ЧОУ ВО «Тольяттинская академия управления»

Кафедра прикладной информатики и высшей математики

Б1.В.09

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	*Очно-заочная*

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

2022

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 ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, 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. ЛИСТ СОГЛАСОВАНИЯ

Составил:

В.Н. Маризина, к.п.н. _____

(подпись)

Заведующий кафедрой

Н.Б.Стрекалова, д.п.н., доцент _____

(подпись)

Заведующий выпускающей кафедрой

Н.Б.Стрекалова, д.п.н., доцент _____

(подпись)