МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кубанский государственный университет»(ФГБОУ ВО «КубГУ»)

Факультет компьютерных технологий и прикладной математики
Кафедра вычислительных технологий

УТВЕРЖДАЮ
Проректор по учебной работе, качеству образования – первый проректор
_____ Хагуров Т.А.
подпись
«02» ___июня____ 2026г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.2 «КРИПТОГРАФИЯ И СЕТЕВАЯ БЕЗОПАСНОСТЬ»

Направление подготовки _____10.03.01 Информационная безопасность_____
(код и наименование направления подготовки/специальности)

Направленность (профиль) _____Информационная безопасность интеллектуальных автоматизированных систем_____
(наименование направленности (профиля) специализации)

Программа подготовки ___академическая_____
(академическая /прикладная)

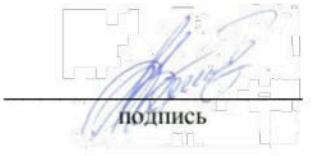
Форма обучения _____очная_____
(очная, очно-заочная, заочная)

Квалификация (степень) выпускника ___бакалавр_____
(бакалавр, магистр, специалист)

Краснодар 2026

Рабочая программа дисциплины «КРИПТОГРАФИЯ И СЕТЕВАЯ БЕЗОПАСНОСТЬ» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

Программу составил(а):
Жук Арсений Сергеевич,
Ф.И.О., должность, ученая степень, ученое звание


подпись

Рабочая программа дисциплины «КРИПТОГРАФИЯ И СЕТЕВАЯ БЕЗОПАСНОСТЬ» утверждена на заседании кафедры Вычислительных технологий протокол № 11 от 14.05.2026 г

И.О. заведующего кафедрой (разработчика) Приходько Т.А.


подпись

Утверждена на заседании учебно-методической комиссии факультета Компьютерных Технологий и Прикладной Математики
протокол № 3 от 15.05.2026 г.

Председатель УМК факультета Добровольская Н.Ю.


подпись

Рецензенты:

Гаркуша О.В., доцент кафедры информационных технологий ФБГОУ ВО «Кубанский государственный университет», кандидат физико-математических наук.

Схаляхо Ч.А., доцент КВВУ им.С.М. Штеменко, кандидат физико-математических наук, доцент

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цели освоения дисциплины

Сформировать у студентов практические навыки применения криптографических протоколов для защиты каналов связи, аутентификации пользователей и обеспечения безопасности веб-приложений, сетевых сервисов и современных инфраструктур

1.2 Задачи дисциплины

1. Освоить архитектуру и настройку TLS/SSL, включая mTLS и анализ уязвимостей.
2. Научиться развёртывать и администрировать IPsec VPN в различных режимах.
3. Получить навыки настройки OpenVPN и WireGuard для защищённых каналов.
4. Изучить структуру и применение JWT-токенов, включая безопасное хранение и уязвимости.
5. Освоить протоколы OAuth 2.0 и OpenID Connect для федеративной аутентификации.
6. Научиться защищать веб-приложения от распространённых атак (OWASP Top 10).
7. Изучить криптографические протоколы для защиты электронной почты (PGP).
8. Освоить защиту сетевых сервисов: SSH, DNSSEC.
9. Изучить протоколы защиты беспроводных сетей (WPA3, 802.1X).
10. Познакомиться с современными трендами: Zero Trust, Service Mesh, постквантовая криптография.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Криптография и сетевая безопасность» относится к Блоку 1 «Дисциплины (модули)» учебного плана, к обязательной части. В соответствии с рабочим учебным планом дисциплина изучается на 1 курсе в 1 семестре по очной форме обучения. Вид промежуточной аттестации: экзамен.

Дисциплина «Криптография и сетевая безопасность» представляет собой преддисциплину для таких дисциплин, как «Основы управления информационной безопасностью», «Безопасность в облачных средах».

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Процесс освоения дисциплины направлен на формирование следующих компетенций: УК-2,ОПК-9,ОПК-10,ОПК-1.1

Код и наименование индикатора*	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	
ОПК-1.1: Знает требования к системе обеспечения информационной безопасности	Знает требования к системе обеспечения информационной безопасности
ОПК-1.2: Умеет разрабатывать проект технического задания на создание системы обеспечения информационной безопасности	Умеет разрабатывать проект технического задания на создание системы обеспечения информационной безопасности
ОПК-1.3: Владеет навыками формулирования и обоснования требований к системам обеспечения информационной безопасности	Владеет навыками формулирования и обоснования требований к системам обеспечения информационной безопасности
ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	
ОПК-5.1: Знает теорию и методологию научного исследования, основы проведения эксперимента и методы обработки экспериментальных данных	Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-5.2: Умеет обрабатывать и оформлять результаты научных исследований и оформлять научно-технические отчеты	Умеет применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-5.3: Владеет навыками подготовки научно-технических отчетов, обзоров, научных докладов и статей в области информационной безопасности	Владеет средствами криптографической и технической защиты информации для решения задач профессиональной деятельности

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утверждённым учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 5 зач. ед. (180 часов), их распределение по видам работ представлено в таблице (для студентов ОФО).

Вид работы		Всего часов	Очная	
			6 семестр (часы)	2 семестр (часы)
Контактная работа в том числе:		56.3	56.3	
Аудиторные занятия (всего):		36	36	
В том числе:				
Занятия лекционного типа		18	18	
Занятия семинарского типа (семинары, практ. занятия)				
Лабораторные занятия		18	18	
Иная контактная работа		20.3	20.3	
Контроль самостоятельной работы		20	20	
Промежуточная аттестация (ИКР)		0.3	0.3	
Самостоятельная работа, в том числе		97	97	
В том числе:				
Курсовая работа		-	-	
Проработка учебного (теоретического) материала		32	32	
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		32	32	
Реферат				
Подготовка к текущему контролю		33	33	
Контроль: экзамен		26,7	26,7	
Общая трудоёмкость	в час	180	180	
	в т.ч. контактная работа	56.3	56.3	

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоёмкости по разделам дисциплины.Разделы дисциплины, изучаемые в 1 семестре *(очная форма)*.

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Протокол TLS/SSL: архитектура, настройка, анализ	20	4		2	14

2.	Протокол IPsec: режимы, IKE, настройка	18	2		2	14
3.	VPN-протоколы: OpenVPN и WireGuard	20	2		4	14
4.	Защита веб-приложений: OWASP, JWT	22	4		4	14
5.	Протоколы аутентификации: OAuth 2.0, OpenID Connect	20	2		4	14
6	Защита сетевых сервисов: SSH, DNSSEC, беспроводные сети (WPA3)	*18*	*2*		*2*	*14*
7	Современные тренды: mTLS, Zero Trust, Service Mesh, постквантовая криптография	*15*	*2*		*0*	*13*
	ИТОГО по разделам дисциплины	133	18		18	97
	Контроль самостоятельной работы (КСР)	20				
	Курсовой проект	-				
	Промежуточная аттестация (ИКР)	0.3				
	Подготовка к экзамену	26,7				
	Общая трудоёмкость по дисциплине	180				

Примечание: Л – лекции, ПЗ – практические занятия / семинары, КСР – контрольные и самостоятельные работы, ЛР – лабораторные занятия, СРС – самостоятельная работа студента, Д-доклад, РГЗ – расчётно-графическое задание.

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
1.	Протокол TLS/SSL: архитектура, настройка, анализ	- Лекция 1. TLS: архитектура, версии 1.2 и 1.3. Handshake, Record Protocol. Уязвимости (POODLE, Heartbleed). - Лекция 2. Сертификаты: типы (DV, OV, EV), цепочки, управление. Mutual TLS (mTLS). - Лекция 3. Настройка HTTPS-серверов (nginx, Apache). HSTS, HPKP. Инструменты анализа: openssl, sslyze, Wireshark.	*зачет, защита ЛР*
2.	Протокол IPsec: режимы, IKE, настройка	- Лекция 4. AH и ESP. Транспортный и туннельный режимы. IKEv1/v2. Способы аутентификации. - Лекция 5. Настройка IPsec на Linux (StrongSwan). Анализ трафика. Типичные проблемы и их решение.	*зачет, защита ЛР*
3.	VPN-протоколы: OpenVPN и WireGuard	- Лекция 6. OpenVPN: TUN/TAP, режимы, аутентификация (сертификаты, LDAP). Маршрутизация. - Лекция 7. WireGuard: архитектура, криптостойкость, генерация ключей, конфигурация. Сравнение с OpenVPN.	*зачет, защита ЛР*

4	Защита веб-приложений: OWASP, JWT	- Лекция 8. OWASP Top 10: SQL-инъекции, XSS, CSRF — принципы и защита. - Лекция 9. JWT: структура, алгоритмы (HS256, RS256, ES256). Жизненный цикл. Уязвимости (alg:none, подбор ключа). - Лекция 10. Безопасное хранение токенов (HttpOnly, Secure, SameSite). Refresh-токены, blacklist.	*зачет, защита ЛР*
5	Протоколы аутентификации: OAuth 2.0, OpenID Connect	- Лекция 11. OAuth 2.0: роли, типы грантов. Безопасность (PKCE, state-параметр). - Лекция 12. OpenID Connect: ID Token, отличие от OAuth 2.0. Интеграция с Keycloak.	*зачет, защита ЛР*
6	Защита сетевых сервисов: SSH, DNSSEC, беспроводные сети (WPA3)	- Лекция 13. SSH: криптография, аутентификация (ключи, агент), туннелирование. Защита от атак. - Лекция 14. DNSSEC: принципы, цепочка доверия. Защита беспроводных сетей: WPA3, 802.1X.	*зачет, защита ЛР*
7	Современные тренды: mTLS, Zero Trust, Service Mesh, постквантовая криптография	- Лекция 15. Zero Trust: принципы, реализация через mTLS и JWT. Service Mesh (Istio, Linkerd). - Лекция 16. Постквантовая криптография: алгоритмы NIST, миграция. Обзор квантово-безопасных протоколов.	*зачет, защита ЛР*

2.3.2 Занятия семинарского типа (практические / семинарские занятия / лабораторные работы)

№	Наименование лабораторных работ	Форма текущего контроля
1	2	3
1.	ЛР №1. TLS: настройка и анализ (4 часа) - Задание 1: Настроить HTTPS-сервер nginx с самоподписанным сертификатом и с Let's Encrypt. Включить HSTS. - Задание 2: Проанализировать TLS-соединение в Wireshark, расшифровать трафик, проверить уязвимости с помощью sslyze и testssl.sh. - Железо: стенд ПЗИ-НСД. - ПО: Linux, nginx, OpenSSL, Wireshark, sslyze, testssl.sh.	Защита лабораторной работы
2.	ЛР №2. IPsec VPN: настройка и анализ (4 часа) - Задание 1: Настроить IPsec в транспортном режиме между двумя Linux-машинами (StrongSwan, предварительный ключ). - Задание 2: Настроить IPsec в туннельном режиме между двумя сетями с сертификатами. Перехватить и проанализировать ESP-трафик. - Железо: стенд ПЗИ-НСД. - ПО: Linux, StrongSwan, Wireshark.	Защита лабораторной работы
3.	ЛР №3. OpenVPN: развёртывание и тонкая настройка (4 часа) - Задание 1: Развернуть OpenVPN сервер в режиме клиент-сервер с сертификатами и аутентификацией через LDAP. - Задание 2: Настроить split tunneling, проверить маршрутизацию, проанализировать туннельный трафик. - Железо: стенд ПЗИ-НСД.	Защита лабораторной работы

	- ПО: Linux, OpenVPN, OpenLDAP, Wireshark.	
4.	ЛР №4. WireGuard: настройка и сравнение (4 часа) - Задание 1: Настроить WireGuard между двумя узлами, затем как сервер для нескольких клиентов. - Задание 2: Провести тесты производительности (iPerf3) для OpenVPN и WireGuard, подготовить отчёт с графиками. - Железо: стенд ПЗИ-НСД. - ПО: Linux, WireGuard, OpenVPN, iPerf3.	Защита лабораторной работы
5.	ЛР №5. Защита веб-приложений: OWASP и JWT (4 часа) - Задание 1: Разработать Flask-приложение с уязвимостями (SQL-инъекция, XSS), эксплуатировать их с помощью Burp Suite и SQLMap. - Задание 2: Устранить уязвимости, внедрить JWT-аутентификацию (HS256) и защиту CSRF. - Железо: стенд ПЗИ-НСД. - ПО: Python (Flask), Burp Suite Community, SQLMap, PyJWT	Защита лабораторной работы
6.	ЛР №6. JWT: углублённая безопасность и атаки (4 часа) - Задание 1: Реализовать генерацию JWT с RS256, проверить атаки (alg:none, подбор слабого ключа, истечение срока). - Задание 2: Внедрить refresh-токены, blacklist, безопасное хранение в HttpOnly cookie. - Железо: стенд ПЗИ-НСД. - ПО: Python (Flask/Django, PyJWT, cryptography), Postman.	Защита лабораторной работы
7.	ЛР №7. OAuth 2.0 и OpenID Connect с Keycloak (4 часа) - Задание 1: Развернуть Keycloak в Docker, настроить realm, клиентов и пользователей. - Задание 2: Интегрировать Flask-приложение с OIDC (Authorization Code Flow), получить ID Token и Access Token, реализовать проверку прав. - Железо: стенд ПЗИ-НСД + сервер. - ПО: Linux, Docker, Keycloak, Python (Flask, python-oidc).	Защита лабораторной работы
8.	ЛР №8. Защита электронной почты: PGP и SSH (4 часа) - Задание 1: Сгенерировать ключевую пару GnuPG, зашифровать и подписать сообщение, проверить подпись. Настроить Thunderbird с Enigmail. - Задание 2: Настроить SSH с аутентификацией по ключам, создать защищённый туннель для проброса портов. - Железо: стенд ПЗИ-НСД. - ПО: Linux/Windows, GnuPG, Thunderbird, Enigmail, OpenSSH	Защита лабораторной работы

2.3.3 Примерная тематика курсовых работ (проектов)

Не предусмотрено

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
	2	3
1	Протокол TLS/SSL: архитектура, настройка, анализ	Основная литература
2	Протокол IPsec: режимы, IKE, настройка	Основная литература
3	VPN-протоколы: OpenVPN и WireGuard	Основная литература
4	Защита веб-приложений: OWASP, JWT	Основная литература
5	Протоколы аутентификации: OAuth 2.0, OpenID Connect	Основная литература
6	Защита сетевых сервисов: SSH, DNSSEC, беспроводные сети (WPA3)	
7	Современные тренды: mTLS, Zero Trust, Service Mesh, постквантовая криптография	

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,
– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,
– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,
– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ, ПРИМЕНЯЕМЫЕ ПРИ ОСВОЕНИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	Количество часов
3	Л	Компьютерные презентации и обсуждение	4
	ЛР	Разбор конкретных ситуаций (задач), тренинги по решению задач, компьютерные симуляции (программирование алгоритмов)	4
Итого:			8

4 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Функциональные последовательности и ряды».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме тестовых заданий, доклада-презентации по проблемным темам разделов дисциплины, разно уровневых заданий и промежуточной аттестации в форме вопросов и заданий к зачёту.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
	ОПК-1.1: Знает требования к системе обеспечения информационной безопасности	Знает требования к системе обеспечения информационной безопасности	опрос по теме, лабораторная работа	Вопросы на экзамене 1-30

	ОПК-1.2: Умеет разрабатывать проект технического задания на создание системы обеспечения информационной безопасности	Умеет разрабатывать проект технического задания на создание системы обеспечения информационной безопасности	опрос по теме, лабораторная работа	Вопросы на экзамене 1-30
	ОПК-1.3: Владеет навыками формулирования и обоснования требований к системам обеспечения информационной безопасности	Владеет навыками формулирования и обоснования требований к системам обеспечения информационной безопасности	опрос по теме, лабораторная работа	Вопросы на экзамене 1-30
	ОПК-5.1: Знает теорию и методологию научного исследования, основы проведения эксперимента и методы обработки экспериментальных данных	Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности	опрос по теме, лабораторная работа	Вопросы на экзамене 1-30
	ОПК-5.2: Умеет обрабатывать и оформлять результаты научных исследований и оформлять научно-технические отчеты	Умеет применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	опрос по теме, лабораторная работа	Вопросы на экзамене 1-30
	ОПК-5.3: Владеет навыками подготовки научно-технических отчетов, обзоров, научных докладов и статей в области информационной безопасности	Владеет средствами криптографической и технической защиты информации для решения задач профессиональной деятельности	опрос по теме, лабораторная работа	Вопросы на экзамене 1-30

Зачётно-экзаменационные материалы для промежуточной аттестации (экзамен)

Перечень вопросов к экзамену

1. TLS Handshake: этапы, отличие TLS 1.2 и 1.3.
2. Mutual TLS: принцип, применение.
3. IPsec: режимы, AH vs ESP.
4. IKEv1 vs IKEv2.
5. OpenVPN: режимы, аутентификация, сертификаты.
6. WireGuard: архитектура, ключи, конфигурация.
7. JWT: структура, алгоритмы, уязвимости.
8. OAuth 2.0: роли, типы грантов.
9. OpenID Connect: отличие от OAuth 2.0, структура ID Token.
10. SQL-инъекции: принцип, защита.
11. XSS: типы, защита.
12. CSRF: принцип, защита.
13. PGP: Web of Trust, генерация ключей, шифрование/подпись.
14. SSH: аутентификация по ключам, туннелирование.
15. DNSSEC: принципы, цепочка доверия.
16. WPA3: отличия от WPA2, SAE.
17. Zero Trust: принципы и реализация.
18. mTLS в микросервисах.
19. Service Mesh: шифрование трафика.
20. Постквантовая криптография: основные алгоритмы.
21. Анализ TLS с помощью Wireshark и openssl.
22. Настройка IPsec на Linux (StrongSwan).
23. Настройка OpenVPN с LDAP.
24. Настройка WireGuard.
25. Безопасное хранение JWT на клиенте.

Критерии оценивания результатов обучения

Оценка	Критерии оценивания по зачёту
Отлично	Даны ответы на вопросы на экзамене, сделано 7 и больше лаб
Хорошо	Даны ответы на вопросы на экзамене, могут быть неточности в формулировках, сделано 6 и больше лаб
Удовлетворительно	Даны ответы на вопросы на экзамене, могут быть неточности в формулировках, сделано 5 и больше лаб
не удовл	Нет ответов на вопросы на экзамене и ответы абсолютно неверны, сделано 4 и меньше лабораторных работ

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на зачёте;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5 ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

5.1 Учебная литература

5.1.1 Основная литература

1. Фомин, Д. В. Информационная безопасность [Электронный ресурс]: учеб.-метод. пособие / Д.В. Фомин; АмГУ, ФМиИ. - Благовещенск: Изд-во Амур. гос. ун-та, 2017. - 60 с. http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/7371.pdf
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/512268.
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998.

5.1.2 Дополнительная литература

1. Олифер, В. Г. Безопасность компьютерных сетей : учебник для вузов / В. Г. Олифер, Н. А. Олифер. — Москва : Горячая линия-Телеком, 2015. — 648 с. — ISBN 978-5-9912-0420-0.

2. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8.

5.2 Периодическая литература

1. Автоматика и вычислительная техника.
2. Реферативный журнал ВИНИТИ
3. Базы данных компании «Ист Вью» http://dlib.eastview.com
4. Электронная библиотека GREBENNIKON.RU https://grebennikon.ru/

5.3 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):
1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.comЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:
1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com

4. Журналы издательства Wiley https://onlinelibrary.wiley.com/

5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/

6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru

7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/

8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/

9. Электронная коллекция Оксфордского Российского Фонда
https://ebookcentral.proquest.com/lib/kubanstate/home.action

10. Springer Journals https://link.springer.com/

11. Nature Journals https://www.nature.com/siteindex/index.html

12. Springer Nature Protocols and Methods
https://experiments.springernature.com/sources/springer-protocols

13. Springer Materials http://materials.springer.com/

14. zbMath https://zbmath.org/

15. Nano Database https://nano.nature.com/

16. Springer eBooks: https://link.springer.com/

17. "Лекториум ТВ" http://www.lektorium.tv/

18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/

2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/

3. КиберЛенинка (http://cyberleninka.ru/);

4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/ ;

5. Федеральный портал "Российское образование" http://www.edu.ru/ ;

6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/ ;

7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .

8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);

9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/ ;

10. Справочно-информационный портал "Русский язык" http://gramota.ru/ ;

11. Служба тематических толковых словарей http://www.glossary.ru/ ;

12. Словари и энциклопедии http://dic.academic.ru/ ;

13. Образовательный портал "Учеба" http://www.ucheba.com/ ;

14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

15. Philology.ru [Электронный ресурс]: [филологический портал]. - Режим доступа:– http://www.philology.ru/ , свободный (дата обращения: 2.02.2017) (библиотека филологических текстов (монографий, статей, методических пособий).

16. Языкознание.ру [Электронный ресурс] : [образовательный портал]. – Режим доступа:– http://yazykoznanie.ru , свободный (дата обращения: 2.02.2017) (ресурс для изучающих различные лингвистические дисциплины).

17. Linguists [Электронный ресурс]: [образовательный портал]. – Режим доступа: http://linguists.narod.ru , свободный (дата обращения: 12.02.2017) (Ресурсы для переводчиков и лингвистов, содержит список других сетевых ресурсов).

18. Лингвистика для школьников [Электронный ресурс]: [образовательный сайт]. – Режим доступа: – http://lingling.ru/ , свободный (дата обращения: 2.02.2017).

19. COGNITIV [Электронный ресурс]: [образовательный портал]. – Режим доступа: http://cognitiv.narod.ru , свободный (дата обращения: 5.01.2017) (Сайт для ученых-языковедов всех специальностей (обмен новейшей информацией в области лингвистики; обсуждение фундаментальных и прикладных проблем языкознания, а также вопросов взаимоотношения

языка, культуры и общества).

20. Лингвистический энциклопедический словарь [Электронный ресурс]: [он- лайн-словарь]. – Режим доступа: http://lingvisticheskiy-slovar.ru/ , свободный (дата обращения: 17.01.2017).

21. Linguistics Dictionary Glossary Terms Lexicon Online [Электронный ресурс]: [образовательный ресурс]. – Режим доступа: http://www.glossary.sil.org/ , свободный (дата обращения: 12.02.2017) (глоссарий, содержащий более 950 лингвистических терминов с перекрестными ссылками и списком источников (SIL International).

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru ;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для освоения учебного материала студенту необходимо ознакомиться со структурой курса и методикой овладения материалом. Весь курс построен от простого к сложному, и каждая его тема основана на материалах предыдущих тем. В этой связи студенту необходимо не терять логику курса и строго ей следовать. В лекционном материале даются, как правило, теоретические сведения, которые раскрываются на практических примерах. Для закрепления теоретических знаний студент получает индивидуальное задание к циклу лабораторных работ, который охватывает весь теоретический материал. Каждая лабораторная работы защищается по мере выполнения. Таким образом, выполняя весь цикл лабораторных работ, студент получает и осваивает знания в соответствии с компетенциями курса. По выступлениям на круглом столе с преподавателем согласовывается тема выступления и готовится само выступление. Во время текущей аттестации могут проводиться контрольные опросы по начитанному теоретическому и практическому материалу.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся-инвалидом или лицом с ограниченными возможностями здоровья.

7. Перечень информационных технологий, используемых при осуществления образовательного процесса по дисциплине

7.1. Перечень информационных технологий.

Информационные технологии – не предусмотрены.

7.2. Перечень необходимого программного обеспечения.

Программное обеспечение - не предусмотрено.

7.3. Перечень информационных справочных систем:

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
2. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)
3. Электронная библиотечная система «Университетская библиотека ONLINE» (http://www.biblioclub.ru)

Для освоения дисциплины инвалидами и лицами с ограниченными возможностямиздоровья имеются издания в электронном виде в электронно-библиотечных системах

«Лань» и «Юрайт».

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Наименование специальных помещений	Оснащённость специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа (ауд. 129, 131, А305).	Мебель: учебная мебель Технические средства обучения: проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО)	PowerPoint, доступ к Microsoft Teams
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроляи промежуточной аттестации ауд. 129, 131, А305	Мебель: учебная мебель Технические средства обучения: экран, компьютер Оборудование: кондиционер	PowerPoint, доступ к Microsoft Teams
Учебные аудитории для проведения лабораторных работ. Лаборатория (ауд. 102-106, А301-303).	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование: Учебный стенд «Программные средства защиты информации от НСД» (ПЗИ-НСД) | 2 шт. | Базовая платформа для всех лабораторных работ. Включает 4 ПК (ОС Windows), ПО Secret Net Studio, коммутатор. | ПАК «Соболь» (версия 4.0, PCI-E) 2 шт. Модуль доверенной загрузки для ЛР №1 и проектов по аппаратной защите. | Сервер (уже имеется) 1 шт. Для развёртывания SIEM (Wazuh/nano), системы резервного копирования (Kopia/Bareos), Cuckoo Sandbox, хранения образов виртуальных машин.	Linux (Ubuntu Server) - OpenSSL, nginx, Apache - Wireshark, sslyze, testssl.sh - StrongSwan - OpenVPN, WireGuard - Python (Flask, Django, PyJWT, cryptography, requests-oauthlib) - Keycloak (Docker) - GnuPG, Thunderbird, Enigmail - Burp Suite Community, SQLMap, Postman - Docker, docker-compose - iPerf3 - OpenLDAP (опционально) - OpenSSH, Bind9 (для DNSSEC), FreeRADIUS (для WPA3)

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащённые компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащённость помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Доступ печатным и электронным информационным ресурсам
Помещение для самостоятельной работы обучающихся (ауд. 146)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы	
Наименование помещений для самостоятельной работы обучающихся	Оснащённость помещений для самостоятельной работы обучающихся	
	Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	