

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Стрельникова Светлана Евгеньевна
 Должность: ректор
 Дата подписания: 28.09.2026 16:46:35
 Уникальный программный ключ:
 ed7e7ef871ef28d870011250a92f17921078cc18

**Автономная некоммерческая образовательная организация высшего образования
 «Контур Университет»**



**МОДУЛЬ 3. ОСНОВЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
 И ПРОГРАММИРОВАНИЯ**
Информационная безопасность
 рабочая программа дисциплины (модуля)

Учебный план	09.03.03_ИИС_2026.plx 09.03.03 Прикладная информатика		
Квалификация	бакалавр		
Форма обучения	очная		
Общая трудоемкость	3 ЗЕТ		
Часов по учебному плану	108	Виды контроля	в семестрах:
в том числе:		экзамены	6
аудиторные занятия	32		
самостоятельная работа	67		
часов на контроль	9		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Неделя	17 2/6			
Вид занятий	уп	рп	уп	рп
Лекции	16	16	16	16
Практические	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	67	67	67	67
Часы на контроль	9	9	9	9
Итого	108	108	108	108

Рабочая программа дисциплины

Информационная безопасность

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки
09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

составлена на основании учебного плана:

09.03.03 Прикладная информатика

Одобрена Ученым советом вуза

Протокол от 15.09.2026 № 05.

Одобрена учебно-методической комиссией

Протокол от 10.09.2026 г. № 01

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель освоения дисциплины:
1.2	Формирование у обучающихся системы знаний в области информационной безопасности и способности выявлять угрозы информационной безопасности в профессиональной деятельности, применять средства защиты информации, обеспечивать базовые требования безопасности при работе с данными, а также учитывать нормативно-правовые требования при разработке технической документации и оценивать её соответствие стандартам.
1.3	Задачи изучения дисциплины:
1.4	Сформировать знания об основных понятиях информационной безопасности: угрозах, уязвимостях, рисках, моделях нарушителя.
1.5	Сформировать умение выявлять типовые угрозы (вредоносное программное обеспечение, несанкционированный доступ, фишинг, утечки данных) и применять средства защиты.
1.6	Сформировать навыки обеспечения базовых требований информационной безопасности: шифрования, безопасной аутентификации, резервного копирования.
1.7	Сформировать знания о нормативно-правовой базе в области защиты информации и требованиях регуляторов.
1.8	Сформировать навыки разработки организационно-распорядительной и технической документации по защите информации и оценки её соответствия стандартам.
1.9	Сформировать умение строить модель угроз и определять состав мер защиты информационной системы.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О.03
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Операционные системы
2.1.2	Компьютерные сети
2.1.3	Базы данных и SQL
2.1.4	Правоведение
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Разработка и интеграция информационных систем
2.2.2	Цифровая этика и управление рисками AGI
2.2.3	Производственная практика (эксплуатационная)

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ	
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
ОПК-3.2: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности	

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Примечание
	Раздел 1.			
1.1	Информационная безопасность: основные понятия. Конфиденциальность, целостность, доступность. Активы, угрозы, уязвимости, риски. Модель нарушителя /Лек/	6	2	
1.2	Информационная безопасность: основные понятия. Конфиденциальность, целостность, доступность. Активы, угрозы, уязвимости, риски. Модель нарушителя /Пр/	6	2	

1.3	Информационная безопасность: основные понятия. Конфиденциальность, целостность, доступность. Активы, угрозы, уязвимости, риски. Модель нарушителя /Ср/	6	8	
1.4	Классификация угроз информационной безопасности. Вредоносное программное обеспечение, несанкционированный доступ, фишинг и социальная инженерия, утечки данных. Средства антивирусной защиты /Лек/	6	2	
1.5	Классификация угроз информационной безопасности. Вредоносное программное обеспечение, несанкционированный доступ, фишинг и социальная инженерия, утечки данных. Средства антивирусной защиты /Пр/	6	2	
1.6	Классификация угроз информационной безопасности. Вредоносное программное обеспечение, несанкционированный доступ, фишинг и социальная инженерия, утечки данных. Средства антивирусной защиты /Ср/	6	8	
1.7	Криптографическая защита информации: симметричные и асимметричные алгоритмы, хэш-функции, электронная подпись, инфраструктура открытых ключей. Отечественные криптографические стандарты /Лек/	6	2	
1.8	Криптографическая защита информации: симметричные и асимметричные алгоритмы, хэш-функции, электронная подпись, инфраструктура открытых ключей. Отечественные криптографические стандарты /Пр/	6	2	
1.9	Криптографическая защита информации: симметричные и асимметричные алгоритмы, хэш-функции, электронная подпись, инфраструктура открытых ключей. Отечественные криптографические стандарты /Ср/	6	8	
1.10	Идентификация, аутентификация, авторизация. Парольные политики, многофакторная аутентификация, управление учётными записями и привилегированным доступом /Лек/	6	2	
1.11	Идентификация, аутентификация, авторизация. Парольные политики, многофакторная аутентификация, управление учётными записями и привилегированным доступом /Пр/	6	2	
1.12	Идентификация, аутентификация, авторизация. Парольные политики, многофакторная аутентификация, управление учётными записями и привилегированным доступом /Ср/	6	8	
1.13	Защита информации в информационных системах и сетях: сегментация, межсетевое экранирование, обнаружение вторжений, защита рабочих мест, резервное копирование и обеспечение непрерывности /Лек/	6	2	
1.14	Защита информации в информационных системах и сетях: сегментация, межсетевое экранирование, обнаружение вторжений, защита рабочих мест, резервное копирование и обеспечение непрерывности /Пр/	6	2	
1.15	Защита информации в информационных системах и сетях: сегментация, межсетевое экранирование, обнаружение вторжений, защита рабочих мест, резервное копирование и обеспечение непрерывности /Ср/	6	8	
1.16	Нормативно-правовое обеспечение защиты информации: федеральные законы, постановления Правительства, требования регуляторов, стандарты серии ISO/IEC 27000, требования к защите персональных данных /Лек/	6	2	
1.17	Нормативно-правовое обеспечение защиты информации: федеральные законы, постановления Правительства, требования регуляторов, стандарты серии ISO/IEC 27000, требования к защите персональных данных /Пр/	6	2	
1.18	Нормативно-правовое обеспечение защиты информации: федеральные законы, постановления Правительства, требования регуляторов, стандарты серии ISO/IEC 27000, требования к защите персональных данных /Ср/	6	9	

1.19	Организационно-распорядительная и техническая документация по защите информации: политика безопасности, регламенты, модель угроз, техническое задание в части защиты информации. Оценка соответствия документации требованиям /Лек/	6	2	
1.20	Организационно-распорядительная и техническая документация по защите информации: политика безопасности, регламенты, модель угроз, техническое задание в части защиты информации. Оценка соответствия документации требованиям /Пр/	6	2	
1.21	Организационно-распорядительная и техническая документация по защите информации: политика безопасности, регламенты, модель угроз, техническое задание в части защиты информации. Оценка соответствия документации требованиям /Ср/	6	9	
1.22	Управление рисками информационной безопасности. Аудит и контроль защищённости. Безопасная разработка программного обеспечения. Защита критической информационной инфраструктуры /Лек/	6	2	
1.23	Управление рисками информационной безопасности. Аудит и контроль защищённости. Безопасная разработка программного обеспечения. Защита критической информационной инфраструктуры /Пр/	6	2	
1.24	Управление рисками информационной безопасности. Аудит и контроль защищённости. Безопасная разработка программного обеспечения. Защита критической информационной инфраструктуры /Ср/	6	9	
1.25	/Экзамен/	6	9	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации

Темы для обсуждения на практических занятиях:

Семинар № 1. Социальная инженерия и человеческий фактор (к теме 1.2)

Цель занятия: сформировать умение распознавать приёмы социальной инженерии и предлагать организационные меры защиты.

Вопросы для обсуждения: 1. Почему человек считается наиболее уязвимым элементом системы защиты. 2. Типовые приёмы: фишинговые рассылки, обращение от имени руководства, создание срочности, использование публично доступных сведений о сотрудниках. 3. Признаки фишингового сообщения. 4. Ограниченность технических мер противодействия. 5. Обучение и повышение осведомлённости персонала как мера защиты. 6. Порядок действий сотрудника при получении подозрительного сообщения.

Практические задания: разбор пяти предложенных сообщений с выявлением признаков фишинга и обоснованием вывода; разработка памятки для сотрудников организации; обсуждение сценария, при котором сотрудник уже перешёл по ссылке и ввёл учётные данные, с определением порядка действий.

Семинар № 2. Нормативные требования к защите информации (к теме 1.6)

Цель занятия: сформировать умение определять применимые к информационной системе нормативные требования.

Вопросы для обсуждения: 1. Система нормативных правовых актов в области защиты информации. 2. Требования к защите персональных данных: уровни защищённости и состав мер. 3. Требования к государственным информационным системам. 4. Защита объектов критической информационной инфраструктуры. 5. Стандарты серии ISO/IEC 27000: назначение и структура. 6. Соотношение обязательных требований и рекомендуемых практик. 7. Ответственность за нарушение требований защиты информации.

Практические задания: для трёх описаний информационных систем определить применимый набор нормативных требований и обосновать вывод; составить перечень документов, которые организация обязана иметь; разбор ситуации, в которой требования разных регуляторов накладываются друг на друга.

Семинар № 3. Управление рисками информационной безопасности (к теме 1.8)

Цель занятия: сформировать умение оценивать риски и обосновывать выбор мер защиты.

Вопросы для обсуждения: 1. Понятие риска; вероятность и ущерб. 2. Качественные и количественные методы оценки рисков. 3. Способы обработки риска: снижение, принятие, передача, избегание. 4. Соотношение стоимости меры защиты и величины предотвращаемого ущерба. 5. Остаточный риск и порядок его принятия. 6. Периодичность пересмотра оценки рисков.

Практические задания: построение реестра рисков для предложенной информационной системы с качественной оценкой; выбор способа обработки для каждого риска с обоснованием; расчёт целесообразности внедрения меры защиты при заданных стоимости и ожидаемом ущербе.

Практико-ориентированные задания:

Задание № 1 «Инвентаризация активов и модель нарушителя» (к теме 1.1)

Цель: сформировать навыки определения защищаемых активов и построения модели нарушителя.

Условие: организация эксплуатирует учётную систему, файловый сервер, корпоративную почту и веб-сайт с формой обратной связи; в системах обрабатываются персональные данные сотрудников и клиентов.

Задания для обучающихся: 1. Составьте перечень информационных активов с указанием их ценности для организации. 2. Для каждого актива определите, какие свойства безопасности критичны и почему. 3. Постройте модель нарушителя: категории, мотивация, возможности, уровень доступа. 4. Определите наиболее вероятные векторы атаки для каждой категории нарушителя. 5. Обоснуйте, какие нарушители являются актуальными для данной организации, а какие могут быть исключены.

Форма отчётности: аналитическая записка с перечнем активов и моделью нарушителя.

Задание № 2 «Анализ инцидента и признаки компрометации» (к теме 1.2)

Цель: сформировать навыки выявления признаков компрометации и применения средств защиты.

Условие: предоставлены выдержки из журналов событий рабочей станции и сервера, а также отчёт средства антивирусной защиты.

Задания для обучающихся: 1. Выявите в предоставленных материалах признаки компрометации и перечислите их. 2. Определите наиболее вероятный вектор проникновения. 3. Восстановите хронологию событий инцидента. 4. Определите, какие данные могли быть затронуты. 5. Предложите порядок неотложных действий по локализации. 6. Обоснуйте, какие технические меры предотвратили бы инцидент, а какие лишь ускорили бы его обнаружение.

Форма отчётности: отчёт об анализе инцидента с хронологией событий.

Задание № 3 «Применение криптографических средств» (к теме 1.3)

Цель: сформировать навыки практического применения средств криптографической защиты.

Задания для обучающихся: 1. Выполните симметричное шифрование файла и объясните, как обеспечивается защищённая передача ключа. 2. Сформируйте ключевую пару, зашифруйте сообщение открытым ключом и расшифруйте закрытым. 3. Вычислите хэш-значение файла, измените один байт и объясните наблюдаемый результат. 4. Сформируйте и проверьте электронную подпись документа. 5. Объясните, какие свойства безопасности обеспечивает шифрование, а какие — электронная подпись. 6. Укажите отечественные криптографические стандарты и область их обязательного применения.

Форма отчётности: отчёт с протоколом выполненных операций и пояснениями.

Задание № 4 «Настройка аутентификации и резервного копирования» (к теме 1.4)

Цель: сформировать навыки обеспечения базовых требований безопасности.

Задания для обучающихся: 1. Разработайте парольную политику для организации и обоснуйте каждое требование. 2. Настройте парольную политику в операционной системе. 3. Настройте многофакторную аутентификацию для доступа к сервису и проверьте её работу. 4. Разграничьте права учётных записей по принципу минимальных привилегий, выделив привилегированные учётные записи. 5. Настройте резервное копирование критичных данных с шифрованием копий. 6. Проведите учебное восстановление и подтвердите целостность данных. 7. Объясните, почему требование частой смены сложных паролей может снижать реальную защищённость.

Форма отчётности: отчёт с конфигурациями и протоколами проверки.

Задание № 5 «Разработка политики безопасности» (к теме 1.7)

Цель: сформировать навыки разработки организационно-распорядительной документации.

Задания для обучающихся: 1. Разработайте проект политики информационной безопасности организации, включающий разделы о целях, области действия, ролях и ответственности, правилах работы с учётными записями, данными и съёмными носителями, порядке реагирования на инциденты. 2. Разработайте регламент предоставления и отзыва доступа. 3. Определите, какие требования нормативных актов реализуются каждым разделом, и приведите ссылки. 4. Оцените разработанный документ по критериям полноты, исполнимости и проверяемости. 5. Предложите порядок контроля соблюдения политики. Форма отчётности: комплект документов с пояснительной запиской.

Примеры кейсовых заданий:

Кейс № 1 «Реагирование на инцидент» (к темам 1.2, 1.5)

Цель: сформировать навыки реагирования на инцидент информационной безопасности.

Фабула: утром понедельника сотрудники обнаружили, что файлы на общем сетевом ресурсе переименованы и не открываются; в каталогах присутствует текстовый файл с требованием оплаты. Часть рабочих станций не загружается. Резервное копирование выполнялось на тот же файловый сервер. В пятницу один из сотрудников сообщил в ИТ-отдел о письме с вложением от имени контрагента, но обращение не было обработано. Средство антивирусной защиты установлено не на всех станциях, обновление баз выполнялось нерегулярно.

Задания для обучающихся: 1. Определите порядок неотложных действий и обоснуйте очередность. 2. Объясните, почему отключение заражённых узлов от сети предшествует их исследованию. 3. Оцените возможность восстановления данных при описанной схеме резервного копирования. 4. Восстановите вероятный вектор проникновения и цепочку развития инцидента. 5. Определите, какие сведения подлежат фиксации для последующего расследования. 6. Оцените, требуется ли уведомление регулятора, и обоснуйте вывод. 7. Предложите комплекс технических и организационных мер, предотвращающих повторение, разделив их на неотложные и долгосрочные.

Форма отчётности: письменное решение кейса с планом реагирования, устная защита.

Кейс № 2 «Оценка защищённости информационной системы» (к темам 1.5, 1.8)

Цель: сформировать навыки комплексной оценки защищённости и обоснования мер защиты.

Фабула: организация внедряет систему обработки заявок клиентов, доступную из сети «Интернет». В системе обрабатываются фамилия, имя, отчество, телефон, адрес электронной почты и сведения о заказах. Планируется размещение в арендуемом дата-центре. Разработчик предлагает разместить базу данных и веб-приложение на одном сервере с прямым доступом из сети «Интернет», аутентификацию организовать по паре «логин — пароль» без ограничений на сложность, журналирование не вести.

Задания для обучающихся: 1. Определите категорию обрабатываемых данных и применимые нормативные требования. 2. Постройте модель угроз для описанной системы. 3. Оцените предложенное разработчиком решение и укажите его

недостатки с обоснованием. 4. Предложите целевую архитектуру с сегментацией и разграничением доступа. 5. Определите состав мер защиты: технических и организационных. 6. Обоснуйте необходимость журналирования и определите состав фиксируемых событий. 7. Оцените остаточный риск после внедрения предложенных мер.

Форма отчётности: письменное решение кейса с моделью угроз и перечнем мер, устная защита.

Кейс № 3 «Экспертиза технического задания» (к темам 1.6–1.7)

Цель: сформировать навыки оценки соответствия технической документации нормативным требованиям.

Фабула: на согласование поступило техническое задание на создание информационной системы для государственного заказчика. В разделе требований к защите информации указано: «Система должна быть защищена от несанкционированного доступа». Требования к резервному копированию, журналированию, разграничению доступа и применению сертифицированных средств защиты отсутствуют. Класс защищённости системы не определён. Персональные данные упоминаются, но категория не указана.

Задания для обучающихся: 1. Оцените приведённую формулировку требования на проверяемость и предложите корректный вариант. 2. Определите, какие обязательные разделы и требования отсутствуют в техническом задании. 3. Укажите нормативные акты, которыми установлены соответствующие требования. 4. Определите порядок установления класса защищённости и уровня защищённости персональных данных. 5. Сформулируйте недостающие требования в проверяемом виде. 6. Оцените риски принятия документа в текущей редакции для заказчика и исполнителя. 7. Подготовьте заключение с перечнем замечаний и предложений.

Форма отчётности: экспертное заключение по техническому заданию, устная защита.

Примерный перечень вопросов к экзамену:

1. Информационная безопасность: понятие и основные свойства защищаемой информации.
2. Активы, угрозы, уязвимости, риски: соотношение понятий.
3. Модель нарушителя: назначение и порядок построения.
4. Классификация угроз информационной безопасности.
5. Вредоносное программное обеспечение: виды и механизмы распространения.
6. Средства антивирусной защиты: принципы работы и ограничения.
7. Несанкционированный доступ: способы реализации и меры противодействия.
8. Социальная инженерия и фишинг: приёмы и защита.
9. Утечки данных: каналы и меры предотвращения.
10. Признаки компрометации информационной системы.
11. Симметричные криптографические алгоритмы: назначение и проблема распределения ключей.
12. Асимметричные криптографические алгоритмы: принцип и области применения.
13. Хэш-функции: свойства и применение.
14. Электронная подпись: назначение, виды, порядок проверки.
15. Инфраструктура открытых ключей и удостоверяющие центры.
16. Отечественные криптографические стандарты и область их применения.
17. Идентификация, аутентификация, авторизация: разграничение понятий.
18. Парольные политики: требования и их обоснованность.
19. Многофакторная аутентификация: факторы и их сочетание.
20. Управление привилегированным доступом.
21. Разграничение доступа: дискреционная, мандатная, ролевая модели.
22. Сегментация сети как мера защиты.
23. Межсетевое экранирование и системы обнаружения вторжений.
24. Защита рабочих мест пользователей.
25. Резервное копирование как мера обеспечения доступности.
26. Обеспечение непрерывности деятельности и восстановления после сбоев.
27. Журналирование событий безопасности: состав и порядок хранения.
28. Нормативно-правовая база защиты информации в Российской Федерации.
29. Требования к защите персональных данных; уровни защищённости.
30. Требования к государственным информационным системам.
31. Критическая информационная инфраструктура: понятие, субъекты, категорирование.
32. Стандарты серии ISO/IEC 27000: назначение и структура.
33. Политика информационной безопасности: назначение и структура документа.
34. Модель угроз как документ: состав и порядок разработки.
35. Требования к защите информации в техническом задании: критерии проверяемости.
36. Оценка соответствия документации нормативным требованиям.
37. Управление рисками информационной безопасности: этапы и методы.
38. Способы обработки риска и обоснование выбора меры защиты.
39. Аудит информационной безопасности: виды и порядок проведения.
40. Безопасная разработка программного обеспечения: основные принципы.
41. Реагирование на инциденты: этапы и порядок фиксации сведений.
42. Ответственность за нарушение требований в области защиты информации.

5.2. Темы письменных работ

не предусмотрены

5.3. Фонд оценочных средств

Тестовые задания:

РАЗДЕЛ 1. ВОПРОСЫ НА СООТВЕТСТВИЕ (№ 1–4)

Инструкция: к каждому элементу из левого столбца подберите ОДИН соответствующий элемент из правого столбца. Ответ

запишите в виде сочетания цифр и букв (например: 1-А, 2-Б, 3-В, 4-Г). Каждая буква используется только один раз.

ОПК-3.2. Вопрос № 1. Установите соответствие между свойством информации и его нарушением:

1. Конфиденциальность — 2. Целостность — 3. Доступность — 4. Неотказуемость.

Варианты: А. Несанкционированное изменение данных; Б. Ознакомление с данными лицом, не имеющим на это права; В. Отказ отправителя от факта совершения действия; Г. Невозможность получения данных законным пользователем в требуемый момент.

Ответ: 1 __, 2 __, 3 __, 4 __

ОПК-3.2. Вопрос № 2. Установите соответствие между криптографическим средством и обеспечиваемым свойством:

1. Симметричное шифрование — 2. Хэш-функция — 3. Электронная подпись — 4. Асимметричное шифрование.

Варианты: А. Контроль целостности данных; Б. Конфиденциальность при наличии общего секретного ключа; В. Конфиденциальность без предварительного обмена секретом; Г. Подтверждение авторства и целостности документа.

Ответ: 1 __, 2 __, 3 __, 4 __

ОПК-3.2. Вопрос № 3. Установите соответствие между фактором аутентификации и его примером:

1. Фактор знания — 2. Фактор владения — 3. Биометрический фактор — 4. Контекстный фактор.

Варианты: А. Аппаратный ключ или одноразовый код на устройстве; Б. Пароль или кодовое слово; В. Расположение и время попытки входа; Г. Отпечаток пальца или рисунок лица.

Ответ: 1 __, 2 __, 3 __, 4 __

ОПК-3.2. Вопрос № 4. Установите соответствие между документом и его назначением: 1. Политика информационной безопасности — 2. Модель угроз — 3. Регламент предоставления доступа — 4. Журнал событий безопасности.

Варианты: А. Описание актуальных угроз и нарушителей для конкретной системы; Б. Закрепление целей, принципов и правил обеспечения безопасности в организации; В. Фиксация фактических действий пользователей и системных событий; Г. Порядок оформления, согласования и исполнения заявок на доступ.

Ответ: 1 __, 2 __, 3 __, 4 __

РАЗДЕЛ 2. ВОПРОСЫ С ОДНИМ ВЕРНЫМ ОТВЕТОМ (№ 5–9)

Инструкция: прочитайте текст, выберите правильный вариант ответа и запишите только букву выбранного варианта ответа (А, Б, В или Г).

ОПК-3.2. Вопрос № 5. Что является уязвимостью?

А) Событие, приводящее к ущербу; Б) Недостаток системы, использование которого нарушителем приводит к реализации угрозы; В) Средство защиты информации; Г) Оценка вероятности ущерба.

Ответ:

ОПК-3.2. Вопрос № 6. Какое свойство обеспечивает электронная подпись документа?

А) Конфиденциальность содержимого; Б) Подтверждение авторства и неизменности документа; В) Сжатие документа; Г) Ускорение передачи документа.

Ответ:

ОПК-3.2. Вопрос № 7. Какой признак наиболее характерен для фишингового сообщения?

А) Наличие подписи отправителя; Б) Побуждение к срочным действиям с переходом по ссылке или вводом учётных данных; В) Указание темы письма; Г) Отправка в рабочее время.

Ответ:

ОПК-3.2. Вопрос № 8. Почему резервные копии не следует хранить только на том же сервере, что и защищаемые данные?

А) Это замедляет работу сервера; Б) При отказе или компрометации сервера будут утрачены и данные, и копии; В) Это увеличивает стоимость лицензий; Г) Копии станут недоступны пользователям.

Ответ:

ОПК-3.2. Вопрос № 9. Какое требование к защите информации в техническом задании является проверяемым?

А) «Система должна быть надёжно защищена»; Б) «Доступ пользователей осуществляется с применением многофакторной аутентификации; события входа фиксируются в журнале с хранением не менее шести месяцев»; В) «Система должна соответствовать современным требованиям»; Г) «Защита обеспечивается на высоком уровне».

Ответ:

РАЗДЕЛ 3. ВОПРОСЫ С ОДНИМ АРГУМЕНТИРОВАННЫМ ОТВЕТОМ (№ 10–13)

Инструкция: Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа.

ОПК-3.2. Вопрос № 10. Достаточно ли установки средства антивирусной защиты для обеспечения безопасности организации?

А) Да, это исчерпывающая мера; Б) Нет, антивирусная защита противодействует лишь части угроз и не заменяет разграничение доступа, резервное копирование, обучение персонала и организационные меры; В) Да, при условии ежедневного обновления баз; Г) Нет, поскольку антивирусные средства бесполезны.

Ответ:

ОПК-3.2. Вопрос № 11. Почему требование ежемесячной смены сложных паролей может снижать реальную защищённость?

А) Оно увеличивает нагрузку на сервер; Б) Пользователи начинают применять предсказуемые модификации и записывать

пароли, что облегчает компрометацию; В) Смена паролей не поддерживается операционными системами; Г) Оно противоречит принципу минимальных привилегий.

Ответ:

ОПК-3.2 Вопрос № 12. Каково первое действие при обнаружении шифровальщика на рабочих станциях организации?
А) Оплатить требуемую сумму; Б) Изолировать поражённые узлы от сети, сохранив их состояние для последующего расследования; В) Немедленно переустановить операционные системы; Г) Перезагрузить все серверы.

Ответ:

ОПК-3.2 Вопрос № 13. Почему формулировка «система должна быть защищена от несанкционированного доступа» непригодна для технического задания?

А) Она слишком длинная; Б) Требование не является проверяемым: не определены механизмы, критерии и порядок подтверждения его выполнения; В) Такая формулировка запрещена стандартами; Г) Она относится к разделу о стоимости работ.

Ответ:

РАЗДЕЛ 4. ВОПРОСЫ С НЕСКОЛЬКИМИ ВЕРНЫМИ ОТВЕТАМИ (№ 14–17)

Инструкция: прочитайте текст, выберите не менее двух правильных вариантов ответов и запишите только буквы выбранных вариантов ответов (А, Б, В или Г).

ОПК-3.2. Вопрос № 14. Какие явления относятся к угрозам информационной безопасности?

А) Вредоносное программное обеспечение; Б) Несанкционированный доступ; В) Утечка данных через съёмные носители; Г) Плановое обновление документации.

Ответ:

ОПК-3.2 Вопрос № 15. Какие меры относятся к обеспечению базовых требований безопасности при работе с данными?
А) Шифрование данных при хранении и передаче; Б) Многофакторная аутентификация; В) Резервное копирование с проверкой восстановления; Г) Отключение журналирования для экономии места.

Ответ:

ОПК-3.2. Вопрос № 16. Какие документы разрабатываются в организации в области защиты информации?

А) Политика информационной безопасности; Б) Модель угроз; В) Регламент предоставления и отзыва доступа; Г) Рекламный буклет организации.

Ответ:

ОПК-3.2. Вопрос № 17. Какие сведения фиксируются при реагировании на инцидент?

А) Время обнаружения и хронология событий; Б) Затронутые информационные активы; В) Выполненные действия по локализации; Г) Личные оценки квалификации коллег.

Ответ:

РАЗДЕЛ 5. ВОПРОСЫ С ОТКРЫТЫМ РАЗВЁРНУТЫМ ОТВЕТОМ (№ 18–21)

Инструкция: Прочитайте текст и запишите развернутый обоснованный ответ.

ОПК-3.2 Вопрос № 18. Опишите порядок построения модели угроз информационной системы.

Ответ:

ОПК-3.2. Вопрос № 19. Опишите комплекс мер по защите учётных записей пользователей организации.

Ответ:

ОПК-3.2. Вопрос № 20. Опишите структуру политики информационной безопасности организации и назначение её разделов.

Ответ:

ОПК-3.2. Вопрос № 21. Объясните, как обеспечивается защищённость резервных копий и почему одного лишь факта их создания недостаточно.

Ответ:

РАЗДЕЛ 6. ВОПРОСЫ НА УСТАНОВЛЕНИЕ ПОСЛЕДОВАТЕЛЬНОСТИ (№ 22–23)

Инструкция: Прочитайте текст, установите правильную последовательность действий и запишите аргументы, обосновывающие выбранный порядок.

ОПК-3.2 Вопрос № 22. Установите последовательность этапов реагирования на инцидент информационной безопасности.

А) Локализация и изоляция затронутых узлов; Б) Обнаружение и регистрация инцидента; В) Восстановление работоспособности систем; Г) Устранение причины и последствий; Д) Анализ инцидента и выработка мер предупреждения повторения.

Ответ:

ОПК-3.2. Вопрос № 23. Установите последовательность действий при определении требований к защите информации создаваемой системы.

А) Построение модели угроз и определение актуальных угроз; Б) Определение состава обрабатываемой информации и её категории; В) Включение требований в техническое задание в проверяемых формулировках; Г) Установление применимых

нормативных требований и класса (уровня) защищённости; Д) Выбор состава мер защиты.

Ответ:

5.4. Перечень видов оценочных средств и критерии оценивания

Контроль результатов освоения дисциплины является формой управления качеством образования.

Контроль результатов освоения дисциплины осуществляется в виде текущего контроля и промежуточной аттестации (экзамена).

Система текущего контроля включает:

- 1) контроль работы на лекционных и практических занятиях;
- 2) контроль выполнения индивидуальных заданий и кейсов;
- 3) контроль выполнения заданий для самостоятельной работы;
- 4) тестирование;
- 5) проверку разработанных комплектов документации.

Промежуточная аттестация осуществляется в виде экзамена, включающего теоретический вопрос и практическое задание на построение модели угроз либо оценку соответствия документации требованиям.

Задачи промежуточной аттестации:

1. определить общий уровень освоения дисциплины в целом;
2. определить уровень основных знаний по каждой теме курса;
3. объективизировать результат контроля, минимизировать возможную субъективность преподавателя.

Критерии и рубрики оценивания (элемент контроля / критерий / индикаторы / уровни 0–3–5 / комментарий к уровню «5»)

Задание № 1 «Инвентаризация активов и модель нарушителя» — полнота анализа защищаемых активов / ОПК-3.2/ 0 – 3 – 5 / Перечень активов полон, ценность каждого обоснована; критичные свойства безопасности определены с пояснением; модель нарушителя содержит категории, мотивацию, возможности и уровень доступа; векторы атаки соотнесены с категориями; исключение неактуальных нарушителей аргументировано.

Задание № 2 «Анализ инцидента и признаки компрометации» — выявление угроз и признаков компрометации / ОПК-3.2/ 0 – 3 – 5 / Все признаки компрометации выявлены; вектор проникновения определён верно; хронология событий восстановлена по журналам; затронутые данные определены; порядок неотложных действий обоснован; разграничены меры предотвращения и меры ускорения обнаружения.

Задание № 3 «Применение криптографических средств» — владение средствами криптографической защиты / ОПК-3.2/ 0 – 3 – 5 / Все операции выполнены корректно; объяснена проблема распределения ключей при симметричном шифровании; продемонстрирован и объяснён эффект изменения одного байта на хэш-значение; электронная подпись сформирована и проверена; чётко разграничены свойства, обеспечиваемые шифрованием и подписью; указаны отечественные стандарты и область их применения.

Задание № 4 «Настройка аутентификации и резервного копирования» — обеспечение базовых требований безопасности / ОПК-3.2/ 0 – 3 – 5 / Парольная политика обоснована и настроена; многофакторная аутентификация работает; права разграничены по принципу минимальных привилегий с выделением привилегированных учётных записей; резервное копирование настроено с шифрованием; восстановление проведено с подтверждением целостности; корректно объяснён эффект частой принудительной смены паролей.

Задание № 5 «Разработка политики безопасности» — качество организационно-распорядительной документации / ОПК-3.2/ 0 – 3 – 5 / Политика содержит все требуемые разделы, положения исполнимы и проверяемы; регламент предоставления доступа детализирован до конкретных действий и ответственных; каждое положение соотнесено с нормативным требованием со ссылкой; документ оценён по заявленным критериям; предложен работоспособный порядок контроля соблюдения.

Кейс № 1 «Реагирование на инцидент» — практика реагирования на инцидент / ОПК-3.2/ 0 – 3 – 5 / Порядок неотложных действий корректен и обоснован; объяснена необходимость изоляции до исследования; возможность восстановления данных оценена реалистично; вектор проникновения и цепочка развития инцидента восстановлены; определён состав фиксируемых сведений; вывод о необходимости уведомления регулятора обоснован; меры разделены на неотложные и долгосрочные.

Кейс № 2 «Оценка защищённости информационной системы» — комплексная оценка защищённости / ОПК-3.2/ 0 – 3 – 5 / Категория данных и применимые требования определены верно; модель угроз построена полно; недостатки предложенного решения выявлены с обоснованием; целевая архитектура предусматривает сегментацию и разграничение доступа; состав технических и организационных мер полон; состав журналируемых событий определён; остаточный риск оценён и обоснован.

Кейс № 3 «Экспертиза технического задания» — оценка соответствия документации требованиям / ОПК-3.2/ 0 – 3 – 5 / Непроверяемая формулировка выявлена и переработана корректно; перечень отсутствующих требований полон; приведены ссылки на конкретные нормативные акты; порядок установления класса и уровня защищённости описан верно; недостающие требования сформулированы в проверяемом виде; риски для обеих сторон оценены; заключение оформлено по правилам служебного документа.

Семинары № 1–3 — участие в обсуждении и качество аргументации / ОПК-3.2/ 0 – 3 – 5 / Обучающийся распознаёт приёмы социальной инженерии и обосновывает вывод, корректно определяет применимые нормативные требования, строит реестр рисков и аргументирует выбор способа их обработки.

Тест — корректность ответов по информационной безопасности / ОПК-3.2/ % → балл / ≥ 90 % — 5; 75–89 % — 4; 60–74 % — 3; < 60 % — 2.

Критерии экзаменационной оценки: «отлично» — исчерпывающий ответ со ссылками на нормативные требования и безошибочно выполненное практическое задание; «хорошо» — ответ с несущественными неточностями;

«удовлетворительно» — фрагментарный ответ при понимании базовых понятий и мер защиты; «неудовлетворительно» — незнание базовых понятий информационной безопасности либо невыполнение практического задания.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

Основная литература:

1. Суворова, Г. М. Информационная безопасность : учебник для вузов . — 2-е изд., пер. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567672>
2. Внуков, А. А. Защита информации : учебник для вузов . — 3-е изд., пер. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561313>
3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов . — Москва : Издательство Юрайт, 2025. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560977>
4. Лось, А. Б., Нестеренко, А. Ю., Рожков, М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов . — 2-е изд. — Москва : Издательство Юрайт, 2026. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/583156>
5. Фомичёв, В. М., Мельников, Д. А. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / под ред. В. М. Фомичёва . — Москва : Издательство Юрайт, 2025. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560804>
6. Чернова, Е. В. Информационная безопасность человека : учебник для вузов . — 3-е изд., пер. и доп. — Москва : Издательство Юрайт, 2026. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587699>
8. Информационные технологии в кибербезопасности : учебник для вузов . — Москва : Издательство Юрайт, 2026. — (Высшее образование). — ISBN 978-5-534-22095-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/600794>

Дополнительная литература и нормативные источники

Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ. — Текст : электронный // Официальный интернет-портал правовой информации. — URL: <http://pravo.gov.ru/>

О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ. — Текст : электронный // Официальный интернет-портал правовой информации. — URL: <http://pravo.gov.ru/> (дата обращения: 27.07.2026).

О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017 г. № 187-ФЗ. — Текст : электронный // Официальный интернет-портал правовой информации. — URL: <http://pravo.gov.ru/>

Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119. — Текст : электронный // Справочная правовая система «КонсультантПлюс». — URL: <http://www.consultant.ru/>

Нормативные и методические документы ФСТЭК России в области защиты информации; банк данных угроз безопасности информации. — URL: <https://fstec.ru/>

ГОСТ Р ИСО/МЭК 27001. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — Текст : электронный // Росстандарт. — URL: <https://protect.gost.ru>

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Сетевые ресурсы Государственного автономного учреждения культуры Свердловской области «Свердловская областная универсальная научная библиотека им. В.Г. Белинского». Режим доступа: https://book.uraic.ru/el_library/resursy_dostup
Э2	Образовательная платформа Юрайт. Режим доступа: https://urait.ru/
Э3	Научная библиотека Cyberleninka. Режим доступа: https://cyberleninka.ru/
Э4	Опубликование стандартов, классификаторов, сводов правил. Режим доступа: https://protect.gost.ru

6.3.1 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

6.3.1.1	Операционная система Astra Linux
6.3.1.2	Офисная система LibreOffice
6.3.1.3	Средства антивирусной защиты отечественного производства; средства криптографической защиты информации.
6.3.1.4	Средства виртуализации для развёртывания учебных стендов; средства резервного копирования; анализатор сетевого трафика
6.3.1.5	Контур.Класс
6.3.1.6	Контур.Толк
6.3.1.7	1С:Университет ПРОФ
6.3.1.8	Среда электронного обучения 3LK (русский Moodle)

7. МТО (оборудование и технические средства обучения)

7.1	Учебные аудитории для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенные оборудованием и техническими средствами обучения: Адрес (местоположение) учебных аудиторий Перечень оборудования и технических средств обучения 620014, Свердловская область, г.о. город Екатеринбург, г Екатеринбург, пр-кт Ленина, стр. 20а, этаж № 5, кабинет № 3 площадью 66,2 м² в помещении 501 Стол – 13 шт. Стул – 25 шт. ПК (с возможностью подключения к сети «Интернет») – 1 шт. Телевизор (75") – 1 шт. Беспроводная система презентаций – 1 шт. Спикерфон – 1 шт. ПК (ноутбук) – 12 шт. 620014, Свердловская область, г.о. город Екатеринбург, г Екатеринбург, пр-кт Ленина, стр. 20а, этаж № 5, кабинет № 19 площадью 31,7 м² в помещении 501 Стол – 7 шт. Стул – 13 шт. ПК (с возможностью подключения к сети «Интернет») – 1 шт. Магнитно-маркерная доска – 1 шт. Телевизор (75") – 1 шт. 620014, Свердловская область, г.о. город Екатеринбург, г Екатеринбург, пр-кт Ленина, стр. 20а, этаж № 5, кабинет № 21 площадью 35,6 м² в помещении 501 Стол – 7 шт. Стул – 13 шт. ПК (с возможностью подключения к сети «Интернет») – 1 шт. Магнитно-маркерная доска – 1 шт. Телевизор (75") – 1 шт. Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета: Адрес (местоположение) помещения для самостоятельной работы обучающихся Перечень компьютерной техники и оборудования 620014, Свердловская область, г.о. город Екатеринбург, г Екатеринбург, пр-кт Ленина, стр. 20а, этаж № 5, кабинет № 5 площадью 44,3 м² в помещении 501 ПК (ноутбук) – 9 шт. Стол – 11 шт. Стул – 11 шт.
-----	---

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для успешного освоения дисциплины рекомендуется ознакомиться с рабочей программой, целями и задачами дисциплины, её связями с другими дисциплинами образовательной программы, изучить основную и дополнительную литературу, нормативные документы и перечень заданий.

Дисциплина имеет выраженную нормативную составляющую: работу с федеральными законами, постановлениями Правительства и документами регуляторов следует вести по действующим редакциям в справочных правовых системах, а не по учебным пересказам.

Все практические работы выполняются исключительно на предоставленных изолированных учебных стендах; применение изучаемых приёмов к системам, не входящим в учебный стенд, недопустимо и влечёт ответственность, установленную законодательством.

Соотношение объёма самостоятельной работы и аудиторных занятий требует регулярности: изучение нормативных документов и подготовку комплектов документации следует распределять по неделям, а не откладывать к концу семестра.

При подготовке документации полезно проверять каждое требование вопросом «как именно будет подтверждено его выполнение при приёме» — это формирует навык написания проверяемых формулировок.

При пропуске занятия следует самостоятельно изучить материал и предоставить преподавателю отчёт по пропущенной теме в часы индивидуальных консультаций.

При подготовке к экзамену необходимо повторить весь материал дисциплины, уделив внимание нормативным требованиям и порядку построения модели угроз, и быть готовым выполнить практическое задание.