Приложение
к ОПОП СПО 09.02.11 Разработка и управление программным обеспечением

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН «ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ Р.Н. АШУРАЛИЕВА»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

учебной дисциплины ОП.05 Основы информационной безопасности

Специальность: 09.02.11 Разработка и управление программным обеспечением

Квалификация программист

Махачкала, 2026г.

ОДОБРЕНО

предметной (цикловой) комиссией УГС 09.00.00. Информатика и вычислительная техника и 10.00.00 Информационная безопасность

Председатель П(Ц)К

 Ш.М. Мусаева

Протокол № 8 от 30 апреля 2026 г.

Фонд оценочных средств учебной дисциплины ОП.05 Основы информационной безопасности разработан на основе требований:

- Приказа Минпросвещения России от 24.02.2025 N 138 "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением" (Зарегистрировано в Минюсте России 31.03.2025 N 81696);
- Рабочей программы учебной дисциплины ОП.05 Основы информационной безопасности;

с учетом:

- Примерной образовательной программы «Профессионалитет» по специальности 09.02.11 Разработка и управление программным обеспечением, утвержденная протоколом ФУМО в системе СПО по УГПС 09.00.00 Информатика и вычислительная техника от 29.08.2025 № 6/2025, зарегистрирована в государственном реестре примерных образовательных программ – регистрационный номер 18/2025. Реквизиты утверждающего документа –приказ ФГБОУ ДПО ИРПО № 01-09-581/2025 от 13.10.2025;

Разработчик:

- Азизова Лилия Насруллаховна, к.п.н., преподаватель ГБПОУ РД «Технический колледж имени Р.Н. Ашуралиева»

© Азизова Лилия Насруллаховна 2026

© ГБПОУ РД «Технический колледж имени Р.Н. Ашуралиева» 2026

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ 4
2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ учебной дисциплины 4
3. ФОРМЫ И МЕТОДЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ....5
4. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНОЙ ДИСЦИПЛИНЫ....7
5. ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ....10
5.1. Типовые задания для оценки знаний и умений 10
5.2. Критерии оценивания....41
5.2.1. Критерии оценивания устного ответа 41
5.2.2. Критерии оценивания выполнения заданий на лабораторных занятиях 42
5.2.3. Критерии оценивания тестовых заданий....42
5.2.4. Общая классификация ошибок....42
6. ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО УЧЕБНОЙ ДИСЦИПЛИНе 43
6.1. Вопросы к экзамену по учебной дисциплине 43
6.2. Критерии оценивания ответов на экзамене....45
7. учебно-методическое обеспечение....45

1. ОБЩИЕ ПОЛОЖЕНИЯ

Фонд оценочных средств (далее – ФОС) учебной дисциплины ОП.05 Основы информационной безопасности является частью программы подготовки специалистов среднего звена специальности 09.02.11 Разработка и управление программным обеспечением.

ФОС позволяет оценить достижение, запланированных по учебной дисциплине, результатов обучения.

ФОС включают оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации по учебной дисциплине.

Текущий контроль успеваемости осуществляется с целью регулярного наблюдения за ходом поэтапного освоения обучающимися учебной дисциплине, оптимизации управления образовательной деятельностью обучающихся, своевременной корректировки персональных образовательных результатов, обучающихся педагогическими средствами.

Текущему контролю успеваемости подлежат все обучающиеся, осваивающие учебную дисциплину.

Текущий контроль проводится в пределах учебного времени, отведенного на изучение учебной дисциплины традиционными и инновационными методами с использованием современных технологий.

Результаты текущего контроля успеваемости обучающихся в виде оценки в балльном выражении («5», «4», «3», «2») записываются в журнале учебных занятий.

Текущий контроль освоения обучающимися программного материала учебной дисциплины может иметь следующие виды: оперативный и рубежный контроль.

Оперативный контроль проводится с целью объективной оценки качества освоения программы учебной дисциплины, а также стимулирования учебной работы обучающихся, мониторинга результатов образовательной деятельности, подготовки к промежуточной аттестации и обеспечения максимальной эффективности учебно-воспитательного процесса.

Рубежный контроль является контрольной точкой и проводится с целью комплексной оценки уровня освоения программного материала.

Промежуточная аттестация по учебной дисциплине проводится с целью оценки уровня освоения теоретических знаний, умений, приобретенного практического опыта.

Формы и периодичность промежуточной аттестации по учебной дисциплине определяются учебным планом образовательной программы: экзамен в 3 семестре.

Экзамен проводится непосредственно после завершения освоения учебной дисциплины, в сроки, установленные календарным учебным графиком. Экзамен проводится в день, освобожденный от других форм учебной нагрузки.

Экзаменационные вопросы и задания составляются на основе рабочей программы учебной дисциплины. Экзаменационные вопросы и задания должны соответствовать проверяемым результатам обучения и доводятся до сведения обучающихся в течение первых двух месяцев от начала обучения.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Учебная дисциплина «ОП.05 Основы информационной безопасности» принадлежит общепрофессиональному циклу ОП.00. обязательной части ФГОС специальности 09.02.11 Разработка и управление программным обеспечением.

Освоение учебной дисциплины должно способствовать формированию общих компетенций:

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

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

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

В результате освоения учебной дисциплины обучающийся должен **уметь:**

Код умения	**Название умения**
У1	Классифицировать защищаемую информацию по видам тайны и степеням секретности
У2	Классифицировать основные угрозы безопасности информации

В результате освоения учебной дисциплины обучающийся должен **знать:**

Код знания	**Название знания**
З1	Сущность и понятие информационной безопасности, характеристику ее составляющих
З2	Место информационной безопасности в системе национальной безопасности страны
З3	Виды, источники и носители защищаемой информации
З4	Источники угроз безопасности информации и меры по их предотвращению
З5	Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах
З6	Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи
З7	Современные средства и способы обеспечения информационной безопасности
З8	Основные методики анализа угроз и рисков информационной безопасности

3. ФОРМЫ И МЕТОДЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ

Формы текущего контроля по учебной дисциплине:

– устный опрос (фронтальный, индивидуальный, комбинированный);

– тестирование (письменное или компьютерное);

– письменная проверка (ответы на вопросы, решение задач и примеров, составление тезисов, рефератов, выполнение схем, выполнение заданий для самостоятельной работы и др.);

– практическая проверка (при проведении лабораторных занятий);

– самоконтроль и взаимопроверка.

Возможны и другие формы текущего контроля успеваемости, в том числе инновационные на основе информационно-коммуникационных технологий.

Преподаватель на одном учебном занятии может использовать одну или несколько форм текущего контроля.

Результаты обучения	**Критерии оценки**	**Формы и методы оценки**
Перечень знаний, осваиваемых в рамках учебной дисциплины:	Оценка **«отлично»** - теоретическое содержание курса	

- Сущность и понятие информационной безопасности, характеристику ее составляющих. - Место информационной безопасности в системе национальной безопасности страны. - Виды, источники и носители защищаемой информации. - Источники угроз безопасности информации и меры по их предотвращению. - Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах. - Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи. - Современные средства и способы обеспечения информационной безопасности. – Основные методики анализа угроз и рисков информационной безопасности.	освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. Оценка **«хорошо»** - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. Оценка **«удовлетворительно»** - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. Оценка **«неудовлетворительно»** - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	– Экзамен в форме собеседования. – Устный опрос. – Тестирование. – Защита отчетов по лабораторным занятиям. – Интерпретация результатов наблюдений за деятельностью обучающегося.
Перечень умений, осваиваемых в рамках учебной дисциплины: - Классифицировать защищаемую информацию по видам тайны и степеням секретности. - Классифицировать основные угрозы безопасности информации.		

4. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 Основы информационной безопасности

№	Наименование темы	Результаты обучения (освоенныеумения и знаний)	ПК, ОК	Текущий контроль успеваемости	Промежуточная аттестация
1	2	3	4	5	6
	ОП.09 Основы информационной безопасности				
	Тема 1.1. Теоретические основы информационной безопасности				
1.	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем	З1, З2, З3	ОК 01, ОК 02, ОК 09	Устный опрос, тестирование	Экзамен
2.	Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности	З4, З8		Устный опрос, тестирование	
	Тема 1.2. Основы защиты информации				
3.	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации	З1, З3	ОК 01, ОК 02, ОК 09	Устный опрос, тестирование	
4.	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи	З6		Устный опрос, тестирование	
5.	Цели и задачи защиты информации. Основные понятия в области защиты информации	З1, З5		Устный опрос, тестирование	
6.	Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности	З8, З4		Устный опрос, тестирование	
7.	Определение объектов защиты на типовом объекте информатизации	У1, У2		Отчет по лабораторному занятию	
8.	Классификация защищаемой информации по видам тайны и степеням конфиденциальности	У1, У2		Отчет по лабораторному занятию	
	Тема 1.3. Угрозы безопасности защищаемой информации				
9.	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к уязвимости информации. Методы оценки уязвимости информации	З4, З5, З8	ОК 01, ОК 02, ОК 09	Устный опрос, тестирование	
10.	Определение угроз объекта информатизации и их классификация	У1, У2		Отчет по лабораторному занятию	
	Раздел 2. Методология защиты информации				
	Тема 2.1. Методологические подходы к защите информации				
11.	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка	З4, З5, З8	ОК 01, ОК 02, ОК 09	Устный опрос, тестирование	

	факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации				
	Тема 2.2. Нормативно правовое регулирование защиты информации				
12.	Организационная структура системы защиты информации Законодательные акты в области защиты информации.	З1, З2		Устный опрос, тестирование	
13.	Российские и международные стандарты, определяющие требования к защите информации.	З7, З8		Устный опрос, тестирование	
14.	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации	З7, З8		Устный опрос, тестирование	
15.	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	У1, У2		Отчет по лабораторному занятию	
	Тема 2.3. Защита информации в автоматизированных (информационных) системах				
16.	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	З4, З5, З7		Устный опрос, тестирование	
17.	Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации	З5, З7		Устный опрос, тестирование	
18.	Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	З1, З4, З7		Устный опрос, тестирование	
19.	Выбор мер защиты информации для автоматизированного рабочего места	У1, У2		Отчет по лабораторному занятию	
20.	Тестирование на проникновение и анализ уязвимостей	У1, У2		Отчет по лабораторному занятию	
21.	Выполнение резервного копирования и восстановления данных. Управление доступом к данным	У1, У2		Отчет по лабораторному занятию	
	Самостоятельная работа обучающихся:				
22.	Изучить теоретический материал и составить тезисы (краткий конспект) по следующим темам:				
23.	Основы криптографии: симметричные и асимметричные алгоритмы.	З7		Конспект, устный опрос	
24.	Хэширование и цифровые подписи.	З7		Конспект, устный опрос	
25.	Применение криптографии в приложениях. Стеганография.	З7			
26.	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.)	З4, З7		Конспект, устный опрос	
27.	Использование VPN и межсетевых экранов.	З7		Конспект, устный опрос	
28.	Уязвимости веб-приложений (OWASP Top Ten).	З4, З5, З8			
29.	Шифрование данных в покое и в транзите.	З7		Конспект, устный опрос	

30.	Резервное копирование и восстановление данных. Управление доступом к данным.	37		Конспект, устный опрос	
31.	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	37, 38		Конспект, устный опрос	

5. ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ
ОП.05 Основы информационной безопасности

5.1. Типовые задания для оценки знаний и умений

Раздел 1. Теоретические основы информационной безопасности

Тема 1.1. Основные понятия и задачи информационной безопасности

1. Задание для устного опроса по темам

1. Дайте определения понятиям «информация», «сообщение» и «информационный процесс» в контексте информационной безопасности. Какие объекты (информация, системы, каналы связи, люди) подлежат защите? Перечислите основные категории защищаемых объектов и систем.
2. Что понимается под «угрозой информации»? Опишите классификацию угроз по источникам возникновения (природные, техногенные, антропогенные), по виду воздействия (нарушение конфиденциальности, целостности, доступности) и по степени преднамеренности. Приведите по одному примеру для каждого типа.
3. Раскройте понятие «риска информационной безопасности». Из каких компонентов складывается риск (вероятность реализации угрозы, уязвимости, величина возможного ущерба)? Как выполняется качественная и количественная оценка рисков?
4. Приведите примеры преступлений в сфере информации и информационных технологий, известных из практики (например, фишинг, вредоносное ПО, DDoS-атаки, утечки данных, кибершпионаж, мошенничество с использованием ИТ). Предложите их классификацию по объекту посягательства и по способу совершения.
5. В чем сущность функционирования системы защиты информации? Опишите ее основные цели и задачи. Какие методы и средства (правовые, организационные, технические, программно-аппаратные) используются для построения эффективной системы защиты? Приведите примеры взаимосвязи этих методов.
6. Что понимается под «опасной информацией» и какую угрозу она представляет для человека? Какие механизмы защиты от опасной информации (дезинформация, манипуляции, пропаганда, фейки) существуют на уровне государства, общества и личности? Приведите примеры способов противодействия.
7. Опишите проблему «неинформированности в области информационной безопасности». Какими последствиями она грозит для отдельных граждан, организаций и государства? Какие меры могут быть приняты для повышения уровня осведомленности сотрудников и населения в целом?
8. Перечислите и охарактеризуйте основные защищаемые объекты информационной безопасности (информационные ресурсы, телекоммуникационные системы, автоматизированные системы управления, информационная инфраструктура, личные данные пользователей). Для каждого из них укажите наиболее актуальные угрозы.
9. Какие виды угроз для информации, циркулирующей в информационных системах, выделяются по характеру воздействия на защищаемые свойства информации (конфиденциальность, целостность, доступность)? Приведите примеры нарушений каждого из этих свойств.

10. Какую роль играет человеческий фактор в обеспечении информационной безопасности? Опишите основные риски, связанные с действиями пользователей (халатность, неосторожность, недостаток знаний, социальная инженерия). Предложите комплекс мер по снижению этих рисков, включая обучение, регулярное информирование и организационные регламенты.

Тестовые вопросы

Тема 1.1. Основные понятия и задачи информационной безопасности

Вариант 1

1. Что из перечисленного является объектом информационной безопасности?

А) Принтер

Б) База данных с персональными данными

В) Электрическая сеть

Г) Кондиционер

2. Какое свойство информации нарушается при несанкционированном изменении данных?

А) Доступность

Б) Конфиденциальность

В) Целостность

Г) Достоверность

3. Какой из перечисленных факторов относится к антропогенным угрозам информации?

А) Землетрясение

Б) Отказ оборудования

В) Ошибка администратора системы

Г) Затопление серверной

4. Риск информационной безопасности – это:

А) Вероятность реализации угрозы с учетом возможного ущерба

Б) Наличие уязвимости в системе

В) Стоимость защиты информации

Г) Мера сложности взлома системы

5. Какой вид преступления в сфере ИТ связан с незаконным сбором и использованием персональных данных?

А) Фишинг

Б) DDoS-атака

В) Нарушение конфиденциальности

Г) Распространение вредоносного ПО

6. Что из перечисленного относится к техническим мерам защиты информации?

А) Разработка политики безопасности

Б) Использование антивирусных программ

В) Проведение инструктажей

Г) Заключение договоров о неразглашении

7. Какая угроза направлена на нарушение доступности информации?

А) Перехват пароля

Б) DDoS-атака на веб-сервер

В) Внесение изменений в базу данных
Г) Копирование файлов

8. Что понимается под «опасной информацией»?

А) Информация, содержащая нецензурную лексику
Б) Информация, которая может причинить вред личности, обществу или государству
В) Информация, не прошедшая государственную регистрацию
Г) Информация, содержащая технические ошибки

9. Какая мера наиболее эффективна для защиты от социальной инженерии?

А) Установка межсетевого экрана
Б) Регулярное обучение сотрудников правилам безопасности
В) Использование шифрования данных
Г) Резервное копирование информации

10. Примером преступления в сфере информационных технологий является:

А) Нарушение правил дорожного движения
Б) Незаконное распространение вредоносного ПО
В) Неуплата налогов
Г) Нарушение правил пожарной безопасности

11. К защищаемым объектам информационной безопасности относятся:

А) Здания и сооружения
Б) Информационные ресурсы и системы
В) Транспортные средства
Г) Сельскохозяйственные угодья

12. Что из перечисленного относится к организационным методам защиты информации?

А) Внедрение системы обнаружения вторжений
Б) Разработка инструкций по работе с конфиденциальными документами
В) Применение криптографических алгоритмов
Г) Установка аппаратных ключей

13. Какой из рисков информационной безопасности является наиболее опасным для коммерческой организации?

А) Риск утечки интеллектуальной собственности
Б) Риск выхода из строя кондиционера
В) Риск задержки доставки обеда в офис
Г) Риск потери ключей от кабинета

14. Защита человека от неинформированности в области ИБ предполагает:

А) Повышение уровня цифровой грамотности населения
Б) Установку антивирусов на все устройства
В) Изоляцию от интернета
Г) Использование только проверенных сайтов

15. Система защиты информации функционирует для:

А) Обеспечения бесперебойного электропитания
Б) Предотвращения ущерба от реализации угроз
В) Ускорения работы компьютерных сетей
Г) Снижения затрат на обслуживание оборудования

Вариант 2

1. Информационный процесс – это:

А) Хранение информации на жестком диске

Б) Совокупность действий по сбору, обработке, передаче и хранению информации

В) Установка программного обеспечения

Г) Обмен данными между компьютерами

2. Какое свойство информации нарушается при несанкционированном доступе к ней посторонних лиц?

А) Доступность

Б) Конфиденциальность

В) Целостность

Г) Релевантность

3. Примером техногенной угрозы информации является:

А) Ураган

Б) Сбой в работе сервера из-за ошибки в программном обеспечении

В) Хакерская атака

Г) Несанкционированное копирование данных сотрудником

4. Оценка риска информационной безопасности включает:

А) Определение стоимости актива и вероятности реализации угрозы

Б) Только анализ уязвимостей

В) Подбор паролей для доступа

Г) Установку системы видеонаблюдения

5. Какое преступление в сфере ИТ связано с манипуляцией пользователем для получения конфиденциальной информации?

А) Фишинг

Б) Сниффинг

В) Спам

Г) Взлом пароля

6. Что относится к правовым методам защиты информации?

А) Принятие законов и нормативных актов в области ИБ

Б) Использование межсетевых экранов

В) Найм специалистов по безопасности

Г) Проведение аудита безопасности

7. Какая угроза направлена на нарушение конфиденциальности информации?

А) Уничтожение базы данных

Б) Перехват трафика в сети

В) Блокировка доступа пользователя

Г) Модификация содержимого файла

8. Что из перечисленного относится к опасной информации для общества?

А) Информация о способах мошенничества

Б) Научные статьи

В) Прогноз погоды

Г) Рецепты блюд

9. Основная причина уязвимости человека к социальной инженерии – это:

А) Недостаточная техническая защищенность устройств

Б) Психологические особенности: доверчивость, страх, желание помочь

В) Отсутствие антивируса
Г) Низкая скорость интернета

10. Примером преступления в области информационной безопасности является:

А) Мошенничество с использованием электронных писем (фишинг)
Б) Нарушение трудовой дисциплины
В) Неисполнение должностных инструкций
Г) Загрязнение окружающей среды

11. Защищаемыми объектами в информационной безопасности являются также:

А) Кадровый состав организации
Б) Информационная инфраструктура государства
В) Производственное оборудование
Г) Транспортная логистика

12. Какая мера защиты от неинформированности сотрудников наиболее эффективна?

А) Проведение регулярных тренингов и тестирований по ИБ
Б) Установка паролей на все компьютеры
В) Ограничение доступа к интернету
Г) Использование только лицензионного ПО

13. Сущность системы защиты информации заключается в:

А) Создании непреодолимых барьеров для всех угроз
Б) Снижении рисков до приемлемого уровня путем комплекса мер
В) Полном отказе от использования информационных технологий
Г) Передаче всей информации в облачное хранилище

14. Что из перечисленного не является угрозой информации?

А) Вирус-шифровальщик
Б) Перехват данных по Wi-Fi
В) Регулярное резервное копирование данных
Г) Инсайдерская деятельность

15. Защита человека от опасной информации включает:

А) Развитие критического мышления и проверку источников
Б) Полную изоляцию от всех СМИ
В) Использование только государственных новостных каналов
Г) Установку блокировщиков рекламы

Ключ к тестам

Вариант 1		Вариант 2	
№ вопроса	Правильный ответ	№ вопроса	Правильный ответ
1	Б	1	Б
2	В	2	Б
3	В	3	Б
4	А	4	А
5	В	5	А
6	Б	6	А
7	Б	7	Б
8	Б	8	А
9	Б	9	Б
10	Б	10	А
11	Б	11	Б

12	Б	12	А
13	А	13	Б
14	А	14	В
15	Б	15	А

Тема 1.2. Основы защиты информации

1. Задание для устного опроса по темам

1. Раскройте содержание понятий «целостность», «доступность» и «конфиденциальность» информации как трех базовых свойств информационной безопасности. Приведите примеры ситуаций, когда каждое из этих свойств нарушается, и опишите возможные последствия.
2. Опишите классификацию информации по видам тайны и степеням конфиденциальности. Какие категории информации относятся к государственной тайне, а какие – к конфиденциальной информации? Приведите примеры для каждой категории.
3. Дайте определения понятиям «государственная тайна» и «конфиденциальная информация». В чем их принципиальное различие с точки зрения правового режима, порядка доступа и ответственности за разглашение?
4. Опишите жизненный цикл конфиденциальной информации от момента ее создания до уничтожения. Какие этапы (создание, обработка, передача, хранение, использование, уничтожение) выделяются в этом цикле и какие меры защиты должны применяться на каждом этапе?
5. Сформулируйте основные цели и задачи защиты информации. Как они соотносятся с обеспечением трех базовых свойств информации (конфиденциальность, целостность, доступность)? Приведите примеры задач для каждой из целей.
6. Дайте определения основным понятиям в области защиты информации: «объект защиты», «источник угроз», «уязвимость», «средство защиты», «политика безопасности». Как эти понятия взаимосвязаны между собой?
7. Перечислите основные элементы процесса менеджмента информационной безопасности (идентификация активов, оценка рисков, выбор мер защиты, внедрение, мониторинг, аудит). Опишите, как они взаимосвязаны и образуют непрерывный цикл управления.
8. Опишите модель интеграции информационной безопасности в основную деятельность организации. На каких уровнях (стратегическом, тактическом, операционном) должна быть реализована безопасность и как она должна быть встроена в бизнес-процессы?
9. Раскройте понятие «политика безопасности». Какие виды политик безопасности существуют (базовая, частные, оперативные)? Из каких разделов должна состоять политика безопасности организации и какие вопросы она должна регламентировать?
10. Как жизненный цикл конфиденциальной информации связан с политикой безопасности организации? Приведите пример того, как политика безопасности должна регламентировать действия с конфиденциальной информацией на каждом этапе ее жизненного цикла.

Тестовые вопросы

Тема 1.2. Основы защиты информации

Вариант 1

1. Какое свойство информации означает, что информация доступна только уполномоченным субъектам?

А) Целостность

Б) Доступность

В) Конфиденциальность

Г) Достоверность

2. Какой вид тайны относится к информации, распространение которой может нанести ущерб национальным интересам государства?

А) Коммерческая тайна

Б) Государственная тайна

В) Служебная тайна

Г) Профессиональная тайна

3. Жизненный цикл конфиденциальной информации завершается этапом:

А) Создания

Б) Передачи

В) Уничтожения

Г) Хранения

4. Основной целью защиты информации является:

А) Полное устранение всех угроз

Б) Обеспечение конфиденциальности, целостности и доступности информации

В) Максимальное ускорение обработки данных

Г) Снижение затрат на информационные технологии

5. Что из перечисленного является уязвимостью информации?

А) Антивирусное ПО

Б) Недостаток парольной политики

В) Межсетевой экран

Г) Шифрование данных

6. Политика безопасности организации – это:

А) Совокупность правил и процедур, регламентирующих защиту информации

Б) Перечень используемого антивирусного ПО

В) Инструкция по работе с компьютерной техникой

Г) Правила оформления документов

7. Какой этап жизненного цикла конфиденциальной информации предполагает ее передачу по каналам связи?

А) Создание

Б) Обработка

В) Передача

Г) Хранение

8. Что из перечисленного относится к конфиденциальной информации (не являющейся государственной тайной)?

А) Сведения о секретных разработках вооружений

Б) Персональные данные сотрудников

В) Данные о дислокации воинских частей
Г) Сведения о шифрах специальной связи

9. Менеджмент информационной безопасности включает в себя:

А) Только установку антивирусов
Б) Непрерывный цикл оценки рисков, выбора мер и мониторинга
В) Разработку веб-сайтов
Г) Найм сотрудников

10. На каком уровне менеджмента ИБ разрабатывается общая стратегия безопасности организации?

А) Операционный
Б) Тактический
В) Стратегический
Г) Технический

11. Интеграция ИБ в деятельность организации предполагает:

А) Встраивание мер безопасности во все бизнес-процессы
Б) Создание изолированного отдела безопасности
В) Полный отказ от автоматизации
Г) Разрешение всех рисков

12. Какая степень конфиденциальности обычно присваивается информации ограниченного доступа, не содержащей государственной тайны?

А) «Особой важности»
Б) «Совершенно секретно»
В) «Конфиденциально» или «Для служебного пользования»
Г) «Открыто»

13. На каком этапе жизненного цикла конфиденциальной информации применяется криптографическая защита?

А) Только при создании
Б) На этапах передачи, хранения и обработки
В) Только при уничтожении
Г) Ни на одном из этапов

14. Документ, определяющий цели и задачи системы защиты информации организации, называется:

А) Технический регламент
Б) Политика безопасности
В) Инструкция по охране труда
Г) Устав организации

15. Что входит в задачи защиты информации?

А) Увеличение количества сотрудников отдела ИТ
Б) Обеспечение непрерывности работы и минимизация ущерба
В) Полный запрет на использование интернета
Г) Переход на бумажный документооборот

Вариант 2

1. Какое свойство информации означает, что информация не может быть изменена или уничтожена несанкционированно?

А) Конфиденциальность

Б) Доступность
В) Целостность
Г) Своевременность

2. Информация, составляющая государственную тайну, – это:

А) Информация о способах защиты авторских прав
Б) Сведения, разглашение которых может нанести ущерб безопасности государства
В) Персональные данные работников предприятия
Г) Бухгалтерская отчетность организации

3. Жизненный цикл конфиденциальной информации начинается с этапа:

А) Хранения
Б) Передачи
В) Обработки
Г) Создания

4. Задача защиты информации по обеспечению доступности означает:

А) Информация должна быть доступна только узкому кругу лиц
Б) Информация должна быть доступна авторизованным пользователям в нужное время
В) Информация должна храниться в одном экземпляре
Г) Информация должна быть понятной для всех

5. Что из перечисленного является источником угроз информации?

А) Антивирус
Б) Злоумышленник, пытающийся получить несанкционированный доступ
В) Брандмауэр
Г) Система контроля доступа

6. Частные политики безопасности регламентируют:

А) Общие принципы и цели безопасности организации
Б) Конкретные области (например, управление доступом, использование интернета)
В) Технические характеристики серверного оборудования
Г) Штатное расписание отдела информационной безопасности

7. Какой этап жизненного цикла конфиденциальной информации включает внесение изменений в ее содержание?

А) Создание
Б) Передача
В) Обработка
Г) Хранение

8. Коммерческая тайна – это пример:

А) Государственной тайны
Б) Конфиденциальной информации
В) Открытой информации
Г) Секретной информации

9. Модель интеграции ИБ в основную деятельность предполагает:

А) Выделение ИБ в отдельный бизнес-процесс
Б) Рассмотрение ИБ как неотъемлемой части всех процессов организации
В) Полный отказ от ИБ в пользу производительности
Г) Передачу всех функций ИБ внешнему подрядчику

10. Основным элементом процесса менеджмента ИБ является:

А) Покупка нового оборудования

Б) Управление рисками
В) Найм сотрудников
Г) Разработка сайта

11. На каком уровне менеджмента ИБ реализуются конкретные технические меры защиты?

А) Стратегическом
Б) Тактическом
В) Операционном
Г) Административном

12. Какая мера защиты применяется на этапе уничтожения конфиденциальной информации?

А) Архивация
Б) Шифрование
В) Физическое уничтожение носителей или гарантированное удаление
Г) Копирование

13. Что из перечисленного не является объектом защиты информации?

А) Информационные ресурсы
Б) Системы обработки данных
В) Мебель в офисе
Г) Каналы связи

14. Политика безопасности должна пересматриваться:

А) Один раз при создании
Б) Регулярно при изменении условий (угроз, технологий, законодательства)
В) Только при смене руководства
Г) Никогда

15. Обеспечение конфиденциальности информации предполагает:

А) Шифрование данных
Б) Удаление всех копий информации
В) Публикацию информации в открытом доступе
Г) Увеличение скорости передачи данных

Ключ к тестам

Вариант 1		Вариант 2	
№ вопроса	Правильный ответ	№ вопроса	Правильный ответ
1	В	1	В
2	Б	2	Б
3	В	3	Г
4	Б	4	Б
5	Б	5	Б
6	А	6	Б
7	В	7	В
8	Б	8	Б
9	Б	9	Б
10	В	10	Б
11	А	11	В
12	В	12	В
13	Б	13	В

14	Б	14	Б
15	Б	15	А

Лабораторные занятия № 1-2:

1. Определение объектов защиты на типовом объекте информатизации
2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности

Тема 1.3. Угрозы безопасности защищаемой информации

1. Задание для устного опроса по темам

1. Понятия сетевой модели. Модель взаимодействия «открытых систем» OSI: основные понятия.
2. Дайте определение «угрозы безопасности информации». Из каких обязательных элементов (источник угрозы, способ реализации, объект воздействия, последствия) она состоит? Приведите пример полной формулы угрозы.
3. Опишите системную классификацию угроз безопасности информации по следующим признакам: по природе возникновения (объективные/субъективные), по степени преднамеренности (умышленные/неумышленные), по отношению к объекту (внутренние/внешние), по стадии воздействия (начальная, промежуточная, завершающая). Приведите по одному примеру для каждой категории.
4. Перечислите основные каналы несанкционированного доступа (НСД) к информации. Разделите их на технические (аппаратные, программные) и организационные (человеческий фактор). Для каждого канала укажите конкретный пример реализации НСД.
5. В чем суть методов несанкционированного доступа? Опишите такие методы, как: перехват (пассивный и активный), подслушивание, внедрение программных закладок, использование уязвимостей программного обеспечения. Приведите примеры защитных мер против каждого метода.
6. Раскройте понятие «уязвимость информации». Как уязвимость связана с угрозами и рисками? Какие факторы делают информацию уязвимой (например, недостатки технологий, ошибки персонала, слабости организационных мер)?
7. Опишите количественные методы оценки уязвимости информации. Какие показатели используются (например, CVSS – Common Vulnerability Scoring System)? Как оценивается степень тяжести уязвимости и как это влияет на приоритизацию мер защиты?
8. Опишите качественные методы оценки уязвимости информации (например, метод экспертных оценок, матрицы рисков). В чем преимущества и ограничения качественного подхода по сравнению с количественным?
9. Какие модели описания уязвимостей существуют (например, CWE – Common Weakness Enumeration, OWASP Top 10)? Как они помогают систематизировать знания о типовых уязвимостях и разрабатывать эффективные контрмеры?
10. Опишите процесс оценки уязвимости информации в рамках управления рисками: этапы (идентификация активов, идентификация уязвимостей, анализ угроз, оценка последствий, определение уровня риска). Какие инструменты используются для автоматизации этого процесса?

11. Как каналы НСД соотносятся с методами оценки уязвимости? Приведите пример: если выявлен канал НСД (например, небезопасный Wi-Fi), то какие уязвимости он создает и как их оценить и устранить в рамках системы защиты информации?

Тестовые вопросы

Тема 1.3. Угрозы безопасности защищаемой информации

Вариант 1

1. Что такое угроза безопасности информации?

А) Наличие ошибок в программном обеспечении

Б) Совокупность условий и факторов, создающих опасность нарушения безопасности информации

В) Отсутствие антивирусной защиты

Г) Несанкционированное копирование файлов

2. Какой из перечисленных признаков относится к классификации угроз по природе возникновения?

А) Внутренние и внешние

Б) Объективные и субъективные

В) Умышленные и неумышленные

Г) Активные и пассивные

3. Что является примером внутренней угрозы безопасности информации?

А) Атака хакеров из-за пределов сети

Б) Ошибка сотрудника при работе с конфиденциальными данными

В) Отключение электроэнергии

Г) Вирус, проникший через интернет

4. Какой канал несанкционированного доступа относится к техническим каналам?

А) Убеждение сотрудника передать пароль по телефону

Б) Перехват данных через неэкранированный кабель

В) Кража документов из сейфа

Г) Подбор пароля по словарю

5. Какой метод несанкционированного доступа предполагает активное воздействие на канал связи?

А) Пассивный перехват

Б) Подслушивание

В) Активный перехват с подменой данных

Г) Анализ побочных электромагнитных излучений

6. Уязвимость информации – это:

А) Свойство информации, делающее ее доступной для угроз

Б) Совокупность мер защиты информации

В) Аппаратное средство защиты

Г) Набор криптографических ключей

7. Какая система используется для количественной оценки уязвимостей и присвоения им баллов?

А) CWE

Б) CVSS

В) OWASP
Г) ISO 27001

8. Что из перечисленного относится к качественным методам оценки уязвимости?

А) Расчет вероятности реализации угрозы на основе статистики
Б) Экспертная оценка уровня риска по шкале «низкий – средний – высокий»
В) Определение точного значения ущерба в денежном выражении
Г) Использование математических моделей для расчета рисков

9. Модель CWE (Common Weakness Enumeration) предназначена для:

А) Оценки финансовых потерь от уязвимостей
Б) Систематизации и описания типовых уязвимостей программного обеспечения
В) Расчета времени восстановления системы
Г) Определения стоимости активов

10. Какой канал НСД связан с использованием человеческого фактора?

А) Сканирование портов
Б) Перехват сетевого трафика
В) Социальная инженерия
Г) Внедрение вредоносного ПО

11. Какой этап процесса оценки уязвимости предполагает определение ценности информации для организации?

А) Идентификация уязвимостей
Б) Идентификация активов
В) Оценка последствий
Г) Анализ угроз

12. Что из перечисленного является методом несанкционированного доступа, основанным на внедрении в программное обеспечение?

А) Подслушивание телефонных разговоров
Б) Использование аппаратного закладного устройства
В) Внедрение программной закладки (трояна)
Г) Перехват электромагнитных излучений

13. Что такое «канал несанкционированного доступа»?

А) Путь физического проникновения в здание
Б) Путь или среда, через которую злоумышленник может получить доступ к информации
В) Программа для взлома паролей
Г) Официальный канал связи между отделами

14. Какая из перечисленных уязвимостей относится к организационным?

А) Отсутствие регулярного обновления программного обеспечения
Б) Использование слабых паролей
В) Отсутствие инструкций по работе с конфиденциальными документами
Г) Наличие SQL-инъекции в веб-приложении

15. Приоритизация мер защиты в первую очередь определяется:

А) Стоимостью средств защиты
Б) Степенью тяжести уязвимости и величиной риска
В) Мнением руководства
Г) Сложностью реализации меры

Вариант 2

1. Угроза безопасности информации всегда предполагает наличие:

А) Антивирусной защиты

Б) Источника угрозы, способа реализации и объекта воздействия

В) Шифрования данных

Г) Высококвалифицированных сотрудников

2. К внешним угрозам безопасности информации относятся:

А) Действия недовольных сотрудников

Б) Ошибки системных администраторов

В) Атаки из глобальной сети Интернет

Г) Неправильное хранение документов

3. Какой тип угроз связан с непреднамеренными действиями человека?

А) Умышленный

Б) Неумышленный

В) Активный

Г) Внешний

4. Какой канал несанкционированного доступа является основным для атак через интернет?

А) Акустический канал

Б) Сетевой канал (протоколы TCP/IP)

В) Канал виброакустический

Г) Оптический канал

5. Пассивный перехват информации означает:

А) Изменение данных при передаче

Б) Несанкционированное копирование данных без их изменения

В) Уничтожение данных

Г) Блокирование доступа к данным

6. Какой из перечисленных факторов делает информацию уязвимой?

А) Использование сертифицированных средств защиты

Б) Отсутствие системы резервного копирования

В) Регулярное обучение сотрудников

Г) Внедрение многофакторной аутентификации

7. Качественная оценка уязвимости обычно выражается в:

А) Процентах

Б) Баллах (CVSS)

В) Категориях (например, «высокая», «средняя», «низкая»)

Г) Денежных единицах

8. Что является результатом количественной оценки уязвимости?

А) Описание характера уязвимости

Б) Численное значение риска (например, вероятность × ущерб)

В) Перечень мер по устранению уязвимости

Г) Список эксплойтов для данной уязвимости

9. Модель OWASP Top 10 используется для:

А) Оценки безопасности сетевого оборудования

Б) Систематизации наиболее критичных уязвимостей веб-приложений

В) Расчета стоимости информационных активов
Г) Определения политики паролей

10. Что из перечисленного относится к методу НСД «использование уязвимостей программного обеспечения»?

А) Подкуп сотрудника
Б) Эксплуатация неисправленной ошибки в браузере
В) Анализ электромагнитных излучений
Г) Подслушивание разговоров в офисе

11. К организационным уязвимостям относятся:

А) Недостатки в системе контроля доступа
Б) Отсутствие политики безопасного хранения паролей
В) Неисправность аппаратного обеспечения
Г) Вирусы в программном обеспечении

12. Какой этап оценки уязвимости предполагает определение возможных путей реализации угроз?

А) Идентификация активов
Б) Идентификация уязвимостей
В) Анализ угроз
Г) Оценка последствий

13. Какой из методов является методом НСД?

А) Шифрование данных
Б) Сниффинг (перехват трафика)
В) Аутентификация пользователей
Г) Ведение журналов событий

14. Какая модель описания уязвимостей наиболее детализирует причины их возникновения в коде?

А) CVSS
Б) CWE
В) OWASP Top 10
Г) ISO 27005

15. Как взаимосвязаны каналы НСД и методы оценки уязвимости?

А) Не связаны между собой
Б) Оценка уязвимости позволяет выявить и закрыть каналы НСД
В) Каналы НСД не влияют на оценку уязвимости
Г) Методы оценки не учитывают каналы НСД

Ключ к тестам

Вариант 1		Вариант 2	
№ вопроса	Правильный ответ	№ вопроса	Правильный ответ
1	Б	1	Б
2	Б	2	В
3	Б	3	Б
4	Б	4	Б
5	В	5	Б
6	А	6	Б
7	Б	7	В
8	Б	8	Б
9	Б	9	Б

10	В	10	Б
11	Б	11	Б
12	В	12	В
13	Б	13	Б
14	В	14	Б
15	Б	15	Б

Лабораторные занятия № 3:

1. Определение угроз объекта информатизации и их классификация

Раздел 2. Методология защиты информации

Тема 2.1. Методологические подходы к защите информации

1. Задание для устного опроса по темам

1. Перечислите и охарактеризуйте основные методики определения требований к защите информации, применяемые в Российской Федерации (например, методика ФСТЭК, ГОСТ Р ИСО/МЭК 27001, подходы на основе оценки рисков). В чем их сходства и различия? Какие из них являются обязательными для государственных информационных систем?
2. Опишите параметры защищаемой информации, которые подлежат оценке при определении требуемого уровня защиты (например, категория конфиденциальности, степень критичности, объем, срок жизни, ценность для владельца). Как эти параметры влияют на выбор средств защиты?
3. Назовите факторы, влияющие на требуемый уровень защиты информации, и обоснуйте их значимость. Какие из факторов являются внешними (законодательство, угрозы) и внутренними (бизнес-процессы, бюджет, технические возможности)? Приведите примеры.
4. Раскройте суть методики оценки рисков как инструмента определения требований к защите информации. Какие этапы включает эта методика и как результаты оценки рисков преобразуются в конкретные требования к системе защиты?
5. Охарактеризуйте виды мер защиты информации: организационные (административные), правовые, технические, физические, программно-аппаратные. Для каждого вида приведите по два примера конкретных мер и укажите, какие угрозы они предотвращают.
6. Перечислите и раскройте основные принципы защиты информации. Какие из них являются базовыми (например, законность, комплексность, непрерывность, экономическая целесообразность, разумная достаточность)? В чем заключается принцип «защита в глубину» (defense in depth) и как он реализуется на практике?
7. Как комплексность мер защиты обеспечивает надежную защиту информации? Приведите пример, когда отдельно взятая мера (например, только шифрование или только организационные меры) не может гарантировать безопасность, а их сочетание дает нужный эффект.
8. Опишите, как оценка факторов, влияющих на требуемый уровень защиты, помогает выбрать экономически оправданные средства защиты. Как учитывается соотношение «затраты на защиту – потенциальный ущерб от реализации угроз»?

9. Сравните нормативно-правовые и риск-ориентированные методики определения требований к защите информации. В каких случаях каждая из них применяется и какие преимущества и недостатки у каждого подхода?
10. Предложите порядок (алгоритм) определения требований к защите информации для конкретной информационной системы (например, корпоративной базы данных клиентов). Какие исходные данные необходимы, какие методики следует применить и какие меры защиты должны быть выбраны в результате?

Тестовые вопросы

Тема 2.1. Методологические подходы к защите информации

Вариант 1

1. Какая методика определения требований к защите информации основана на оценке рисков и является добровольной для коммерческих организаций?

А) ГОСТ Р ИСО/МЭК 27001

Б) Методика ФСТЭК России

В) Методика оценки соответствия

Г) Методика категорирования

2. Что из перечисленного является параметром защищаемой информации?

А) Скорость передачи данных

Б) Степень конфиденциальности

В) Количество пользователей системы

Г) Частота обновления информации

3. Внешним фактором, влияющим на требуемый уровень защиты информации, является:

А) Бюджет организации

Б) Требования законодательства

В) Квалификация персонала

Г) Наличие собственного центра обработки данных

4. Какой этап методики оценки рисков предшествует выбору мер защиты?

А) Внедрение средств защиты

Б) Мониторинг эффективности

В) Оценка последствий реализации угроз

Г) Разработка политики безопасности

5. Какая мера защиты относится к организационным (административным)?

А) Использование межсетевого экрана

Б) Разработка инструкций по работе с конфиденциальными документами

В) Шифрование данных

Г) Установка системы видеонаблюдения

6. Какой принцип защиты информации означает, что затраты на защиту не должны превышать потенциальный ущерб от реализации угрозы?

А) Комплексность

Б) Непрерывность

В) Экономическая целесообразность

Г) Законность

7. Что такое принцип «защита в глубину» (defense in depth)?

А) Использование только одной мощной системы защиты

Б) Организация нескольких последовательных уровней защиты для компенсации недостатков отдельных мер

В) Глубокое шифрование всех данных

В) Полная изоляция системы от внешних сетей

8. Какая мера защиты относится к программно-аппаратным средствам?

А) Проведение инструктажей

Б) Использование электронной цифровой подписи

В) Заключение договоров о неразглашении

Г) Разработка политики безопасности

9. Принцип комплексности защиты информации предполагает:

А) Использование только одной технологии защиты

Б) Сочетание организационных, технических и правовых мер

В) Защиту только самой важной информации

Г) Отказ от дорогих средств защиты

10. Какое из утверждений о факторах, влияющих на требуемый уровень защиты, верно?

А) Требуемый уровень защиты всегда одинаков для всех систем

Б) Требуемый уровень защиты зависит от ценности информации и уровня угроз

В) Требуемый уровень защиты определяется только бюджетом организации

Г) Требуемый уровень защиты не учитывает внешние угрозы

11. Что из перечисленного относится к физическим мерам защиты информации?

А) Установка паролей

Б) Охрана помещений и ограничение физического доступа

В) Использование антивирусов

Г) Регулярное обновление ПО

12. Какая методика определения требований к защите является обязательной для государственных информационных систем в РФ?

А) OWASP

Б) Методика ФСТЭК России

В) ISO 27005

Г) COBIT

13. Какой параметр защищаемой информации влияет на срок ее хранения в защищенном виде?

А) Объем информации

Б) Срок жизни (актуальности) информации

В) Формат данных

Г) Язык представления

14. Принцип непрерывности защиты информации означает:

А) Защита осуществляется только в рабочее время

Б) Защита должна осуществляться постоянно на всех этапах жизненного цикла информации

В) Защита осуществляется только при передаче данных

Г) Защита включается по требованию пользователя

15. Что является первым шагом при определении требований к защите информации?

А) Выбор средств защиты

Б) Идентификация и классификация защищаемой информации

В) Разработка политики безопасности

Г) Найм сотрудников по безопасности

Вариант 2

1. Какая методика определения требований к защите информации относится к риск-ориентированному подходу и описана в международном стандарте?

А) Методика категорирования

Б) Методика на основе ГОСТ Р ИСО/МЭК 27005

В) Методика ФСТЭК

Г) Методика аттестации

2. Что из перечисленного является параметром защищаемой информации при определении требований к ее защите?

А) Критичность информации для деятельности организации

Б) Время доступа к информации

В) Количество символов в документе

Г) Формат хранения файла

3. Внутренним фактором, влияющим на требуемый уровень защиты информации, является:

А) Изменения в законодательстве

Б) Появление новых видов угроз в интернете

В) Технические возможности организации по внедрению средств защиты

Г) Требования регуляторов

4. Какой вид мер защиты информации направлен на предотвращение несанкционированного доступа на физическом уровне?

А) Организационные меры

Б) Правовые меры

В) Физические меры

Г) Программные меры

5. Какой принцип защиты информации означает, что меры защиты должны быть соразмерны ценности информации и уровню угроз?

А) Разумная достаточность

Б) Комплексность

В) Непрерывность

Г) Законность

6. Что из перечисленного является примером технической меры защиты информации?

А) Подписание соглашения о неразглашении

Б) Использование системы обнаружения вторжений (IDS)

В) Проведение аудита безопасности

Г) Разработка должностных инструкций

7. Принцип законности в защите информации означает:

А) Защита должна быть дешевой

Б) Меры защиты должны соответствовать законодательству, в том числе в области персональных данных

В) Защита должна быть скрытой от пользователей

Г) Защита не должна применяться к открытой информации

8. Какая мера относится к правовым методам защиты информации?

А) Установка брандмауэра

Б) Принятие закона о персональных данных

В) Организация пропускного режима

Г) Использование SSL-сертификатов

9. Что такое экономическая целесообразность как принцип защиты информации?

А) Защита должна быть максимально дорогой

Б) Затраты на защиту должны быть сопоставимы с возможным ущербом от нарушения безопасности

В) Защита должна быть бесплатной

Г) Защита не должна учитывать бюджет организации

10. Какие факторы в первую очередь определяют требуемый уровень защиты информации?

А) Только стоимость оборудования

Б) Только мнение руководства

В) Ценность информации и оценка рисков

Г) Только требования регуляторов

11. Что из перечисленного относится к организационным мерам защиты информации?

А) Шифрование данных на диске

Б) Регулярное обучение сотрудников правилам ИБ

В) Установка системы видеонаблюдения

Г) Использование межсетевого экрана

12. Методика ФСТЭК России применяется в первую очередь для:

А) Коммерческих организаций

Б) Государственных информационных систем и систем, обрабатывающих информацию ограниченного доступа

В) Образовательных учреждений

Г) Интернет-магазинов

13. Какой параметр защищаемой информации влияет на выбор криптографических средств?

А) Степень конфиденциальности и срок хранения

Б) Язык написания документа

В) Количество страниц

Г) Цветовая гамма изображений

14. Принцип разумной достаточности мер защиты предполагает:

А) Использование всех существующих средств защиты без ограничений

Б) Выбор мер, адекватных реальным угрозам и ценности информации

В) Использование только бесплатных средств

Г) Отказ от дорогих решений

15. Какой этап оценки рисков является ключевым для определения конкретных требований к защите?

А) Идентификация активов

Б) Идентификация уязвимостей

В) Расчет уровня риска (вероятность × ущерб)

Г) Документирование результатов

Ключ к тестам

Вариант 1		Вариант 2	
№ вопроса	Правильный ответ	№ вопроса	Правильный ответ
1	А	1	Б
2	Б	2	А
3	Б	3	В
4	В	4	В
5	Б	5	А
6	В	6	Б
7	Б	7	Б
8	Б	8	Б
9	Б	9	Б
10	Б	10	В
11	Б	11	Б
12	Б	12	Б
13	Б	13	А
14	Б	14	Б
15	Б	15	В

Тема 2.2. Нормативно правовое регулирование защиты информации

1. Задание для устного опроса по темам

1. Организационная структура СЗИ. Опишите типовую организационную структуру системы защиты информации (СЗИ) на предприятии. Какие подразделения и должностные лица входят в систему управления информационной безопасностью (СУИБ)? Как распределяются функции и ответственность между ними?
2. Уровни управления СЗИ. На каких уровнях (стратегическом, тактическом, операционном) строится организационная структура защиты информации? Какие задачи решаются на каждом уровне и кто за них отвечает?
3. Взаимодействие СЗИ с другими подразделениями. Как организовано взаимодействие службы защиты информации с другими структурными подразделениями организации (ИТ-отдел, служба персонала, юридический отдел, руководство)? Почему такое взаимодействие критически важно для эффективной защиты?
4. Руководство и ответственность. Кто в организации несет персональную ответственность за состояние защиты информации? Что означает принцип «первой ответственности» (accountability) в контексте ИБ и как он реализуется на практике?
5. Базовые федеральные законы. Перечислите основные федеральные законы Российской Федерации, регулирующие отношения в сфере защиты информации. Раскройте содержание Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Законодательство о персональных данных. Какой закон регулирует защиту персональных данных в РФ? Какие основные требования к операторам

персональных данных устанавливает этот закон и какова ответственность за его нарушение?

7. Административная и уголовная ответственность. Какие статьи Кодекса Российской Федерации об административных правонарушениях (КоАП) и Уголовного кодекса РФ устанавливают ответственность за нарушения в области защиты информации? Приведите примеры санкций.
8. Иерархия нормативных правовых актов. Опишите иерархию нормативных правовых актов в области защиты информации в РФ (от федеральных законов до ведомственных приказов и локальных нормативных актов). Приведите примеры документов каждого уровня.
9. ГОСТ Р ИСО/МЭК 27001. Опишите содержание и назначение национального стандарта РФ ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Для каких организаций он предназначен и какие требования устанавливает?
10. Стандарты серии ГОСТ Р ИСО/МЭК 27000. Перечислите основные стандарты семейства ИСО/МЭК 27000, применяемые в России. В чем различие между стандартами на требования (27001) и стандартами-руководствами (27002, 27005)?
11. Отечественные стандарты защиты информации. Какие российские стандарты (ГОСТ) регламентируют требования к средствам защиты информации, классификации информационных систем и порядку аттестации объектов информатизации? Приведите примеры.
12. Соотношение международных и российских стандартов. Как соотносятся международные стандарты ИСО/МЭК и российские национальные стандарты в области ИБ? В каких случаях применение международных стандартов обязательно, а в каких – рекомендательно?
13. Система сертификации средств защиты информации. Опишите систему сертификации средств защиты информации, созданную ФСТЭК России. Каковы ее основные цели, состав участников и нормативная основа?
14. Объекты и порядок сертификации. Какие объекты подлежат сертификации в области защиты информации (средства защиты информации, системы, процессы)? Опишите порядок проведения сертификации: от подачи заявки до получения сертификата.
15. Основные документы системы сертификации. Какие документы составляют нормативно-методическую базу системы сертификации средств защиты информации в РФ? Охарактеризуйте содержание Положения о системе сертификации средств защиты информации и роль ФСТЭК России в его утверждении.

Тестовые вопросы

Тема 2.2. Нормативно правовое регулирование защиты информации

Вариант 1

1. Кто в организации несет персональную ответственность за состояние защиты информации в соответствии с принципом «первой ответственности» (accountability)?

А) Начальник службы безопасности

Б) Руководитель организации (собственник)

В) Системный администратор

Г) Внешний аудитор

2. Какой федеральный закон является базовым в сфере регулирования отношений, связанных с информацией и информационными технологиями?

А) Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о

защите информации»
Б) Федеральный закон № 152-ФЗ «О персональных данных»
В) Федеральный закон № 63-ФЗ «Об электронной подписи»
Г) Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры»

3. Какой нормативный акт устанавливает административную ответственность за нарушения в области защиты информации?

А) Гражданский кодекс РФ
Б) Кодекс РФ об административных правонарушениях (КоАП)
В) Трудовой кодекс РФ
Г) Налоговый кодекс РФ

4. На каком уровне организационной структуры СЗИ разрабатывается стратегия информационной безопасности организации?

А) Операционный
Б) Тактический
В) Стратегический
Г) Технический

5. Какой международный стандарт, гармонизированный в России как ГОСТ Р ИСО/МЭК 27001, устанавливает требования к системе менеджмента информационной безопасности?

А) ИСО/МЭК 27002
Б) ИСО/МЭК 27005
В) ИСО/МЭК 27001
Г) ИСО/МЭК 27017

6. Какой документ является основным для системы сертификации средств защиты информации в РФ?

А) Положение о системе сертификации средств защиты информации
Б) Технический регламент о безопасности информации
В) ГОСТ Р ИСО/МЭК 15408
Г) Руководящий документ «Автоматизированные системы. Защита от НСД»

7. Какой федеральный закон регулирует обработку персональных данных?

А) 149-ФЗ
Б) 152-ФЗ
В) 187-ФЗ
Г) 63-ФЗ

8. Какое из перечисленных подразделений не является обязательным для организационной структуры защиты информации?

А) Служба информационной безопасности
Б) Отдел кадров
В) Юридический отдел
Г) Отдел технической поддержки

9. Какие объекты подлежат сертификации в области защиты информации?

А) Только программное обеспечение
Б) Только аппаратные средства
В) Средства защиты информации, системы и процессы
Г) Только криптографические средства

10. Какой стандарт серии ИСО/МЭК 27000 является руководством по управлению рисками информационной безопасности?

А) 27001

Б) 27002

В) 27005

Г) 27017

11. Какова роль ФСТЭК России в системе сертификации?

А) Проведение сертификационных испытаний

Б) Утверждение нормативных документов и выдача сертификатов

В) Оказание консультационных услуг

Г) Обучение персонала

12. Что из перечисленного является законодательным актом прямого действия в сфере ИБ?

А) ГОСТ Р ИСО/МЭК 27001

Б) Положение о системе сертификации

В) Федеральный закон № 149-ФЗ

Г) Методические рекомендации ФСТЭК

13. Какие задачи решаются на тактическом уровне управления СЗИ?

А) Разработка стратегии ИБ

Б) Реализация конкретных защитных мер и управление повседневной деятельностью

В) Оценка рисков и выбор политик

Г) Аудит и мониторинг

14. Какой международный стандарт содержит набор практических рекомендаций по выбору и внедрению мер защиты?

А) ИСО/МЭК 27001

Б) ИСО/МЭК 27002

В) ИСО/МЭК 27005

Г) ИСО/МЭК 27006

15. В каком документе закреплены основные правила и порядок сертификации средств защиты информации в России?

А) Технический регламент «О безопасности информации»

Б) Положение о системе сертификации средств защиты информации (утверждено ФСТЭК)

В) ГОСТ Р ИСО/МЭК 15408

Г) Федеральный закон № 184-ФЗ «О техническом регулировании»

Вариант 2

1. Какой принцип означает, что ответственное лицо должно отчитываться за состояние безопасности?

А) Принцип законности

Б) Принцип персональной ответственности

В) Принцип экономической целесообразности

Г) Принцип комплексности

2. Какой федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры?

А) 149-ФЗ
Б) 152-ФЗ
В) 187-ФЗ
Г) 63-ФЗ

3. Какой из перечисленных документов является кодексом об уголовной ответственности за преступления в сфере компьютерной информации?

А) КоАП РФ
Б) Уголовный кодекс РФ (гл. 28)
В) Гражданский кодекс РФ
Г) Налоговый кодекс РФ

4. На каком уровне управления СЗИ осуществляется аудит и контроль эффективности защитных мер?

А) Стратегический
Б) Тактический
В) Операционный
Г) Административный

5. Какой российский стандарт является аналогом международного стандарта ИСО/МЭК 27001 и устанавливает требования к СУИБ?

А) ГОСТ Р ИСО/МЭК 27001-2021
Б) ГОСТ Р ИСО/МЭК 27002-2021
В) ГОСТ Р ИСО/МЭК 27005-2021
Г) ГОСТ Р ИСО/МЭК 27006-2021

6. Какая организация в РФ уполномочена на создание системы сертификации средств защиты информации и выдачу сертификатов?

А) Минцифры России
Б) ФСТЭК России
В) ФСБ России
Г) Роскомнадзор

7. Какой федеральный закон регулирует использование электронной подписи?

А) 149-ФЗ
Б) 152-ФЗ
В) 63-ФЗ
Г) 187-ФЗ

8. Какое подразделение в организационной структуре СЗИ обычно отвечает за правовое сопровождение вопросов ИБ?

А) Служба ИБ
Б) Юридический отдел
В) Отдел кадров
Г) ИТ-отдел

9. Что является обязательным условием для ввода в эксплуатацию системы, обрабатывающей информацию ограниченного доступа, в части сертификации?

А) Наличие сертификата ФСТЭК на систему в целом
Б) Наличие сертификата на используемые средства защиты информации
В) Достаточно аттестации объекта
Г) Сертификация не требуется

10. Какой стандарт семейства ИСО/МЭК 27000 содержит руководство по применению СУИБ (дополнительные требования)?

А) 27001

Б) 27002

В) 27003

Г) 27006

11. Какие документы входят в нормативную базу системы сертификации средств защиты информации?

А) Только законы

Б) Положение о системе сертификации, методики испытаний, перечни показателей

В) Только ГОСТы

Г) Только международные стандарты

12. Какой уровень управления СЗИ отвечает за разработку оперативных процедур реагирования на инциденты?

А) Стратегический

Б) Тактический

В) Операционный

Г) Внешний аудит

13. Что из перечисленного является задачей организационной структуры СЗИ?

А) Разработка алгоритмов шифрования

Б) Внедрение политик безопасности и контроль их исполнения

В) Установка сетевого оборудования

Г) Разработка веб-сайта

14. Какой международный стандарт определяет критерии оценки безопасности информационных технологий (общие критерии)?

А) ИСО/МЭК 27001

Б) ИСО/МЭК 15408

В) ИСО/МЭК 27002

Г) ИСО/МЭК 27005

15. В каком случае организация обязана проходить сертификацию в системе ФСТЭК?

А) При добровольном желании

Б) При обработке информации ограниченного доступа и в соответствии с законодательством

В) При наличии более 50 сотрудников

Г) При использовании открытого ПО

Ключ к тестам

Вариант 1		Вариант 2	
№ вопроса	Правильный ответ	№ вопроса	Правильный ответ
1	Б	1	Б
2	А	2	В
3	Б	3	Б
4	В	4	В
5	В	5	А
6	А	6	Б
7	Б	7	В

8	Б	8	Б
9	В	9	Б
10	В	10	В
11	Б	11	Б
12	В	12	В
13	Б	13	Б
14	Б	14	Б
15	Б	15	Б

Лабораторные занятия № 4:

1. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности

Тема 2.3. Защита информации в автоматизированных (информационных) системах

1. Задание для устного опроса по темам

1. Перечислите и охарактеризуйте основные механизмы защиты информации**:** идентификация, аутентификация, авторизация, разграничение доступа, шифрование, контроль целостности, аудит. Какова роль каждого из этих механизмов в обеспечении безопасности?
2. Дайте определение системы защиты информации (СЗИ)**.** Из каких основных компонентов (организационные, технические, правовые, программные) она состоит? Как эти компоненты взаимосвязаны?
3. В чем отличие системы защиты информации от отдельных средств защиты? Почему комплексный подход к построению СЗИ является более эффективным, чем использование разрозненных мер?
4. Опишите классификацию мер защиты информации, реализуемых в автоматизированных системах. Разделите их на системные (ОС, СУБД), прикладные (приложения) и сетевые. Приведите примеры мер каждого уровня.
5. Какие меры защиты применяются на уровне операционной системы (контроль доступа, изоляция процессов, аудит, антивирус)? Приведите примеры конкретных механизмов в популярных ОС.
6. Как реализуется защита на уровне прикладного программного обеспечения (валидация входных данных, защита от SQL-инъекций, XSS, шифрование данных, логирование)? Приведите примеры уязвимостей и способов их устранения.
7. Какие меры защиты применяются на сетевом уровне (межсетевые экраны, VPN, системы обнаружения вторжений, сегментация сетей)? Как они предотвращают атаки из внешней сети?
8. Дайте классификацию программных средств защиты информации. Какие классы средств выделяют (антивирусы, межсетевые экраны, криптографические средства, СЗИ от утечек, средства контроля доступа)? Приведите примеры для каждого класса.
9. Что такое программно-аппаратные средства защиты информации? В чем их отличие от чисто программных решений? Приведите примеры: HSM (аппаратные модули безопасности), аппаратные ключи, межсетевые экраны на базе специализированных устройств.
10. Какие функции выполняют средства криптографической защиты информации (СКЗИ)? Какие задачи решаются с помощью симметричного и асимметричного шифрования, электронной подписи, хеширования?
11. Что такое инженерная защита объектов информатизации? Какие физические барьеры и технические средства охраны применяются (ограждения, двери, замки, системы видеонаблюдения, охранные датчики, системы контроля доступа)?
12. Опишите систему технической охраны объекта информатизации**.** Из каких подсистем она состоит (охранная сигнализация, пожаротушение, контроль доступа,

видеонаблюдение)? Как эти подсистемы интегрируются для обеспечения комплексной безопасности?

13. Как инженерная защита взаимодействует с программно-аппаратными средствами? Приведите пример, когда физическая защита предотвращает несанкционированный доступ даже при наличии программных уязвимостей.
14. Раскройте содержание организационно-распорядительной защиты информации. Какие виды деятельности она включает (разработка политик, инструкций, приказов; организация пропускного режима; работа с персоналом)? Опишите основные документы, регламентирующие организационно-распорядительные меры.
15. Опишите принципы построения организационно-распорядительной системы защиты информации**.** Какие этапы включает ее создание (анализ рисков, разработка политики, внедрение, контроль)? Как осуществляется работа с кадрами (подбор, обучение, инструктажи, проверки) и внутриобъектовый режим (доступ, пропускная система, порядок обращения с документами)?

Тестовые вопросы

Тема 2.3. Защита информации в автоматизированных (информационных) системах

Вариант 1

1. Какой механизм защиты информации обеспечивает проверку подлинности пользователя по предъявленным данным (паролю, биометрии)?

А) Идентификация

Б) Аутентификация

В) Авторизация

Г) Аудит

2. Что из перечисленного относится к мерам защиты на уровне операционной системы?

А) Валидация входных данных

Б) Контроль доступа к файлам и процессам

В) Шифрование сообщений

Г) Использование межсетевого экрана

3. Какое программное средство предназначено для обнаружения и блокировки вредоносного ПО?

А) Антивирус

Б) Межсетевой экран

В) Криптографическое средство

Г) Средство контроля доступа

4. Что является примером программно-аппаратного средства защиты информации?

А) Программный антивирус

Б) Аппаратный модуль безопасности (HSM)

В) Текстовый редактор

Г) Компилятор

5. Какая мера защиты на сетевом уровне предотвращает несанкционированный доступ из внешней сети?

А) VPN

Б) Межсетевой экран

В) Антивирус

Г) Криптографическое средство

6. Что из перечисленного относится к элементам инженерной защиты объекта информатизации?

А) Система видеонаблюдения

Б) Программный антивирус

В) Политика безопасности

Г) Инструкция по работе с документами

7. Какой документ является основным для организационно-распорядительной защиты?

А) Технический паспорт оборудования

Б) Политика безопасности организации

В) Руководство пользователя

Г) Коммерческое предложение

8. Какой этап построения организационно-распорядительной системы является первым?

А) Внедрение мер

Б) Разработка политики безопасности

В) Анализ рисков

Г) Обучение сотрудников

9. Что такое идентификация в системе защиты информации?

А) Присвоение пользователю уникального имени (идентификатора)

Б) Проверка подлинности пользователя по паролю

В) Определение прав доступа к ресурсам

Г) Регистрация всех действий пользователя

10. Какое средство защиты относится к криптографическим?

А) Антивирус

Б) Межсетевой экран

В) Средство электронной цифровой подписи

Г) Система видеонаблюдения

11. Что из перечисленного является прикладной мерой защиты информации?

А) Защита от SQL-инъекций в веб-приложении

Б) Установка пароля на BIOS

В) Сегментация сети

Г) Охрана помещений

12. Какой механизм защиты отвечает за запись всех действий пользователя для последующего анализа?

А) Шифрование

Б) Аутентификация

В) Аудит

Г) Авторизация

13. Какая система технической охраны предназначена для контроля доступа на объект?

А) Охранная сигнализация

Б) Система контроля доступа (СКУД)

В) Пожаротушение

Г) Система видеонаблюдения

14. Работа с кадрами в организационно-распорядительной защите включает:
А) Только прием на работу
Б) Инструктажи, обучение, проверки, увольнение с соблюдением правил ИБ
В) Только увольнение
Г) Только проведение собеседований
15. Что из перечисленного является примером системной меры защиты?
А) Валидация входных данных в веб-форме
Б) Разграничение прав доступа в файловой системе ОС
В) Использование межсетевого экрана
Г) Физическая охрана серверной

Вариант 2
1. Какой механизм защиты определяет права доступа пользователя к ресурсам после успешной проверки подлинности?
А) Идентификация
Б) Аутентификация
В) Авторизация
Г) Аудит
2. Что из перечисленного относится к сетевым мерам защиты?
А) Шифрование диска
Б) Использование VPN
В) Антивирусная проверка
Г) Контроль целостности файлов
3. Какое программное средство предназначено для фильтрации сетевого трафика?
А) Антивирус
Б) Межсетевой экран
В) Криптографическое средство
Г) Средство резервного копирования
4. Что является примером программного средства защиты от утечек данных (DLP)?
А) Антивирус Касперского
Б) Система контроля конфиденциальных документов
В) Межсетевой экран
Г) VPN-клиент
5. Какой механизм защиты обеспечивает конфиденциальность информации при передаче по сети?
А) Аутентификация
Б) Шифрование
В) Аудит
Г) Разграничение доступа
6. Что из перечисленного относится к техническим средствам охраны объекта?
А) Инструкция по работе с документами
Б) Охранный датчик движения
В) Политика паролей
Г) Должностная инструкция

7. Какой документ организационно-распорядительной защиты определяет правила обработки информации ограниченного доступа?

А) Устав предприятия

Б) Инструкция по делопроизводству

В) Приказ о назначении ответственного за ИБ

Г) Политика обработки персональных данных

8. Принцип построения организационно-распорядительной системы «разумная достаточность» означает:

А) Меры должны быть максимально дорогими

Б) Меры должны быть соразмерны рискам и ценности информации

В) Меры должны быть только техническими

Г) Меры не должны учитывать человеческий фактор

9. Что такое авторизация в системе защиты информации?

А) Присвоение идентификатора

Б) Проверка подлинности

В) Определение разрешенных действий пользователя

Г) Запись всех событий

10. Какое средство криптографической защиты используется для подтверждения авторства документа?

А) Симметричное шифрование

Б) Электронная подпись

В) Хеширование пароля

Г) Стеганография

11. Какая мера защиты относится к прикладному уровню?

А) Настройка прав доступа в СУБД

Б) Валидация данных, вводимых в веб-форму

В) Установка межсетевого экрана

Г) Физическая охрана

12. Какой механизм защиты позволяет отследить несанкционированные изменения данных?

А) Шифрование

Б) Контроль целостности

В) Аутентификация

Г) Авторизация

13. Что является элементом инженерной защиты объекта?

А) Программный антивирус

Б) Противопожарная система

В) Политика паролей

Г) Инструкция по работе с конфиденциальными документами

14. Внутриобъектовый режим в организационно-распорядительной защите включает:

А) Регулирование доступа сотрудников на объект и в отдельные зоны

Б) Только охрану периметра

В) Только видеонаблюдение

Г) Только пропускную систему на входе

15. Что из перечисленного является примером общесистемной меры защиты?

А) Ограничение прав доступа к базе данных

Б) Настройка журналирования событий ОС

В) Проверка входящих данных веб-приложения

Г) Использование SSL-сертификата

Ключ к тестам

Вариант 1		Вариант 2	
№ вопроса	Правильный ответ	№ вопроса	Правильный ответ
1	Б	1	В
2	Б	2	Б
3	А	3	Б
4	Б	4	Б
5	Б	5	Б
6	А	6	Б
7	Б	7	Г
8	В	8	Б
9	А	9	В
10	В	10	Б
11	А	11	Б
12	В	12	Б
13	Б	13	Б
14	Б	14	А
15	Б	15	Б

Лабораторные занятия № 5-7:

1. Выбор мер защиты информации для автоматизированного рабочего места
2. Тестирование на проникновение и анализ уязвимостей
3. Выполнение резервного копирования и восстановления данных. Управление доступом к данным

5.2. Критерии оценивания

5.2.1. Критерии оценивания устного ответа

При оценке устного ответа, обучающегося учитывается:

1) полнота и правильность ответа;
2) степень осознанности, понимания изученного;

Отметка «5»: ответ правильный, полный в соответствии с изученным материалом; материал изложен в определенной логической последовательности, литературным языком.

Отметка «4»: ответ правильный, полный в соответствии с изученным материалом; материал изложен в определенной логической последовательности; возможны отдельные затруднения в формулировке выводов.

Отметка «3»: ответ, в котором в основном правильно, но схематично или с отклонениями от последовательности изложения раскрыт материал или неполный, несвязный ответ, изложенный нелогично

Отметка «2»: при ответе обнаружено непонимание обучающимся основного содержания учебного материала, неумение его анализировать допущены существенные ошибки, которые обучающийся не смог исправить при наводящих вопросах преподавателя, отсутствует логика в изложении материала, нет необходимых обобщений и самостоятельной оценки фактов; недостаточно сформированы навыки устной речи.

5.2.2. Критерии оценивания выполнения заданий на лабораторных занятиях

Отметка «5»: работа выполнена полностью и правильно; сделаны правильные выводы.

Отметка «4»: работа выполнена правильно с учетом 1-2 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Отметка «3»: работа выполнена правильно не менее чем на половину или допущены 3-4 существенные ошибки.

Отметка «2»: допущены 5 и более существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя.

Задания к лабораторным занятиям представлены в методических указаниях к лабораторным занятиям по ОП.05 Основы информационной безопасности.

Методы оценки:

– Защита отчетов по выполненному заданию на лабораторных занятиях.

– Интерпретация результатов наблюдений за деятельностью обучающегося на лабораторных занятиях.

5.2.3. Критерии оценивания тестовых заданий

Оценка в баллах	Степень выполнения задания
Неуд.	Выполнено от 0 до 49,9 % предложенных заданий
Удов.	Выполнено от 50 до 69,9% предложенных заданий
Хор.	Выполнено от 70 до 89,9% предложенных заданий
Отл.	Выполнено от 90 до 100% предложенных заданий

5.2.4. Общая классификация ошибок

При оценке знаний и умений учитываются ошибки и недочеты в работе.

Грубыми считаются ошибки:

- незнание определения основных понятий, законов, общепринятых символов обозначений величин;
- неумение выделить в ответе главное;
- обобщить результаты изучения;
- неумение применить знания для решения задач;
- неумение использовать полученные данные для выводов;
- неумение пользоваться первоисточниками, учебником, справочником;
- нарушение техники безопасности, небрежное отношение к оборудованию

Негрубыми считаются ошибки:

- неточность формулировок, определений, понятий, законов, вызванная неполнотой охвата основных признаков определяемого понятия или заменой 1-3 из этих признаков второстепенными;
- ошибки, вызванные несоблюдением условий проведения лабораторных занятий;
- недостаточно продуманный план устного ответа (нарушение логики изложения, подмена отдельных основных вопросов второстепенными);
- нерациональные методы работы со справочной литературой;
- неумение выполнять лабораторные задания в общем виде.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ОП.05 Основы информационной безопасности

Промежуточная аттестация по учебной дисциплине ОП.05 Основы информационной безопасности проводится в форме экзамена.

6.1. Вопросы к экзамену по учебной дисциплине

1. Дайте определение понятиям «информация», «сообщение» и «информационный процесс» в контексте информационной безопасности. Какие объекты (информация, системы, каналы связи, люди) подлежат защите и почему?
2. Охарактеризуйте место информационной безопасности в системе национальной безопасности Российской Федерации. Какие стратегические документы определяют приоритеты в этой области?
3. Раскройте понятие «угроза информации». Из каких обязательных элементов она состоит? Приведите классификацию угроз по источникам возникновения и по виду воздействия на информацию.
4. Что понимается под «риском информационной безопасности»? Как выполняется качественная и количественная оценка рисков? Приведите пример расчета уровня риска.
5. Перечислите примеры преступлений в сфере информации и информационных технологий, известных из судебной практики. Предложите их классификацию по объекту посягательства и способу совершения.
6. В чем сущность функционирования системы защиты информации? Какие цели и задачи она решает? Опишите комплексный подход к построению системы защиты.
7. Что понимается под «опасной информацией» и какую угрозу она представляет для человека? Какие механизмы защиты от опасной информации существуют на уровне государства, общества и личности?
8. Опишите проблему «неинформированности в области информационной безопасности». Какими последствиями она грозит и какие меры могут быть приняты для повышения уровня осведомленности?
9. Раскройте содержание трех базовых свойств информации: целостность, доступность и конфиденциальность. Приведите примеры ситуаций, когда каждое из этих свойств нарушается.
10. Опишите классификацию информации по видам тайны и степеням конфиденциальности. В чем различие между государственной тайной и конфиденциальной информацией? Приведите примеры.
11. Дайте определения понятиям «государственная тайна» и «конфиденциальная информация». Каков правовой режим доступа к этим категориям и ответственность за их разглашение?
12. Опишите жизненный цикл конфиденциальной информации от момента ее создания до уничтожения. Какие меры защиты должны применяться на каждом этапе?
13. Сформулируйте основные цели и задачи защиты информации. Как они соотносятся с обеспечением трех базовых свойств информации (конфиденциальность, целостность, доступность)?

14. Дайте определения основным понятиям в области защиты информации: «объект защиты», «источник угроз», «уязвимость», «средство защиты», «политика безопасности». Как эти понятия взаимосвязаны?
15. Перечислите основные элементы процесса менеджмента информационной безопасности (идентификация активов, оценка рисков, выбор мер защиты, внедрение, мониторинг, аудит). Опишите, как они образуют непрерывный цикл управления.
16. Опишите модель интеграции информационной безопасности в основную деятельность организации. На каких уровнях (стратегическом, тактическом, операционном) должна быть реализована безопасность?
17. Раскройте понятие «политика безопасности». Какие виды политик безопасности существуют (базовая, частные, оперативные)? Из каких разделов должна состоять политика безопасности организации?
18. Опишите системную классификацию угроз безопасности информации: по природе возникновения, по степени преднамеренности, по отношению к объекту, по стадии воздействия.
19. Перечислите основные каналы несанкционированного доступа (НСД) к информации. Разделите их на технические и организационные. Для каждого канала укажите пример реализации НСД.
20. В чем суть методов несанкционированного доступа: перехват (пассивный и активный), подслушивание, внедрение программных закладок, использование уязвимостей ПО? Приведите примеры защитных мер против каждого метода.
21. Опишите количественные методы оценки уязвимости информации (например, CVSS). Как оценивается степень тяжести уязвимости и как это влияет на приоритизацию мер защиты?
22. Опишите качественные методы оценки уязвимости (например, метод экспертных оценок, матрицы рисков). В чем преимущества и ограничения качественного подхода по сравнению с количественным?
23. Раскройте содержание основных методик определения требований к защите информации, применяемых в РФ (методика ФСТЭК, ГОСТ Р ИСО/МЭК 27001, подходы на основе оценки рисков). В чем их сходства и различия?
24. Назовите факторы, влияющие на требуемый уровень защиты информации, и обоснуйте их значимость. Какие из факторов являются внешними, а какие – внутренними?
25. Перечислите и раскройте основные принципы защиты информации: законность, комплексность, непрерывность, экономическая целесообразность, разумная достаточность. В чем заключается принцип «защита в глубину» (defense in depth)?
26. Опишите типовую организационную структуру системы защиты информации на предприятии. Какие подразделения и должностные лица входят в СУИБ и как распределяются функции между ними?
27. Перечислите основные федеральные законы Российской Федерации, регулирующие отношения в сфере защиты информации (ФЗ № 149, 152, 187, 63). Раскройте содержание каждого из них.
28. Опишите содержание и назначение национального стандарта РФ ГОСТ Р ИСО/МЭК 27001-2021. Для каких организаций он предназначен и какие требования устанавливает? В чем различие между стандартами 27001, 27002 и 27005?

29. Опишите систему сертификации средств защиты информации, созданную ФСТЭК России. Каковы ее цели, состав участников и нормативная основа? Какие объекты подлежат сертификации?
30. Перечислите виды мер защиты информации: организационные (административные), правовые, технические, физические, программно-аппаратные. Для каждого вида приведите по два примера конкретных мер и укажите, какие угрозы они предотвращают.

6.2. Критерии оценивания ответов на экзамене

– оценка **«отлично»**, если студент обладает глубокими и прочными знаниями программного материала; при ответе на вопросы продемонстрировал исчерпывающее, последовательное и логически стройное изложение; правильно сформулировал понятия и закономерности по вопросам; сделал вывод по излагаемому материалу;

– оценка **«хорошо»**, если студент обладает достаточно полным знанием программного материала; его ответ представляет грамотное изложение учебного материала; но имеются существенные неточности в формулировании понятий и закономерностей по вопросам; не полностью сделаны выводы по излагаемому материалу;

– оценка **«удовлетворительно»**, если студент имеет общие знания основного материала без усвоения некоторых существенных положений; формулирует основные понятия с некоторой неточностью; затрудняется в приведении примеров, подтверждающих теоретические положения;

– оценка **«неудовлетворительно»**, если студент не знает значительную часть программного материала; допустил существенные ошибки в процессе изложения; не умеет выделить главное и сделать вывод; приводит ошибочные определения; ни один вопрос не рассмотрен до конца, наводящие вопросы не помогают.

–

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Основные печатные издания и/или электронные издания

1. Внуков, А. А. Основы информационной безопасности: 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

2. Казарин, О. В. Основы информационной безопасности: 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 (дата обращения: 15.05.2025).978-5-8199-0754-2. - Текст: электронный. - URL: https://znanium.com/catalog/product/1910870