Федеральное государственное автономное образовательное учреждение высшего образования
"Самарский государственный экономический университет"

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Уровень высшего образования: бакалавриат

Направление подготовки: 01.03.05 Статистика

Направленность (профиль)подготовки: Информационные системы на финансовых рынках

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2026

Срок получения образования: 4 года

Объем: в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

г. Самара, 2026

Разработчики:
Не имеет Колотилина М. А.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 01.03.05 Статистика, утвержденного приказом Минобрнауки от 14.08.2020 № 1032, с учетом трудовых функций профессиональных стандартов: "Статистик", утвержден приказом Минтруда России от 05.09.2025 № 534н; "Специалист в области инновационных финансовых технологий", утвержден приказом Минтруда России от 13.07.2022 № 413н; "Специалист по финансовому консультированию", утвержден приказом Минтруда России от 19.03.2015 № 167н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Кафедра экономической теории	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Коновалова М. Е.	Рассмотрено	20.05.2026, № 13

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у студентов системного понимания принципов, методов и средств обеспечения информационной безопасности, а также практических навыков их применения для защиты информационных систем и данных в профессиональной деятельности на финансовых рынках с учетом требований регуляторов и современных угроз.

Задачи изучения дисциплины:

- Изучить базовые понятия, модели угроз, нормативно-правовую базу (ФЗ-152, 187-ФЗ, PCI DSS, положения Банка России) и организационно-правовые основы обеспечения информационной безопасности в финансовой сфере.;
- Сформировать практические навыки применения программно-аппаратных средств защиты информации (криптография, ЭП, DLP, SIEM, межсетевые экраны, многофакторная аутентификация) для защиты финансовых информационных систем и данных клиентов.;
- Развить компетенции по выявлению и оценке угроз информационной безопасности, управлению рисками, реагированию на инциденты и обеспечению непрерывности бизнес-процессов финансовых организаций в условиях киберугроз..

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

ОПК-4.1 Понимает принципы работы современных информационных технологий

Знать:

ОПК-4.1/Зн1 Фундаментальные принципы работы современных информационных технологий (архитектура ЭВМ, сетевые протоколы, операционные системы, базы данных, облачные вычисления, криптографические алгоритмы), модели и методы защиты информации, нормативно-правовую базу в области ИБ финансового сектора (ФЗ-152, 187-ФЗ, положения Банка России, международные стандарты ISO/IEC 27001, PCI DSS).

Уметь:

ОПК-4.1/Ум1 Применять знания о принципах работы ИТ для анализа уязвимостей и угроз информационной безопасности в финансовых системах, интерпретировать технические параметры работы ИТ-инфраструктуры с позиции безопасности, понимать последствия сбоев и нарушений работы технологий для финансовых операций и данных клиентов.

Владеть:

ОПК-4.1/Нв1 Навыками системного анализа ИТ-инфраструктуры финансовой организации с точки зрения безопасности, методиками выявления рисков, связанных с использованием современных информационных технологий, навыками обоснования требований к защите информации на основе понимания принципов функционирования ИТ-систем.

ОПК-4.2 Использует современные информационные технологии для решения задач профессиональной деятельности

Знать:

ОПК-4.2/Зн1 Современные информационные технологии и программные средства, используемые для обеспечения информационной безопасности в финансовой сфере (системы криптографической защиты, электронная подпись, DLP-системы, SIEM-решения, межсетевые экраны, системы антивирусной защиты, средства многофакторной аутентификации), их функциональные возможности и области применения.

Уметь:

ОПК-4.2/Ум1 Применять современные ИТ-решения для защиты информационных систем финансовых организаций, использовать программные средства для выявления угроз и инцидентов безопасности, настраивать средства защиты информации, применять технологии шифрования и ЭП при обработке финансовых транзакций и документообороте.

Владеть:

ОПК-4.2/Нв1 Практическими навыками работы с современными средствами защиты информации (настройка политик безопасности, управление доступом, мониторинг событий, анализ журналов безопасности), навыками использования криптографических средств, администрирования СЗИ и систем обнаружения вторжений для решения профессиональных задач по защите финансовых информационных систем.

ОПКЭ-6 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

ОПКЭ-6.1 Понимает и руководствуется принципами работы современных информационных технологий при постановке профессиональных задач

Знать:

ОПКЭ-6.1/Зн1 Принципы функционирования современных ИТ-систем (клиент-сервер, облачные сервисы, базы данных, сетевые протоколы, криптографические средства), их уязвимости и угрозы безопасности, нормативно-правовую базу в области защиты информации на финансовых рынках (ФЗ-152, 187-ФЗ, положения Банка России, PCI DSS, стандарты ЦБ РФ).

Уметь:

ОПКЭ-6.1/Ум1 Анализировать профессиональные задачи в сфере финансовых рынков, определять требования к информационной безопасности (конфиденциальность, целостность, доступность данных), формулировать ограничения и требования к ИТ-решениям на основе принципов работы современных технологий, учитывать риски при постановке задач.

Владеть:

ОПКЭ-6.1/Нв1 Навыками постановки профессиональных задач с учетом принципов информационной безопасности, методиками выявления и оценки угроз для финансовых информационных систем, навыками формулирования требований к защите информации в технических заданиях и проектной документации.

ОПКЭ-6.2 Использует современные информационные технологии для решения задач профессиональной деятельности

Знать:

ОПКЭ-6.2/Зн1 Современные информационные технологии и программно-аппаратные средства защиты информации, используемые в финансовой сфере (СЗИ, SIEM-системы, DLP-решения, криптографические средства, электронная подпись, средства аутентификации и управления доступом), их функциональные возможности и сценарии применения.

Уметь:

ОПКЭ-6.2/Ум1 Применять современные ИТ-решения для защиты информационных систем финансовых организаций, настраивать средства защиты, проводить мониторинг событий безопасности, использовать технологии шифрования и электронной подписи при обработке финансовых данных, внедрять меры защиты в соответствии с требованиями регуляторов.

Владеть:

ОПКЭ-6.2/Нв1 Практическими навыками работы с современными средствами информационной безопасности (антивирусные средства, межсетевые экраны, системы обнаружения вторжений, средства криптографической защиты), навыками настройки политик безопасности, управления доступом, аудита и контроля защищенности информационных систем на финансовых рынках.

ОПКЭ-6.3 Осуществляет постановку профессиональных задач, опираясь на возможности их решения путем применения современных информационно-коммуникационных технологий

Знать:

ОПКЭ-6.3/Зн1 Современные ИКТ-решения и платформы для обеспечения информационной безопасности финансовых организаций, их функциональные возможности, ограничения и области применения (BI-системы, облачные сервисы, DLP, SIEM, PKI, средства криптографической защиты, системы управления рисками и комплаенс-решения).

Уметь:

ОПКЭ-6.3/Ум1 Анализировать профессиональные задачи в области финансовых рынков с точки зрения возможности их решения с применением современных ИКТ, определять требования к информационной безопасности, формулировать технические задания, декомпозировать задачи на компоненты, оценивать соответствие ИКТ-решений нормативным требованиям (ФЗ, положения Банка России, PCI DSS).

Владеть:

ОПКЭ-6.3/Нв1 Навыками постановки технического задания для разработчиков и внедренцев систем защиты информации, методиками оценки рисков информационной безопасности при внедрении ИКТ, навыками обоснования выбора технологических решений и защиты их перед стейкхолдерами, методами контроля эффективности внедренных ИКТ-решений в финансовой сфере.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Основы информационной безопасности» относится к обязательной части образовательной программы и изучается в семестре(ах): 3.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ОПК-4 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности		

ОПК-4.1 Понимает принципы работы современных информационных технологий	Основы алгоритмизации и программирования, Технологии цифровой экономики	Кибербезопасность, Основы алгоритмизации и программирования, Пакеты прикладных статистических программ, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации, Учебная практика: ознакомительная практика
ОПК-4.2 Использует современные информационные технологии для решения задач профессиональной деятельности	Основы алгоритмизации и программирования, Технологии цифровой экономики	Кибербезопасность, Основы алгоритмизации и программирования, Пакеты прикладных статистических программ, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации, Учебная практика: ознакомительная практика
ОПКЭ-6 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности		
ОПКЭ-6.1 Понимает и руководствуется принципами работы современных информационных технологий при постановке профессиональных задач	Основы алгоритмизации и программирования, Технологии цифровой экономики	Кибербезопасность, Основы алгоритмизации и программирования, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации

ОПКЭ-6.2 Использует современные информационные технологии для решения задач профессиональной деятельности	Основы алгоритмизации и программирования, Технологии цифровой экономики	Кибербезопасность, Основы алгоритмизации и программирования, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации
ОПКЭ-6.3 Осуществляет постановку профессиональных задач, опираясь на возможности их решения путем применения современных информационно-коммуникационных технологий	Основы алгоритмизации и программирования, Технологии цифровой экономики	Кибербезопасность, Основы алгоритмизации и программирования, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лекционные занятия (часы)	Практические занятия (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Третий семестр	108	3	54	18	36	0,15	35,85	Зачет
Всего	108	3	54	18	36	0,15	35,85	18

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа

Раздел 1. Информационная безопасность	**90**	**18**	**36**	**35,85**
Тема 1.1. Информационная безопасность	10	2	4	4
Тема 1.2. Принципы криптографической защиты информации	10	2	4	4
Тема 1.3. Современные симметричные криптосистемы	10	2	4	4
Тема 1.4. Асимметричные криптосистемы	8	2	2	4
Тема 1.5. Идентификация и проверка подлинности	10,15	2	4	4
Тема 1.6. Электронная цифровая подпись	10	2	4	4
Тема 1.7. Управление криптографическими ключами	12	2	6	4
Тема 1.8. Политика ИБ и Оценка рисков ИБ	10	2	4	4
Тема 1.9. Программные средства защиты информации	9,85	2	4	3,85

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестирование
Промежуточная аттестация	Зачет

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Информационная безопасность	Тестирование	Зачет

6. Оценочные материалы текущего контроля

1. Информационная безопасность Тестирование

№ п/п	Содержание вопроса	Компетенция
	Правильный ответ (ключ ответа)	
1	Дайте ответ Выберете один вариант ответа Конфиденциальность данных (информации) это? 1. внутреннее свойство информации; 2. статус, представляемый данным и определяющий степень их защиты; 3. значительные объемы информации; 4. информация, предназначенная для передачи. Ответ: 2	ОПК-4
2	Дайте ответ Выберете один вариант ответа В чём отличие санкционированного (СД) и несанкционированного (НСД) доступа к информации? 1. НСД не нарушает установленные правила разграничения доступа; 2. СД не нарушает установленные правила разграничения доступа; 3. СД обеспечивает конфиденциальность информации; 4. СД обеспечивает целостность информации.	ОПК-4

	Ответ:	2	
3	Дайте ответ Выберете один вариант ответа Субъект информационной системы это? 1. пользователь системы; 2. активный компонент системы, который может стать причиной потока информации от объекта к субъекту; 3. отправитель сообщения; 4. получатель сообщения.		ОПК-4
	Ответ:	2	
4	Дайте ответ Выберете один вариант ответа Целостность информации это: 1. скрытность информации; 2. важность информации; 3. подлинность информации; 4. объем информации		ОПК-4
	Ответ:	3	
5	Дайте ответ Выберете один вариант ответа Цель процедуры идентификации заключается в: 1. предъявлении субъектом своего уникального имени по запросу системы; 2. доказательстве подлинности; 3. доказательстве целостности; 4. применении электронной цифровой подписи.		ОПК-4
	Ответ:	1	
6	Дайте ответ Напишите правильный ответ на вопрос 1 словом Как называется раздел науки, изучающий защиту информации с помощью шифрования?		ОПК-4
	Ответ:	Криптография	
7	Дайте ответ Напишите правильный ответ на вопрос 1 словом Как называется процедура подтверждения личности пользователя?		ОПК-4
	Ответ:	Аутентификация	
8	Дайте ответ Напишите правильный ответ на вопрос 1 словом Как называется свойство информации быть доступной только уполномоченным лицам?		ОПК-4
	Ответ:	Конфиденциальность	
9	Дайте ответ Напишите правильный ответ на вопрос 1 словом Как называется процедура предоставления пользователю прав на выполнение определенных действий в системе?		ОПК-4
	Ответ:	Авторизация	
10	Дайте ответ Напишите правильный ответ на вопрос 1 словом Как называется вид шифрования с одним и тем же ключом для шифрования и расшифрования?		ОПК-4
	Ответ:	Симметричное	
11	Дайте ответ Напишите правильный ответ на вопрос 1 словом Как называется вид шифрования, где используются открытый и закрытый ключи?		ОПК-4
	Ответ:	Асимметричное	
12	Дайте ответ Напишите правильный ответ на вопрос 1 словом Как называется секретный параметр, используемый в криптографии?		ОПК-4
	Ответ:	Ключ	
13	Дайте ответ Напишите правильный ответ на вопрос 1 словом Как называется характеристика, отражающая вероятность реализации угрозы?		ОПК-4
	Ответ:	Риск	

14	Дайте ответ Установите соответствие между 1. Информационная безопасность 2. Угроза 3. Уязвимость А Возможность нарушения защищенности информации вследствие наличия слабого места в системе. Б. Состояние защищенности информации от несанкционированного доступа, искажения и уничтожения. В. Потенциальное событие или действие, способное нанести вред информации или системе. Ответ: 1-Б 2-В 3-А	ОПК-4
15	Дайте ответ Установите соответствие между 1. Конфиденциальность 2. Целостность 3. Доступность А Свойство информации быть доступной только уполномоченным лицам. Б Свойство информации, гарантирующее, что авторизованные пользователи могут беспрепятственно и своевременно получать, использовать или изменять нужную информацию, имея на это соответствующие законные полномочия В Свойство информации сохранять точность и неизменность при хранении и передаче. Ответ: 1-А 2-В 3-Б	ОПК-4
16	Дайте ответ Установите соответствие между 1. Идентификация 2. Авторизация 3. Аутентификация А Процедура проверки подлинности пользователя или устройства Б Процесс распознавания и установления тождественности объекта или личности по их уникальным признакам или идентификаторам. В Процесс предоставления пользователю прав на выполнение определенных действий в системе Ответ: 1-Б 2-В 3-А	ОПК-4
17	Дайте ответ Установите верную последовательность. Расположите этапы в правильной последовательности для процесса аутентификации пользователя. 1. Пользователь вводит учетные данные. 2. Система проверяет их подлинность. 3. Пользователь получает доступ к ресурсам. 4. Система принимает решение о допуске. Ответ: 1, 2, 4, 3	ОПК-4
18	Дайте ответ Установите верную последовательность Расположите этапы в правильной последовательности для процесса формирование электронной подписи 1. Хэш подписывается закрытым ключом 2. Подписанный документ передается получателю 3. Получатель проверяет подпись открытым ключом. 4. Документ преобразуется в хэш. Ответ: 4, 1, 2, 3	ОПК-4
19	Дайте ответ Выберете один вариант ответа Какова основная функция электронной цифровой подписи (ЭЦП) при работе с электронными документами? 1. Создание резервной копии документа на защищенном сервере 2. Обеспечение только конфиденциальности содержимого документа 3. Подтверждение авторства и неизменности документа с момента подписания 4. Сокращение объема передаваемых по сети данных Ответ: 3	ОПК-4

20	Дайте ответ Выберете один вариант ответа Что лучше всего описывает процесс управления криптографическими ключами в организации? 1. Исключительно процедура выпуска цифровых сертификатов центром сертификации 2. Только техническое хранение ключей в зашифрованном виде 3. Совокупность процедур генерации, распределения, хранения, смены и уничтожения ключей 4. Использование одного и того же ключа для всех сотрудников для упрощения администрирования Ответ: 3	ОПК-4
21	Дайте ответ Выберете один вариант ответа Какой из перечисленных шагов является ключевой частью процесса оценки рисков информационной безопасности? 1. Игнорирование маловероятных угроз, чтобы сократить список рисков до минимума 2. Определение вероятности реализации угроз и возможного ущерба для активов 3. Обязательное шифрование всех файлов, независимо от их ценности 4. Установка антивируса на все рабочие станции компании Ответ: 2	ОПК-4
22	Дайте ответ Выберете один вариант ответа Какова основная цель политики информационной безопасности в организации? 1. Техническое описание алгоритмов шифрования, применяемых в компании 2. Формальное определение принципов, правил и обязанностей по защите информации 3. Детальное описание всех аппаратных средств, используемых в ИТ-инфраструктуре 4. Перечисление всех возможных вирусов и вредоносных программ Ответ: 2	ОПК-4
23	Дайте ответ Установите соответствие между 1. Криптографические средства 2. Программные средства 3. Аппаратные средства А. Технические устройства, встраиваемые в систему для защиты от несанкционированного доступа и утечек. Б. Программы и программные комплексы, предназначенные для контроля, хранения и защиты информации. В. Системы и устройства, которые обеспечивают защиту информации путем преобразования данных и использования ключей. Ответ: 1-В 2-Б 3-А	ОПК-4
24	Дайте ответ Установите соответствие между 1. Физические средства 2. Организационные средства 3. Межсетевые экраны А Средства, создающие физические препятствия доступу к информации, например замки и камеры. Б Средства сетевой защиты, контролирующие и фильтрующие трафик между сетями. В Средства, регламентирующие порядок работы с информацией, документооборот и действия персонала. Ответ: 1-А 2-В 3-Б	ОПК-4
25	Дайте ответ Установите соответствие между 1. Электронная подпись 2. Хэш-функция 3. Иерархия ключей А Математическая функция, преобразующая данные в фиксированное значение и используемая для контроля целостности. Б Последовательность уровней криптографических ключей, применяемая для их безопасного хранения и использования. В Криптографический реквизит документа, подтверждающий его подлинность и целостность. Ответ: 1-В 2-А 3-Б	ОПК-4

26	Дайте ответ Установите верную последовательность Расположите этапы в правильной последовательности для работы асимметричной криптосистемы 1. Сообщение расшифровывается закрытым ключом 2. Сообщение шифруется открытым ключом 3. Открытый ключ передается другим пользователям. 4.. Пользователь создает пару ключей Ответ: 4, 3, 2, 1	ОПК-4
27	Дайте ответ Установите верную последовательность Расположите этапы в правильной последовательности для обеспечения безопасности сетей 1. Настраиваются правила доступа. 2. Определяются возможные угрозы 3. Выбираются средства защиты 4. Организуется контроль трафика. Ответ: 2, 3, 1, 4	ОПК-4
28	Дайте ответ Выберете один вариант ответа Какой из перечисленных примеров лучше всего иллюстрирует программные средства защиты информации? 1. Физический сейф для хранения бумажных документов с ограниченным доступом 2. Договор о неразглашении (NDA), подписанный сотрудниками 3. Антивирусное программное обеспечение и межсетевой экран (firewall) 4. Регламент доступа сотрудников в серверную комнату и правила проверки пропусков Ответ: 3	ОПК-4
29	Какая современная информационная технология используется для обеспечения конфиденциальности данных при передаче финансовой информации по открытым каналам связи? А) Технология межсетевого экранирования (Firewall) Б) Технология криптографического шифрования (SSL/TLS, VPN) В) Система обнаружения вторжений (IDS) Г) Технология DLP (Data Loss Prevention) Д) Антивирусное программное обеспечение Ответ: Б	ОПКЭ-6
30	Какой современный ИТ-инструмент позволяет автоматически выявлять и блокировать попытки несанкционированной передачи конфиденциальной информации из финансовой организации? А) SIEM-система Б) DLP-система В) VPN-сервер Г) Межсетевой экран Д) Электронная подпись Ответ: Б	ОПКЭ-6
31	Для решения какой профессиональной задачи в финансовой сфере используется технология электронной подписи (ЭП)? А) Для шифрования базы данных клиентов Б) Для обеспечения юридической значимости электронных документов и подтверждения авторства в финансовых транзакциях В) Для антивирусной проверки входящих писем Г) Для фильтрации сетевого трафика Д) Для резервного копирования финансовой отчетности Ответ: Б	ОПКЭ-6
32	Какое современное ИТ-решение используется для централизованного сбора, корреляции и анализа событий безопасности в информационных системах финансовых организаций? А) DLP-система Б) SIEM-система (Security Information and Event Management) В) СКЗИ (средство криптографической защиты информации) Г) VPN-сервер Д) Система резервного копирования Ответ: Б	ОПКЭ-6
33	Какая современная информационная технология позволяет обеспечить защиту от несанкционированного доступа к корпоративной сети финансовой организации при подключении удаленных сотрудников? А) Технология DLP Б) Технология виртуализации В) Технология VPN с многофакторной аутентификацией Г) Технология электронного документооборота Д) Технология облачных вычислений Ответ: В	ОПКЭ-6
34	Установите соответствие между современной информационной технологией и её применением для решения профессиональных задач в области финансовой безопасности.	ОПКЭ-6

Информационная технология (А-Д)	Применение для решения профессиональных задач (1-5)
А. Криптографическое шифрование	1. Обеспечение юридической значимости финансовых документов и транзакций
Б. Электронная подпись	2. Обнаружение и предотвращение утечек конфиденциальной информации клиентов
В. DLP-система	3. Защита данных клиентов при передаче через открытые сети
Г. SIEM-система	4. Защита корпоративной сети при удаленном доступе сотрудников
Д. VPN-технология	5. Централизованный мониторинг и корреляция событий безопасности

Ответ: А-3, Б-1, В-2, Г-5, Д-4

35 Установите соответствие между типом угрозы информационной безопасности и современной ИТ-технологией, используемой для её нейтрализации. ОПКЭ-6

Тип угрозы (А-Д)	Технология защиты (1-5)
А. Перехват данных при передаче по сети	1. Технология SSL/TLS-шифрования и VPN
Б. Вредоносное ПО и вирусы	2. Антивирусные средства и системы обнаружения вторжений
В. Несанкционированный доступ к БД клиентов	3. Средства многофакторной аутентификации и управления доступом (IAM)
Г. Утечка конфиденциальной информации через каналы связи	4. DLP-системы и системы контроля сетевых потоков
Д. Сбой в работе критической финансовой системы	5. Системы резервного копирования и Disaster Recovery

Ответ: А-1, Б-2, В-3, Г-4, Д-5

36 Установите соответствие между профессиональной задачей в финансовой сфере и современной ИТ-технологией, применяемой для её решения. ОПКЭ-6

Профессиональная задача (А-Д)	ИТ-технология для решения (1-5)
А. Обеспечение безопасного удаленного доступа сотрудников к корпоративным ресурсам	1. Технология виртуализации (VDI, VMware)
Б. Шифрование персональных данных клиентов в базах данных	2. Технология TLS/SSL и средства криптографической защиты СКЗИ
В. Выявление инцидентов и реагирование на кибератаки в реальном времени	3. SIEM-система с модулями SOAR
Г. Создание изолированной среды для тестирования финансовых приложений	4. Многофакторная аутентификация и VPN
Д. Проверка целостности и подлинности электронных финансовых документов	5. Технологии электронной подписи и PKI (инфраструктура открытых ключей)

Ответ: А-4, Б-2, В-3, Г-1, Д-5

37 Расположите в правильной последовательности этапы использования современных ИТ-технологий для обработки инцидента информационной безопасности в финансовой организации. Все 4 варианта должны быть использованы. ОПКЭ-6

1 Использование SIEM-системы для обнаружения и идентификации инцидента безопасности

2 Локализация угрозы с помощью межсетевого экрана и сегментации сети

3 Проведение расследования с использованием инструментов логирования и анализа данных

4 Восстановление работоспособности систем с использованием резервных копий и мониторинг состояния после инцидента

Ответ: 1 → 2 → 3 → 4

38 Расположите в правильной последовательности применение современных ИТ-технологий при обеспечении безопасного электронного документооборота в финансовой организации. Все 4 варианта должны быть использованы. ОПКЭ-6

1.
1 Использование VPN-соединения для защищенной передачи документов

2 Применение средств криптографической защиты (СКЗИ) для шифрования содержимого

3 Подписание документа с использованием технологии электронной подписи (ЭП)

4 Проверка целостности и подлинности документа получателем с помощью сертификата проверки ЭП

Ответ: 1 → 2 → 3 → 4

39 Дайте развернутый письменный ответ (объемом 3-5 предложений) на поставленный вопрос. Ответ должен содержать обоснование использования конкретной ИТ-технологии для решения профессиональной задачи. ОПКЭ-6
В финансовой организации (банк) произошла утечка персональных данных клиентов при передаче отчетности через незащищенный канал связи. Какие современные ИТ-технологии необходимо использовать для решения данной профессиональной задачи по защите данных при передаче? Обоснуйте выбор.

	Ответ:	Для решения задачи необходимо использовать технологии криптографического шифрования (SSL/TLS) и VPN-соединения при передаче финансовой отчетности, что обеспечивает конфиденциальность и защиту от перехвата данных. Также следует внедрить DLP-систему для мониторинга и контроля исходящих потоков данных, которая блокирует передачу конфиденциальной информации в открытом виде и предотвращает утечки в будущем. Дополнительно рекомендуется использовать средства электронной подписи для подтверждения целостности и подлинности передаваемых документов, что соответствует требованиям ФЗ-152 и стандартам Банка России. Обоснование: SSL/TLS и VPN обеспечивают защиту каналов передачи данных, DLP предотвращает несанкционированную передачу, ЭП гарантирует юридическую значимость и целостность финансовой информации.	
40	Дайте развернутый письменный ответ (объемом 3-5 предложений) на поставленный вопрос. Ответ должен содержать конкретное ИТ-решение и его обоснование. Для банка требуется внедрить систему, обеспечивающую мониторинг и анализ событий безопасности в режиме реального времени, а также автоматическое реагирование на инциденты. Выберите подходящую современную ИТ-технологию и опишите её функционал для решения профессиональных задач по защите финансовой информационной системы.		ОПКЭ-6
	Ответ:	В качестве современного ИТ-решения предлагается внедрение SIEM-системы (Security Information and Event Management) с модулями SOAR (Security Orchestration, Automation, and Response), например, MaxPatrol, ArcSight, QRadar. SIEM-система обеспечивает централизованный сбор и корреляцию событий со всех сетевых устройств, систем защиты и серверов, позволяет в реальном времени выявлять аномалии и признаки атак, а автоматизированные плейбуки SOAR обеспечивают быстрое реагирование на инциденты без участия человека. Обоснование: SIEM-система позволяет решить задачи оперативного выявления кибератак, снижения времени реагирования (MTTR), а также соответствует регуляторным требованиям Банка России по централизованному мониторингу событий безопасности.	
41	Дайте развернутый письменный ответ (объемом 3-5 предложений) на поставленный вопрос. Ответ должен содержать анализ применения ИТ-технологий для конкретной профессиональной ситуации. В финансовой организации внедряется система электронного документооборота (СЭД) между головным офисом и филиалами. Какие современные ИТ-технологии необходимо применить для обеспечения юридической значимости и безопасности финансовых документов при передаче? Опишите последовательность применения данных технологий.		ОПКЭ-6
	Ответ:	При внедрении СЭД необходимо использовать три ключевые технологии: 1) VPN- или TLS-соединение для защищенного канала передачи документов между офисами; 2) средства криптографической защиты (СКЗИ) для шифрования передаваемых файлов; 3) технологию электронной подписи (ЭП) с сертифицированным удостоверяющим центром для придания документам юридической значимости в соответствии с ФЗ-63 «Об электронной подписи». Последовательность применения: документ подписывается квалифицированной ЭП, шифруется СКЗИ, передается по защищенному VPN-каналу, на стороне получателя расшифровывается и проверяется подлинность ЭП. Это обеспечивает целостность, конфиденциальность и юридическую силу финансовых документов.	
42	Сформулируйте развернутый ответ на задачу с указанием современной ИТ-технологии, её преимуществ и практического применения. В банке требуется организовать защищенный удаленный доступ для сотрудников, работающих из дома, к корпоративной сети и финансовым системам. Опишите, какие современные ИТ-технологии необходимо применить для решения данной профессиональной задачи, и укажите дополнительные меры безопасности.		ОПКЭ-6
	Ответ:	Для организации защищенного удаленного доступа необходимо использовать современную VPN-технологию (например, OpenVPN или корпоративные решения Cisco AnyConnect, FortiClient) с обязательной многофакторной аутентификацией (MFA) на базе одноразовых паролей (TOTP) или аппаратных токенов. Дополнительными мерами безопасности являются: сегментация сети и принцип наименьших привилегий (Zero Trust), установка антивирусного ПО на удаленные рабочие станции, регулярный аудит журналов доступа через SIEM-систему. Обоснование: VPN-технология с MFA позволяет исключить риски несанкционированного доступа при компрометации учетных данных сотрудника, соответствует требованиям Банка России по организации удаленного доступа к информационным системам кредитных организаций (Положение 727-П).	
43	Дайте развернутый ответ, содержащий обоснование выбора современных ИТ-технологий и их практического применения для решения профессиональных задач в финансовой сфере. Финансовая организация планирует провести модернизацию системы обеспечения информационной безопасности с внедрением современных ИТ-технологий для защиты от внутренних и внешних угроз. Опишите, какие современные ИТ-технологии и программные средства необходимо внедрить для решения следующих профессиональных задач: (1) защита от внешних сетевых атак, (2) контроль действий сотрудников и предотвращение утечек данных, (3) обеспечение непрерывности работы финансовых систем при сбоях.		ОПКЭ-6

	Ответ:	Для защиты от внешних сетевых атак необходимо внедрить современные межсетевые экраны следующего поколения (NGFW) с функциями IPS/IDS и средствами защиты от DDoS-атак, что позволяет блокировать вредоносный трафик на границе сети. Для контроля действий сотрудников и предотвращения утечек данных следует внедрить DLP-систему с анализом контекста и контента (например, Solar Dozor, InfoWatch Traffic Monitor) с интеграцией в SIEM-систему для централизованного мониторинга. Для обеспечения непрерывности работы финансовых систем внедряются системы резервного копирования с технологией Disaster Recovery (CDP — непрерывная защита данных) и развертывание резервных центров обработки данных (ЦОД) с географической удаленностью. Обоснование: NGFW-системы обеспечивают сетевую защиту на уровне L7 и соответствуют требованиям регуляторов; DLP и SIEM решают задачи контроля персонала и соответствия ФЗ-152; CDP и DR-решения гарантируют непрерывность бизнес-процессов (RPO, RTO) согласно стандартам Банка России и ISO 22301.	

7. Оценочные материалы промежуточной аттестации

Зачет третий семестр

№ п/п	Содержание вопроса	Правильный ответ (ключ ответа)	Компетенция
1	Дайте развернутый ответ Что такое информационная безопасность?		ОПК-4, ОПКЭ-6
	Ответ:	Это состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, целостность и доступность.	
2	Дайте развернутый ответ Что относится к основным угрозам информационной безопасности?		ОПК-4, ОПКЭ-6
	Ответ:	Несанкционированный доступ, утечка данных, вирусные атаки, искажение информации, отказ в обслуживании.	
3	Дайте развернутый ответ В чем состоит отличие симметричной криптосистемы от асимметричной?		ОПК-4, ОПКЭ-6
	Ответ:	В симметричной криптосистеме для шифрования и расшифрования используется один ключ, а в асимметричной — пара ключей, открытый и закрытый.	
4	Дайте развернутый ответ Что такое аутентификация?		ОПК-4, ОПКЭ-6
	Ответ:	Это процедура проверки подлинности пользователя, устройства или сообщения.	
5	Дайте развернутый ответ Для чего используется электронная цифровая подпись?		ОПК-4, ОПКЭ-6
	Ответ:	Она используется для подтверждения подлинности документа и контроля его целостности.	
6	Дайте развернутый ответ Что такое хэш-функция?		ОПК-4, ОПКЭ-6
	Ответ:	Это функция, которая преобразует данные в фиксированное значение, используемое для проверки целостности информации.	
7	Дайте развернутый ответ Что включает в себя управление криптографическими ключами?		ОПК-4, ОПКЭ-6
	Ответ:	Генерацию, распределение, хранение, замену и уничтожение ключей.	
8	Дайте развернутый ответ Что такое политика информационной безопасности?		ОПК-4, ОПКЭ-6
	Ответ:	Это совокупность правил, процедур и требований, определяющих порядок защиты информации в организации.	
9	Дайте развернутый ответ Что понимается под оценкой рисков информационной безопасности?		ОПК-4, ОПКЭ-6
	Ответ:	Это процесс выявления угроз, анализа уязвимостей и определения вероятности и последствий возможных инцидентов.	
10	Дайте развернутый ответ Какие средства относятся к программным средствам защиты информации?		ОПК-4, ОПКЭ-6
	Ответ:	Антивирусы, межсетевые экраны, средства аутентификации, системы обнаружения вторжений и средства контроля доступа.	

7.1. Уровни овладения

Компетенция: ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Индикатор достижения компетенции: ОПК-4.1 Понимает принципы работы современных информационных технологий.

Уровень	Характеристика	Оценка в баллах

Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Индикатор достижения компетенции: ОПК-4.2 Использует современные информационные технологии для решения задач профессиональной деятельности.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Компетенция: ОПКЭ-6 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Индикатор достижения компетенции: ОПКЭ-6.1 Понимает и руководствуется принципами работы современных информационных технологий при постановке профессиональных задач.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100

Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Индикатор достижения компетенции: ОПКЭ-6.2 Использует современные информационные технологии для решения задач профессиональной деятельности.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Индикатор достижения компетенции: ОПКЭ-6.3 Осуществляет постановку профессиональных задач, опираясь на возможности их решения путем применения современных информационно-коммуникационных технологий.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Полякова, Т. А. Организационное и правовое обеспечение информационной безопасности: учебник для вузов / Т. А. Полякова, С. Г. Чубукова, В. А. Ниесов; Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова.. - 2-е изд. - Москва: Юрайт, 2026. - 357 с - 978-5-534-19108-0. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/583236 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2026. - 312 с - 978-5-9916-9043-0. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/584673 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Суворова, Г. М. Информационная безопасность: учебник для вузов / Г. М. Суворова. - 2-е изд. - Москва: Юрайт, 2026. - 277 с - 978-5-534-16450-3. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588515 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Щербак, А. В. Информационная безопасность: учебник для вузов / А. В. Щербак. - 2-е изд. - Москва: Юрайт, 2026. - 252 с - 978-5-9916-4299-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589902 (дата обращения: 21.05.2026). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. http://www.pravo.gov.ru/ips/ - Информационно-правовая система «Законодательство России»

2. https://rosstat.gov.ru/ - Федеральная служба государственной статистики (Росстат)

3. https://www.economy.gov.ru/ - Министерство экономического развития Российской Федерации (Минэкономразвития России)

4. https://www.planetaexcel.ru/ - Планета Excel

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

1. Средство анализа защищенности "Сканер-ВС" лицензия на 1 IP-адрес (специальная версия);
2. СЗИ Security Studio Endpoint Protection: Antivirus, Personal Firewall, ;
3. СКЗИ "КриптоПро CSP";
4. Консультант Плюс;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения