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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «КИБЕРБЕЗОПАСНОСТЬ»

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: 5 з.е.
в академических часах: 180 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 системных знаний о современных киберугрозах, методах и средствах защиты информационных систем, а также практических навыков выявления, предотвращения и реагирования на кибератаки в профессиональной деятельности.

Задачи изучения дисциплины:

- Изучить классификацию и модели киберугроз, тактики и техники атакующих (MITRE ATT&CK), уязвимости информационных систем и современные векторы атак.;
- Сформировать практические навыки применения средств защиты (межсетевые экраны, IDS/IPS, антивирусы, SIEM, DLP, криптография, системы управления уязвимостями) для предотвращения и обнаружения кибератак.;
- Развить компетенции по управлению инцидентами кибербезопасности, проведению расследований, восстановлению после атак (включая вымогательское ПО) и обеспечению непрерывности бизнес-процессов организаций..

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 компьютерных сетей, операционные системы, базы данных, облачные вычисления, криптографические алгоритмы, протоколы передачи данных), модели и методы обеспечения кибербезопасности, нормативно-правовую базу в финансовом секторе (ФЗ-152, 187-ФЗ, положения Банка России, ГОСТ Р 56545-2015, стандарты ISO/IEC 27001, PCI DSS).

Уметь:

ОПК-4.1/Ум1 Применять знания о принципах работы ИТ для анализа уязвимостей информационных систем финансовых организаций, понимать механизмы реализации кибератак (фишинг, вредоносное ПО, атаки на веб-приложения, DDoS), интерпретировать параметры работы ИТ-инфраструктуры с позиции кибербезопасности и оценивать последствия нарушений для финансовых операций и данных клиентов.

Владеть:

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

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

Знать:

ОПК-4.2/Зн1 Современные информационные технологии и программно-аппаратные средства обеспечения кибербезопасности, используемые в финансовой сфере (межсетевые экраны нового поколения (NGFW), системы обнаружения и предотвращения вторжений (IDS/IPS), SIEM-решения, DLP-системы, средства криптографической защиты (СКЗИ), электронная подпись, системы многофакторной аутентификации, средства защиты конечных точек (EDR/XDR), антивирусные комплексы), их функциональные возможности, архитектуру и сценарии применения для защиты финансовых информационных систем.

Уметь:

ОПК-4.2/Ум1 Применять современные ИТ-решения для выявления, предотвращения и нейтрализации кибератак на финансовые организации, настраивать средства защиты информации в соответствии с требованиями регуляторов (Банк России, ФСТЭК), использовать технологии шифрования и электронной подписи для защиты финансовых транзакций и документооборота, проводить мониторинг событий безопасности с использованием SIEM-систем, анализировать журналы безопасности и выявлять признаки компрометации.

Владеть:

ОПК-4.2/Нв1 Практическими навыками работы с современными средствами кибербезопасности (настройка политик безопасности, управление доступом, мониторинг и корреляция событий, анализ инцидентов), навыками использования криптографических средств и ЭП, администрирования систем защиты конечных точек (EDR), проведения анализа уязвимостей и применения средств защиты для обеспечения безопасности финансовых информационных систем в условиях постоянно меняющегося ландшафта угроз.

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 информационно-коммуникационных технологий (архитектура сетей, операционные системы, базы данных, облачные платформы, криптографические протоколы, средства защиты информации), модели угроз и уязвимости, присущие различным ИТ-архитектурам, а также нормативно-правовую базу в области кибербезопасности финансового сектора (ФЗ-152, 187-ФЗ, 486-ФЗ, положения Банка России, стандарты Банка России по обеспечению информационной безопасности, ГОСТ Р 57580.1-2017).

Уметь:

ОПКЭ-6.1/Ум1 Анализировать профессиональные задачи в сфере финансовых рынков с учетом принципов работы современных ИТ, определять требования к кибербезопасности (конфиденциальность, целостность, доступность, наблюдаемость, управляемость), выявлять возможные угрозы и уязвимости на этапе постановки задачи, формулировать ограничения по безопасности, связанные с особенностями ИТ-архитектуры, и учитывать их при формулировании технических заданий на разработку и внедрение информационных систем в финансовой организации.

Владеть:

ОПКЭ-6.1/Нв1 Навыками постановки профессиональных задач с учетом принципов кибербезопасности и руководствуясь требованиями регуляторов финансового рынка, методиками выявления и оценки угроз для финансовых информационных систем на основе понимания принципов работы ИТ, навыками формулирования требований к защите информации в технических заданиях, проектной документации и регламентах, а также навыками обоснования выбора архитектурных решений с позиции безопасности перед руководством и стейкхолдерами.

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

Знать:

ОПКЭ-6.2/Зн1 Современные информационные технологии и программно-аппаратные средства обеспечения кибербезопасности, применяемые в финансовой сфере (межсетевые экраны следующего поколения (NGFW), системы обнаружения и предотвращения вторжений (IDS/IPS), SIEM-решения, DLP-системы, средства криптографической защиты информации (СКЗИ), электронная подпись, системы многофакторной аутентификации, EDR/XDR-решения, антивирусные комплексы, системы управления уязвимостями и сканеры безопасности), их функциональные возможности, архитектуру, методы развертывания и эксплуатации.

Уметь:

ОПКЭ-6.2/Ум1 Применять современные ИТ-решения для защиты финансовых информационных систем от кибератак, настраивать и администрировать средства защиты информации в соответствии с требованиями регуляторов (Банк России, ФСТЭК, ФСБ), использовать технологии шифрования и электронной подписи при обработке финансовых транзакций и электронного документооборота, проводить мониторинг событий безопасности с использованием SIEM-систем, осуществлять анализ журналов, выявлять индикаторы компрометации (IOC) и оперативно реагировать на инциденты.

Владеть:

ОПКЭ-6.2/Нв1 Практическими навыками работы с современными средствами кибербезопасности (настройка политик безопасности, управление доступом и привилегиями, мониторинг и корреляция событий, анализ инцидентов и реагирование), навыками использования криптографических средств и электронной подписи для обеспечения безопасности финансовых операций, администрирования систем защиты конечных точек (EDR/XDR), проведения сканирования уязвимостей, анализа защищенности и применения средств защиты для обеспечения непрерывности и безопасности финансовых информационных систем в условиях современного ландшафта киберугроз.

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 кибербезопасности финансовых организаций (SIEM/SOAR-системы, DLP-решения, NGFW, WAF, средства криптографической защиты и PKI, системы управления уязвимостями и безопасностью контейнеров/облачных сред, сервисы Threat Intelligence, платформы для автоматизации реагирования на инциденты), их функциональные возможности, архитектуру, ограничения, сценарии внедрения и соответствие требованиям регуляторов (Банк России, ФСТЭК, ФСБ).

Уметь:

ОПКЭ-6.3/Ум1 Анализировать профессиональные задачи в сфере финансовых рынков с целью определения возможности их решения с применением современных ИКТ для кибербезопасности, формулировать технические требования к системам защиты с учетом архитектурных особенностей и регуляторных норм, декомпозировать задачи на компоненты, оценивать соответствие ИКТ-решений требованиям безопасности, проводить сравнительный анализ альтернативных решений и обосновывать выбор оптимального технологического стека для защиты финансовых информационных систем.

Владеть:

ОПКЭ-6.3/Нв1 Навыками постановки технического задания для разработчиков, внедренцев и эксплуатационного персонала систем защиты информации, методиками оценки рисков информационной безопасности при внедрении ИКТ в финансовых организациях, навыками обоснования выбора технологических решений и защиты их перед руководством и стейкхолдерами (комитет по ИБ, правление, регуляторы), методами контроля эффективности внедренных ИКТ-решений, навыками формирования требований к безопасности на всех этапах жизненного цикла информационной системы.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Кибербезопасность» относится к обязательной части образовательной программы и изучается в семестре(ах): 7.

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, Основы информационной безопасности, Пакеты прикладных статистических программ, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации, Учебная практика: ознакомительная практика	Пакеты прикладных статистических программ, Подготовка к процедуре защиты и защита выпускной квалификационной работы
ОПК-4.2 Использует современные информационные технологии для решения задач профессиональной деятельности	Основы алгоритмизации и программирования, Основы информационной безопасности, Пакеты прикладных статистических программ, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации, Учебная практика: ознакомительная практика	Пакеты прикладных статистических программ, Подготовка к процедуре защиты и защита выпускной квалификационной работы
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, Основы информационной безопасности, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации	Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика
ОПКЭ-6.2 Использует современные информационные технологии для решения задач профессиональной деятельности	Основы алгоритмизации и программирования, Основы информационной безопасности, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации	Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика
ОПКЭ-6.3 Осуществляет постановку профессиональных задач, опираясь на возможности их решения путем применения современных информационно-коммуникационных технологий	Основы алгоритмизации и программирования, Основы информационной безопасности, Современные технологии и языки программирования, Технологии цифровой экономики, Управление информационными сервисами и контентом информационных ресурсов организации	Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика

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)	Групповая контактная работа (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Седьмой семестр	180	5	72	36	36	2	0,3	71,7	Экзамен
Всего	180	5	72	36	36	2	0,3	71,7	34

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. Кибербезопасность	**146**	**36**	**36**	**71,7**

Тема 1.1. Введение в кибербезопасность. Основные понятия, принципы и стандарты Определение кибербезопасности, базовые термины (угроза, уязвимость, атака, риск, активы, инцидент). Основные принципы обеспечения кибербезопасности (конфиденциальность, целостность, доступность — CIA Triad). Модели безопасности (модель Белла-ЛаПадулы, Кларка-Уилсона, RBAC, Mandatory Access Control). Обзор международных и национальных стандартов (ISO/IEC 27001, NIST SP 800-53, ГОСТ Р 57580.1-2017 для финансовой сферы, PCI DSS). Законодательная база РФ в области кибербезопасности (ФЗ-152, 187-ФЗ, 486-ФЗ, 149-ФЗ, приказы ФСТЭК, положения Банка России).	26	6	8	12
Тема 1.2. Угрозы и уязвимости программного обеспечения. Методы анализа рисков Классификация киберугроз (внешние/внутренние, преднамеренные/непреднамеренные, техногенные/природные). Типы атак: вредоносное ПО (вирусы, черви, трояны, программы-вымогатели, шпионское ПО), фишинг и социальная инженерия, сетевые атаки (DDoS, перехват трафика, MITM), атаки на веб-приложения (OWASP Top 10: SQL-инъекции, XSS, CSRF), атаки на цепочку поставок. Методы анализа рисков: количественный и качественный подходы (FAIR, OCTAVE, CRAMM). Методика оценки уязвимостей: CVSS (Common Vulnerability Scoring System), базы уязвимостей (CVE, NVD, BDU). Построение профиля угроз для финансовых организаций согласно стандартам Банка России.	28	6	8	14

Тема 1.3. Механизмы реализации кибербезопасности: защита по умолчанию, минимальные привилегии, безопасность встроенная Принципы построения защищенных систем: защита по умолчанию (secure by default), минимальные привилегии (least privilege), безопасность встроенная (security by design), принцип нулевого доверия (Zero Trust). Механизмы реализации: идентификация и аутентификация (парольная, биометрическая, токены, многофакторная MFA), авторизация и управление доступом (RBAC, ABAC, мандатное управление). Криптографические механизмы защиты: симметричное и асимметричное шифрование, хеширование, электронная подпись, инфраструктура открытых ключей (PKI). Средства антивирусной защиты и EDR/XDR-решения. Защита каналов связи (VPN, TLS/SSL).	38	6	8	24
Тема 1.4. Управление безопасностью на этапах жизненного цикла ПО Жизненный цикл разработки защищенного ПО (Security SDLC). Основные этапы: анализ требований безопасности, проектирование архитектуры с учетом угроз (Threat Modeling — STRIDE, DREAD), разработка с соблюдением безопасных практик кодирования (включая правила CERT, OWASP), тестирование безопасности (SAST, DAST, IAST, RASP), развертывание и эксплуатация, сопровождение и реагирование на инциденты. Модели управления безопасностью в Agile/DevOps: DevSecOps, CI/CD с интеграцией сканеров безопасности. Обеспечение безопасности в облачных средах (Cloud Security). Роль службы безопасности на всех этапах. Документирование процессов управления безопасностью.	28	8	6	14

Тема 1.5. Применение кибербезопасности в современных ИТ-решениях Особенности обеспечения кибербезопасности в облачных вычислениях (IaaS, PaaS, SaaS, модели ответственности провайдера и клиента — Shared Responsibility Model). Безопасность систем на базе искусственного интеллекта (атаки на модели ML, отравление данных, состязательные атаки). Защита интернета вещей (IoT Security). Безопасность мобильных приложений и веб-сервисов. Современные технологии защиты: SIEM-системы, SOAR-платформы, Threat Intelligence (управление угрозами), UEBA (аналитика поведения пользователей). Внедрение кибербезопасности в финансовых организациях: защита банковских систем, криптовалютных платформ, платежных шлюзов. Обеспечение непрерывности бизнеса и восстановления после атак (DRP, BCP). Кибербезопасность в условиях санкций и импортозамещения (российские решения: ViPNet, Secret Net, Solar, Kaspersky).	26	10	6	7,7

5.2. Контрольные мероприятия по дисциплине

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

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Кибербезопасность	Тестирование	Экзамен

6. Оценочные материалы текущего контроля

1. Кибербезопасность Тестирование

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	

1	Выберите один вариант ответа Что из перечисленного является ключевым принципом кибериммунного подхода к разработке ПО? а) Использование только открытого программного обеспечения б) Изоляция компонентов системы друг от друга и от внешней среды в) Постоянное обновление антивирусных баз г) Размещение всех данных в облачном хранилище		ОПК-4
	Ответ:	б	
2	Дайте верный ответ Опишите, как применение кибериммунного подхода может снизить риски, связанные с «неизвестными уязвимостями» (zero-day).		ОПК-4
	Ответ:	Кибериммунный подход снижает риски zero-day уязвимостей за счёт изоляции компонентов: даже если злоумышленник найдёт уязвимость в одном компоненте, он не сможет получить доступ к другим частям системы. Кроме того, минимизация доверенной вычислительной базы сокращает количество кода, в котором могут быть обнаружены уязвимости. Контроль взаимодействий между компонентами не позволяет атакующему развить атаку и получить контроль над всей системой	
3	Дайте верный ответ Сравните традиционный подход к обеспечению информационной безопасности (защита «периметра») и кибериммунный подход. В чём ключевые различия? Приведите не менее трёх отличий.		ОПК-4
	Ответ:	1. Время обеспечения безопасности 2. Реакция на атаки 3. Архитектура	
4	Дайте верный ответ Разработайте план мероприятий по обеспечению информационной безопасности на этапе разработки ПО с использованием кибериммунного подхода. План должен включать не менее 5 этапов с обоснованием каждого.		ОПК-4
	Ответ:	1. Анализ угроз и моделирование атак 2. Проектирование архитектуры с изоляцией компонентов 3. Разработка политик взаимодействия 4. Реализация с использованием безопасных языков и практик программирования 5. Тестирование безопасности (пен-тестирование, анализ уязвимостей) —	
5	Дайте верный ответ Вам необходимо найти актуальные научные публикации по теме «Методы обеспечения кибериммунности встроенных систем». Опишите последовательность действий с указанием конкретных информационно-коммуникационных технологий и библиографических источников, которые вы будете использовать.		ОПК-4
	Ответ:	1. Сформулирую ключевые слова: «кибериммунность», «встроенные системы», «secure by design», «изоляция компонентов». 2. Выполню поиск в научных электронных библиотеках: eLibrary.ru (российские публикации), Google Scholar и Scopus (международные). 3. Отфильтрую результаты по релевантности, цитируемости и дате публикации (за последние 5 лет). 4. Сохраню найденные источники с помощью библиографического менеджера Mendeley. 5. Оформлю список литературы в соответствии с ГОСТ 7.1-2003 (или актуальной версией).	
6	Дайте верный ответ Опишите три основных принципа кибериммунного подхода к разработке ПО. Для каждого принципа приведите пример его реализации в архитектуре системы.		ОПК-4
	Ответ:	1. Изоляция компонентов 2. Минимизация доверенной вычислительной базы (ДВБ) 3. Secure by Design	
7	Установите правильную последовательность Расположите шаги выполнения библиографического поиска в правильном порядке: 1. Оценка релевантности и качества найденных источников 2. Формулирование темы и ключевых слов для поиска 3. Оформление списка литературы в соответствии с требованиями 4. Поиск в специализированных базах данных (eLibrary, Google Scholar, Scopus) 5. Сохранение найденных источников с использованием библиографического менеджера		ОПК-4
	Ответ:	2, 4, 1, 5, 3.	
8	Установите правильную последовательность Расположите этапы проектирования кибериммунной системы в правильном порядке: 1. Определение доменов безопасности и изоляция компонентов 2. Анализ угроз и рисков для разрабатываемой системы 3. Разработка политик взаимодействия между компонентами 4. Реализация и тестирование системы 5. Формулирование требований к безопасности на этапе проектирования		ОПК-4
	Ответ:	5, 2, 1, 3, 4.	

9	Установите соответствие Соотнесите вид информационно-коммуникационной технологии с её назначением: Технология — Назначение 1. Система управления базами данных (СУБД) — А. Организация совместной работы над документами 2. Облачные платформы (Яндекс.Облако, Google Cloud) — Б. Хранение и структурированное извлечение данных 3. Библиографические базы данных (eLibrary, Scopus) — В. Поиск и анализ научных публикаций 4. Средства совместной работы (Google Docs) — Г. Хранение и обработка данных с удалённым доступом Ответ: 1-Б, 2-Г, 3-В, 4-А.	ОПК-4
10	Установите соответствие Соотнесите вид угрозы информационной безопасности с примером её реализации: Угроза — Пример 1. Вредоносное ПО — А. Поддельное письмо от «банка» с просьбой ввести логин и пароль 2. Социальная инженерия — Б. Программа-шифровальщик, блокирующая доступ к файлам 3. DDoS-атака — В. Злоумышленник подбирает пароль к учётной записи 4. Брутфорс — Г. Перегрузка сервера большим количеством ложных запросов Ответ: 1-Б, 2-А, 3-Г, 4-В.	ОПК-4
11	Установите соответствие Соотнесите принцип кибериммунного подхода с его описанием: Принцип — Описание 1. Изоляция компонентов — А. Система сохраняет работоспособность даже при наличии атак 2. Минимизация ДВБ — Б. Система делится на части (домены), изолированные друг от друга 3. Secure by Design — В. Безопасность закладывается на этапе проектирования, а не добавляется позже 4. Устойчивость к атакам — Г. Сокращение объёма кода, который должен быть безусловно надёжным Ответ: 1-Б, 2-Г, 3-В, 4-А.	ОПК-4
12	Выберите один вариант ответа Для решения стандартной задачи поиска научной литературы по теме «Кибериммунная разработка ПО» наиболее эффективно использовать: а) Поисковую систему Яндекс б) Научную электронную библиотеку eLibrary.ru в) Социальную сеть «ВКонтакте» г) Википедию Ответ: б	ОПК-4
13	Выберите один вариант ответа Какой из перечисленных стандартов используется при создании кибериммунных решений? а) ГОСТ Р ИСО/МЭК 12207 б) Common Criteria в) IEEE 802.11 г) RFC 791 Ответ: б	ОПК-4
14	Выберите один вариант ответа Что такое минимизация доверенной вычислительной базы (ДВБ) в контексте кибериммунного подхода? а) Уменьшение количества пользователей, имеющих доступ к системе б) Сокращение объёма кода и компонентов, которые должны быть безусловно надёжными в) Установка минимального количества антивирусных программ г) Ограничение времени работы системы Ответ: б	ОПК-4
15	Выберите один вариант ответа Какая операционная система разработана по принципу Secure by Design и является основой для создания кибериммунных решений? а) Windows б) Linux в) KasperskyOS г) macOS Ответ: в	ОПК-4
16	Что из перечисленного является фундаментальным принципом обеспечения кибербезопасности, означающим, что каждый пользователь или процесс должен иметь доступ только к той информации и ресурсам, которые необходимы для выполнения его профессиональных задач? А) Защита по умолчанию (Secure by Default) Б) Принцип минимальных привилегий (Least Privilege) В) Принцип нулевого доверия (Zero Trust) Г) Принцип экономии механизмов Д) Разделение обязанностей Ответ: Б	ОПКЭ-6

17	Какая модель угроз описывает воздействие на конфиденциальность, целостность и доступность информации и используется при Threat Modeling на этапе проектирования защищенного ПО? А) STRIDE Б) DREAD В) OCTAVE Г) CRAMM Д) FAIR Ответ: А	ОПКЭ-6
18	Какой нормативный документ устанавливает требования к обеспечению защиты информации при осуществлении банковской деятельности и является основным для финансовых организаций? А) ГОСТ Р ИСО/МЭК 27001-2021 Б) ФЗ-152 «О персональных данных» В) ГОСТ Р 57580.1-2017 «Защита информации. Банковская деятельность» Г) ФЗ-187 «О безопасности критической информационной инфраструктуры» Д) PCI DSS (Payment Card Industry Data Security Standard) Ответ: В	ОПКЭ-6
19	Какой тип атаки на веб-приложения, включенный в OWASP Top 10, заключается во внедрении вредоносного кода в веб-страницу с целью выполнения его в браузере пользователя, что требует понимания принципов работы современных веб-технологий для постановки задач защиты? А) SQL-инъекция (SQL Injection) Б) Межсайтовый скриптинг (XSS — Cross-Site Scripting) В) Подделка межсайтового запроса (CSRF) Г) Переполнение буфера (Buffer Overflow) Д) Человек посередине (MITM — Man-In-The-Middle) Ответ: Б	ОПКЭ-6
20	В какой модели обеспечения безопасности облачных вычислений, основанной на понимании принципов работы современных ИТ, организация (клиент) несет ответственность за защиту своих данных, учетных записей и настройку доступа, а провайдер — за защиту физической инфраструктуры и гипервизора, что необходимо учитывать при постановке задач по кибербезопасности? А) Модель общей ответственности (Shared Responsibility Model) Б) Модель «защита по умолчанию» В) Модель нулевого доверия (Zero Trust) Г) Модель безопасности встроенная (Security by Design) Д) Модель управления доступом на основе ролей (RBAC) Ответ: А	ОПКЭ-6
21	Установите соответствие между типом уязвимости ПО и ее описанием в соответствии с OWASP Top 10, используя знание принципов работы современных информационных технологий для решения профессиональных задач по кибербезопасности. **Тип уязвимости (А-Д)** / **Описание (1-5)** А. SQL Injection — 1. Внедрение вредоносного кода на серверную страницу с последующим выполнением в браузере пользователя Б. Cross-Site Scripting (XSS) — 2. Подделка запроса со стороны авторизованного пользователя без его ведома В. Cross-Site Request Forgery (CSRF) — 3. Внедрение SQL-запроса в пользовательский ввод для доступа к базе данных Г. Broken Authentication — 4. Ошибки в механизмах аутентификации, позволяющие получить несанкционированный доступ Д. Security Misconfiguration — 5. Некорректные настройки серверов и приложений, ведущие к уязвимостям Ответ: А-3, Б-1, В-2, Г-4, Д-5	ОПКЭ-6
22	Установите соответствие между методом анализа/тестирования безопасности и его описанием, применяемым для решения профессиональных задач по обеспечению кибербезопасности с использованием современных ИТ-инструментов. **Метод (А-Д)** / **Описание (1-5)** А. SAST (Static Application Security Testing) — 1. Тестирование работающего приложения с имитацией атак извне (черный ящик) Б. DAST (Dynamic Application Security Testing) — 2. Анализ исходного кода на наличие уязвимостей до его запуска (белый ящик) В. IAST (Interactive Application Security Testing) — 3. Гибридный метод, анализирующий приложение во время выполнения изнутри Г. RASP (Runtime Application Self-Protection) — 4. Встроенный в приложение механизм самозащиты во время выполнения Д. Penetration Testing (Pentest) — 5. Комплексное тестирование с моделированием реальной кибератаки Ответ: А-2, Б-1, В-3, Г-4, Д-5	ОПКЭ-6
23	Установите соответствие между этапом жизненного цикла разработки защищенного ПО (Security SDLC) и его содержанием, используя понимание принципов работы современных ИТ-технологий для постановки профессиональных задач по кибербезопасности. **Этап Security SDLC (А-Д)** / **Содержание (1-5)** А. Анализ требований безопасности — 1. Выполнение SAST/DAST, проверка кода и пентест Б. Threat Modeling (анализ угроз) — 2. Определение требований к защите, конфиденциальности и целостности данных	ОПКЭ-6

	данных	
В. Безопасное кодирование	3. Внедрение механизмов мониторинга и реагирования на инциденты	
Г. Тестирование безопасности	4. Написание кода с соблюдением правил OWASP и CERT, использование защищенных API	
Д. Эксплуатация и сопровождение	5. Идентификация и оценка угроз с использованием моделей STRIDE, DREAD	

	Ответ:	А-2, Б-5, В-4, Г-1, Д-3
24	Расположите в правильной последовательности этапы процесса реагирования на инцидент кибербезопасности в финансовой организации, используя современные информационные технологии для решения профессиональных задач по защите информационных систем. Выявление и обнаружение инцидента с использованием SIEM-системы и мониторинга событий безопасности на основе принципов работы современных ИТ Сдерживание и локализация атаки с помощью сегментации сети и изоляции зараженных узлов с применением современных сетевых технологий Искоренение (удаление вредоносного ПО, устранение уязвимостей) и восстановление работоспособности систем из резервных копий с использованием технологий Disaster Recovery Проведение пост-инцидентного анализа (lessons learned), корректировка политик и мер защиты с использованием современных аналитических инструментов	ОПКЭ-6
	Ответ:	1 → 2 → 3 → 4
25	Расположите в правильной последовательности порядок проведения оценки рисков информационной безопасности в финансовой организации, опираясь на понимание принципов работы современных информационных технологий для постановки профессиональных задач. 1. Идентификация активов организации (информационные системы, данные, оборудование) и определение их ценности с использованием современных методов инвентаризации 2. Выявление и классификация угроз для идентифицированных активов (включая моделирование атак на основе актуальных данных Threat Intelligence) 3. Оценка уязвимостей активов и вероятности реализации угроз (количественная/качественная оценка рисков с применением современных методик CVSS, FAIR) 4. Выбор и внедрение мер реагирования на риски (снижение, передача, принятие, избегание) с учетом стоимости и эффективности, использование современных ИКТ-решений для автоматизации управления рисками	ОПКЭ-6
	Ответ:	1 → 2 → 3 → 4
26	Дайте развернутый письменный ответ (объемом 3-5 предложений) на поставленный вопрос. Ответ должен содержать обоснование применения современных ИКТ-решений для обеспечения кибербезопасности и ключевые слова проверяемой компетенции: «принципы работы современных информационных технологий», «использование», «решение профессиональных задач», «постановка профессиональных задач». В банке произошла атака с использованием программы-вымогателя (Ransomware), в результате которой были зашифрованы финансовые данные и системы временно недоступны. Опишите последовательность применения современных ИКТ-технологий для восстановления работоспособности и защиты от подобных атак в будущем. Какие технологии необходимо внедрить для предотвращения повторения инцидента? Обоснуйте выбор с учетом принципов работы современных информационных технологий.	ОПКЭ-6
	Ответ:	Для восстановления работоспособности необходимо использовать системы резервного копирования с технологией непрерывной защиты данных (CDP) и географически распределенные резервные копии, что позволит восстановить системы из неповрежденных бекапов на основе принципов работы современных систем хранения данных. Для предотвращения повторных атак требуется внедрение комплексной системы защиты конечных точек (EDR/XDR) с функциями поведенческого анализа на основе машинного обучения, а также SIEM-системы для раннего обнаружения атак по аномалиям сетевого трафика с использованием современных методов корреляции событий. Обоснование: CDP-решения и EDR/XDR обеспечивают защиту от программ-вымогателей на уровне поведенческого анализа, а SIEM позволяет выявить инцидент на ранней стадии до активации вредоносного ПО, что соответствует требованиям ГОСТ Р 57580.1-2017 и принципам работы современных ИТ-систем. Ключевые слова: современные информационные технологии, решение профессиональных задач, постановка профессиональных задач, принципы работы ИТ.
27	Дайте развернутый письменный ответ (объемом 3-5 предложений) на поставленный вопрос. Ответ должен содержать современную ИТ-технологию, ее обоснование и ключевые слова проверяемой компетенции. Финансовая организация внедряет удаленную работу сотрудников (WfH — Work from Home). Какие современные ИТ-технологии и инструменты кибербезопасности необходимо применить для обеспечения безопасного доступа к корпоративным ресурсам и финансовым данным, используя понимание принципов работы современных информационных технологий для постановки профессиональных задач по защите?	ОПКЭ-6

	Ответ:	Для безопасного удаленного доступа необходимо внедрить технологию VPN с многофакторной аутентификацией (MFA) для защиты канала связи и проверки подлинности сотрудников на основе принципов работы современных криптографических протоколов. Дополнительно следует использовать технологию Zero Trust Network Access (ZTNA), которая обеспечивает сегментацию доступа на уровне конкретных приложений, а также системы защиты конечных точек (EDR) на рабочих станциях сотрудников для предотвращения заражения вредоносным ПО с использованием современных методов поведенческого анализа. Обоснование: VPN с MFA обеспечивает конфиденциальность передачи данных на основе принципов криптографии, ZTNA ограничивает доступ сотрудников только к необходимым ресурсам в соответствии с принципом минимальных привилегий, EDR защищает конечные точки от вредоносных атак. Данные технологии соответствуют требованиям Банка России по организации удаленного доступа (Положение 727-П). Ключевые слова: современные информационные технологии, решение профессиональных задач, принципы работы современных ИТ.	
28	Дайте развернутый письменный ответ (объемом 3-5 предложений) на поставленный вопрос. Ответ должен содержать описание процесса Threat Modeling для постановки задач безопасности и ключевые слова проверяемой компетенции. При проектировании новой информационной системы для обработки персональных данных клиентов банка необходимо провести анализ угроз (Threat Modeling) на этапе архитектурного проектирования. Опишите, какие задачи и этапы Threat Modeling должны быть выполнены для данной системы, какие современные ИКТ-решения могут быть применены для выявления угроз, и как результаты анализа используются для постановки профессиональных задач по кибербезопасности.		ОПКЭ-6
	Ответ:	Threat Modeling включает следующие этапы, основанные на понимании принципов работы современных информационных технологий: 1) декомпозиция системы и построение диаграммы потоков данных (DFD) для визуализации всех элементов системы, границ доверия, потоков данных и точек входа/выхода с использованием современных инструментов моделирования; 2) идентификация угроз с использованием модели STRIDE (подмена, модификация, отказ в обслуживании и др.) для каждого компонента на основе понимания архитектуры современных ИТ-систем; 3) оценка рисков с помощью DREAD или CVSS для ранжирования угроз по критичности; 4) формирование требований к мерам защиты для нейтрализации выявленных угроз и постановка профессиональных задач для разработчиков и администраторов безопасности. В качестве современных ИКТ-решений рекомендуется использование автоматизированных инструментов Threat Modeling (например, Microsoft Threat Modeling Tool, OWASP Threat Dragon) для формализации процесса и ускорения выявления угроз, что позволяет эффективно решать профессиональные задачи по обеспечению кибербезопасности. Ключевые слова: понимание принципов работы ИТ, постановка профессиональных задач, использование современных ИКТ-решений.	
29	Сформулируйте развернутый ответ на задачу с указанием современных ИКТ-решений, нормативных требований и ключевых слов проверяемой компетенции. Для банка требуется внедрение системы централизованного сбора, корреляции и анализа событий безопасности для обеспечения соответствия требованиям регулятора в области мониторинга информационной безопасности. Выберите современное ИТ-решение, опишите его функционал, нормативные основания для внедрения в финансовой организации и укажите, как данная система используется для решения профессиональных задач по кибербезопасности.		ОПКЭ-6
	Ответ:	Для централизованного сбора и корреляции событий безопасности необходимо внедрение SIEM-системы (например, MaxPatrol SIEM, ArcSight, QRadar или отечественный аналог Kaspersky Unified Monitoring and Analysis Platform) на основе понимания принципов работы современных систем сбора и обработки данных. SIEM-система обеспечивает сбор данных из всех источников (межсетевые экраны, антивирусы, серверы, СУБД), их нормализацию, корреляцию на основе правил, автоматическое оповещение о подозрительной активности и генерацию отчетности для регуляторов, что позволяет эффективно решать профессиональные задачи по выявлению и реагированию на инциденты. Нормативные основания: в соответствии с ГОСТ Р 57580.1-2017 «Защита информации. Банковская деятельность» и рекомендациями Банка России, кредитные организации обязаны внедрять системы централизованного мониторинга событий безопасности для обеспечения непрерывного контроля защищенности информационных систем, что учитывается при постановке профессиональных задач по кибербезопасности. Ключевые слова: современные информационные технологии, решение профессиональных задач, постановка профессиональных задач, понимание принципов работы ИТ.	
30	Дайте развернутый ответ, содержащий обоснование выбора современных ИКТ-технологий и их практического применения для решения профессиональных задач в области кибербезопасности, с обязательным использованием ключевых слов проверяемой компетенции. Финансовая организация планирует переход к модели DevSecOps для ускорения разработки и внедрения защищенного ПО. Опишите, какие современные ИКТ-технологии и инструменты необходимо интегрировать в CI/CD-конвейер для обеспечения безопасности на всех этапах разработки. Какие задачи они решают, какова их роль в обеспечении кибербезопасности и как они используются для постановки профессиональных задач по защите информационных систем?		ОПКЭ-6

	Ответ:	При переходе к DevSecOps необходимо интегрировать в CI/CD-конвейер следующие современные ИКТ-технологии, основанные на понимании принципов работы современных систем автоматизации разработки: 1) инструменты статического анализа безопасности кода (SAST) — например, SonarQube, Checkmarx — для выявления уязвимостей на этапе написания кода, что позволяет решать профессиональные задачи по обеспечению безопасности на ранних этапах разработки; 2) инструменты сканирования зависимостей (SCA — Software Composition Analysis) для проверки открытых библиотек на наличие известных уязвимостей; 3) инструменты динамического тестирования (DAST) и интерактивного тестирования (IAST) для проверки работающих приложений в соответствии с принципами работы современных веб-технологий; 4) инструменты анализа контейнеров и образов (например, Docker Scan, Trivy) для выявления уязвимостей в контейнеризированных средах, что особенно актуально для облачных решений. Обоснование: интеграция данных инструментов в CI/CD позволяет автоматизировать проверку безопасности на всех этапах разработки, реализовать принцип «security by design», сократить стоимость исправления уязвимостей (исправление на этапе написания кода в 10-100 раз дешевле, чем на этапе эксплуатации) и обеспечить непрерывный контроль безопасности при каждом обновлении ПО, что является ключевой задачей при использовании современных информационных технологий в финансовой организации. Ключевые слова: понимание принципов работы современных ИТ, использование современных информационных технологий, решение профессиональных задач, постановка профессиональных задач.	

7. Оценочные материалы промежуточной аттестации

Экзамен седьмой семестр

№ п/п	Содержание вопроса	Правильный ответ (ключ ответа)	Компетенция
1	Дайте развернутый ответ Дайте определение кибериммунного подхода к разработке ПО. Перечислите его основные принципы.		ОПК-4, ОПКЭ-6
	Ответ:	Кибериммунный подход — методология разработки ПО, позволяющая создавать системы, устойчивые к кибератакам даже при наличии неизвестных уязвимостей. Основные принципы: изоляция компонентов, минимизация доверенной вычислительной базы, Secure by Design, контроль взаимодействий между компонентами	
2	Дайте развернутый ответ Что такое «изоляция компонентов» в кибериммунном подходе и почему она важна для информационной безопасности?		ОПК-4, ОПКЭ-6
	Ответ:	Изоляция компонентов — это разделение системы на изолированные части (домены), каждая из которых имеет строго определённые права доступа. Это важно, потому что даже при компрометации одного компонента злоумышленник не может получить доступ к другим частям системы, что ограничивает распространение атаки	
3	Дайте развернутый ответ Какие информационно-коммуникационные технологии вы будете использовать для поиска и анализа научной литературы по теме «Кибериммунная разработка ПО»?		ОПК-4, ОПКЭ-6
	Ответ:	Буду использовать научные электронные библиотеки (eLibrary.ru, Google Scholar, Scopus), системы управления библиографией (Mendeley, Zotero), а также поисковые системы с расширенными возможностями фильтрации. Методика: формулирование ключевых слов → поиск → фильтрация по релевантности и цитируемости → сохранение источников → оформление списка литературы по ГОСТ.	
4	Дайте развернутый ответ Какие стандарты и нормативные документы регулируют создание кибериммунных систем?		ОПК-4, ОПКЭ-6
	Ответ:	Common Criteria, ASPICE, ISO 26262. Эти стандарты определяют требования к безопасности на всех этапах жизненного цикла разработки. KasperskyOS соответствует указанным стандартам	
5	Дайте развернутый ответ Опишите навыки работы с библиографическими источниками, необходимые для решения стандартных задач профессиональной деятельности		ОПК-4, ОПКЭ-6
	Ответ:	Навыки включают: формулирование поисковых запросов, работу с научными базами данных (eLibrary, Scopus), критический анализ источников, использование библиографических менеджеров (Mendeley, Zotero), оформление списка литературы в соответствии с ГОСТ 7.1-2003, оценку релевантности и достоверности источников.	
6	Дайте развернутый ответ Как учитывать требования информационной безопасности при разработке ПО с использованием кибериммунного подхода?		ОПК-4, ОПКЭ-6
	Ответ:	Требования ИБ учитываются на всех этапах: анализ угроз на этапе проектирования, изоляция компонентов, минимизация доверенной вычислительной базы, разработка политик взаимодействия, тестирование безопасности, использование Secure by Design	
7	Дайте развернутый ответ Какие методы анализа уязвимостей применяются в кибериммунном подходе?		ОПК-4, ОПКЭ-6
	Ответ:	Моделирование угроз, анализ векторов атак, статический и динамический анализ кода, пен-тестирование, анализ контрольных сумм и целостности данных, проверка политик взаимодействия между компонентами.	

8	Дайте развернутый ответ Что такое «микроядро» и какую роль оно играет в кибериммунной архитектуре?		ОПК-4, ОПКЭ-6
	Ответ:	Микроядро — минимальный набор функций, необходимых для работы системы, разработанный с акцентом на безопасность. В кибериммунной архитектуре микроядро обеспечивает изоляцию компонентов и контроль взаимодействий, являясь минимальной доверенной вычислительной базой.	
9	Дайте развернутый ответ Какие методы информационной культуры применяются при решении профессиональных задач в области разработки ПО?		ОПК-4, ОПКЭ-6
	Ответ:	Работа с научной литературой, поиск в специализированных базах данных, критический анализ информации, использование систем управления знаниями, оформление результатов исследований в соответствии с требованиями, применение ИКТ для автоматизации рутинных задач.	
10	Дайте развернутый ответ Опишите сценарий атаки на систему, не обладающую кибериммунностью, и объясните, как кибериммунный подход предотвращает развитие этой атаки.		ОПК-4, ОПКЭ-6
	Ответ:	В традиционной системе атакующий может через уязвимость в одном компоненте получить доступ к другим частям системы и развить атаку. В кибериммунной системе изоляция компонентов и контроль взаимодействий не позволяют атакующему распространиться на другие домены. Система продолжает выполнять критические функции даже в условиях агрессивной среды.	

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. Кириченко, А.А. Операционные системы. Практикум: Учебное пособие / А.А. Кириченко, С.В. Назаров, Л.П. Гудыно. - Москва: КноРус, 2020. - 372 с. - 978-5-406-07707-8. - Текст: электронный // book_ru: [сайт]. - URL: https://book.ru/book/933567 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Гаврилов, М. В. Архитектура ЭВМ и системное программное обеспечение: учебник для вузов / М. В. Гаврилов, В. А. Климов. - 6-е изд. - Москва: Юрайт, 2026. - 84 с - 978-5-534-20334-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589930 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Чернышев, С. А. Принципы, паттерны и методологии разработки программного обеспечения: учебник для вузов / С. А. Чернышев. - Москва: Юрайт, 2026. - 176 с - 978-5-534-14383-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588769 (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

1. https://minfin.gov.ru/ - Министерство финансов Российской Федерации (Минфин России)
2. http://www.gks.ru/ - Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики

Ресурсы «Интернет»

1. http://www.gov.ru - Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия"
2. https://cyberleninka.ru/ - Научная электронная библиотека «КиберЛенинка»
3. 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)
Не используется.

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 СП
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения