла выставляется студенту, если правильные ответы даны на 65-84% практических заданий

- 3 балла выставляется студенту, если правильные ответы даны на 50-64% практических заданий

- 2 балла выставляется студенту, если правильные ответы даны на менее 50% практических заданий

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций состоит из текущего контроля.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации и учитываются при оценивании знаний, умений, навыков и (или) опыта деятельности.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

ОП. 06 Основы информационной безопасности

Методические указания для студентов по освоению дисциплины «Основы информационной безопасности» являются частью рабочей программы дисциплины (РПД) (приложением к рабочей программе).

РПД – рабочая программа, утвержденная директором колледжа для изучения дисциплины «Основы информационной безопасности». Она определяет цели и задачи дисциплины, формируемые в ходе ее изучения компетенции и их компоненты, содержание изучаемого материала, виды занятий и объем выделяемого учебного времени, а также порядок изучения и преподавания дисциплины «Основы информационной безопасности».

Для самостоятельной учебной работы студента важное значение имеют разделы «Структура и содержание дисциплины (модуля)» и «Учебно-методическое и информационное обеспечение дисциплины (модуля)». В первом указываются разделы и темы изучаемой дисциплины «Основы информационной безопасности», а также виды занятий и планируемый объем (в академических часах), во втором – рекомендуемая литература и перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Для подготовки к текущему контролю студенты могут воспользоваться оценочными средствами, представленными в Приложении 1 к рабочей программе дисциплины.

1. Описание последовательности действий студента

Приступая к изучению дисциплины «Основы информационной безопасности» необходимо в первую очередь ознакомиться с содержанием РПД, где в разделе «Структура и содержание дисциплины (модуля)» приведено общее распределение часов аудиторных занятий и самостоятельной работы по темам дисциплины «Основы информационной безопасности».

Залогом успешного освоения дисциплины «Основы информационной безопасности» является регулярное посещение занятий и выполнение предусмотренных программой заданий. Пропуск одного, а тем более нескольких занятий может осложнить освоение разделов курса.

Лекции имеют целью дать систематизированные основы научных знаний по содержанию дисциплины «Основы информационной безопасности». При изучении и проработке теоретического материала необходимо:

– повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

– при самостоятельном изучении теоретической темы подготовить конспект, используя рекомендованные в РПД литературные источники и электронные образовательные ресурсы.

Практические занятия проводятся с целью углубления и закрепления знаний, полученных на лекциях и в процессе самостоятельной работы с учебной литературой.

В процессе практического занятия, как вида учебных занятий, обучающиеся выполняют одно или несколько практических заданий под руководством преподавателя в соответствии с изучаемым содержанием учебного материала.

Выполнение обучающимся практических работ проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений;
- углубления теоретических знаний в соответствии с заданной темой;
- формирования умений применять теоретические знания при решении поставленных задач;
- развития профессиональных компетенций у обучающихся;
- развития творческой инициативы, самостоятельности, ответственности и организованности.

Выполнение обучающимися практических заданий направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

При подготовке к практическому занятию необходимо изучить или повторить лекционный материал по соответствующей теме.

2. Самостоятельная работа студента

Самостоятельная работа студента – самостоятельная учебная деятельность студента, организуемая колледжем и осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем.

Цели самостоятельной работы:

– систематизация и закрепление полученных теоретических знаний и практических умений студентов;

– углубление и расширение теоретических знаний;

– формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;

– развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

– формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

– воспитание самостоятельности, как личностного качества будущего специалиста.

Самостоятельная работа студента по дисциплине выполняется:

– самостоятельно вне расписания учебных занятий;

– с использованием современных образовательных технологий;

– работа со специальной литературой для подготовки к тестовым, практическим заданиям.

3. Рекомендации по работе с литературой и источниками

Работу с литературой следует начинать с анализа РПД, содержащей список основной и дополнительной литературы, а также знакомства с учебно-методическими разработками.

В случае возникновения затруднений в понимании учебного материала следует обратиться к другим источникам, где изложение может оказаться более доступным.

Работа с литературой не только полезна как средство более глубокого изучения дисциплины «Основы информационной безопасности», но и является неотъемлемой частью профессиональной деятельности будущего выпускника.