АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ СОЦИАЛЬНЫЙ ИНСТИТУТ»

Утверждаю
Декан факультета
_____Ж.В. Игнатенко
«15» сентября 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Профессия: 09.01.03 Оператор информационных систем и ресурсов

Квалификация: оператор информационных систем и ресурсов

Направленность: техническая обработка и размещение информационных ресурсов на сайте

Разработана
канд.пед. наук, доцент
_____О.А. Кудряшов

Согласована
зав. кафедрой ПИМ
_____Ж.В. Игнатенко

Рекомендована
на заседании кафедры ПИМ
от «15» сентября 2025г.
протокол № 2
Зав. кафедрой _____ Д.Г. Ловянников

Одобрена
на заседании учебно-методической
комиссии факультета
от «15» сентября 2025г.
протокол № 2
Председатель УМК _____
Ж.В. Игнатенко

Ставрополь, 2025 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель изучения дисциплины «Информационная безопасность» является получение теоретических знаний по основам информационной безопасности в сфере профессиональной деятельности обучаемых;

Задачами изучения дисциплины «Информационная безопасность» являются:

– умение анализировать, выделять составные части и описывать значимость решения задач по защите программного обеспечения компьютерных систем в своей профессиональной деятельности;

– умение анализировать риски и применять актуальные методы защиты программного обеспечения компьютерных систем в соответствии с нормативно-правовой документацией;

– умение оценивать результат и последствия своих действий по защите компьютерных систем программными и аппаратными средствами;

– умение грамотно излагать свои мысли при оформлении документов по защите компьютерных систем программными и аппаратными средствами;

– усвоение значимости решения задач по защите программного обеспечения компьютерных систем в своей профессиональной деятельности;

– усвоение основных актуальных средств и методов защиты компьютерных систем программными и аппаратными средствами в соответствии с нормативно-правовой документацией;

– усвоение современной научной и профессиональной терминологии и возможных траекторий профессионального развития и самообразования по вопросам защиты компьютерных систем программными и аппаратными средствами;

– усвоение правил оформления документов и построения устных сообщений по вопросам защиты компьютерных систем программными и аппаратными средствами;

– усвоение психологических основ деятельности коллектива и особенностей личности при решении задач защиты компьютерных систем программными и аппаратными средствами.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность» относится к общепрофессиональному циклу, входит в его вариативную часть и находится в логической и содержательно-методической связи с другими дисциплинами ОПОП.

Предшествующие дисциплины (курсы, модули, практики)	Последующие дисциплины (курсы, модули, практики)
Основы информационных технологий	Операционные системы, Цифровые технологии, Периферийные устройства

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций по данной специальности:

Код и наименование компетенции	Результаты обучения
ОК 1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.	**уметь:** применять средства ввода графической и текстовой информации
ОК 2 Использовать современные средства поиска, анализа и интерпретации информации, и информационные	**знать:** виды и назначения периферийных устройств, их устройство и принцип действия, интерфейсы

технологии для выполнения задач профессиональной деятельности.	подключения и правила эксплуатации; средства сканирования и распознавания текста
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках.	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 1.1 Выполнять ввод и обработку текстовых данных.	Выполнять ввод и обработку текстовых данных;
ПК 1.5 Выполнять подготовку цифровых данных для дальнейшей обработки и архивирования.	Выполнять подготовку цифровых данных для дальнейшей обработки и архивирования.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общий объем дисциплины составляет 60 часов.

Вид учебной работы	Всего часов	Семестр
		2(4)
Аудиторные занятия (работа обучающихся во взаимодействии с преподавателем) (всего)	**48**	**48**
в том числе:		
Лекции (Л)	28	28
Практические занятия (ПЗ)	18	18
Семинары (С)		
Лабораторные работы (ЛР)		
Консультация	2	2
Самостоятельная работа (всего) (СР)	**6**	**6**
в том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Контрольная работа		
Реферат		
Самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям)	6	6
Промежуточная аттестация	**6**	
Вид промежуточной аттестации	Экзамен	
Общий объем, час	**60**	**60**

5. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

5.1. Содержание дисциплины

№ раздела (темы)	Наименование раздела (темы)	Содержание раздела (темы)
1	Борьба с угрозами несанкционированного доступа к информации	Актуальность проблемы обеспечения безопасности информации. Виды мер обеспечения информационной безопасности (ИБ). Основные принципы построения систем защиты информации
2	Борьба с вирусным заражением	Проблемы вирусного заражения. Разновидности и структура современных компьютерных вирусов.

	информации	Угрозы для мобильных устройств Методы защиты от вредоносных программ. Средства защиты от вредоносных программ.
3	Организационно-правовое обеспечение информационной безопасности	Основы теории правового обеспечения информационной безопасности. Федеральная нормативная база обеспечения информационной безопасности. Защита персональных данных.

5.2. Структура дисциплины

№ раздела (темы)	Наименование раздела (темы)	Количество часов					
		Всего	Л	ПЗ	С	ЛР	СР
1.	Борьба с угрозами несанкционированного доступа к информации	16	8	6	-	-	2
2.	Борьба с вирусным заражением информации	18	10	6	-	-	2
3.	Организационно-правовое обеспечение информационной безопасности	18	10	6	-	-	2
	Консультация	2	--		-	-	-
	Промежуточная аттестация	6			-	-	
	Общий объем, час	60	28	18	0	0	6

5.3. Практические занятия и семинары

№ п/п	№ раздела (темы)	Вид (ПЗ, С)	Тема	Количество часов
1	1	ПЗ	Актуальность проблемы обеспечения безопасности информации	2
2	1	ПЗ	Виды мер обеспечения информационной безопасности (ИБ)	2
3	1	ПЗ	Основные принципы построения систем защиты информации	2
4	2	ПЗ	Проблемы вирусного заражения. Разновидности и структура современных компьютерных вирусов.	2
5	2	ПЗ	Угрозы для мобильных устройств	2
6	2	ПЗ	Методы защиты от вредоносных программ.	2
7	3	ПЗ	Проблемы вирусного заражения. Разновидности и структура современных компьютерных вирусов.	2
8	3	ПЗ	Угрозы для мобильных устройств	2
9	3	ПЗ	Методы защиты от вредоносных программ.	2

5.4. Лабораторные работы

не предусмотрены

5.5. Самостоятельное изучение разделов (тем) дисциплины

№ раздела (темы)	Вопросы, выносимые на самостоятельное изучение	Количество часов
1	Своевременная компьютерная профилактика.	2
2	Обязательное использование антивирусной защиты.	2
3	Физическое отключение внутренней сети организации от Интернета и использование для выхода в Интернет выделенных компьютеров.	2

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Основные технологии обучения:

– работа с информацией, в том числе с использованием ресурсов сети Интернет;

– подготовка и реализация проектов (мультимедийных презентаций и пр.) по заранее заданной теме;

– исследование конкретной темы и оформление результатов в виде доклада с презентацией;

– работа с текстами учебника, дополнительной литературой;

– выполнение индивидуальных заданий.

Информационные технологии:

– сбор, хранение, систематизация, обработка и представление учебной и научной информации;

– обработка различного рода информации с применением современных информационных технологий;

– самостоятельный поиск дополнительного учебного и научного материала, с использованием поисковых систем и сайтов сети Интернет, электронных энциклопедий и баз данных;

– использование электронной почты преподавателей и обучающихся для рассылки, переписки и обсуждения возникших учебных проблем.

– использование дистанционных образовательных технологий (при необходимости)

Используемые активные и интерактивные образовательные технологии

№ раздела (темы)	Вид занятия (Л, ПЗ, С, ЛР)	Используемые интерактивные и активные образовательные технологии	Количество часов
1	Л	Лекция-дискуссия.	10
2	ПЗ	Работа малыми группами	8
3	Л	Лекция-визуализация	10

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Типовые задания для текущего контроля.

Перечень типовых контрольных вопросов для устного опроса

1. Что такое конфиденциальность информации?
2. Какие существуют основные угрозы для информационной системы организации?

3. Чем отличается аутентификация от авторизации?
4. Какое значение имеет шифрование данных?
5. Что такое парольный аудит и зачем он нужен?
6. Перечислите известные типы вредоносного ПО и приведите примеры каждого типа.
7. Что такое фишинговая атака и как защититься от нее?
8. Опишите механизм атаки SQL-инъекции и способы предотвращения таких атак.
9. Что представляет собой кросс-сайт скриптинг (XSS)?
10. Объясните термин DDoS-атаки и предложите методы противодействия таким угрозам.
11. Назовите ключевые международные стандарты информационной безопасности (например ISO).
12. Зачем нужны политики и процедуры управления доступом?
13. Что включает в себя комплекс мер по защите персональных данных согласно российскому законодательству?
14. Почему важно регулярно обновлять программное обеспечение?
15. Какова роль аудитов информационной безопасности?
16. Что такое межсетевые экраны (firewall)? Какие виды сетевых экранов используются?
17. Для чего применяются VPN-технологии?
18. Расскажите принцип работы антивирусных решений и систем обнаружения вторжений (IDS).
19. Как работает двухфакторная аутентификация (2FA)?
20. Какие меры принимаются для защиты беспроводных сетей Wi-Fi?
21. Какие этапы входят в процесс анализа рисков информационной безопасности?
22. Приведите пример типичного инцидента в области кибербезопасности и расскажите, как правильно реагировать на него.
23. Что входит в понятие «резервное копирование» и почему оно критично для бизнеса?
24. Какие шаги предпринимаются при расследовании утечки данных?
25. Обсудите важность подготовки сотрудников и повышение осведомленности персонала в сфере информационной безопасности.

Типовые задания в тестовой форме

1. Какой метод позволяет защитить персональные данные путем преобразования исходной информации в зашифрованный вид?

A. Аутентификация
B. Шифрование
C. Авторизация
D. Архивирование

Правильный ответ: B. Шифрование

2. Фишинговые атаки представляют угрозу потому, что злоумышленники...

A. Получают физический доступ к компьютеру жертвы
B. Используют социальные сети для распространения спама
C. Отправляют поддельные письма, маскирующиеся под легитимные источники
D. Взламывают веб-сайты компаний

Правильный ответ: C. Отправляют поддельные письма, маскирующиеся под легитимные источники

3. Основной целью внедрения межсетевого экрана является защита сети от...

A. Внутренних пользователей, имеющих доступ к ресурсам сети
B. Внешних несанкционированных подключений и угроз
C. Физического повреждения оборудования
D. Неисправностей серверов
Правильный ответ: B. Внешних несанкционированных подключений и угроз
4. Процесс проверки подлинности субъекта называется...
A. Криптографией
B. Идентификацией
C. Аутентификацией
D. Авторизацией
Правильный ответ: C. Аутентификацией
5. Какая технология обеспечивает безопасный удаленный доступ к корпоративным ресурсам через публичные сети?
A. NAT
B. IDS
C. Firewall
D. VPN
Правильный ответ: D. VPN
6. Атака методом SQL-инъекции нацелена на...
A. Выполнение произвольного SQL-кода в базе данных
B. Преобразование файлов с использованием вируса
C. Утечку памяти приложения
D. Отказ в обслуживании сервера
Правильный ответ: A. Выполнение произвольного SQL-кода в базе данных
7. Двухфакторная аутентификация повышает безопасность, поскольку требует...
A. Использование исключительно сложных паролей
B. Вход по отпечаткам пальцев или сканированию лица
C. Двойное подтверждение адреса электронной почты
D. Второго уровня подтверждения помимо основного пароля
Правильный ответ: D. Второго уровня подтверждения помимо основного пароля
8. Один из ключевых принципов стандартов информационной безопасности ISO 27001 заключается в...
A. Обязательном внедрении криптографии везде
B. Разграничении ответственности и полномочий внутри организации
C. Запрете использования облачных сервисов
D. Постоянном мониторинге социальных сетей
Правильный ответ: B. Разграничении ответственности и полномочий внутри организации
9. Что означает аббревиатура «DDoS»?
A. Data Defense Operation System
B. Distributed Denial of Service
C. Dynamic Disk Operating System
D. Digital Document Overload Syndrome
Правильный ответ: B. Distributed Denial of Service
10. Метод хранения хешированных паролей помогает защитить систему от взлома, потому что...
A. Хэшированные пароли легко восстанавливаются
B. Даже зная пароль, нельзя восстановить оригинальный текст
C. Пароль хранится в открытом виде
D. Все пароли одинаковы для всех пользователей
Правильный ответ: B. Даже зная пароль, нельзя восстановить оригинальный текст
11. Основной способ борьбы с ботнетами — это...

A. Установка дополнительного программного обеспечения

B. Регулярное обновление операционных систем и приложений

C. Уничтожение зараженных компьютеров

D. Применение метода социального инжиниринга

Правильный ответ: B. Регулярное обновление операционных систем и приложений

12. Резервное копирование данных необходимо для...

A. Улучшения производительности системы

B. Создания дополнительной копии важных данных на случай потери оригинала

C. Повышения скорости передачи данных

D. Экономии места на жестком диске

Правильный ответ: B. Создания дополнительной копии важных данных на случай потери оригинала

13. Атаку XSS используют для...

A. Подмены DNS-записей сайта

B. Исполнения JavaScript-кода в браузере пользователя

C. Полностью блокировки работы сайта

D. Получения полного контроля над операционной системой

Правильный ответ: B. Исполнения JavaScript-кода в браузере пользователя

14. Основные принципы обработки персональных данных включают в себя...

A. Сбор минимального объема данных и ограничение сроков хранения

B. Открытый доступ ко всей личной информации

C. Возможность продажи персональных данных третьим лицам

D. Автоматическое удаление учетных записей через полгода неактивности

Правильный ответ: A. Сбор минимального объема данных и ограничение сроков хранения

15. По какой причине важна регулярная смена паролей?

A. Чтобы легче было запомнить новый пароль

B. Из-за возможных попыток подбора старых паролей

C. Потому что старые пароли теряют свою силу

D. Так принято по закону

Правильный ответ: B. Из-за возможных попыток подбора старых паролей

16. Типичным примером социальной инженерии является...

A. Нападение хакера на базу данных компании

B. Предложение помощи незнакомым людям, представляясь сотрудником службы поддержки

C. Покупка нелегальных копий программного обеспечения

D. Проверка наличия вирусов на компьютере

Правильный ответ: B. Предложение помощи незнакомым людям, представляясь сотрудником службы поддержки

17. Антивирусные программы помогают предотвратить...

A. Попытки изменения паролей пользователями

B. Воздействие вредоносного ПО на компьютер

C. Открытие защищённых документов

D. Выход из строя аппаратуры компьютера

Правильный ответ: B. Воздействие вредоносного ПО на компьютер

18. Целью стандарта PCI DSS является защита...

A. Платежных карт клиентов

B. Информационной инфраструктуры банков

C. Социальных сетей от взлома

D. Электронных почтовых сообщений

Правильный ответ: A. Платежных карт клиентов

19. Какую технологию используют для безопасной передачи трафика по открытым каналам связи?

A. SSH

B. FTP

C. HTTP

D. SMTP

Правильный ответ: A. SSH

20. Одно из преимуществ использования брандмауэра состоит в...

A. Контролировании входящего и исходящего трафика

B. Увеличении пропускной способности сети

C. Освобождении места на жёстких дисках

D. Скоростном доступе к файлам

Правильный ответ: A. Контролировании входящего и исходящего трафика

21. Если сотрудник получает письмо с просьбой срочно обновить платежные реквизиты клиента, первое, что он должен сделать, это...

A. Немедленно внести изменения

B. Обратиться к руководству или ответственному сотруднику для подтверждения операции

C. Просто удалить сообщение

D. Сохранить письмо в архиве

Правильный ответ: B. Обратиться к руководству или ответственному сотруднику для подтверждения операции

22. Пример серьезного нарушения конфиденциальности данных — это...

A. Пользователь забыл пароль к своей почте

B. Компания потеряла резервную копию своего сайта

C. В результате инсайдера произошла утечка клиентских баз данных

D. Компьютер завис из-за нехватки оперативной памяти

Правильный ответ: C. В результате инсайдера произошла утечка клиентских баз данных

23. Система обнаружения вторжений (IDS) предназначена для...

A. Определения действий нарушителей и предупреждения администраторов

B. Непосредственного устранения выявленных угроз

C. Ограничения прав доступа пользователей

D. Организация каналов передачи данных

Правильный ответ: A. Определения действий нарушителей и предупреждения администраторов

24. Термином «перехват сеанса» обозначается ситуация, когда злоумышленник...

A. Вводит неверный пароль многократно

B. Осуществляет прослушивание телефонных разговоров

C. Заблокировал работу корпоративного почтового сервиса

D. Захватывает контроль над активной сессией пользователя

Правильный ответ: D. Захватывает контроль над активной сессией пользователя

25. Методом, позволяющим ограничить круг лиц, имеющих доступ к данным, является...

A. Ротация ключей шифрования

B. Мониторинг активности пользователей

C. Принцип наименьших привилегий

D. Бэкап данных

Правильный ответ: C. Принцип наименьших привилегий

Типовые практические/ситуационные задачи

Задача №1: Утечка данных сотрудника

Вы работаете специалистом по информационной безопасности в крупной организации. Сотрудник случайно отправил конфиденциальные данные компании внешнему контрагенту по ошибочной ссылке в письме. Какие действия вам необходимо предпринять немедленно?

Варианты решения:

- Провести расследование и определить степень ущерба.
- Сообщить руководителю отдела и принять меры для восстановления ситуации.
- Изменить права доступа к документам и заблокировать аккаунт сотрудника временно.
- Проинформировать пострадавшего контрагента о случившейся ситуации и провести дополнительный инструктаж сотрудников.

Задача №2: Безопасность мобильных устройств

Руководство вашей компании планирует расширить использование корпоративных смартфонов среди сотрудников. Однако существует угроза кражи или компрометации данных на устройствах. Разработайте рекомендации по обеспечению безопасности мобильных устройств.

Возможные варианты рекомендаций:

- Настройка автоматического стирания данных при потере устройства.
- Требования к обязательной установке антивирусного ПО и регулярного обновления ОС.
- Блокировка возможности установки стороннего непроверенного ПО.
- Создание политики ограничений доступа к рабочим приложениям и сервисам с личного мобильного телефона.

Задача №3: Phishing-атака

Ваш коллега получил электронное письмо якобы от банка с предложением обновить личные данные. Письмо выглядит официально, но адрес отправителя вызывает сомнения. Ваши дальнейшие действия?

Рекомендуемые действия:

- Сообщить специалисту по информационной безопасности о подозрительном письме.
- Проверьте источник письма перед вводом любых данных.
- Никогда не переходите по сомнительным ссылкам.
- Обязательно используйте антифишинговую защиту на рабочих станциях.

Задача №4: Защита сети Wi-Fi

Компания открывает новое представительство и решает организовать точку доступа Wi-Fi для сотрудников и гостей офиса. Ваша задача обеспечить максимальную безопасность этой точки доступа.

Предлагаемые меры:

- Включить фильтрацию MAC-адресов.
- Применять современные протоколы шифрования WPA3/WPA2.
- Установить сложный уникальный ключ доступа и менять его периодически.
- Отделить гостевую сеть от внутренней корпоративной сети.

Задача №5: Backups and Recovery

Система мониторинга вашего предприятия зафиксировала отказ диска на одном из серверов, содержащего важные базы данных. Необходимо оперативно восстановить работоспособность системы. Составьте порядок действий по восстановлению данных.

План восстановления:

- Оценить состояние поврежденного диска и убедиться, что резервные копии являются полными и свежими.
- Остановить работу служб и приложений на проблемном сервере.
- Произвести восстановление из актуальной резервной копии.
- После успешного восстановления запустить проверку целостности данных.

Задача №6: Обнаружение аномалий в трафике

Мониторинг сети показывает резкое увеличение трафика, направленного на определенный внутренний ресурс. Возможно, система подверглась DoS/DDoS-атаке. Какие меры следует применить?

Действия специалиста:

- Ограничить доступ к атакуемому ресурсу извне.
- Выявить характер атаки и тип используемого инструмента.
- Приложить усилия для локализации и изоляции пораженной части сети.
- Активация заранее подготовленной стратегии реагирования на подобные события.

Задача №7: Анализ риска утечек данных

Организация проводит оценку рисков относительно возможного сценария утечки данных. Нужно составить сценарий оценки вероятности возникновения подобной проблемы и потенциального вреда бизнесу.

Ключевые факторы для оценки:

- Количество используемых точек входа в корпоративную сеть.
- Уровень зрелости системы контроля доступа и учета активности сотрудников.
- Наличие автоматизированных механизмов отслеживания поведения пользователей.
- Определение последствий возможной утечки данных для финансовой устойчивости компании.

Задача №8: Критерии выбора надежного поставщика услуг ИТ-инфраструктуры

При выборе внешнего подрядчика для предоставления услуг хостинга и управления инфраструктурой компания столкнулась с множеством предложений. Подготовьте критерии для оценки надежности потенциальных поставщиков.

Важные критерии:

- Надежность и репутация провайдера.
- Гарантированное качество обслуживания (SLA).
- Доступность технической поддержки и реакция на инцидентные случаи.
- Опыт реализации аналогичных проектов.

Задача №9: Инцидентный мониторинг

Внутренняя проверка показала, что ряд сотрудников активно использовал флеш-накопители без согласования с отделом безопасности. Как решить проблему и минимизировать риски утраты данных?

Мероприятия:

- Проведение внутреннего расследования с установлением виновников нарушений.
- Интеграция системы контроля USB-портов на рабочие станции.
- Организация тренингов и разъяснительных мероприятий для повышения осведомлённости сотрудников.

Задача №10: Тестирование на проникновение

Для проверки эффективности принятых мер безопасности планируется проведение теста на проникновение («penetration testing»). Как грамотно подготовить компанию к этому процессу?

Этапы подготовки:

- Согласовать условия тестирования с руководством компании.
- Предоставить специалистам тестируемый периметр и согласованные правила игры.
- Заранее уведомить персонал компании о проведении мероприятия.
- Следить за результатами и проводить детальное изучение найденных уязвимостей.

Каждая из перечисленных ситуаций позволит углубиться в практику информационной безопасности и научиться эффективно справляться с возникающими проблемами.

7.2. Типовые задания для промежуточной аттестации (экзамен)

Контрольные вопросы к экзамену

1. Что такое конфиденциальность информации и какие существуют уровни её классификации?
2. Какие цели преследует информационная безопасность? Перечислите три основных аспекта (конфиденциальность, целостность, доступность).
3. Дайте определение понятия «информационные активы».
4. Перечислите наиболее распространённые угрозы информационной безопасности организаций.
5. Назовите пять основных типов вредоносного ПО и опишите каждый из них.
6. Опишите разницу между аутентификацией и авторизацией.
7. Какой стандарт международного уровня регламентирует создание системы менеджмента информационной безопасности?
8. Объясните суть концепции «нулевого доверия» ("Zero Trust") в информационной безопасности.
9. Почему необходимы регулярные обновления программного обеспечения и операционных систем?
1. Охарактеризуйте основной смысл модели CIA (Confidentiality, Integrity, Availability) в информационной безопасности.
2. Расшифруйте термин DDoS-атака и поясните, каким образом такая атака влияет на инфраструктуру компании.
3. Предложите последовательность шагов по предотвращению и устранению последствий фишингового мошенничества.
4. Обоснуйте необходимость применения многоуровневой системы защиты (defense in depth) в современных организациях.
5. Как реализуется политика разграничения доступа (RBAC) и какие преимущества она даёт предприятию?
6. Определите стратегию реагирования на инцидент информационной безопасности и перечислите основные этапы плана ликвидации последствий.
7. Проведите сравнительный анализ симметричного и асимметричного методов шифрования, выделяя достоинства и недостатки обоих подходов.
8. Поясните, как устроены механизмы идентификации и аутентификации пользователей в системах Active Directory и LDAP.
9. Оцените влияние человеческого фактора на уровень информационной безопасности организации и предложите пути снижения рисков.
10. Используя концепцию Threat Modeling, оцените возможные угрозы для небольшого онлайн-магазина и разработайте защитные меры.
11. Докажите целесообразность резервного копирования и укажите лучшие практики для разработки эффективной стратегии backup'ов.
12. Изложите причины появления угрозы Insider Threats (внутренней угрозы) и назовите эффективные инструменты и подходы для её выявления и нейтрализации.
13. Подробно раскройте содержание понятия «регуляторные требования в области информационной безопасности» применительно к российским компаниям. Приведите конкретные законодательные нормы.
14. Представьте ситуацию: крупный международный ритейлер столкнулся с массированной атакой хакерской группы. Какие первые шаги должна предпринять служба информационной безопасности для смягчения последствий и начала разбирательства?
15. Рассмотрите особенности моделей информационной безопасности в государственных структурах и коммерческих компаниях. Выделите сходства и различия.
16. Разработайте план обеспечения непрерывности бизнес-процессов (Business Continuity Plan, BCP) для небольшой компании с учётом возможных сбоев в работе информационно-коммуникационной инфраструктуры.

Практические задачи к экзамену

Используя инструмент nmap, проведите разведку IP-диапазона и определите доступные сервисы и порты целевого хоста.

1. Скачайте образец вредоносного файла и проанализируйте его поведение с помощью утилиты VirusTotal.
2. Спланируйте простую атаку методом перебора паролей (brute force) против заданного ресурса (без реального воздействия на реальную цель).
3. Проверьте настройки безопасности локальной сети Windows Server и устраните обнаруженные слабые стороны.
4. Используйте встроенную команду Linux chattr для назначения атрибутов файла, обеспечивающих повышенную защиту от модификации.
6. Постройте топологию виртуальной среды (используя VMware Workstation или VirtualBox) с одним сервером и двумя клиентами, настроив политику межсетевого экранирования с помощью iptables.
7. Создайте SELinux-политику для ограничения доступа процесса Apache httpd к определенным каталогам.
8. Организуйте многослойную защиту веб-приложения с применением Web Application Firewall (WAF) и фильтрации на уровне базы данных.
9. Реализуйте полноценную схему шифрования и дешифровки данных средствами OpenSSL или аналогичной библиотеки.
10. Рассчитайте показатели эффективности текущего состояния защиты организации, используя формулу оценки рисков VaR (Value at Risk).
11. Найдите и исправьте уязвимость Cross-Site Scripting (XSS) в PHP-приложении, разместив фиксацию непосредственно в коде.
12. Продемонстрируйте процедуру восстановления работоспособности системы из резервной копии, используя средство rsync и tar.
13. Сделайте анализ уязвимостей открытого порта на сервисе MySQL, используя Nessus или OpenVAS.
14. Реализуйте настройку двухфакторной аутентификации (2FA) на примере популярного веб-приложения Google Apps.
15. Разработайте руководство по обработке инцидентов информационной безопасности для конкретной роли сотрудника (например, администратора сети).
16. Проведите тестирование на проникновение (Penetration Testing) корпоративного веб-ресурса, включая исследование слабых мест в аутентификации и контроле доступа.
17. Сформируйте развернутую рекомендацию по выбору эффективного межсетевого экрана (Firewall) для крупного коммерческого банка с распределённой структурой филиалов.
18. Моделируйте атаку на инфраструктуру компании, имитируя внедрение Advanced Persistent Threat (APT)-группы, и сформулируйте адекватные контрмеры.
19. Проведите глубокий анализ архитектурных особенностей механизма Kerberos и создайте сценарии отказа в предоставлении билетов Kerberos.
20. Представьте отчет о готовности компании к выполнению требований Федерального закона №152-ФЗ («О персональных данных») с указанием текущих недостатков и путей улучшения.
21. Сформулируйте программу развития центра компетенций по вопросам информационной безопасности на ближайшие два-три года для среднего российского предприятия.
22. Нарисуйте структуру корпоративной системы информбезопасности и подробно объясните взаимосвязь элементов структуры друг с другом.
23. Разработайте сценарий построения комплексной системы мониторинга и реагирования на инциденты информационной безопасности (SIEM/SOC).

24. Изучите алгоритмы шифрования RSA и AES, напишите небольшую программу на Python для демонстрации шифрования и расшифровки текста.

25. Смоделируйте эксплуатацию уязвимости класса XXE (XML External Entity Attack) в популярном XML-парсере и продемонстрируйте последствия успешной эксплуатации.

Типовые задания в тестовой форме для проведения зачета

1. **Основной задачей информационной безопасности является:**
   - a) Поддержание доступности, целостности и конфиденциальности информации.
   - b) Исключение любого доступа к данным.
   - c) Максимальная прозрачность процессов обработки данных.
   - d) Отсутствие затрат на поддержание информационной безопасности.
2. **Аутентификация – это процедура установления:**
   - a) Прав пользователя на выполнение операций.
   - b) Источника и действительности передаваемых данных.
   - c) Соответствия предъявляемого ключа ожидаемому значению.
   - d) Целостности информации.
3. **Метод шифрования, при котором используется одна пара ключей (открытый и закрытый), называется:**
   - a) Симметричным.
   - b) Асимметричным.
   - c) Алгоритмом хеширования.
   - d) Протоколом SSL/TLS.
4. **Атака «отказ в обслуживании» (Denial-of-service, DoS) направлена на нарушение какого свойства информационной безопасности?**
   - a) Конфиденциальности.
   - b) Ценности информации.
   - c) Доступности.
   - d) Корректности.
5. **Фишинговая атака осуществляется путём:**
   - a) Скрытого подключения к компьютерной сети.
   - b) Обмана пользователя с целью получения его конфиденциальных данных.
   - c) Повреждения аппаратного обеспечения.
   - d) Пересылки огромного количества запросов к серверу.
6. **Какой стандарт описывает международную модель менеджмента информационной безопасности?**
   - a) ГОСТ Р 50922-2006.
   - b) ISO/IEC 27001.
   - c) FISMA.
   - d) GDPR.
7. **Наиболее эффективна для защиты корпоративной сети от проникновения внешний злоумышленник технология:**
   - a) Антивирус.
   - b) Межсетевой экран (FireWall).
   - c) Анти-спам фильтр.
   - d) Брандмауэр уровня приложений.
8. **Безопасность вычислительной сети чаще всего обеспечивается с помощью протокола:**
   - a) HTTP.
   - b) POP3.
   - c) FTP.
   - d) IPSec.
9. **Принцип разделения обязанностей подразумевает, что:**

- a) Ответственность за выполнение каждой задачи распределяется между разными сотрудниками.
- b) Вся ответственность возлагается на одного конкретного сотрудника.
- c) Каждому сотруднику выдаётся полный доступ ко всем ресурсам.
- d) Сотрудники работают коллективно без четкого распределения задач.

10. **Термин «логический мост» в контексте информационной безопасности означает:**
- a) Физическое соединение сегментов сети.
- b) Аппаратное устройство для защиты сети.
- c) Способ обхода защитных барьеров (VPN, Firewall).
- d) Технологию защиты web-серверов.

11. **Самый эффективный способ повысить устойчивость пароля к подбору – это:**
- a) Сделать пароль длинным и сложным.
- b) Использовать только цифры.
- c) Хранить пароль на бумажном носителе.
- d) Менять пароль каждые две недели.

12. **Под двойственным контролем понимается требование, что:**
- a) Любое действие должно выполняться двумя лицами одновременно.
- b) Информация делится на отдельные блоки и доступна двум разным сотрудникам.
- c) Только один человек обладает всеми полномочиями.
- d) Каждый сотрудник контролирует другого.

13. **Какая мера необходима для обеспечения высокого уровня защиты информации?**
- a) Еженедельная смена паролей.
- b) Строгий контроль физического доступа к помещениям.
- c) Периодическое обучение сотрудников правилам информационной безопасности.
- d) Всё вышеперечисленное верно.

14. **При создании политики безопасности организации рекомендуется учитывать:**
- a) Особенности отраслевой специфики и законодательство.
- b) Стоимость покупки самого дорогого антивирусного продукта.
- c) Желания сотрудников.
- d) Локальные законы региона.

15. **Самая частая причина утечек информации связана с фактором:**
- a) Недостаточным уровнем физической охраны помещений.
- b) Низким качеством закупаемого оборудования.
- c) Ненадлежащим поведением сотрудников.
- d) Некорректной работой систем видеонаблюдения.

16. **Задача обеспечения защиты информации решается на уровне:**
- a) Законодательства государства.
- b) Руководящих органов предприятий.
- c) Индивидуально каждым сотрудником.
- d) Всех указанных уровней.

17. **Что является обязательным условием применения сертификата соответствия требованиям информационной безопасности?**
- a) Закупка лицензированного программного обеспечения.
- b) Оформление договора страхования.
- c) Наличие аттестата аккредитации органа сертификации.
- d) Совместимость оборудования с отечественными системами защиты.

18. **Какой метод применяется для исключения повторного использования одноразовых токенов?**
- a) Логический контроль времени истечения срока действия токена.
- b) Использование симметричной схемы шифрования.
- c) Однократная регистрация уникальных серийных номеров.
- d) Проверка по чёрному списку.

19. **Основной элемент политики управления доступом – это:**
- a) Каталогизация объектов доступа.
- b) Распределение ролей и прав доступа.
- c) Ограничение доступа по расписанию.
- d) Ежедневный отчёт по активностям пользователей.

20. **Одним из видов внутренних угроз информационной безопасности является:**
- a) Неблагонадежность партнёров.
- b) Невнимательность сотрудников.
- c) Несанкционированный доступ третьих лиц.
- d) Элементы внешней дестабилизации.

Критерии оценки промежуточной аттестации (экзамен)

Оценка	**Характеристики ответа студента**
«отлично»	Оценка «отлично» выставляется, если студент уверенно, логично, последовательно и грамотно излагает программный материал, опираясь на знания основной и дополнительной литературы, успешно ответил на вопросы преподавателя во время беседы на темы, связанные с изучаемой дисциплиной, верно ответил на 90% вопросов теста, правильно решил практическую задачу. В случае вариативности решения задачи обосновал все возможные варианты решения.
«хорошо»	Оценка «хорошо» выставляется, если студент уверенно, логично, последовательно и грамотно излагает программный материал, допускает незначительные неточности, успешно ответил на вопросы преподавателя во время беседы на темы, связанные с изучаемой дисциплиной, верно ответил 75% вопросов теста, правильно решил практическую задачу.
«удовлетворительно»	Оценка «удовлетворительно» выставляется, если студент неуверенно излагает программный материал, допускает неточности, успешно ответил на 50 % вопросов преподавателя во время беседы на темы, связанные с изучаемой дисциплиной, верно ответил 50% вопросов теста, решил практическую задачу с незначительными неточностями
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется, если студент не усвоил значительной части программного материала; допускает существенные ошибки и неточности при ответе на вопросы преподавателя, успешно ответил менее 50 % вопросов теста, не решил практическую задачу

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2025. – 107 с. – (Высшее образование). – ISBN 978-5-534-16388-9. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/567915

2. Казарин, О. В. Информационная безопасность: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. – 2-е изд. – Москва : Издательство Юрайт, 2025. – 352 с. – (Профессиональное образование). – ISBN 978-5-534-19384-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/580668

3. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2025. – 357 с. – (Высшее образование). – ISBN 978-5-534-19108-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/560516

4. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2025. – 277 с. – (Высшее образование). – ISBN 978-5-534-16450-3. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/567672

8.2. Дополнительная литература

1. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. – Москва : Издательство Юрайт, 2025. – 157 с. – (Высшее образование). – ISBN 978-5-534-17866-1. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/581502

2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. – Москва : Издательство Юрайт, 2024. – 111 с. – (Высшее образование). – ISBN 978-5-534-12769-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/543351

3. Внуков, А. А. Информационная безопасность: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 161 с. – (Профессиональное образование). – ISBN 978-5-534-13948-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/542340

4. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2025. – 252 с. – (Профессиональное образование). – ISBN 978-5-534-20154-3. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/567521

Периодические издания

1. Прикладная информатика : научно-информационный журнал / Издательство университет «Синергия». – 2006. – Москва, 2006-2025. – ISSN 1993-8314. - Текст : электронный. - URL: http://www.iprbookshop.ru/11770.html

2. Программные продукты и системы / Издательство : Научно-исследовательский институт «Центрпрограммсистем». - 1988. - Тверь, 2010-2025. - ISSN 0236-235X. - Текст : электронный. - URL: https://www.iprbookshop.ru/25852.html

8.3. Программное обеспечение

MicrosoftWindows,
Microsoft Office Professional Plus 2019
Консультант-Плюс

Google Chrome

8.4. Базы данных, информационно-справочные и поисковые системы, Интернет-ресурсы

Базы данных (профессиональные базы данных)
– База данных IT специалиста– Режим доступа: http://info-comp.ru/
Информационно-справочные системы
– Справочно-правовая система «КонсультантПлюс» –http://www.consultant.ru/
Поисковые системы
– Поисковая система Яндекс - https://www.yandex.ru
Электронные образовательные ресурсы
– Цифровой образовательный ресурс IPRsmart –https://www.iprbookshop.ru/
– Образовательная платформа Юрайт - https://urait.ru/
– Электронно-библиотечная система Znanium - https://znanium.com/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины требуется следующее материально-техническое обеспечение:

- для проведения лекций - учебная аудитория, оснащенная оборудованием и техническими средствами обучения: специализированная учебная мебель: жалюзи, экран, проектор, колонки, МФУ; компьютерная техника, объединенная в локальную сеть, с возможностью подключения к информационно-телекоммуникационной сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Института, лицензионное и свободно распространяемое программное обеспечение; расходные материалы;

- для проведения практических занятий - учебная аудитория, оснащенная оборудованием и техническими средствами обучения: специализированная учебная мебель: жалюзи, экран, проектор, колонки, МФУ; компьютерная техника, объединенная в локальную сеть, с возможностью подключения к информационно-телекоммуникационной сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Института, лицензионное и свободно распространяемое программное обеспечение; расходные материалы;

для организации самостоятельной работы – помещение для самостоятельной работы, оснащенное оборудованием и техническими средствами: специализированная учебная мебель, экран, проектор, доска учебная демонстрационная, компьютерная техника, объединенная в локальную сеть, с возможностью подключения к информационно-телекоммуникационной сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Института.

для текущего контроля и промежуточной аттестации - учебная аудитория, оснащенная оборудованием и техническими средствами обучения: специализированная учебная мебель: жалюзи, экран, проектор, колонки, МФУ; компьютерная техника, объединенная в локальную сеть, с возможностью подключения к информационно-телекоммуникационной сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Института, лицензионное и свободно распространяемое программное обеспечение; расходные материалы.

10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ЛИЦАМИ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (тьютора), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

– присутствие тьютора, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

– письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,

– специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),

– индивидуальное равномерное освещение не менее 300 люкс,

– при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

– присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

– обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;

– обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются тьютору;

– по желанию обучающегося задания могут выполняться в устной форме.

Программа составлена в соответствии с требованиями ФГОС СПО по профессии 09.01.03 Оператор информационных систем и ресурсов