ЧОУ ВО «Тольяттинская академия управления»

Кафедра прикладной информатики и высшей математики

Б1.В.10

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА)

Учебная дисциплина	*Информационная безопасность*
По направлению подготовки	*09.03.03*
	«Прикладная информатика»
Профиль (программа бакалавриата)	*«Прикладная информатика в цифровой экономике»*
Форма обучения	*Очная*

Оценочные материалы (средства) дисциплины рассмотрены (актуализированы) и утверждены на заседании кафедры прикладной информатики и высшей математики

Протокол заседания № 10 от «25» мая 2026 г.

Заведующий кафедрой Стрекалова Наталья Борисовна

2024

Оглавление

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ И ЭТАПЫ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Оценочные материалы (средства) сформированы в соответствии с ФГОС ВО - бакалавриат по направлению подготовки 09.03.03 «Прикладная информатика», утвержденный приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 922 с изменениями и дополнениями от 26.11.2020, 08.02.2021). В соответствии с матрицей компетенций основной профессиональной образовательной программы «Прикладная информатика в цифровой экономике» (уровень бакалавриата) в процессе обучения по дисциплине «Информационная безопасность» происходит формирование закрепленных за дисциплиной компетенций обучающихся. Оценка сформированности компетенций на каждом этапе обучения происходит через оценку планируемых результатов обучения по дисциплине (знаний, умений, навыков).

Результаты освоения образовательной программы (компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения по дисциплине	Этапы формирования компетенции (семестры и темы)	Оценочное средство
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	**УК-8.3. -** Обеспечивает персональную информационную безопасность в цифровой среде, в том числе средствами криптографии	**Знать:** - нормативно-правовые основы информационной безопасности в Российской Федерации; - международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности; **Уметь:** - разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы **Владеть:** - навыками документирования инцидентов и процессов информационной безопасности.	Тема 2. Стандарты информационной безопасности Тема 10. Организационное управление инцидентами информационной безопасностью	- устный опрос по теме 2 -проверка выполнения практических работ по теме 10 - выполнение курсовой работы - устный ответ на зачете - решение практического задания на зачете -
ПК-1 Способен выявлять информационные потребности пользователей и составлять	**ПК-1.1**. Проводит обследование организаций, выявляет информационные потребности пользователей, используя	**Знать:** - требования безопасности к информационным системам; **Уметь:** - проводить анализ предметной области и	**6 семестр** Тема 1. Введение в информационную безопасность, уровни ее обеспечения Тема 3.	- устный опрос по темам 1,3 - выполнение курсовой работы - устный

техническое задание на разработку информационной системы	цифровые инструменты и облачные решения для сбора данных	выявлять информационные угрозы; **Владеть:** - навыками анализа информационных рисков;	Информационные угрозы	ответ на зачете - решение практического задания на зачете
	ПК-1.2. Составляет техническое задание на разработку информационной системы	**Знать:** - программно-аппаратное, организационное, инженерно-техническое обеспечение защиты информации; **Уметь:** - разрабатывать концептуальное решение по обеспечению защиты информации в разрабатываемых системах; **Владеть:** - навыками оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями;	**6 семестр** Тема 5. Программно-аппаратное обеспечение информационной безопасности Тема 7. Организационное обеспечение защиты информации Тема 8. Инженерно-техническое обеспечение защиты информации Тема 9. Системы управления информационной безопасностью	- устный опрос по темам 6, 7, 9 - практическая работа по темам 5, 8 - выполнение курсовой работы - устный ответ на зачете - решение практического задания на зачете
ПК-3 Способен разрабатывать информационные системы	**ПК-3.3**. Обеспечивает информационную безопасность разрабатываемых информационных систем, в том числе общедоступными средствами мониторинга и выявления потенциальных информационных угроз	**Знать:** - способы и методы обеспечения информационной безопасности в компьютерных сетях, удаленные угрозы и атаки, основы криптографической защиты информации, способы управления инцидентами информационной безопасности; **Уметь:** - определять и обосновывать организационно-технические мероприятия по защите информации в информационных системах; **Владеть:** - навыками использования инструментальных средств защиты информации в ходе	**6 семестр** Тема 1. Введение в информационную безопасность, уровни ее обеспечения Тема 4. Информационная безопасность в компьютерных сетях Тема 6. Криптографическая защита информации Тема 9. Системы управления информационной безопасностью Тема 10. Организационное управление инцидентами информационной безопасностью	**6 семестр** - устный опрос по темам 1,4,6,9 - практическая работа по теме 10 - выполнение курсовой работы - устный ответ на зачете - решение практического задания на зачете

		профессиональной деятельности; - навыками управления инцидентами информационной безопасности;		
ПК-4 Способен управлять процессами создания информационных систем	**ПК-4.2.** Применяет актуальные нормативные документы и стандарты при создании информационных систем, используя общедоступные справочно-правовые системы и профессиональные базы данных сферы ИТ	**Знать:** - нормативно-правовые основы информационной безопасности в Российской Федерации; - международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности; **Уметь:** - разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы **Владеть:** - навыками документирования инцидентов и процессов информационной безопасности;	**6 семестр** Тема 2. Стандарты информационной безопасности Тема 9. Системы управления информационной безопасностью	- устный опрос по теме 2, 9 - выполнение курсовой работы - устный ответ на зачете - решение практического задания на зачете
ПК-5 Способен обеспечивать качество разработки информационных систем	**ПК-5.2** Проводит оценку рисков работы информационных систем в условиях цифровизации бизнеса и применения сквозных цифровых и отраслевых технологий	**Знать:** - возможные риски, возникающие при работе с информационными системами в организации; **Уметь:** - применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем; **Владеть:** - навыками анализа рисков работы информационных систем.	**6 семестр** Тема 3. Информационные угрозы	- устный опрос по теме 3

2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ, ОБЕСПЕЧИВАЮЩИХ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Устные опросы

Вопросы для проведения устного опроса
по теме «Введение в информационную безопасность, уровни ее обеспечения»

1. Теория защиты информации. Основные направления.
2. Обеспечение информационной безопасности и направления защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная).
4. Требования к системе защиты информации.
5. Угрозы информации.
6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки появления угроз.
9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.

Вопросы для *проведения устного опроса*
по теме «Стандарты информационной безопасности»

1. Общая модель процесса нарушения физической целостности информации.
2. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
3. Методологические подходы к оценке уязвимости информации.
4. Модель защиты системы с полным перекрытием.
5. Рекомендации по использованию моделей оценки уязвимости информации.
6. Допущения в моделях оценки уязвимости информации.
7. Методы определения требований к защите информации.
8. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
9. Классификация требований к средствам защиты информации.
10. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
11. Требования к защите, обуславливаемые видом защищаемой информации.
12. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации.
13. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США». Основные положения.
14. Руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 году. Часть 1.
15. Классы защищенности средств вычислительной техники от несанкционированного доступа.

Вопросы для проведения устного опроса
по теме «Информационные угрозы»

1. Дайте определение понятий «угроза», «уязвимость» и «атака».
2. Какие классификационные схемы угроз ИБ вам известны?
3. Перечислите источники угроз ИБ.
4. Назовите каналы проникновения в автоматизированную систему и утечки информации.
5. Какие факторы лежат в основе формирования модели нарушителя?
6. Каковы цели разработки моделей угроз и нарушителей?
7. В чем разница между нарушителем и злоумышленником?
8. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты.
9. Методы формирования функций защиты.
10. События, возникающие при формировании функций защиты.

Вопросы для проведения устного опроса
по теме «Информационная безопасность в компьютерных сетях»

1. В чем заключается основная причина предоставления служб пользователям?
2. Почему системы, к которым осуществляется доступ из внешней среды, не могут пользоваться полным доверием?
3. Почему протокол ICMP является важным компонентом сети?
4. Скольким внутренним системам разрешается использовать NTP в интернете?
5. Можно ли рассматривать использование SSH как реализацию VPN?
6. Почему пользовательские VPN требуют строгой аутентификации?
7. Может ли шифрование полностью защитить данные, передаваемые через VPN.
8. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
9. Является ли один из типов межсетевых экранов более безопасным, нежели другой?
10. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
11. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?

Вопросы для проведения устного опроса
по теме «Программно-аппаратное обеспечение информационной безопасности»

1. Понятие угрозы безопасности компьютерной системы. Методы «взлома» компьютерных систем.
2. Защита компьютерной системы от «взлома». Программные закладки.
3. Методы уничтожения информации, хранимой на энергонезависимых носителях. Уровни степеней надежности.
4. Защита программного обеспечения. Превентивные меры защиты.
5. Защита программного обеспечения. Средства собственной защиты.
6. Защита программного обеспечения. Средства защиты в составе вычислительной системы.
7. Защита программного обеспечения. Средства защиты с запросом информации.
8. Защита программного обеспечения. Средства активной защиты.
9. Защита программного обеспечения. Средства пассивной защиты.

10. Технология защиты информации на основе: электронных ключей, смарт-карт, персональных идентификаторов.
11. Принципы и методы создания защищенной операционной системы.
12. Цели и средства защиты информации. Типичный набор функциональных подсистем.
13. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.

Вопросы для проведения устного опроса
по теме «Криптографическая защита информации»

1. Что является предметом науки Криптография
2. Первая практическая реализация криптографии с открытым ключом
3. Использование в криптографии модели открытого текста, учитывающие зависимость букв текста от предыдущих букв.
4. В чем состоит принципиальное отличие нового стандарта ГОСТ Р 34.10 – 2001 на алгоритм формирования и проверки ЭЦП от старого ГОСТ Р 34.10 – 1994.
5. Основной принцип Кергоффса.
6. Что понимается под криптографическим протоколом
7. В чем состоит криптографическая задача обеспечения я целостности.
8. Методы с целью обеспечения аутентификации

Вопросы для проведения устного опроса
по теме «Организационное обеспечение защиты информации»

1. Модель защиты системы с полным перекрытием.
2. Рекомендации по использованию моделей оценки уязвимости информации.
3. Допущения в моделях оценки уязвимости информации.
4. Методы определения требований к защите информации.
5. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
6. Классификация требований к средствам защиты информации.
7. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
8. Требования к защите, обуславливаемые видом защищаемой информации.
9. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации.

Вопросы для проведения устного опроса
по теме «Инженерно-техническое обеспечение защиты информации»

1. Стратегии защиты информации.
2. Способы и средства защиты информации.
3. Способы «абсолютной системы защиты».
4. Архитектура систем защиты информации. Требования.
5. Общеметодологических принципов архитектуры системы защиты информации.
6. Построение средств защиты информации.
7. Ядро системы защиты.
8. Семирубежная модель защиты.

Вопросы для проведения устного опроса

по теме «Системы управления информационной безопасностью»

1. Анализ рисков
2. Политика информационной безопасности
3. Концепция информационной безопасности
4. Доступ в информационные системы. Политика доступа. Физический доступ.
5. Построение сети. Удаленный доступ.
6. Инциденты. Активы, что требуется защитить.
7. Меры безопасности в контексте ISO 27001
8. Эффективность применяемых методов обеспечения безопасности
9. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
10. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.

Вопросы для проведения устного опроса
по теме «Организационное управление инцидентами информационной безопасностью»

1. Понятие инцидента информационной безопасности
2. Место управления инцидентами в общей системе информационной безопасности
3. Особенности управления событиями безопасности
4. Процедура управления информационной безопасности
5. Устранение причин и последствий события, его расследование
6. Превентивные меры, изменения стандартов и ликвидация последствий

Критерии оценивая устного опроса:

- оценка «*отлично*» выставляется студенту, если он ответил развернуто на один из заданных вопросов, активно дополнял ответы других студентов или задавал им дополнительные вопросы;
- оценка «*хорошо*» выставляется студенту, если он ответил развернуто на один из заданных вопросов или ответил кратко на ряд вопросов;
- оценка «*удовлетворительно*» выставляется студенту, если он кратко ответил на один из задаваемых вопросов или просто дополнял ответы других студентов, задавал им дополнительные вопросы;
- оценка «*неудовлетворительно*» выставляется студенту, если он не смог ответить правильно на заданный вопрос, либо не отвечал на вопросы и не участвовал в их обсуждении.

Подготовка и выступление с докладами

Темы для подготовки докладов
по теме «Программно-аппаратное обеспечение информационной безопасности»

1. Анализ российского рынка средств обеспечения информационной безопасности локальных, корпоративных и беспроводных сетей.
2. Анализ зарубежного рынка средств обеспечения информационной безопасности б локальных, корпоративных и беспроводных сетей.
3. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.
4. Средства обеспечения информационной безопасности банков данных.
5. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.

6. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.

Темы для подготовки докладов
по теме «Организационное управление инцидентами информационной безопасностью»

1. Комплексная защита информации предприятия, организации.
2. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему
3. Концепция политики безопасности и систем контроля доступа для локальных вычислительных сетей.
4. Модель системы управления информационной безопасностью в условиях неопределенности воздействия
5. Организация защиты персональных данных в организации
6. Организация противодействия угрозам безопасности персонала организации.
7. Основные направления, принципы и методы обеспечения информационной безопасности

Критерии оценивая докладов и выступлений:

- оценка «*отлично*» выставляется студенту, если доклад полностью раскрывает тему, структура доклада логично выстроена, обучающийся хорошо ориентируется в материале и текст доклада, в основном, рассказывает (а не читает), отвечает на дополнительные вопросы; сопровождающая доклад презентация выполнена в соответствии с требованиями и дополняет доклад, докладчик уложился в регламент, текст доклада оформлен в соответствии с требованиями;
- оценка «*хорошо*» выставляется студенту, если доклад в целом раскрывает тему, но остаются не освещенные стороны вопросы, не на все дополнительные вопросы обучающийся может дать ответ; структура доклада логично выстроена, текст доклада обучающийся, в основном, рассказывает (а не читает); презентация выполнена в соответствии с требованиями, но есть ряд замечаний по ее оформлению, доклад и презентация дополняют друг друга, докладчик уложился в регламент;
- оценка «*удовлетворительно*» выставляется студенту, если его доклад не раскрывает тему в достаточной мере, не отвечает на дополнительные вопросы; к оформлении доклада много замечаний; презентация выполнена не по требованиям, доклад дублирует презентацию, а не дополняет ее, студент не укладывается в регламент или наоборот;
- оценка «*неудовлетворительно*» выставляется студенту, если доклад отсутствует или доклад совсем не раскрывает тему, не оформлен по требованиям; отсутствует презентация или презентация не соответствует более половины требованиям.

Практические работы

Практическое задание по теме «Инженерно-техническое обеспечение защиты информации»

Индивидуальные задания состоят из двух частей, взаимосвязанных друг с другом по объекту защиты информации. Объект необходимо исследовать таким образом, чтобы можно было применить все основные элементы защиты информации, т.е. определяя местоположение, внешние и внутренние характеристики с учетом естественных

событий. Однако уточнение характеристик не должно приводить к абсолютной конкретизации объекта, т.к. в этом случае будет затруднен анализ объекта.

Первое задание

Для выполнения первой части необходимо для выбранного определенного объекта защиты информации необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

1. виды угроз;
2. характер происхождения угроз;
3. классы каналов несанкционированного получения информации;
4. источники появления угроз;
5. причины нарушения целостности информации;
6. потенциально возможные злоумышленных действий;
7. определить класс защиты информации.

Второе задание

Для выполнения второго задания предложить анализ увеличения защищенности объекта защиты информации по следующим разделам:

1. определить требования к защите информации;
2. классифицировать автоматизированную систему;
3. определить факторы, влияющие на требуемый уровень защиты информации;
4. выбрать или разработать способы и средства защиты информации;
5. построить архитектуру систем защиты информации;
6. сформулировать рекомендации по увеличению уровня защищенности.

Наименование объекта защиты информации:

1. Одиночно стоящий компьютер в бухгалтерии.
2. Сервер.
3. Почтовый сервер.
4. Веб-сервер.
5. Компьютерная сеть Академии.
6. Одноранговая локальная сеть без выхода в Интернет.
7. Одноранговая локальная сеть с выходом в Интернет.
8. Сеть с выделенным сервером без выхода в Интернет.
9. Сеть с выделенным сервером с выхода в Интернет.
10. Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.
11. Телефонная сеть.
12. Средства телекоммуникации (радиотелефоны, мобильные телефоны).
13. Банковские операции (внесение денег на счет и снятие).
14. Операции с банковскими пластиковыми карточками.
15. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
16. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.
17. Материалы для служебного пользования на твердых носителях в производстве.
18. Материалы для служебного пользования на твердых носителях на закрытом предприятии.
19. Материалы для служебного пользования на твердых носителях в архиве.
20. Материалы для служебного пользования на твердых носителях в налоговой инспекции.

21. Комната для переговоров по сделкам на охраняемой территории.
22. Комната для переговоров по сделкам на неохраняемой территории.
23. Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).
24. Судебные материалы (твердая копия).
25. Паспортный стол РОВД.
26. Материалы по владельцам автомобилей (твердая копия, фотографии, электронные носители и др.).
27. Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.).
28. Сведения по тоталитарным сектам и другим общественно-вредным организациям.
29. Сведения по общественно-полезным организациям (красный крест и др.).
30. Партийные списки и руководящие документы.

Критерии оценивая:

- оценка «*отлично*» выставляется студенту, если задание выполнено в полном объеме, студент хорошо ориентируется в технологии разработки инженерно-технического обеспечения защиты информации;
- оценка «*хорошо*» выставляется студенту, если он выполнил задание почти в полном объеме, допускает небольшие «проектно-технологические» ошибки в разработке инженерно-технического обеспечения защиты информации;
- оценка «*удовлетворительно*» выставляется студенту, если он выполнил первое задание;
- оценка «*неудовлетворительно*» выставляется студенту, если он выполнил менее половины первого задания.

3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

ОЦЕНКА ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ ОБУЧАЮЩИХСЯ
ПО РЕЗУЛЬТАТАМ ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Целью курсовой работы по информационной безопасности является систематизация, закрепление и углубление теоретических знаний студентов о методологии и методике аудита информационной безопасности на предприятии, определения исходных данных для проектирования системы защиты информации и собственно проектирования систем защиты информации, а также выработка у них навыков решения практических задач по защите информации.

Задание на курсовую работу: для выбранной предметной области (предприятия, организации) провести анализ защищенности объекта защиты информации по ряду критериев (виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленных действий; определить класс защиты информации) и предложить комплекс мероприятий для увеличения защищенности объекта.

Примерный перечень тем курсовой работы

1. Материалы для служебного пользования на твердых носителях на закрытом предприятии.
2. Материалы для служебного пользования на твердых носителях в архиве.
3. Материалы для служебного пользования на твердых носителях в налоговой инспекции.

4. Комната для переговоров по сделкам на охраняемой территории.
5. Комната для переговоров по сделкам на неохраняемой территории.
6. Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).
7. Судебные материалы (твердая копия).
8. Паспортный стол РОВД.
9. Материалы по владельцам автомобилей (твердая копия, фотографии, электронные носители и др.).
10. Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.).
11. Сведения по тоталитарным сектам и другим общественно-вредным организациям.
12. Сведения по общественно-полезным организациям (красный крест и др.).
13. Партийные списки и руководящие документы.

Структура курсовой работы

1. титульный лист;
2. содержание;
3. введение (2 стр.);
4. основная часть;
5. заключение (3 стр.);
6. список использованных источников;
7. приложения (по тексту изложения работы обязательно должны быть ссылки на номера приложений)

ОЦЕНКА ЗНАНИЙ ПО РЕЗУЛЬТАТАМ ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Примерные вопросы на защите курсовой работы

УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

УК-8.3. - Обеспечивает персональную информационную безопасность в цифровой среде, в том числе средствами криптографии

Обучающийся знает: нормативно-правовые основы информационной безопасности в Российской Федерации, а также международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности

Оценка достижения обучающимся запланированного результата обучения осуществляется во время защиты курсовой работы и ответов на вопросы:

1. Перечислите все ресурсы, на которых может храниться ценная для компании информация? отделы, к которым относятся ресурсы?

ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы

ПК-1.1. Проводит обследование организаций, выявляет информационные потребности пользователей, используя цифровые инструменты и облачные решения для сбора данных

Обучающийся знает: требования безопасности к информационным системам

Оценка достижения обучающимся запланированного результата обучения осуществляется во время защиты курсовой работы и ответов на вопросы:

1. В каких бизнес-процессах компании обрабатывается информация?

ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы

ПК-1.2. Составляет техническое задание на разработку информационной системы

Обучающийся знает: программно-аппаратное, организационное, инженерно-техническое обеспечение защиты информации.

Оценка достижения обучающимся запланированного результата обучения осуществляется во время защиты курсовой работы и ответов на вопросы:

1. Каковы группы пользователей, имеющих доступ к ценной информации?
2. Какие требования к средствам защиты информации можно предъявить для выбранной вами предметной области?

ПК-3 Способен разрабатывать информационные системы

ПК-3.3. Обеспечивает информационную безопасность разрабатываемых информационных систем, в том числе общедоступными средствами мониторинга и выявления потенциальных информационных угроз

Обучающийся знает: способы и методы обеспечения информационной безопасности в компьютерных сетях, удаленные угрозы и атаки, основы криптографической защиты информации, способы управления инцидентами информационной безопасности.

Оценка достижения обучающимся запланированного результата обучения осуществляется во время защиты курсовой работы и ответов на вопросы:

1. Какие риски/информационные угрозы были выявлены при анализе ресурсов ИТ-инфраструктуры?
2. Какие средства защиты информации предлагаете вы для выбранной предметной области?

ПК-4 Способен управлять процессами создания информационных систем

ПК-4.2. Применяет актуальные нормативные документы и стандарты при создании информационных систем, используя общедоступные справочно-правовые системы и профессиональные базы данных сферы ИТ

Обучающийся знает: нормативно-правовые основы информационной безопасности в Российской Федерации; международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности

Оценка достижения обучающимся запланированного результата обучения осуществляется во время защиты курсовой работы и ответов на вопросы:

1. Какая информация является ценной для выбранной организации?
2. Какие нормативные документы/стандарты вы анализировали для выполнения курсовой работы? Каковы основные положения некоторых из них?

ПК-5 Способен обеспечивать качество разработки информационных систем

ПК-5.2 Проводит оценку рисков работы информационных систем в условиях цифровизации бизнеса и применения сквозных цифровых и отраслевых технологий

Обучающийся знает: возможные риски, возникающие при работе с информационными системами в организации

Оценка достижения обучающимся запланированного результата обучения осуществляется во время защиты курсовой работы и ответов на вопросы:

1. Какие подсистемы вы выделяете в интегрированной архитектуре систем ИБ для выбранной предметной области?
2. Перечислите ущерб для каждого вида ценной информации по трем видам угроз: внешние, внутренние, комбинированные.

ОЦЕНКА УМЕНИЙ И НАВЫКОВ ПО РЕЗУЛЬТАТАМ ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

УК-8.3. - Обеспечивает персональную информационную безопасность в цифровой среде, в том числе средствами криптографии

Обучающийся умеет: разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы

Обучающийся владеет: навыками документирования инцидентов и процессов информационной безопасности.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения раздела курсовой работы: глава 1 основной части (в части описания общей характеристики предприятия/организации, предпроектного обследования системы защиты информации всей компании (если предприятие небольшое) или информационной безопасности отдельных ИТ-систем (сетей передачи данных, вычислительных систем и систем хранения данных, и др.) для крупной компании)

ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы

ПК-1.1. Проводит обследование организаций, выявляет информационные потребности пользователей, используя цифровые инструменты и облачные решения для сбора данных

Обучающийся умеет: проводить анализ предметной области и выявлять угрозы информационной безопасности

Обучающийся владеет: навыками проведения аудита информационной безопасности и анализа рисков информационной безопасности.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения раздела курсовой работы: глава 1 основной части (в части описания общей характеристики предприятия/организации, предпроектного обследования системы защиты информации всей компании (если предприятие небольшое) или информационной безопасности отдельных ИТ-систем (сетей передачи данных, вычислительных систем и систем хранения данных, и др.) для крупной компании)

ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы

ПК-1.2. Составляет техническое задание на разработку информационной системы

Обучающийся умеет: разрабатывать концептуальное решение по обеспечению защиты информации в разрабатываемых системах.

Обучающийся владеет: навыками оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения раздела курсовой работы: глава 1 основной части (в части описания общей характеристики предприятия/организации, предпроектного обследования системы защиты информации всей компании (если предприятие небольшое) или информационной безопасности отдельных ИТ-систем (сетей передачи данных, вычислительных систем и систем хранения данных, и др.) для крупной компании)

ПК-3 Способен разрабатывать информационные системы

ПК-3.3. Обеспечивает информационную безопасность разрабатываемых информационных систем, в том числе общедоступными средствами мониторинга и выявления потенциальных информационных угроз

Обучающийся умеет: определять и обосновывать организационно-технические мероприятия по защите информации в информационных системах

Обучающийся владеет: навыками использования инструментальных средств защиты информации в ходе профессиональной деятельности, навыками управления инцидентами информационной безопасности

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения раздела курсовой работы: глава 2 основной части, посвященной проектированию архитектуры системы информационной безопасности.

ПК-4 Способен управлять процессами создания информационных систем

ПК-4.2. Применяет актуальные нормативные документы и стандарты при создании информационных систем, используя общедоступные справочно-правовые системы и профессиональные базы данных сферы ИТ

Обучающийся умеет: разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы

Обучающийся владеет: навыками документирования инцидентов и процессов информационной безопасности

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения раздела курсовой работы: введение (в котором обосновывается актуальность выбранной темы), глава 1 основной части – в которой рассматриваются теоретические аспекты обеспечения информационной безопасности для выбранной предметной области, обосновывается актуальность следования тем или иным стандартам обеспечения информационной безопасности для нее.

ПК-5 Способен обеспечивать качество разработки информационных систем

ПК-5.2 Проводит оценку рисков работы информационных систем в условиях цифровизации бизнеса и применения сквозных цифровых и отраслевых технологий

Обучающийся умеет: применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем

Обучающийся владеет: навыками анализа рисков работы информационных систем.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения раздела курсовой работы: глава 1 основной части (в части анализа возможных рисков, возникающих на предприятия/организации, предпроектного обследования системы защиты информации всей компании (если предприятие небольшое) или информационной безопасности отдельных ИТ-систем (сетей передачи данных, вычислительных систем и систем хранения данных, и др.) для крупной компании)

ОЦЕНКА ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ ОБУЧАЮЩИХСЯ НА ЗАЧЕТЕ

ОЦЕНКА ЗНАНИЙ ОБУЧАЮЩИХСЯ НА ЗАЧЕТЕ

Список вопросов для подготовки к зачету

УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

УК-8.3. - Обеспечивает персональную информационную безопасность в цифровой среде, в том числе средствами криптографии

Обучающийся знает: нормативно-правовые основы информационной безопасности в Российской Федерации, а также международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности

1. Общая модель процесса нарушения физической целостности информации.

2. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
3. Методологические подходы к оценке уязвимости информации.
4. Модель защиты системы с полным перекрытием.
5. Рекомендации по использованию моделей оценки уязвимости информации.
6. Допущения в моделях оценки уязвимости информации.

ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы
ПК-1.1. Проводит обследование организаций, выявляет информационные потребности пользователей, используя цифровые инструменты и облачные решения для сбора данных
Обучающийся знает: требования безопасности к информационным системам.
Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам его участия в устных опросах и ответа на зачете.

1. Методы определения требований к защите информации.
2. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
3. Классификация требований к средствам защиты информации.
4. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
5. Требования к защите, обуславливаемые видом защищаемой информации.
6. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации.
7. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США». Основные положения.

ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы
ПК-1.2. Составляет техническое задание на разработку информационной системы
Обучающийся знает: программно-аппаратное, организационное, инженерно-техническое обеспечение защиты информации.
Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам его участия в устных опросах и ответа на зачете.

1. Руководящем документе Гостехкомиссии России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 году. Часть 1.
2. Классы защищенности средств вычислительной техники от несанкционированного доступа.
3. Что является предметом науки Криптография
4. Первая практическая реализация криптографии с открытым ключом
5. Использование в криптографии модели открытого текста, учитывающие зависимость букв текста от предыдущих букв.
6. В чем состоит принципиальное отличие нового стандарта ГОСТ Р 34.10 – 2001 на алгоритм формирования и проверки ЭЦП от старого ГОСТ Р 34.10 – 1994.
7. Основной принцип Кергоффса.
8. Что понимается под криптографическим протоколом
9. В чем состоит криптографическая задача обеспечения я целостности.
10. Методы с целью обеспечения аутентификации
11. Меры безопасности в контексте ISO 27001
12. Эффективность применяемых методов обеспечения безопасности

13. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
14. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.

ПК-3 Способен разрабатывать информационные системы
ПК-3.3. Обеспечивает информационную безопасность разрабатываемых информационных систем, в том числе общедоступными средствами мониторинга и выявления потенциальных информационных угроз
Обучающийся знает: способы и методы обеспечения информационной безопасности в компьютерных сетях, удаленные угрозы и атаки, основы криптографической защиты информации, способы управления инцидентами информационной безопасности.
Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам его участия в устных опросах и ответа на зачете

1. Стратегии защиты информации.
2. Способы и средства защиты информации.
3. Способы «абсолютной системы защиты».
4. Архитектура систем защиты информации. Требования.
5. Общеметодологических принципов архитектуры системы защиты информации.
6. Построение средств защиты информации.
7. Ядро системы защиты.
8. Семирубежная модель защиты.
9. Процедура управления информационной безопасности
10. Устранение причин и последствий события, его расследование
11. Превентивные меры, изменения стандартов и ликвидация последствий

ПК-4 Способен управлять процессами создания информационных систем
ПК-4.2. Применяет актуальные нормативные документы и стандарты при создании информационных систем, используя общедоступные справочно-правовые системы и профессиональные базы данных сферы ИТ

Обучающийся знает: нормативно-правовые основы информационной безопасности в Российской Федерации; международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности.
Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам его участия в устных опросах и ответа на зачете.

1. В чем заключается основная причина предоставления служб пользователям?
2. Почему системы, к которым осуществляется доступ из внешней среды, не могут пользоваться полным доверием?
3. Почему протокол ICMP является важным компонентом сети?
4. Скольким внутренним системам разрешается использовать NTP в интернете?
5. Можно ли рассматривать использование SSH как реализацию VPN?
6. Почему пользовательские VPN требуют строгой аутентификации?
7. Может ли шифрование полностью защитить данные, передаваемые через VPN.
8. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
9. Является ли один из типов межсетевых экранов более безопасным, нежели другой?
10. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
11. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?

12. Понятие угрозы безопасности компьютерной системы. Методы «взлома» компьютерных систем.
13. Защита компьютерной системы от «взлома». Программные закладки.
14. Методы уничтожения информации, хранимой на энергонезависимых носителях. Уровни степеней надежности.
15. Защита программного обеспечения. Превентивные меры защиты.
16. Защита программного обеспечения. Средства собственной защиты.
17. Защита программного обеспечения. Средства защиты в составе вычислительной системы.
18. Защита программного обеспечения. Средства защиты с запросом информации.
19. Защита программного обеспечения. Средства активной защиты.
20. Защита программного обеспечения. Средства пассивной защиты.
21. Технология защиты информации на основе: электронных ключей, смарт-карт, персональных идентификаторов.
22. Принципы и методы создания защищенной операционной системы.
23. Цели и средства защиты информации. Типичный набор функциональных подсистем.
24. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.
25. Модель защиты системы с полным перекрытием.
26. Рекомендации по использованию моделей оценки уязвимости информации.
27. Допущения в моделях оценки уязвимости информации.
28. Методы определения требований к защите информации.
29. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
30. Классификация требований к средствам защиты информации.
31. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
32. Требования к защите, обуславливаемые видом защищаемой информации.
33. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации.

ПК-5 Способен обеспечивать качество разработки информационных систем

ПК-5.2 Проводит оценку рисков работы информационных систем в условиях цифровизации бизнеса и применения сквозных цифровых и отраслевых технологий

Обучающийся знает: возможные риски, возникающие при работе с информационными системами в организации.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам его участия в устных опросах и ответа на зачете.

1. Анализ рисков
2. Политика информационной безопасности
3. Концепция информационной безопасности
4. Доступ в информационные системы. Политика доступа. Физический доступ.
5. Построение сети. Удаленный доступ.
6. Инциденты. Активы, что требуется защитить.
7. Меры безопасности в контексте ISO 27001
8. Эффективность применяемых методов обеспечения безопасности
9. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
10. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
11. Понятие инцидента информационной безопасности

12. Место управления инцидентами в общей системе информационной безопасности
13. Особенности управления событиями безопасности

ОЦЕНКА УМЕНИЙ И НАВЫКОВ ОБУЧАЮЩИХСЯ НА ЗАЧЕТЕ

УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

УК-8.3. - Обеспечивает персональную информационную безопасность в цифровой среде, в том числе средствами криптографии

Обучающийся умеет: разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы

Обучающийся владеет: навыками документирования инцидентов и процессов информационной безопасности.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения практического задания:

Типовое задание: *Найти местоположение «троянских» программ. Очистить наиболее уязвимые разделы системного реестра от записей «троянских» программ.*

Типовое задание: *Восстановить зараженные файлы 9очистить их содержимое от макровирусов), включить защиту от вирусов.*

ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы

ПК-1.1. Проводит обследование организаций, выявляет информационные потребности пользователей, используя цифровые инструменты и облачные решения для сбора данных

Обучающийся умеет: проводить анализ предметной области и выявлять угрозы информационной безопасности.

Обучающийся владеет: навыками анализа информационных рисков.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения практического задания.

Типовое задание: *провести поиск уязвимостей в предложенной виртуальной сети любыми известными и доступными средствами, сформировать отчет с предложениями по их предупреждению и/или ликвидации.*

ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы

ПК-1.2. Составляет техническое задание на разработку информационной системы

Обучающийся умеет: разрабатывать концептуальное решение по обеспечению защиты информации в разрабатываемых системах.

Обучающийся владеет: навыками оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения практического задания.

Типовое задание: *настроить шифрование заданной директории средствами операционной системы, продемонстрировать недоступность информации сторонним лицам.*

ПК-3 Способен разрабатывать информационные системы

ПК-3.3. Обеспечивает информационную безопасность разрабатываемых информационных систем, в том числе общедоступными средствами мониторинга и выявления потенциальных информационных угроз

Обучающийся умеет: определять и обосновывать организационно-технические мероприятия по защите информации в информационных системах.

Обучающийся владеет: навыками использования инструментальных средств защиты информации в ходе профессиональной деятельности и управления инцидентами информационной безопасности.

Типовое задание: *разработать схему защиты образовательной организации от потери информации и план мероприятий организационного, технологического и программного характера.*

Типовое задание: *в предложенной виртуальной сети выполнить настройку уровней доступа для разных пользователей (менеджеры, операторы, администраторы). Распределение возможностей между ролями выполнить самостоятельно.*

ПК-4 Способен управлять процессами создания информационных систем

ПК-4.2. Применяет актуальные нормативные документы и стандарты при создании информационных систем, используя общедоступные справочно-правовые системы и профессиональные базы данных сферы ИТ

Обучающийся умеет: разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы.

Обучающийся владеет: навыками документирования инцидентов и процессов информационной безопасности.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения практических работ.

Типовое задание: *выполнить настройку брандмауэра Windows для защиты удаленного доступа.*

ПК-5 Способен обеспечивать качество разработки информационных систем

ПК-5.2 Проводит оценку рисков работы информационных систем в условиях цифровизации бизнеса и применения сквозных цифровых и отраслевых технологий

Обучающийся умеет: применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем.

Обучающийся владеет: навыками анализа рисков работы информационных систем.

Оценка достижения обучающимся запланированного результата обучения осуществляется по результатам выполнения практических работ.

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНОВАНИЯ ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

КРИТЕРИИ ОЦЕНИВАНИЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов **УК-8.3. -** Обеспечивает персональную информационную безопасность в цифровой среде, в том числе средствами криптографии					
Знать: - нормативно-правовые основы информационной безопасности в Российской Федерации; - международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности	Не знает	Фрагментарные знания о нормативно-правовых основах информационной безопасности в Российской Федерации, международных и отечественных стандартах, регламентирующих профессиональную деятельность в области информационной безопасности	Общие, но не структурированные знания о нормативно-правовых основах информационной безопасности в Российской Федерации, международных и отечественных стандартах, регламентирующих профессиональную деятельность в области информационной безопасности	Сформированные, но содержащие отдельные пробелы знания о нормативно-правовых основах информационной безопасности в Российской Федерации, международных и отечественных стандартах, регламентирующих профессиональную деятельность в области информационной безопасности	Сформированные систематизированные прочные знания о нормативно-правовых основах информационной безопасности в Российской Федерации, международных и отечественных стандартах, регламентирующих профессиональную деятельность в области информационной безопасности
Уметь: - разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы	Не умеет	Частично освоенные умения разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы	В целом освоенные, но не подкрепляемые знаниями и самостоятельностью выполнения умения разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-	В целом сформированные и самостоятельно выполняемые, но не всегда интеллектуально обоснованные умения разрабатывать политику информационной безопасности программных продуктов и организаций с	Успешно сформированные, самостоятельно и осознанно выполняемые умения разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
			правовые документы	опорой на нормативно-правовые документы	
Владеть: - навыками документирования инцидентов и процессов информационной безопасности	Не владеет	Фрагментарно сформированные навыки документирования инцидентов и процессов информационной безопасности	В целом сформированные, но выполняемые на элементарном уровне навыки документирования инцидентов и процессов информационной безопасности	Сформированные, но не устойчивые в сложных ситуациях навыки документирования инцидентов и процессов информационной безопасности	Успешно сформированные, устойчивые, технологически грамотно выполняемые навыки документирования инцидентов и процессов информационной безопасности
ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы **ПК-1.1**. Проводит обследование организаций, выявляет информационные потребности пользователей, используя цифровые инструменты и облачные решения для сбора данных					
Знать: -требования безопасности к информационным системам	Не знает	Фрагментарные знания о требованиях безопасности к информационным системам	Общие, но не структурированные знания о требованиях безопасности к информационным системам	Сформированные, но содержащие отдельные пробелы знания о требованиях безопасности к информационным системам	Сформированные систематизированные прочные знания о требованиях безопасности к информационным системам
Уметь: - проводить анализ предметной области и выявлять угрозы информационной безопасности;	Не умеет	Частично освоенные умения проводить анализ предметной области и выявлять угрозы информационной безопасности;	В целом освоенные, но не подкрепляемые знаниями и самостоятельностью выполнения умения проводить анализ предметной области и выявлять угрозы информационной безопасности;	В целом сформированные и самостоятельно выполняемые, но не всегда интеллектуально обоснованные умения проводить анализ предметной области и выявлять угрозы информационной	Успешно сформированные, самостоятельно и осознанно выполняемые умения проводить анализ предметной области и выявлять угрозы информационной безопасности;

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
				безопасности;	
Владеть: - навыками анализа информационных рисков	Не владеет	Фрагментарно сформированные навыки проведения аудита информационной безопасности и анализа рисков информационной безопасности	В целом сформированные, но выполняемые на элементарном уровне навыки проведения аудита информационной безопасности и анализа рисков информационной безопасности	Сформированные, но не устойчивые в сложных ситуациях навыки проведения аудита информационной безопасности и анализа рисков информационной безопасности	Успешно сформированные, устойчивые, технологически и грамотно выполняемые навыки проведения аудита информационной безопасности и анализа рисков информационной безопасности
ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы **ПК-1.2**. Составляет техническое задание на разработку информационной системы					
Знать: программно-аппаратное, организационное, инженерно-техническое обеспечение защиты информации	Не знает	Фрагментарные знания о программно-аппаратном, организационном, инженерно-техническом обеспечении защиты информации	Общие, но не структурированные знания о программно-аппаратном, организационном, инженерно-техническом обеспечении защиты информации	Сформированные, но содержащие отдельные пробелы знания о программно-аппаратном, организационном, инженерно-техническом обеспечении защиты информации	Сформированные систематизированные прочные знания о программно-аппаратном, организационном, инженерно-техническом обеспечении защиты информации
Уметь: разрабатывать концептуальное решение по обеспечению защиты информации в разрабатываемых системах	Не умеет	Частично освоенные умения разрабатывать концептуальное решение по обеспечению защиты информации в разрабатываемых системах	В целом освоенные, но не подкрепляемые знаниями и самостоятельностью выполнения умения разрабатывать концептуальное решение по обеспечению защиты информации в разрабатываемых системах	В целом сформированные и самостоятельно выполняемые, но не всегда интеллектуально обоснованные умения разрабатывать концептуальное решение по обеспечению	Успешно сформированные, самостоятельно и осознанно выполняемые умения разрабатывать концептуальное решение по обеспечению защиты информации в разрабатываемых системах

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
				защиты информации в разрабатываемых системах	
Владеть: навыками оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями	Не владеет	Фрагментарно сформированные навыки оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями	В целом сформированные, но выполняемые на элементарном уровне навыки оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями	Сформированные, но не устойчивые в сложных ситуациях навыки оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями	Успешно сформированные, устойчивые, технологически и грамотно выполняемые навыки оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями
ПК-3 Способен разрабатывать информационные системы **ПК-3.3**. Обеспечивает информационную безопасность разрабатываемых информационных систем, в том числе общедоступными средствами мониторинга и выявления потенциальных информационных угроз					
Знать: способы и методы обеспечения информационной безопасности в компьютерных сетях, удаленные угрозы и атаки, основы криптографической защиты информации, способы управления инцидентами информационной безопасности	Не знает	Фрагментарные знания о способах и методах обеспечения информационной безопасности в компьютерных сетях, об удаленных угрозах и атаках, основах криптографической защиты информации, способах управления инцидентами информационной безопасности	Общие, но не структурированные знания о способах и методах обеспечения информационной безопасности в компьютерных сетях, об удаленных угрозах и атаках, основах криптографической защиты информации, способах управления инцидентами информационной безопасности	Сформированные, но содержащие отдельные пробелы знания о способах и методах обеспечения информационной безопасности в компьютерных сетях, об удаленных угрозах и атаках, основах криптографической защиты информации, способах управления инцидентами	Сформированные систематизированные прочные знания о способах и методах обеспечения информационной безопасности в компьютерных сетях, об удаленных угрозах и атаках, основах криптографической защиты информации, способах управления инцидентами информационн

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
				информационной безопасности	ой безопасности
Уметь: определять и обосновывать организационно-технические мероприятия по защите информации в информационных системах	Не умеет	Частично освоенные умения определять и обосновывать организационно-технические мероприятия по защите информации в информационных системах	В целом освоенные, но не подкрепляемые знаниями и самостоятельностью выполнения умения определять и обосновывать организационно-технические мероприятия по защите информации в информационных системах	В целом сформированные и самостоятельно выполняемые, но не всегда интеллектуально обоснованные умения определять и обосновывать организационно-технические мероприятия по защите информации в информационных системах	Успешно сформированные, самостоятельно и осознанно выполняемые умения определять и обосновывать организационно-технические мероприятия по защите информации в информационных системах
Владеть: - навыками использования инструментальных средств защиты информации в ходе профессиональной деятельности; - навыками управления инцидентами информационной безопасности	Не владеет	Фрагментарно сформированные навыки использования инструментальных средств защиты информации в ходе профессиональной деятельности и управления инцидентами информационной безопасности	В целом сформированные, но выполняемые на элементарном уровне навыки использования инструментальных средств защиты информации в ходе профессиональной деятельности и управления инцидентами информационной безопасности	Сформированные, но не устойчивые в сложных ситуациях навыки использования инструментальных средств защиты информации в ходе профессиональной деятельности и управления инцидентами информационной безопасности	Успешно сформированные, устойчивые, технологически и грамотно выполняемые навыки использования инструментальных средств защиты информации в ходе профессиональной деятельности и управления инцидентами информационной безопасности
ПК-4 Способен управлять процессами создания информационных систем **ПК-4.2.** Применяет актуальные нормативные документы и стандарты при создании информационных систем, используя общедоступные справочно-правовые системы и профессиональные базы данных сферы ИТ					
Знать: -нормативно-	Не знает	Фрагментарные знания о	Общие, но не структурирова	Сформированные, но	Сформированные

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
правовые основы информационной безопасности в Российской Федерации; - международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности		нормативно-правовых основах информационной безопасности в Российской Федерации, международных и отечественных стандартах, регламентирующих профессиональную деятельность в области информационной безопасности	нные знания о нормативно-правовых основах информационной безопасности в Российской Федерации, международных и отечественных стандартах, регламентирующих профессиональную деятельность в области информационной безопасности	содержащие отдельные пробелы знания о нормативно-правовых основах информационной безопасности в Российской Федерации, международных и отечественных стандартах, регламентирующих профессиональную деятельность в области информационной безопасности	систематизированные прочные знания о нормативно-правовых основах информационной безопасности в Российской Федерации, международных и отечественных стандартах, регламентирующих профессиональную деятельность в области информационной безопасности
Уметь: разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы	Не умеет	Частично освоенные умения разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы	В целом освоенные, но не подкрепляемые знаниями и самостоятельностью выполнения умения разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы	В целом сформированные и самостоятельно выполняемые, но не всегда интеллектуально обоснованные умения разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы	Успешно сформированные, самостоятельно и осознанно выполняемые умения разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы
Владеть: навыками документирования	Не владеет	Фрагментарно сформированные навыки документирова	В целом сформированные, но выполняемые	Сформированные, но не устойчивые в сложных	Успешно сформированные, устойчивые,

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
инцидентов и процессов информационной безопасности		ния инцидентов и процессов информационной безопасности	на элементарном уровне навыки документирования инцидентов и процессов информационной безопасности	ситуациях навыки документирования инцидентов и процессов информационной безопасности	технологически грамотно выполняемые навыки документирования инцидентов и процессов информационной безопасности
ПК-5 Способен обеспечивать качество разработки информационных систем **ПК-5.2** Проводит оценку рисков работы информационных систем в условиях цифровизации бизнеса и применения сквозных цифровых и отраслевых технологий					
Знать: возможные риски, возникающие при работе с информационными системами в организации	Не знает	Фрагментарные знания о возможных рисках, возникающих при работе с информационными системами в организации/предприятии	Общие, но не структурированные знания о возможных рисках, возникающих при работе с информационными системами в организации/предприятии	Сформированные, но содержащие отдельные пробелы знания о возможных рисках, возникающих при работе с информационными системами в организации/ предприятии	Сформированные систематизированные прочные знания о способах и возможных рисках, возникающих при работе с информационными системами в организации/предприятии
Уметь: применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем	Не умеет	Частично освоенные умения применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем	В целом освоенные, но не подкрепляемые знаниями и самостоятельностью выполнения умения применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем	В целом сформированные и самостоятельно выполняемые, но не всегда интеллектуально обоснованные умения применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем	Успешно сформированные, самостоятельно и осознанно выполняемые умения разрабатывать применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем
Владеть:	Не владеет	Фрагментарно	В целом	Сформирован	Успешно

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
навыками анализа рисков работы информационных систем		сформированные навыки анализа рисков работы информационных систем	сформированные, но выполняемые на элементарном уровне навыки анализа рисков работы информационных систем	ные, но не устойчивые в сложных ситуациях навыки анализа рисков работы информационных систем	сформированные, устойчивые, технологически и грамотно выполняемые навыки анализа рисков работы информационных систем

ПРОЦЕДУРА ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ И КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Для контроля усвоения обучающимися данной дисциплины учебным планом предусмотрены зачет и курсовая работа.

Отметка «**зачтено**» выставляется обучающемуся, который показал сформированные систематизированные знания о нормативно-правовых основах информационной безопасности в Российской Федерации; международных и отечественных стандартах, регламентирующих профессиональную деятельность в области информационной безопасности; требованиях безопасности к информационным системам; знание понятия информационной безопасности, ее составляющие и уровни обеспечения; выполнил все практические работы на отметку не менее чем «удовлетворительно».

Отметка «**не зачтено**» выставляется обучающемуся, который имеет фрагментарные знания учебного материала, не выполнил в полном объеме практические работы.

Отметка за курсовую работу с учетом ее содержания и ее защиты студенту выставляется по пятибалльной системе.

Отметка «**отлично**» выставляется при условии, что:

- работа выполнена самостоятельно, носит творческий характер, собран, обобщен, и проанализирован большой объем нормативных правовых актов, учебной литературы, статистической информации и других практических материалов, позволивший всесторонне изучить тему и сделать аргументированные выводы и практические рекомендации;

- в теоретической части работы приведены мнения различных авторов, являющихся экспертами в рассматриваемой области, отражена дискуссия и высказано мнение автора по исследуемому вопросу;

- в практической части работы выполнены расчёты, сформулированы выводы, а также рекомендации для данной организации; -

полностью соответствует требованиям, предъявляемым к содержанию и оформлению курсовых работ;

- на защите освещены все вопросы исследования, ответы студента на вопросы профессионально грамотны, исчерпывающие, подкрепляются положениями нормативно-правовых актов, выводами и расчетами, отраженными в работе.

Отметка «**хорошо**» ставится, если:

- работа выполнена самостоятельно, носит творческий характер, собран, обобщен, и проанализирован достаточный объем нормативных правовых актов, учебной литературы, статистической информации и других практических материалов, позволивший достаточно полно изучить тему, но не по всем аспектам исследуемой темы сделаны выводы и обоснованы практические рекомендации;

- тема работы раскрыта, однако выводы и рекомендации не всегда оригинальны и/или не имеют практической значимости, есть неточности при освещении отдельных вопросов темы;

- в теоретической части работы приведены мнения отдельных специалистов, но не отражена дискуссия и не высказано мнение автора по исследуемому вопросу;

- в практической части работы выполнены расчёты, написаны выводы, в которых не достаточно полно или не точно отражены особенности рассматриваемого канала 30 утечки, а также даны слишком обобщенные рекомендации автора работы по дальнейшей оптимизации работы организации;

- есть отдельные недостатки в оформлении работы;

- на защите освещены все вопросы исследования, ответы студента на вопросы были неполные и недостаточно подкреплены положениями нормативно-правовых актов, выводами и расчетами, отраженными в работе.

Отметка «**удовлетворительно**» ставится, когда:

- работа выполнена самостоятельно, но носит поверхностный характер, собран, обобщен, и проанализирован небольшой объем нормативных правовых актов, учебной литературы, статистической информации и других практических материалов, который не позволил полно изучить тему, выводы и практические рекомендации не всегда обоснованы;

- тема работы раскрыта частично, выводы и рекомендации бессистемны и не имеют практической значимости, есть существенные недостатки при освещении почти всех вопросов темы;

- в теоретической части работы не отражено мнение специалистов, не отражена дискуссия и не высказано мнение автора по исследуемому вопросу;

- в практической части работы выполнены расчёты с ошибками, написаны слишком общие выводы, в которых не отражены особенности рассматриваемого канала утечки, а также автором не даны рекомендации для организации;

- есть существенные недостатки в оформлении работы;

- на защите освещены некоторые вопросы исследования, студент испытывал затруднения при ответах на вопросы.

Отметка «**неудовлетворительно**» ставится, если:

- содержание работы не раскрывает тему, вопросы изложены бессистемно и поверхностно, нет анализа практического материала, основные положения и рекомендации не имеют обоснования;

- работа не оригинальна, основана па компиляции публикаций по теме;

- работа несвоевременно представлена, не в полном объеме по содержанию и оформлению соответствует предъявляемым требованиям;

- на защите студент показал поверхностные знания по исследуемой теме, отсутствие представлений об актуальных проблемах по теме работы, не ответил на заданные вопросы.

5. ДИАГНОСТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ, ХАРАКТЕРИЗУЮЩИХ УРОВЕНЬ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Компетенция УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.

Обучающийся знает: нормативно-правовые основы информационной безопасности в Российской Федерации; международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности.

Обучающийся умеет: разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы.

Обучающийся владеет: навыками документирования инцидентов и процессов информационной безопасности.

ЗАДАНИЯ ЗАКРЫТОГО ТИПА

Задание 1. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата

а) черный пиар
б) фишинг
в) нигерийские письма
г) источник слухов
д) пустые письма

Ответ: а.

Задание 2. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

а) ГОСТ Р 50922-2006
б) ГОСТ Р ИСО/МЭК 27001-2021
в) ГОСТ Р 53114-2008
г) ГОСТ Р 50.1.056-2005

Ответ: в.

Задание 3. Конфиденциальность информации - это ее свойство…

а) быть известной только допущенным и прошедшим проверку (авторизованным) субъектам системы, а для остальных субъектов системы эта информация должна быть неизвестной
б) быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий
в) быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов

Ответ: а.

Задание 4. Целостность информации - это ее свойство...

а) быть известной только допущенным и прошедшим проверку (авторизованным) субъектам системы, а для остальных субъектов системы эта информация должна быть неизвестной
б) быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий
в) быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов

Ответ: б.

Задание 5. Доступность информации - это ее свойство…

а) быть известной только допущенным и прошедшим проверку (авторизованным) субъектам системы, а для остальных субъектов системы эта информация должна быть неизвестной
б) быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий
в) быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов
Ответ: в.

Задание 6. Целостность информации можно подразделить на:
а) Аутентическую
б) Динамическую
в) Параболическую
г) Статическую
Ответ: б, г.

Задание 7. Информация ограниченного доступа классифицируется на:
а) Приватную
б) Секретную
в) Закрытую
г) Конфиденциальную
Ответ: б, г.

Задание 8. На общедоступную информацию не распространяется принцип
а) Доступности информации
б) Конфиденциальности информации
в) Целостности информации
г) Нет верного варианта ответа
Ответ: б.

Задание 9. Неверное утверждение...
а) Информационная безопасность скрывает общедоступные данные
б) У конфиденциальных данных есть уровни конфиденциальности
в) У секретных данных есть уровни секретности
г) Информационная безопасность обеспечивает доступность общедоступных данных
Ответ: а.

Задание 10. Защита информации - это деятельность по предотвращению…
а) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками
б) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации
в) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации
г) утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
Ответ: г.

ЗАДАНИЯ ОТКРЫТОГО ТИПА

Задание 1. Как называлась первая в мире шифровальная машина?
Ответ: Энигма

Задание 2. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
Ответ: OECD

Задание 3. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей. Как это называется?
Ответ: фишинг

Задание 4. К какому виду угроз относится неправомерный доступ к информации
Ответ: К угрозам конфиденциальности

Задание 5. Метод шифрования, при котором единицы открытого текста заменяются зашифрованным текстом определённым образом с помощью ключа – это…
Ответ: Метод подстановки

Задание 6. Метод шифрования, при котором символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности – это…
Ответ: Метод гаммирования

Задание 7. Метод шифрования, при котором символы шифруемого текста переставляются по определённым правилам внутри шифруемого блока символов – это…
Ответ: Метод перестановки

Задание 8. Для чего предназначена цифровая подпись?
Ответ: Для аутентификации лица, подписавшего электронное сообщение.

Задание 9. Что такое ключ проверки электронной подписи?
Ответ: Ключ проверки электронной подписи - это уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Задание 10. Что такое сертификат ключа проверки электронной подписи?
Ответ: Сертификат ключа проверки электронной подписи - это электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи

Задание 11. CobiT относится к разработке систем информационной безопасности и программ безопасности – это…
Ответ: Открытый стандарт, определяющий цели контроля

Задание 12. CobiT состоит из четырех доменов, перечислите их.
Ответ: Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

Задание 13. CobiT разработан на основе структуры COSO. Что является основными целями и задачами COSO?
Ответ: COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень

Задание 14. Назовите принципы, на которых основывается деятельность государственных органов по обеспечению информационной безопасности
Ответ: Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

Задание 15. Дайте определение электронной подписи.
Ответ: Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

Компетенция ПК-1 Способен выявлять информационные потребности пользователей и составлять техническое задание на разработку информационной системы.
Обучающийся знает: требования безопасности к информационным системам; программно-аппаратное, организационное, инженерно-техническое обеспечение защиты информации.
Обучающийся умеет: проводить анализ предметной области и выявлять информационные угрозы; разрабатывать концептуальное решение по обеспечению защиты информации в разрабатываемых системах.
Обучающийся владеет: навыками анализа информационных рисков; навыками оформления документов на разработку информационной системы в части информационной безопасности в соответствии с требованиями.

ЗАДАНИЯ ЗАКРЫТОГО ТИПА

Задание 1. По механизму защиты ... сканируют операционную систему, файлы, которые запускаются на устройстве, а также загрузочные секторы жёстких дисков, и способны не только обнаружить вирус, но и вылечить заражённый файл, удалив вредоносный код
а) Антивирусные сканеры
б) Мониторы (антивирусные сторожа)
в) Ревизоры
г) Блокировщики
д) Полифаги
Ответ: д.

Задание 2. По механизму защиты ... работают в фоновом режиме и без перерывов отслеживают происходящие на устройстве процессы
а) Антивирусные сканеры
б) Мониторы (антивирусные сторожа)
в) Ревизоры
г) Блокировщики
д) Полифаги
Ответ: б.

Задание 3. По механизму защиты ... активируются после запуска устройства или по запросу пользователя и периодически проверяют оперативную память и файловую систему
а) Антивирусные сканеры
б) Мониторы (антивирусные сторожа)
в) Ревизоры

г) Блокировщики
д) Полифаги
Ответ: а.

Задание 4. По механизму защиты ... обнаруживают и останавливают вирусы на ранней стадии размножения, когда те записываются в загрузочный сектор жёсткого диска
а) Антивирусные сканеры
б) Мониторы (антивирусные сторожа)
в) Ревизоры
г) Блокировщики
д) Полифаги
Ответ: г.

Задание 5. По механизму защиты ... запоминают исходное состояние приложений и файлов и контролируют изменения в нём
а) Антивирусные сканеры
б) Мониторы (антивирусные сторожа)
в) Ревизоры
г) Блокировщики
д) Полифаги
Ответ: в.

Задание 6. Какие вирусы активизируются в самом начале работы с операционной системой?
а) загрузочные вирусы?
б) троянцы
в) черви
Ответ: а.

Задание 7. Stuxnet – это
а) троянская программа
б) макровирус
в) промышленный вирус
Ответ: в.

Задание 8. Техническая защита информации. Основные термины и определения
а) ГОСТ Р 50922-2006
б) ГОСТ Р ИСО/МЭК 27001-2021
в) ГОСТ Р 53114-2008
г) ГОСТ Р 50.1.056-2005
Ответ: г.

Задание 9. Защита информации. Основные термины и определения
а) ГОСТ Р 50922-2006
б) ГОСТ Р ИСО/МЭК 27001-2021
в) ГОСТ Р 53114-2008
г) ГОСТ Р 50.1.056-2005
Ответ: а.

Задание 10. Системный администратор, работающий в штате организации, относится к
а) антропогенным источникам угроз
б) техногенным источникам угроз
в) внешним источникам угроз
г) внутренним источникам угроз
Ответ: а.

ЗАДАНИЯ ОТКРЫТОГО ТИПА

Задание 1. Сопоставьте код ГОСТа с его описанием

Код		Описание	
1.	ГОСТ Р 50922-2006	A.	Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
2.	ГОСТ Р ИСО/МЭК 27001-2021	B.	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
3.	ГОСТ Р 53114-2008	C.	Техническая защита информации. Основные термины и определения
4.	ГОСТ Р 50.1.056-2005	D.	Защита информации. Основные термины и определения

Ответ: 1-D, 2-B, 3-A, 4-C

Вопрос 2. Дайте краткую классификацию рискам информационной безопасности, возникающим при работе с информационными системами в организации и приведите примеры.

Ответ: Например, приведем следующую классификацию рисков

Случайные. Объединяют непредвиденные события, когда происходит стечение обстоятельств, приводящее к неблагоприятным последствиям. Как правило, это внезапные, сложно прогнозируемые риски разного характера.

Примеры – выход из строя технического оборудования, чрезвычайные ситуации, перебои электроэнергии, повреждение коммуникационных каналов, поломка блокирующих устройств, ограничивающих доступ к информации.

Субъективные. Возникают из-за ошибок и неправильных действий персонала при обработке, хранении информации.

Примеры – пренебрежение внутренними правилами и регламентом безопасности, принятыми в организации (нарушение режима тайны, несанкционированный доступ к сведениям, нарушение правил передачи информации, использование незащищенных информационных каналов).

Объективные. Возникают в ходе преодоления злоумышленниками защитных систем и сопутствующего технического защитного оборудования.

Примеры – проникновение в информационную систему вредоносного программного обеспечения, внедрения следящего, шпионского оборудования, реализованные отказы в обслуживании.

Вопрос 3. Приведите примеры случайных рисков информационной безопасности

Ответ: Случайные риски – это результат (или предположение о наступлении события) по воле случая, непредвиденного события, когда происходит стечение обстоятельств, приводящее к неблагоприятным последствиям. Как правило, это внезапные, сложно прогнозируемые риски разного характера.

Примеры – выход из строя технического оборудования, чрезвычайные ситуации, перебои электроэнергии, повреждение коммуникационных каналов, поломка блокирующих устройств, ограничивающих доступ к информации.

Вопрос 4. Приведите примеры субъективных рисков информационной безопасности

Ответ: Субъективные риски возникают из-за ошибок и неправильных действий субъекта (персонала) при обработке, хранении информации.

Примеры – пренебрежение внутренними правилами и регламентом безопасности, принятыми в организации (нарушение режима тайны, несанкционированный доступ к сведениям, нарушение правил передачи информации, использование незащищенных информационных каналов).

Вопрос 5. Приведите примеры объективных рисков информационной безопасности

Ответ: Объективные риски возникают в ходе преодоления злоумышленниками защитных систем и сопутствующего технического защитного оборудования.

Примеры – проникновение в информационную систему вредоносного программного обеспечения, внедрения следящего, шпионского оборудования, реализованные отказы в обслуживании сервисов.

Вопрос 6. Охарактеризуйте общедоступную информацию. Какие требования предъявляются к такой информации?
Ответ: Согласно 149-ФЗ к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Однако, обладатель информации, ставшей общедоступной по его решению (автор), вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Вместе с тем, если информация, размещаемая в форме открытых данных, не должна содержать сведений, доступ к которым ограничивается в соответствии с законодательством, например, о государственной тайне, о персональных данных, о банковской тайне.

Вопрос 7. Приведите примеры отраслевых стандартов обеспечения информационной безопасности?
Ответ: В сфере искусственного интеллекта – семейство стандартов ГОСТ Р 59921
В банковской сфере (кредитные организации) – семейство стандартов ГОСТ Р 57580, а также стандарты Банка России СТО БР ИББС
В сфере здравоохранения – ГОСТ Р ИСО 27799-2015 (идентичен международному стандарту ИСО 27799:2008)

Задание 8. Назовите виды информации в зависимости от категории доступа к ней.
Ответ: В соответствии с законодательством Российской Федерации, информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

В зависимости от порядка предоставления или распространения информации она подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Вопрос 9. Приведите примеры документов, регламентирующих создание автоматизированных (информационных) систем в защищенном исполнении
Ответ: ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения
ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования и другие.

Вопрос 10. Предложите концепцию обеспечения информационной безопасности

Ответ: Предложим минимальный

1)на территорию предприятия доступ ограничивается в соответствии с категорией доступа помещения (общий, обслуживающий персонал, переговорные)

2)приняты ряд документов, регламентирующих работу с компьютерной и организационной техникой, с работников взяты обязательства о неразглашении

3)все входящие потоки данных анализируются антивирусными средствами, межсетевыми экранами нового поколения (NGFW) и тд

4)для подтверждении авторства и целостности передаваемых сообщений электронной почты используется электронная подпись

5)весь исходящий трафик анализируется на наличие возможной конфиденциальной информации системами класса DLP

6)резервное копирование данных и резервирование техники хранения и обработки данных

7)источники событий операционной системы и средств защиты информации подключены к SIEM

Вопрос 11. Дайте понятие угрозы информационной безопасности

Ответ: Угрозы информационной безопасности – это процессы, которые теоретически способны навредить компании или производству, а также рассекретить конфиденциальные данные. В случае реализации угрозы информационной безопасности наносят компании материальный ущерб. Сами угрозы могут быть прямыми или косвенными, а список потенциальных опасностей состоит из сотен позиций. Чтобы выбрать стратегию защиты данных и составить перечень требований к системе защиты, достаточно ознакомиться с наиболее распространенными видами угроз информации.

Вопрос 12. Приведите пример классификации угроз информационной безопасности

Ответ: Угрозы информационной безопасности могут классифицировать по следующим основаниям

ПРЕДНАМЕРЕННОСТЬ

–угрозы утечки информации, которые возникают спонтанно из-за небрежности работы сотрудников, например, случайного разглашения данных, неправильного ввода сведений, некорректного использования методов защиты;

–угрозы утечки информации, преднамеренно разработанные или реализованные злоумышленниками.

ХАРАКТЕР ПРОЯВЛЕНИЯ

–искусственно созданные угрозы безопасности;

–естественные угрозы безопасности, которые возникают из-за природных факторов.

ПРИЧИНА

–удаление данных, отказы в правильном функционировании ОС, санкционированные аппаратные фонды;

–действие природных стихий;

–деятельность человека: мошенника или инсайдера в компании, действия сотрудника, разглашение информации;

–действие вирусов и других несанкционированных программ на ПК или серверах с информацией.

АКТИВНОСТЬ И ЗАВИСИМОСТЬ ОТ ИС(АС)

–угрозы утечки информации появляются только в момент передачи или обработки данных, например, рассылка вирусного ПО;

–угрозы реализуются независимо от активности АС, например, вскрываются шифры и другие разновидности защиты.

Вопрос 13. Предложите классификацию источников угроз информационной безопасности

Ответ: Источники угроз информационных систем

СОСТОЯНИЕ ИСТОЧНИКА УГРОЗЫ

–источник находится непосредственно в самой информационной системе;

–источник располагается в пределах воздействия информационной системы;

–источник находится за периметром действия информационной системы, в таком случае данные перехватываются с помощью считывания излучений.

СТЕПЕНЬ ВОЗДЕЙСТВИЯ УГРОЗЫ НА ИНФОРМАЦИЮ

–активные угрозы, которые не только воздействуют на систему, но еще и меняют ряд ее сведений, такими свойствами обладают, например, вирусное и вредоносное ПО;

–пассивные угрозы, которые не влияют на сами информационные системы, а незаметно считывают информации. Такие виды угроз воздействуют на систему более длительное время, пока ИБ-специалисты компании не обнаружат утечки данных.

СПОСОБ ДОСТУПА

–канал доступа является несанкционированным, замаскированным с предполагает использование скрытых путей к ПО и работой с ОС в целях мошенников;

–канал доступа является лицензионным и санкционированным. В таком случае в систему вводят неправильные данные и затем маскируют деятельность под деятельность рядового сотрудника компании, например, мошенники находят пароли к учетным записям и пользуются стандартными каналами для получения данных.

МЕСТО ХРАНЕНИЯ ДАННЫХ ИС(АС) И СПОСОБ ПРОХОДА УГРОЗЫ

–проход угроз со стороны прикладных программ, а также доступ к системной части мест хранения информации;

–проход к специальным внешним носителям информации, чаще всего означает копирование данных с жесткого внешнего диска;

–получение информации с терминалов во время записи на видеокамеры;

–получение информации и реализация угроз через каналы связи, например, подключение к каналам связи, введение ложных данных, модификация и передача данных.

Вопрос 14. На какие свойства безопасности информации может быть направлена угроза
Ответ: Свойства безопасности информации – это конфиденциальность, целостность, доступность. Следовательно, на эти свойства безопасности информации направлены угрозы

Вопрос 15. Приведите примеры подсистем защиты информации ИС(АС)
Ответ: Например, руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992), определяет какие защитные подсистемы должны быть реализованы на действующих и проектируемых ИС(АС) учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

Защитные подсистемы:

–подсистема управления доступом

–подсистема регистрации и учета

–криптографическая подсистема

– подсистема обеспечения целостности

Компетенция ПК-3 Способен разрабатывать информационные системы.

Обучающийся знает: способы и методы обеспечения информационной безопасности в компьютерных сетях, удаленные угрозы и атаки, основы криптографической защиты информации, способы управления инцидентами информационной безопасности.

Обучающийся умеет: определять и обосновывать организационно-технические мероприятия по защите информации в информационных системах.

Обучающийся владеет: навыками использования инструментальных средств защиты информации в ходе профессиональной деятельности; навыками управления инцидентами информационной безопасности.

ЗАДАНИЯ ЗАКРЫТОГО ТИПА

Задание 1. Активный перехват информации это перехват, который
а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации
б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций
в) неправомерно использует технологические отходы информационного процесса
г) осуществляется путем использования оптической техники
д) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера
Ответ: д.

Задание 2. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации, называется
а) активный перехват
б) пассивный перехват
в) аудиоперехват
г) видеоперехват
д) просмотр мусора
Ответ: в.

Задание 3. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций, называется
а) активный перехват
б) пассивный перехват
в) аудиоперехват
г) видеоперехват
д) просмотр мусора
Ответ: б.

Задание 4. Перехват, который осуществляется путем использования оптической техники, называется
а) активный перехват
б) пассивный перехват
в) аудиоперехват
г) видеоперехват
д) просмотр мусора
Ответ: г.

Задание 5. По активности защитного воздействия меры по обеспечения безопасности информации делят на (несколько вариантов ответа)
а) пассивные
б) активные
в) полупассивные
г) полуактивные
Ответ: а, б.

Задание 6. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации
Ответ: в.

Задание 7. Вам нужно классифицировать данные по степени конфиденциальности. Что самое главное необходимо продумать?

а) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
б) необходимый уровень доступности, целостности и конфиденциальности
в) оценить уровень риска и отменить контрмеры
г) управление доступом, которое должно защищать данные

Ответ: б.

Задание 8. Федеральный закон "Об электронной подписи"

а) 149-ФЗ
б) 152-ФЗ
в) 63-ФЗ
г) 5485-1

Ответ: в.

Задание 9. Закон РФ "О государственной тайне"

а) 149-ФЗ
б) 152-ФЗ
в) 63-ФЗ
г) 5485-1

Ответ: г.

Задание 10. Федеральный закон "О персональных данных"

а) 149-ФЗ
б) 152-ФЗ
в) 63-ФЗ
г) 5485-1

Ответ: б.

ЗАДАНИЯ ОТКРЫТОГО ТИПА

Задание 1. Сопоставьте название закона с его номером.

№		НАЗВАНИЕ	
1.	5485-1	A.	Федеральный закон "Об информации, информационных технологиях и о защите информации"
2.	63-ФЗ	B.	Федеральный закон "Об электронной подписи"
3.	149-ФЗ	C.	Закон РФ "О государственной тайне"
4.	152-ФЗ	D.	Федеральный закон "О персональных данных"

Ответ: A-3, B-2, C-1, D-4

Задание 2. Тактическое планирование - это
Ответ: Среднесрочное планирование

Задание 3. Утечкой информации в системе называется ситуация, характеризуемая…
Ответ: Потерей данных в системе

Задание 4. К каким видам угроз относится нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях)?
Ответ: К преднамеренным искусственным угрозам

Задание 5. Перечислите субъекты информационной безопасности (активные участники процессов)
Ответ: государство, общество, граждане

Задание 6. Перечислите объекты информационной безопасности (пассивные участники процессов)
Ответ: информационные ресурсы, информационные и телекоммуникационные системы

Задание 7. Что относится к функциям системы безопасности?
Ответ: Установление регламента, аудит системы, выявление рисков

Вопрос 8. Перечислите основные каналы утечки информации
Ответ: В любой компании существуют четыре типа каналов утечки данных.

1)Акустический канал, куда относят все случаи общения между сотрудниками, которые могут делиться служебной информацией в рабочих целях. Стоит учесть ситуации, когда сотрудники с более высокими правами доступа к информации нечаянно выдают важные данные другим работникам или конкурентам.

2)Электромагнитный канал, по которому происходит хищение данных за счет считывания электромагнитных волн и наводок технических средств. Выявление факта утечки происходит уже после того, как конкурент получил и использовал данные против компании. Для защиты применяются стандартные приемы, которые поддерживает большинство автоматизированных систем: экранирование и использование генераторов радиочастотного шума.

3)Визуально-оптический канал, по которому возможно хищение прототипов моделей устройств, содержание закрытых совещаний и т.д. Утечка визуального типа невозможна в случае, если предмет интереса находится в помещении, которое полностью изолировано от естественного освещения.

4)Материально-вещественный канал, по которому происходит хищение копий документов, моделей, эскизов в физической и электронной форме, а также кража носителей информации с конфиденциальными данным.

Вопрос 9. Опишите виброакустический канал утечки информации
Ответ: В виброакустическом канале утечка информации происходит за счет распространения звукового сигнала в строительных конструкциях здания (стенах, полах, потолках), а также коммуникационных трубах. Распространение акустических волн приводит к возникновению вибрации в твердых и жидких средах. Для перехвата информации используются:

–акселерометры (специальные датчики, улавливающие вибрационные колебания);
–радиостетоскопы (устройства для перехвата сигналов, поступающих по радиоканалам);
–лазерные системы улавливания вибрации стекол;
–гидроакустические преобразователи – для перехвата информации с помощью сигналов, распространяющихся через воду в трубах водоснабжения и канализации.

Вопрос 10. Предложите пример реализации организационно-технических мероприятий по защите информации в информационных системах
Ответ: В качестве информационной системы рассмотрим автоматизированную банковскую систему, а значит перечень предлагаемых защитных мер должен соответствовать документу ГОСТ 57580.1-2017. Из-за громоздкости и объемности документа переносить сюда не будем.

Вопрос 11. Что такое электронная подпись и зачем она нужна?
Ответ: Электронная подпись (ЭП) это та же подпись, что и на бумаге, только на электронном носителе. ЭП является аналогом обыкновенной подписи. Информация о владельце содержится на специальном носителе похожем на флешку. С юридической точки зрения, ЭП безопасна, так как она гарантирует, что документ подписан конкретным человеком или компанией. Благодаря этому, электронную подпись используют при

различных удаленных сделках, например, при продаже машины или квартиры. Кроме того, подпись пригодится при обмене документами, при подаче иска или жалобы в суд дистанционно, при обращении в госорганы, для сдачи электронной отчетности, для участия в торгах и.т.д. Несомненно электронный документооборот ускоряет рабочие процессы, позволяет затратить меньше сил и энергии для достижения необходимого результата, ведь для этого не требуется выходить из дома или офиса.

Вопрос 12. Какие виды ЭЦП существуют и чем они отличаются друг от друга?
Ответ: Виды электронной подписи

–Простая электронная подпись подтверждает факт подлинности владельца. Этот вид подписи, который используется постоянно. Например, это комбинация кодов доступа при входе в личный кабинет или с помощью логин-пароль в онлайн-банке, полученных из смс. При дальнейшем использовании она имеет юридическую силу и равнозначна обычной подписи. Но с наименьшей степенью защиты.

–Усиленная неквалифицированная электронная подпись или НЭП. В основном такой вид электронной подписи используют во внутреннем и внешнем ЭДО с контрагентами. Усиленная неквалифицированная подпись не используется при участии в электронных торгах. Усиленная неквалифицированная ЭЦП имеет среднюю степень защиты. С помощью нее можно узнать вносились ли изменения в документ, и определить подписанта.

–Усиленная квалифицированная электронная подпись или КЭП – цифровой аналог собственноручной подписи. Квалифицированная ЭЦП подходит для участия в электронных торгах и является гарантом юридической силы. С помощью квалифицированной электронной подписи можно получить доступ к информационным государственным системам и пользоваться порталом госуслуг. Чтобы ее приобрести, нужно обратиться в удостоверяющий центр (УЦ) аккредитованный Минкомсвязи России. Данный УЦ должен иметь лицензию ФСБ России и выдавать соответствующие сертификаты подписей (ст. 5 Закона от 6 апреля 2011 г. № 63-ФЗ). Владелец получает электронную подпись в виде открытого и закрытого ключа, и сертификат подтверждающий личность владельца. Закрытый ключ нужен для подписания документов, а с помощью открытого ключа проверяется подпись.

Вопрос 13. Что такое шифрование информации, и какие есть составляющие шифра
Ответ: Шифрование – это сокрытие или видоизменение данных таким образом, чтобы другие люди не могли их прочитать или понять. Даже если злоумышленникам удастся украсть зашифрованную информацию, они не смогут её использовать, не разгадав код.

Шифрование используют все: дети придумывают собственный язык, который никто кроме них не понимает, а взрослые переписываются в мессенджерах: такая переписка хранится в зашифрованном виде. Криптография – наука о шифровании – выделяет три основных составляющих шифра:

1. Объект. В современном мире закодировать можно практически что угодно: текст, аудио, видео, изображения и любые файлы в любом объёме.
2. Алгоритм. Это правила видоизменения информации, которые подчиняются определённой логике. Простой пример алгоритма шифрования – когда буквы заменяются их порядковым номером в алфавите.

При использовании алгоритма замены букв на их номер в алфавите вместо «К» пишется 12, вместо «О» – 15, а вместо «Т» – 20

3. Ключ. Это код расшифровки информации. В случае с алгоритмом, упомянутым выше, это будет таблица с порядковыми номерами букв алфавита.

Вопрос 14. Перечислите способы и методы шифрования
Ответ: Основные три вида шифрования:

1. Симметричное. Его суть в том, что для кодирования и расшифровки информации используется один и тот же открытый ключ, доступ к которому может получить любой пользователь. Такой способ достаточно уязвим с точки зрения безопасности данных, поэтому он чаще применяется не для передачи, а для хранения информации. К примеру, на симметричном шифровании основано хранение переписки в мессенджерах и передача данных через HTTP.

2. Асимметричное. Более сложный вид шифрования данных, при котором для кодирования и дешифровки используются разные ключи. При этом ключ, который нужен для разгадывания кода, – закрытый, то есть им владеет только нужный получатель. Такой вид шифрования информации считается более надёжным, и его алгоритмы применяются, например, в системе цифровых подписей и блокчейне.

3. Хеш-функция (hash function – перемешивание). Особенность этого вида шифрования в том, что он не имеет обратной силы, то есть хеш-функцию невозможно раскодировать. Исходные данные можно преобразовать миллион раз, и результат всегда будет одинаковый. Однако, если внести изменение в первоначальную информацию, изменится и хеш-функция. Благодаря этому свойству использование этого вида шифрования чаще всего встречается при хранении паролей на сайтах. Когда пользователь вводит набор символов, система создаёт из него хеш-функцию и сверяется с хеш-функцией из хранилища данных. Если они совпадают, пользователь попадает в личный кабинет, если нет – значит, он ввёл неверный пароль.

Вопрос 15. Что представляет собой компрометация ключей электронной подписи? В каких случаях наступает?

Ответ: Компрометация ключей подписи – это утрата доверия к тому, что ключи могут обеспечить безопасность информации. Компрометация может привести к следующим негативным последствиям:

–утечке информации;

–переводу денежных средств с банковских счетов компании;

–предоставлению данных третьей стороне, например, контрагентов;

–передаче инсайдерских данных третьей стороне.

Компрометация наступает в следующих случаях

–Оставление в месте свободного доступа

–Физическая утеря носителя информации

–Передача информации по открытым каналам связи

–Доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков, взлом учётной записи пользователя и т. п.)

–Скимминг и шимминг банковских карт

–Перехват информации вредоносным ПО

–Перехват (подслушивание) звуковой информации

–Перехват ключа при распределении ключей

–Перехват побочных электромагнитных излучений и наводок

Перехват информации с электрических каналов утечки

–Сознательная передача информации постороннему лицу

и другие, в зависимости от вида носителя защищаемой информации и способов работы с ним.

Компетенция ПК-4 Способен управлять процессами создания информационных систем.

Обучающийся знает: нормативно-правовые основы информационной безопасности в Российской Федерации; международные и отечественные стандарты, регламентирующие профессиональную деятельность в области информационной безопасности.

Обучающийся умеет: разрабатывать политику информационной безопасности программных продуктов и организаций с опорой на нормативно-правовые документы.

Обучающийся владеет: навыками документирования инцидентов и процессов информационной безопасности.

ЗАДАНИЯ ЗАКРЫТОГО ТИПА

Задание 1. Принципом информационной безопасности является принцип недопущения

а) Рисков безопасности сети, системы
б) Неоправданных ограничений при работе в сети (системе)
в) Презумпции секретности
г) Презумпции невиновности хакера
Ответ: б.

Задание 2. Принципом политики информационной безопасности является принцип
а) Полного блокирования доступа при риск-ситуациях
б) Усиления основного звена сети, системы
в) Невозможности миновать защитные средства сети (системы)
Ответ: в.

Задание 3. Принципом политики информационной безопасности является принцип
а) Усиления защищенности самого незащищенного звена сети (системы)
б) Перехода в безопасное состояние работы сети, системы
в) Полного доступа пользователей ко всем ресурсам сети, системы
Ответ: а.

Задание 4. Принципом политики информационной безопасности является принцип
а) Одноуровневой защиты сети, системы
б) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
в) Совместимых, однотипных программно-технических средств сети, системы
Ответ: б.

Задание 5. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется
а) Регламентированной
б) Правовой
в) Защищаемой
г) Общедоступной
Ответ: в.

Задание 6. К посторонним лицам нарушителям информационной безопасности относится
а) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации
б) персонал, обслуживающий технические средства
в) технический персонал, обслуживающий здание
г) пользователи
д) сотрудники службы безопасности
е) представители конкурирующих организаций
ж) лица, нарушившие пропускной режим
Ответ: е.

Задание 7. Уверенности в успешном обеспечении безопасности в компании добавляет
а) поддержка высшего руководства
б) эффективные защитные меры и методы их внедрения
в) актуальные и адекватные политики и процедуры безопасности
г) проведение тренингов по безопасности для всех сотрудников
Ответ: а.

Задание 8. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют
а) Внедрение управления механизмами безопасности
б) Классификацию данных после внедрения механизмов безопасности
в) Уровень доверия, обеспечиваемый механизмом безопасности
г) Соотношение затрат / выгод

Ответ: в.

Задание 9. Заключительным этапом построения системы защиты является
а) сопровождение
б) планирование
в) анализ уязвимых мест
г) продажа
Ответ: а.

Задание 10. Политика безопасности – это
а) Пошаговые инструкции по выполнению задач безопасности
б) Общие руководящие требования по достижению определенного уровня безопасности
в) Широкие, высокоуровневые заявления руководства
г) Детализированные документы по обработке инцидентов безопасности
Ответ: в.

ЗАДАНИЯ ОТКРЫТОГО ТИПА

Задание 1. Если взглянуть на разницу в целях безопасности коммерческой и военной организации, у кого уровень безопасности выше?
Ответ: только военные имеют настоящую безопасность

Задание 2. Нарушитель информационной безопасности – это…
Ответ: субъект, осуществляющий пользование информацией с нарушением установленных прав и правил доступа к информации, установленных законом и/или собственником информации

Задание 3. Пользователь (потребитель) информации – это…
Ответ: субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации

Задание 4. Перечислите разновидности угроз безопасности системы.
Ответ: Программные, технические, организационные, технологические

Задание 5. Что является наиболее важным при реализации защитных мер политики безопасности?
Ответ: аудит, анализ уязвимостей, риск-ситуации.

Задание 6. Как называется источник угрозы информационной безопасности, характер возникновения которого обусловлен действиями субъекта.
Ответ: антропогенный источник

Задание 7. Угрозы, реализация которых не влечет за собой изменение структуры данных, называются…
Ответ: пассивные угрозы

Задание 8. Угрозы, реализация которых меняет структуру и содержание компьютерной системы (внедрение специальных программ), называются…
Ответ: активные угрозы

Задание 9. По размерам наносимого ущерба угрозы делятся на…
Ответ: общие, локальные, частные

Задание 10. Степень доступности информации, при которой антропогенный источник угроз имеет полный доступ к техническим и программным средствам обработки защищаемой информации, называется…
Ответ: высокая степень доступности

Задание 11. Степень доступности информации, при которой антропогенный источник угроз имеет очень ограниченную возможность доступа к техническим средствам и программам, обрабатывающим защищаемую информацию, называется…
Ответ: низкая степень доступности

Задание 12. Сбалансированное применение каких методов требует эффективная программа безопасности?
Ответ: Технических и нетехнических методов

Задание 13. В процессе внедрения и сопровождения безопасности задачей руководства является…
Ответ: поддержка, определение цели и границ, делегирование полномочий
Вопрос 14. Назовите организационную основу системы обеспечения информационной безопасности
Ответ: Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Вопрос 15. Назовите участников системы обеспечения информационной безопасности
Ответ: Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Компетенция ПК-5 Способен обеспечивать качество разработки информационных систем.
Обучающийся знает: возможные риски, возникающие при работе с информационными системами в организации.
Обучающийся умеет: применять цифровые и отраслевые технологии для проведения анализа рисков работы информационных систем.
Обучающийся владеет: навыками анализа рисков работы информационных систем.

Задание 1. Наилучшим описанием количественного анализа рисков является
а) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
б) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
в) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков

г) Метод, основанный на суждениях и интуиции

Ответ: в.

Задание 2. Потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации

а) атака
б) угроза
в) уязвимость

Ответ: б.

Задание 3. Какая категория является наиболее рискованной для компании с точки зрения вероятного нарушения безопасности

а) Сотрудники
б) Хакеры
в) Контрагенты (лица, работающие по договору)

Ответ: а.

Задание 4. Естественные угрозы безопасности информации вызваны

а) деятельностью человека
б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
г) корыстными устремлениями злоумышленников
д) ошибками при действиях персонала

Ответ: в.

Задание 5. Искусственные угрозы безопасности информации вызваны

а) деятельностью человека
б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
г) корыстными устремлениями злоумышленников
д) ошибками при действиях персонала

Ответ: а.

Задание 6. К основным непреднамеренным искусственным угрозам автоматизированной системы обработки информации относится

а) физическое разрушение системы путем взрыва, поджога и т.п.
б) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи
в) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.
г) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
д) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы

Ответ: д.

Задание 7. Наиболее распространены угрозы информационной безопасности корпоративной системы

а) Покупка нелицензионного ПО
б) Ошибки эксплуатации и неумышленного изменения режима работы системы
в) Сознательного внедрения сетевых вирусов

Ответ: б.

Задание 8. Источник угрозы информационной безопасности, определяемые технократической деятельностью человека и развитием цивилизации

а) техногенный источник
б) антропогенный источник
в) стихийный источник

Ответ: а.

Задание 9. При проведении анализа рисков следует привлекать специалистов из различных подразделений компании

а) Чтобы убедиться, что проводится справедливая оценка
б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

Ответ: в.

Задание 10. Количественный анализ рисков в чистом виде не достижим

а) Он достижим и используется
б) Он присваивает уровни критичности. Их сложно перевести в денежный вид
в) Это связано с точностью количественных элементов
г) Количественные измерения должны применяться к качественным элементам

Ответ: г.

ЗАДАНИЯ ОТКРЫТОГО ТИПА

Задание 1. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
Ответ: Много информации нужно собрать и ввести в программу

Задание 2. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками. В чем различия между этими методами?
Ответ: NIST и OCTAVE ориентированы на ИТ

Задание 3. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Ответ: Когда стоимость контрмер превышает ценность актива и потенциальные потери.

Задание 4. Наиболее важной техникой при выборе конкретных защитных мер является
Ответ: анализ затрат / выгоды

Задание 5. Опишите цель расчета ожидаемых среднегодовых потерь (ALE)
Ответ: Оценить потенциальные потери от угрозы в год

Задание 6. Метод анализа рисков пытается определить, где вероятнее всего произойдет…
Ответ: Анализ сбоев и дефектов

Вопрос 7. Дайте краткую характеристику методикам оценки рисков информационной безопасности
Ответ: На сегодняшний день существует Количественные и Качественные методики оценки рисков информационной безопасности.
Количественные. Используются с целью расчетов конкретных величин, выраженных в числовых значениях, процентах.
Качественные. Основываются на присвоении риску определенного ранга согласно системе ценностей: баллы, степени.

Вопрос 8. Дайте краткую характеристику *Количественной методике оценки рисков* информационной безопасности

Ответ: Количественные методики используются с целью расчетов конкретных величин, выраженных в числовых значениях, процентах.

Они опираются на сравнение с эталонными величинами, которые заранее известны и приемлемы. При количественном подходе каждому виду риска присваивается конкретная величина, параметры, выраженные в денежных, временных эквивалентах. Это облегчает понимание ситуации, позволяет оценить возможный ущерб, расходы на обеспечение защитных мер, долю резервов, которые придется задействовать.

Для начала необходимо провести оценку всех информационных активов компании в денежном эквиваленте для понимания их важности и критичности.

После этого проводится определение величин возможного ущерба в случае конкретных рисков и отдельных информационных активов.

Следующим шагом станет расчет вероятности наступления каждой возможной угрозы в отношении активов.

Далее рассчитывают суммарный потенциальный ущерб для каждого вида угроз с привязкой к какому-то временному периоду.

В конце выполняют анализ собранных данных и определяют количественный размер ущерба применительно к конкретной угрозе.

Вопрос 9. Дайте краткую характеристику *Качественной методике оценки рисков* информационной безопасности

Ответ: Качественные методики основываются на присвоении риску определенного ранга согласно системе ценностей: баллы, степени.

- Сначала выставляется оценка ценности информационных активов.
- Потом рассчитывается вероятность наступления угрозы по отношению к активу.
- Далее рассчитывают вероятность реализации угрозы, принимая во внимание действующие защитные меры.
- После этого делается вывод о размере риска, исходя из ценности конкретного актива, а также вероятности наступления риска.
- В конце проводится анализ и выставляется оценка в отношении каждой угрозы, величины риска (допустимо / не допустимо, удовлетворительно / хорошо / отлично, низкая / средняя / высока и т.д.).
- Также разрабатываются защитные меры по каждой угрозе для снижения величины ущерба.

Вопрос 10. Что должно учитывать при оценке рисков информационной безопасности:

Ответ: Например, ГОСТ Р ИСО/МЭК 27005-2010 призывает разрабатывать критерии для оценки рисков информационной безопасности с учетом:

– стратегической ценности обработки бизнес-информации;
– критичности затронутых информационных активов;
– законодательно-нормативных требований и договорных обязательств;
– оперативного значения и значения для бизнеса доступности, конфиденциальности и целостности;
– ожидания и реакции причастных сторон, а также негативных последствий для нематериальных активов и репутации.

Вопрос 11. Дайте классификацию концепциям (моделям) управления рисками информационной безопасности

Ответ: Любыми рисками можно управлять и тем самым снизить возможный ущерб от их наступления. Существуют различные подходы, модели для анализа рисков информационной безопасности, их управления:

Процессная модель управления рисками. Основывается на четырех базовых процессах: планирование, реализация, проверка, действие. Представляет непрерывный процесс.

Модель FRAP (Facilitated Risk Analysis Process) – состоит в качественной оценке рисков. Как правило, используются автоматизированные инструменты анализа.

Модель CRAMM (CCTA Risk Analysis & Management Method). Это один из самых зрелых, известных и широко используемых методов оценки рисков, который опирается на количественные и качественные методы анализа.

Модель OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), основанная на качественной оценке рисков модель.

Вопрос 12. Дайте краткую характеристику процессной модели управления рисками информационной безопасности

Ответ: Процессная модель управления рисками основывается на четырех базовых процессах: планирование, реализация, проверка, действие.

Планирование включает выбор политики, методов управления рисками, проведение оценки информационных активов, формирование профилей угроз и их дальнейшую обработку.

На этапе реализации (модели) выполняют развертывание систем безопасности согласно намеченному плану (внедряются защитные меры).

Проверка сводится к выполнению мероприятий, которые подтверждают эффективность принятых мер, полноценную работу механизмов контроля защищенности информации.

Действие заключается в улучшении в том числе управленческих процессов на основе полученных данных этапа Проверки (мониторинга, аудита). Итогом считается внесение корректировок, поправок в нормативную, регулирующую документацию компании, принятие дополнительных защитных мер.

После этапа Действие происходит переход к этапу Планирования. Модель повторяется заново.

Вопрос 13. Дайте краткую характеристику модели рисков информационной безопасности FRAP (Facilitated Risk Analysis Process)

Ответ: Модель FRAP (Facilitated Risk Analysis Process) – состоит в качественной оценке рисков. При этом акценты расставляются в пользу детального изучения информационной системы с помощью автоматизированных инструментов, тщательной идентификации угроз с формированием подробного списка. В ходе оценки рисков информационной безопасности происходит их градация согласно вероятности наступления и величине ущерба.

Вопрос 14. Дайте краткую характеристику модели рисков информационной безопасности CRAMM (CCTA Risk Analysis & Management Method)

Ответ: Модель CRAMM (CCTA Risk Analysis & Management Method). Считается одним из самых зрелых, известных и широко используемых методов оценки рисков, который опирается на количественные и качественные методы анализа. Уделяет повышенное внимание определению ценности информации. Использует для оценки ущерба бальную систему, группирует информационные ресурсы согласно типу угроз, выделяет отдельные уровни угроз, уязвимостей.

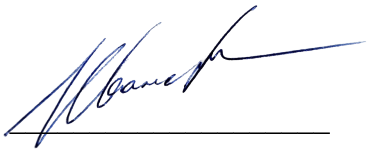
Вопрос 15. Дайте краткую характеристику модели рисков информационной безопасности OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Ответ: Модель OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – основана на качественной оценке рисков. Она ведется в три этапа, где предварительно выполняется группа мероприятий, направленных на создание ролей, планирование рисков. Ключевыми моментами в данной модели являются персональная разработка профиля угроз, исходя из вида информационного актива, точная идентификация уязвимостей по всей инфраструктуре, подбор оптимальных стратегий для обеспечения информационной безопасности.

6. ЛИСТ СОГЛАСОВАНИЯ

Составил:

Н.А. Иванова, ст.преп.



(подпись)

Заведующий кафедрой

Н.Б.Стрекалова, д.п.н., доцент

(подпись)

Заведующий выпускающей кафедрой

Н.Б.Стрекалова, д.п.н., доцент

(подпись)