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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль)подготовки: Прикладная информатика и защита информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очно-заочная

Год набора (приема на обучение): 2026

Срок получения образования: 4 года 6 месяца(-ев)

Объем: в зачетных единицах: 4 з.е.
в академических часах: 144 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 09.03.03 Прикладная информатика, утвержденного приказом Минобрнауки от 19.09.2017 № 922, с учетом трудовых функций профессиональных стандартов: "Специалист по информационным системам", утвержден приказом Минтруда России от 13.07.2023 № 586н; "Руководитель проектов в области информационных технологий", утвержден приказом Минтруда России от 27.04.2023 № 369н; "Системный аналитик", утвержден приказом Минтруда России от 27.04.2023 № 367н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Кафедра прикладной информатики	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Ермолина Л. В.	Рассмотрено	21.05.2026, № 9

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование теоретических знаний и практических навыков по применению криптографических методов и средств для обеспечения конфиденциальности, целостности и аутентичности информации в автоматизированных системах.

Задачи изучения дисциплины:

- Изучить математические основы и классические алгоритмы симметричного и асимметричного шифрования, хеш-функции и электронную подпись.;
- Освоить методы управления криптографическими ключами и протоколы аутентификации (Kerberos, SSL/TLS) в корпоративных ИС.;
- Сформировать навыки применения государственных криптостандартов (ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012) и использования СКЗИ для защиты данных..

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

Компетенции, индикаторы и результаты обучения

ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС

ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

Знать:

ПК-2.2/Зн1 Методы обнаружения инцидентов ИБ с использованием криптоанализа, признаки нарушения целостности и конфиденциальности данных, процедуры реагирования и требования к применению СКЗИ при расследовании инцидентов.

Уметь:

ПК-2.2/Ум1 Выявлять признаки криптографических атак и компрометации ключевой информации, применять средства криптографической защиты для локализации инцидента и обеспечивать сохранность цифровых доказательств.

Владеть:

ПК-2.2/Нв1 Навыками работы с СКЗИ и криптоаналитическими инструментами, методами оперативного реагирования на инциденты, приемами документирования и отчётности по результатам расследования инцидентов ИБ.

ПК-4 Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений

ПК-4.2 Сопровождает разработанные проектные решения и требования к ИС

Знать:

ПК-4.2/Зн1 Методологии выявления требований к криптографической защите, стандарты и нормативные документы по применению СКЗИ, принципы концептуально-логического проектирования систем защиты информации с использованием криптографии, этапы и процедуры сопровождения проектных решений в области криптозащиты на всех стадиях жизненного цикла ИС.

Уметь:

ПК-4.2/Ум1 Анализировать бизнес-процессы и нормативные требования для формирования требований к криптографической защите, разрабатывать концептуальные и логические модели систем криптозащиты, согласовывать проектные решения с заинтересованными сторонами (заказчик, разработчики, регуляторы), вносить изменения в проектную документацию при изменении требований или появлении новых угроз.

Владеть:

ПК-4.2/Нв1 Навыками разработки и актуализации технического задания с разделом криптографической защиты, методами оценки эффективности проектных решений по криптозащите, приемами верификации требований к СКЗИ и документирования результатов экспертизы, методиками сопровождения проектных решений в процессе внедрения и эксплуатации ИС.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Криптографическая защита информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 6.

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

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ПК-2 - Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС		
ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС	Методы и средства защиты информации, Правовая защита информации, Теория информационной безопасности и методология защиты информации, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность Web-приложений, Безопасность мобильных приложений, Выполнение и защита выпускной квалификационной работы, Методы и средства защиты информации, Организационная защита информации, Правовая защита информации, Программно-аппаратная защита информации, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Техническая защита информации
ПК-4 - Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений		

ПК-4.2 Сопровождает разработанные проектные решения и требования к ИС	Информационно-коммуникационные технологии в профессиональной деятельности, Нейросетевые технологии в социальных медиа, Облачные технологии и услуги, Основы проектной деятельности, Учебная практика: технологическая (проектно-технологическая) практика	Выполнение и защита выпускной квалификационной работы, Облачные технологии и услуги, Проектирование и реализация баз данных, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Техническая защита информации, Технологии защищенного документооборота, Управление информационными проектами реализации комплексной безопасности

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
Шестой семестр	144	4	4	2	2	2	0,3	103,7	Экзамен
Всего	144	4	4	2	2	2	0,3	103,7	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. Криптографическая защита информации	**110**	**2**	**2**	**103,7**

Тема 1.1. Введение в криптографическую защиту информации: основные понятия, термины и определения криптографии; классификация криптографических методов и алгоритмов (симметричные, асимметричные, хеш-функции); обзор нормативно-правовой базы применения СКЗИ в РФ (ГОСТ, 152-ФЗ, приказы ФСТЭК); исторический обзор развития криптографии.	110	2	2	103,7

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестовое задание
Промежуточная аттестация	Экзамен

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Криптографическая защита информации	Тестовое задание	Экзамен

6. Оценочные материалы текущего контроля

1. Криптографическая защита информации Тестовое задание

№ п/п	Содержание вопроса / Правильный ответ (ключ ответа)	Компетенция
1	При тестировании ИС для выявления инцидента, связанного с перехватом сетевого трафика, какой протокол обеспечивает защиту передаваемых данных от прослушивания? a) HTTP b) FTP c) TLS/SSL d) Telnet Ответ: c	ПК-2
2	При обнаружении инцидента ИБ, связанного с компрометацией ключевой информации, какое действие должно быть выполнено в первую очередь при сопровождении ИС? a) продолжение работы с компрометированными ключами b) немедленный отзыв (аннулирование) скомпрометированных ключей и генерация новых c) уведомление всех пользователей через месяц d) игнорирование инцидента Ответ: b	ПК-2
3	Какой криптографический алгоритм используется для проверки целостности данных при обнаружении инцидентов ИБ в рамках тестирования ИС? a) AES b) RSA c) SHA-256 (хеш-функция) d) Diffie-Hellman Ответ: c	ПК-2
4	При принятии мер по устранению инцидента ИБ, вызванного утечкой данных, какой метод шифрования рекомендуется для защиты хранимой информации? a) шифрование с помощью XOR b) использование блочного шифра (AES-256) с правильным режимом (GCM/CBC) c) шифрование без ключа d) использование шифра Цезаря	ПК-2

	Ответ: b	
5	Какой документ должен быть оформлен при обнаружении инцидента ИБ в рамках сопровождения ИС? a) техническое задание на разработку ИС b) отчёт об инциденте (акт расследования) c) бизнес-план d) должностная инструкция системного администратора	ПК-2
	Ответ: b	
6	Установите соответствие между типом инцидента ИБ (1–3) и криптографическим методом его обнаружения (A–C) при обнаружении инцидентов ИБ в рамках сопровождения ИС. Тип инцидента ИБ — Криптографический метод обнаружения 1. Изменение данных — A. Проверка ЭЦП или сравнение хеш-сумм 2. Перехват сетевого трафика — B. Анализ TLS-сессий и сертификатов 3. Компрометация ключей — C. Мониторинг использования ключей и проверка сертификатов	ПК-2
	Ответ: 1-A, 2-B, 3-C	
7	Установите соответствие между стадией реагирования на инцидент ИБ (1–3) и её содержанием (A–C) при обнаружении инцидентов ИБ и принятии мер. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Стадия реагирования — Содержание стадии 1. Обнаружение и локализация — A. Обновление ключей, исправление уязвимостей 2. Устранение — B. Мониторинг аномалий, идентификация затронутых компонентов 3. Анализ и предотвращение — C. Документирование, анализ причин, внедрение мер предотвращения	ПК-2
	Ответ: 1-B, 2-A, 3-C	
8	Установите соответствие между инструментом/методом криптографической защиты (1–3) и его назначением при тестировании ИС для обнаружения инцидентов ИБ (A–C). В бланк ответов запишите последовательность (например, 1-C, 2-A, 3-B). Инструмент/метод — Назначение при тестировании ИС 1. Хеш-функции (SHA-256) — A. Проверка подлинности источника данных 2. Электронная подпись — B. Проверка целостности файлов и логов 3. TLS/SSL — C. Защита сетевого трафика от перехвата	ПК-2
	Ответ: 1-B, 2-A, 3-C	
9	Установите правильную последовательность действий при обнаружении инцидента ИБ, связанного с компрометацией ключей в ИС, в рамках сопровождения ИС. A) Обнаружение аномалии (необычная активность с ключами) B) Аннулирование (отзыв) скомпрометированных ключей и сертификатов C) Генерация и распространение новых ключей D) Уведомление заинтересованных сторон и документирование инцидента	ПК-2
	Ответ: A → B → C → D	
10	Установите правильную последовательность этапов проверки целостности данных при тестировании ИС для обнаружения инцидентов ИБ. Расположите буквы (A–D) в верном порядке. A) Сохранение эталонных хеш-сумм в защищённом месте B) Расчёт хеш-суммы файла с помощью криптографической хеш-функции C) Сравнение полученной хеш-суммы с эталонной D) Принятие решения о целостности данных (совпадает/не совпадает)	ПК-2
	Ответ: B → A → C → D	
11	Дайте развернутый ответ Назовите не менее двух криптографических методов, используемых при обнаружении инцидентов ИБ для проверки целостности данных.	ПК-2
	Ответ: хеш-функции (SHA-256), электронная подпись, HMAC.	
12	Дайте развернутый ответ При обнаружении инцидента ИБ, связанного с перехватом сетевого трафика, какой протокол должен быть проверен на корректность настройки?	ПК-2

	Ответ:	TLS/SSL.	
13	Дайте развернутый ответ Назовите не менее двух признаков компрометации ключевой информации при тестировании ИС.		ПК-2
	Ответ:	необычная активность с ключами, множественные ошибки аутентификации, появление неизвестных сертификатов.	
14	Дайте развернутый ответ Какой документ фиксирует информацию об инциденте ИБ при сопровождении ИС?		ПК-2
	Ответ:	отчёт об инциденте / акт расследования инцидента ИБ.	
15	Дайте развернутый ответ Перечислите не менее двух мер по предотвращению инцидентов ИБ, связанных с компрометацией криптографических ключей.		ПК-2
	Ответ:	регулярная смена ключей, использование аппаратных модулей безопасности (HSM), внедрение системы мониторинга использования ключей.	
16	При выявлении требований к Системе, какие требования определяют необходимость использования сертифицированных СКЗИ для защиты данных? a) функциональные требования b) нормативные требования (регуляторные ограничения) c) интерфейсные требования d) требования к производительности		ПК-4
	Ответ:	b	
17	На этапе концептуально-логического проектирования ИС какая модель описывает потоки данных между компонентами системы и зоны доверия? a) ER-диаграмма b) DFD (диаграмма потоков данных) c) UML-диаграмма классов d) BPMN-диаграмма		ПК-4
	Ответ:	b	
18	При выявлении требований к Системе для ИС, обрабатывающей персональные данные, какой нормативный документ определяет требования к криптографической защите? a) ГОСТ 28147-89 b) 152-ФЗ «О персональных данных» c) ISO 9001 d) ITIL		ПК-4
	Ответ:	b	
19	Что является результатом этапа сопровождения разработанных проектных решений в области криптографической защиты? a) исходный код приложения b) актуализированная проектная документация с учётом новых угроз и требований c) протоколы тестирования d) маркетинговый план		ПК-4
	Ответ:	b	
20	При концептуально-логическом проектировании ИС какая модель описывает сущности, атрибуты и связи между ними для проектирования защищённой базы данных? a) физическая модель данных b) логическая модель данных (ER-диаграмма) c) сетевая модель d) иерархическая модель		ПК-4
	Ответ:	b	
21	Установите соответствие между этапом проектирования/сопровождения (1–3) и его содержанием (A–C) в области криптографической защиты. В бланк ответов запишите последовательность (например, 1-B, 2-A, 3-C). Этап — Содержание 1. Выявление требований — A. Актуализация документации при изменении угроз и нормативных требований 2. Концептуально-логическое проектирование — B. Определение классов СКЗИ, алгоритмов и режимов шифрования 3. Сопровождение проектных решений — C. Построение моделей угроз, выбор архитектуры криптозащиты		ПК-4
	Ответ:	1-B, 2-C, 3-A	
22	Установите соответствие между нормативным документом (1–3) и его содержанием (A–C) при выявлении требований к Системе. В бланк ответов запишите последовательность (например, 1-A, 2-B, 3-C). Нормативный документ — Содержание требований 1. 152-ФЗ «О персональных данных» — A. Требования к криптографическим алгоритмам и протоколам		ПК-4

1. 152-ФЗ «О персональных данных»	A. Требования к криптографическим алгоритмам и протоколам	
2. Приказы ФСБ России	B. Требования к защите персональных данных с использованием СКЗИ	
3. ГОСТ Р 34.10-2012	C. Стандарт электронной подписи на основе эллиптических кривых	

	Ответ:	1-B, 2-A, 3-C
23	Установите соответствие между типом требования к криптографической защите (1–3) и его примером (A–C) при выявлении требований к Системе. В бланк ответов запишите последовательность (например, 1-C, 2-B, 3-A).	ПК-4

Тип требования	Пример требования
1. Функциональное	A. «Система должна использовать только сертифицированные СКЗИ»
2. Нефункциональное (безопасность)	B. «Время шифрования блока не должно превышать 10 мс»
3. Ограничение (регуляторное)	C. «Система должна обеспечивать шифрование данных по алгоритму AES-256»

	Ответ:	1-C, 2-B, 3-A
24	Установите правильную последовательность этапов выявления требований к криптографической защите Системы. Расположите буквы (A–D) в верном порядке. A) Анализ нормативно-правовых требований к защите информации B) Проведение интервью с заинтересованными сторонами C) Определение классов угроз и выбор класса СКЗИ D) Формирование и согласование раздела криптографической защиты в ТЗ	ПК-4
	Ответ:	A → B → C → D
25	Установите правильную последовательность сопровождения проектных решений по криптографической защите при изменении требований. Расположите буквы (A–D) в верном порядке. A) Оценка влияния изменений на архитектуру криптозащиты B) Получение запроса на изменение (изменение законодательства, новые угрозы) C) Актуализация проектной документации и повторное согласование D) Разработка плана внедрения изменений в систему	ПК-4
	Ответ:	B → A → D → C
26	Дайте развернутый ответ Назовите не менее двух методов выявления требований к криптографической защите Системы.	ПК-4
	Ответ:	интервьюирование, анализ нормативных документов, анализ рисков, анкетирование.
27	Дайте развернутый ответ Какой артефакт является результатом этапа концептуально-логического проектирования системы криптографической защиты?	ПК-4
	Ответ:	модель угроз, диаграмма потоков данных (DFD), архитектура криптозащиты.
28	Дайте развернутый ответ Для чего используются экспертные методы при выявлении требований к Системе в области криптографической защиты?	ПК-4
	Ответ:	для выявления скрытых рисков, обоснования выбора СКЗИ и проверки реалистичности требований.
29	Дайте развернутый ответ Назовите не менее двух нормативных документов, требования которых должны быть выявлены при проектировании системы криптографической защиты.	ПК-4
	Ответ:	152-ФЗ «О персональных данных», Приказы ФСБ России, ГОСТ Р 34.10-2012.
30	Дайте развернутый ответ Какой раздел технического задания должен быть обязательным при выявлении требований к Системе для ИС, обрабатывающей конфиденциальные данные?	ПК-4
	Ответ:	раздел требований к криптографической защите информации.

7. Оценочные материалы промежуточной аттестации

Экзамен шестой семестр

№ п/п	Содержание вопроса Правильный ответ (ключ ответа)	Компетенция
1	Дайте развернутый ответ При обнаружении инцидента ИБ, связанного с нарушением целостности данных, какой криптографический механизм позволяет подтвердить факт изменения файла?	ПК-2
	Ответ: сравнение хеш-сумм (хеш-функция, например SHA-256).	
2	Дайте развернутый ответ Назовите не менее двух действий, которые должны быть выполнены при принятии мер по устранению инцидента ИБ, вызванного компрометацией ключей шифрования.	ПК-2

	Ответ:	аннулирование (отзыв) скомпрометированных ключей, генерация новых ключей, уведомление заинтересованных сторон.	
3	Дайте развернутый ответ При тестировании ИС для выявления инцидента, связанного с перехватом сетевого трафика, какой протокол должен быть проверен на корректность настройки?		ПК-2
	Ответ:	TLS/SSL.	
4	Дайте развернутый ответ Назовите не менее двух признаков инцидента ИБ, связанного с компрометацией криптографических ключей, которые могут быть выявлены при тестировании ИС.		ПК-2
	Ответ:	необычная активность с ключами, множественные ошибки аутентификации, появление неизвестных сертификатов, неожиданные запросы на расшифровку.	
5	Дайте развернутый ответ Какой документ должен быть оформлен при обнаружении инцидента ИБ в рамках сопровождения ИС?		ПК-2
	Ответ:	отчёт об инциденте (акт расследования инцидента ИБ).	
6	Дайте развернутый ответ Назовите не менее двух методов выявления требований к Системе в области криптографической защиты информации.		ПК-4
	Ответ:	интервьюирование заинтересованных сторон, анализ нормативно-правовых документов, анализ рисков, анкетирование, изучение аналогов.	
7	Дайте развернутый ответ Какой артефакт разрабатывается на этапе концептуально-логического проектирования ИС и описывает потоки данных между компонентами системы?		ПК-4
	Ответ:	диаграмма потоков данных (DFD — Data Flow Diagram).	
8	Дайте развернутый ответ Назовите не менее двух нормативно-правовых документов, требования которых должны быть выявлены при проектировании системы криптографической защиты для ИС, обрабатывающей персональные данные.		ПК-4
	Ответ:	152-ФЗ «О персональных данных», Приказы ФСБ России (№ 66, № 117, № 524), ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012.	
9	Дайте развернутый ответ Какое действие необходимо выполнить при сопровождении разработанных проектных решений в случае изменения нормативных требований к криптографической защите?		ПК-4
	Ответ:	актуализация проектной документации, повторное согласование с заинтересованными сторонами и внедрение изменений.	
10	Дайте развернутый ответ Назовите не менее двух заинтересованных сторон (стейкхолдеров), с которыми проводится согласование требований к криптографической защите при выявлении требований к Системе.		ПК-4
	Ответ:	заказчик, эксперты по информационной безопасности, регуляторы (ФСБ), разработчики, администраторы безопасности.	

7.1. Уровни овладения

Компетенция: ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС.

Индикатор достижения компетенции: ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС.

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: ПК-4 Способен к выявлению требований к Системе, ее концептуально-логическому проектированию и сопровождению разработанных проектных решений.

Индикатор достижения компетенции: ПК-4.2 Сопровождает разработанные проектные решения и требования к ИС.

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. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников. - Москва: Юрайт, 2026. - 209 с - 978-5-9916-7088-3. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/583633 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд. - Москва: Юрайт, 2026. - 424 с - 978-5-534-12474-3. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/583156 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. - Москва: Юрайт, 2026. - 310 с - 978-5-534-02883-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/583783 (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. http://www.gov.ru/ - Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия»

Ресурсы «Интернет»

1. crypto-lab.systemslibrarian.dev - Crypto Lab (crypto-lab.systemslibrarian.dev) — браузерная криптографическая лаборатория, победитель Cybersecurity Excellence Awards 2026. Содержит десятки интерактивных демонстраций: классические алгоритмы (AES, RSA, Diffie-Hellman), пост-квантовые схемы (Kyber/ML-KEM, SPHINCS+), протоколы (Kerberos, TLS, Signal Double Ratchet), атаки (Padding Oracle, Nonce Lattice) и многое другое
2. https://stepik.org - Платформа с онлайн-курсами от авторов-практиков

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. Draw.io (diagrams.net);
2. Консультант Плюс;
3. Мой офис;

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