АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«КУБАНСКИЙ ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»
(АНПОО «КУБАНСКИЙ ИПО»)

ОТДЕЛЕНИЕ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

РАБОЧАЯ ПРОГРАММА

учебной дисциплины
ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
по специальности
09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ
направленность программы: Разработка информационных систем

Краснодар, 2026

СОГЛАСОВАНО
Зам. директора по КОД и МР

_____ / Т.В. Першакова
28.05.2026 г.

УТВЕРЖДАЮ
Директор АНПОО «Кубанский ИПО»

_____ О.Л. Шутов
Приказ №38-О от 28.05.2026 г.

ОДОБРЕНО
Педагогическим советом
Протокол №6 от 28.05.2026 г

РАССМОТРЕНО
на заседании УМО
«Информационные системы и программирование»
Протокол № 5 от 15.05.2026г.
Председатель _____ / С.А. Пясецкий

Рабочая программа учебной дисциплины ОП.05 Основы информационной безопасности предназначена для реализации образовательной программы подготовки специалистов среднего звена.

Разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением (Приказ Министерства Просвещения Российской Федерации от 24 февраля 2025 г. № 138, зарегистрированного Министерством Юстиции России 31 марта 2025 г. № 81696) с учетом примерной образовательной программы, разработанной Федеральным учебно-методическим объединением в системе среднего профессионального образования по укрупненным группам профессий, специальностей 09.00.00 Информатика и вычислительная техника, с учетом профессиональных стандартов: «Программист» (Приказ Министерства труда и социальной защиты РФ от 20 июля 2022 г. № 424н, зарегистрирован Министерством юстиции Российской Федерации от 22 августа 2022г. №69720); «Специалист по информационным системам» (Приказ Министерства труда и социальной защиты РФ от 13 июля 2023 г. № 586н, зарегистрирован Министерством юстиции Российской Федерации от 16 августа 2023 г № 74817) и компетенции «Программные решения для бизнеса».

Организация-разработчик: АНПОО «Кубанский ИПО»

Разработчик:
Пясецкий С.А., преподаватель АНПОО «Кубанский ИПО»

Рецензенты:
1. Варкентин В.Ф. – преподаватель, АНПОО «Кубанский ИПО»
Квалификация по диплому: преподаватель информатики
2. Маслиев Р.О, генеральный директор ООО «Старт Эксперт»

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина ОП.05 Основы информационной безопасности является обязательной частью общепрофессионального цикла образовательной программы в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

Особое значение дисциплина имеет при формировании и развитии общих и профессиональных компетенций:

ОК.01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК.02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

ОК.09. Пользоваться профессиональной документацией на государственном и иностранном языках;

ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации;

ПК 3.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием;

1.2 Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания.

Код ПК, ОК	Умения	Знания
ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09	− распознавать задачу и/или проблему в профессиональном и/или социальном контексте; − анализировать задачу и/или проблему и выделять её составные части; − определять этапы решения задачи; − выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; − определять необходимые ресурсы; − владеть актуальными методами работы в профессиональной и смежных сферах; − оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); − определять задачи для поиска информации; − определять необходимые источники информации; − структурировать получаемую информацию; − выделять наиболее значимое в перечне информации; − оценивать практическую значимость результатов поиска; − оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач;	− основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; − алгоритмы выполнения работ в профессиональной и смежных областях; − структуру плана для решения задач; − приемы структурирования информации; − порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; − лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности − принципы криптографии и методов шифрования данных; − стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; − методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; − законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; − принципов безопасности информационных систем;

	− использовать различные цифровые средства для решения профессиональных задач; − шифровать данные и обеспечивать их конфиденциальность; − анализ требований безопасности информационных систем; − *распознавать задачу в контексте ИБ;* − *выявлять и эффективно искать информацию по угрозам;* − *определять необходимые ресурсы для анализа.* − *анализировать задачу, выделять составные части, определять этапы решения;* − *анализ требований безопасности информационных систем, владение актуальными методами;* − *использовать различные цифровые средства для решения задач в облаке;* − *оформлять результаты поиска, применять средства ИТ для решения профессиональных задач*	− современных методов и технологий в области безопасности информационных систем; − законодательных и нормативных актов в области безопасности информационных систем; − *основные источники информации для оценки угроз (ресурсы CVE, NVD, CERT);* − *лексический минимум для описания инцидентов и средств защиты, социальной инженерии, приемы структурирования информации об угрозах;* − *законодательные акты в области ИБ, структура плана управления рисками;* − *принципы безопасности ИС, современные методы защиты приложений;* − *стандарты безопасности для облаков (CSA, ISO 27017);* − *алгоритмы выполнения работ при расследовании инцидентов;* − *современные методы и технологии в области ИБ;* − *порядок применения протоколов и ПО*

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
ОБЪЕМ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	**68**
в том числе вариативная часть	*36*
- теоретическое обучение	**34**
- практические занятия	**34**
в т.ч. в форме практической подготовки	34
- промежуточная аттестация (дифференцированный зачет)	**2**

Тематический план учебной дисциплины

Наименование разделов и тем	Количество аудиторных часов				
	Всего	в т.ч. в форме практической подготовки	самост. работа	теоретич. обучение	практич. занятия
Раздел 1. Основы информационной безопасности	**68**	**32**	**-**	**34**	**32**
Тема 1.1 Введение в информационную безопасность	4	2	-	2	2
Тема 1.2 Управление безопасностью информации	4	2	-	2	2
Тема 1.3 Процедурный уровень информационной безопасности	4	2		2	2
Тема 1.4 Основы криптографии	4	2	-	2	2
Тема 1.5 Сетевые атаки и защита сети	4	2	-	2	2
Тема 1.6 Безопасность приложений. OWASP Top Ten	4	2	-	2	2
Тема 1.7 Защита данных: шифрование и управление доступом	4	2	-	2	2
Тема 1.8 Безопасность облачных технологий	4	2	-	2	2
Тема 1.9 Инциденты безопасности. Форензика и OSINT	4	2	-	2	2
Тема 1.10 Социальная инженерия	4	2	-	2	2
Тема 1.11 Будущее ИБ. AI и блокчейн	4	2	-	2	2
Тема 1.12 Протоколы аутентификации и авторизации	4	2	-	2	2
Тема 1.13 Правовые и комплаенс-аспекты ИБ	4	2	-	2	2
Тема 1.14 Инструменты цифровой криминалистики	4	2	-	2	2
Тема 1.15 Безопасность беспроводных сетей и IoT	4	2	-	2	2
Тема 1.16 DevSecOps и безопасность CI/CD	6	2	-	4	2
Дифференцированный зачет	**2**	**2**	**-**	**-**	**2**
ВСЕГО	**68**	**34**	**-**	**34**	**34**

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Основы информационной безопасности		**64**	
Тема 1.1 Введение в информационную безопасность	**Содержание учебного материала**	**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	1 **Введение в информационную безопасность** Основные понятия и определения (информация, угроза, уязвимость, атака, риск). История развития ИБ. Актуальные угрозы и риски. Классификация угроз. *Основные источники информации для оценки угроз (ресурсы CVE, NVD, CERT). Лексический минимум для описания инцидентов и средств защиты.*	2	
	в том числе, практических занятий	**2**	
	***ПЗ №1.** Анализ актуальных угроз и источников информации об уязвимостях*	2	
Тема 1.2 Управление безопасностью информации	**Содержание учебного материала**	**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	2 **Управление безопасностью информации** Нормативно-правовое регулирование (законы РФ, GDPR, HIPAA, PCI DSS). Политики и процедуры безопасности. Оценка и управление рисками. Стандарты ISO 27001, 27002. *Законодательные акты в области ИБ, структура плана управления рисками.*	2	
	в том числе, практических занятий	**2**	
	***ПЗ №2.** Разработка фрагмента политики безопасности и оценка рисков*	2	
Тема 1.3 Процедурный уровень информационной безопасности	**Содержание учебного материала**	**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	3 Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Защита информации при работе с посетителями. Организация работы с документами.	2	
	в том числе, практических занятий	**2**	
	***ПЗ №3.** Разработка фрагмента процедур информационной безопасности для офиса.	2	
Тема 1.4 Основы криптографии	**Содержание учебного материала**	**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	4 **Основы криптографии** Симметричные (AES, ГОСТ) и асимметричные (RSA, ECC) алгоритмы. Хэширование (MD5, SHA) и цифровая подпись. Применение криптографии. Стеганография (обзор).	2	
	в том числе, практических занятий	**2**	
	***ПЗ №4.** Работа с симметричным и асимметричным шифрованием	2	
Тема 1.5 Сетевые атаки и	**Содержание учебного материала**	**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02,
	5 **Сетевые атаки и защита сети**	2	

защита сети		Основы сетевой безопасности (модель OSI, угрозы на уровнях). DDoS, MITM, ARP-spoofing. VPN, межсетевые экраны (iptables, nextgen firewall). Стандарты и протоколы безопасности (SSL/TLS, IPsec, SSH).		ОК.09
	в том числе, практических занятий		**2**	
	***ПЗ №5.** Организация защиты от атак. Настройка VPN и межсетевого экрана		2	
Тема 1.6 Безопасность приложений. OWASP Top Ten	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	6	**Безопасность приложений. OWASP Top Ten** Уязвимости приложений (инъекции, XSS, CSRF, broken auth). Безопасное программирование: лучшие практики. *Принципы безопасности ИС, современные методы защиты приложений*	2	
	в том числе, практических занятий		**2**	
	****ПЗ №6.** Тестирование на проникновение*		2	
Тема 1.7. Защита данных: шифрование и управление доступом	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	7	**Защита данных: шифрование и управление доступом** Шифрование данных в покое (диски, БД) и в транзите (TLS). Резервное копирование (3-2-1 правило). Управление доступом (RBAC, MAC, ACL). Методы аутентификации (пароли, сертификаты, биометрия).	2	
	в том числе, практических занятий		**2**	
	***ПЗ №7.** Резервное копирование, восстановление и управление доступом		2	
Тема 1.8. Безопасность облачных технологий	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	8	**Безопасность облачных технологий** Модели IaaS, PaaS, SaaS. Разделение ответственности. Риски облаков (утечка данных, неправильная конфигурация). *Стандарты безопасности для облаков (CSA, ISO 27017)*	2	
	в том числе, практических занятий		**2**	
	****ПЗ №8.** Изучение моделей облачных услуг и их безопасности*		2	
Тема 1.9. Инциденты безопасности. Форензика и OSINT	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	9	**Инциденты безопасности. Форензика и OSINT** Реакция на инциденты (NIST SP 800-61). Цифровая криминалистика (сбор доказательств). Промышленный шпионаж. OSINT (разведка по открытым источникам). *Алгоритмы выполнения работ при расследовании инцидентов*	2	
	в том числе, практических занятий		**2**	
	***ПЗ №9.** Работа с инцидентами и OSINT		2	
Тема 1.10. Социальная инженерия	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	10	**Социальная инженерия** Психология атак (фишинг, претекстинг, кви про кво). Обучение сотрудников. *Лексический минимум по социальной инженерии, приемы структурирования информации об угрозах*	2	
	в том числе, практических занятий		**2**	
	***ПЗ №10.** Разработка политики информационной безопасности для организации		2	
Тема 1.11. Будущее ИБ. AI и	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02,
	11	**Будущее ИБ. AI и блокчейн**	2	

блокчейн		AI/ML в защите и атаках. Блокчейн для целостности данных. Этические аспекты ИБ. *Современные методы и технологии в области ИБ*		ОК.09
	в том числе, практических занятий		**2**	
	***ПЗ №11.** Применение AI для анализа угроз*		2	
Тема 1.12. Протоколы аутентификации и авторизации	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	12	***Протоколы аутентификации и авторизации*** *Kerberos, RADIUS, SAML, OAuth 2.0, JWT. Многофакторная аутентификация. Порядок применения протоколов и ПО*	2	
	в том числе, практических занятий		**2**	
	***ПЗ №12.** Настройка аутентификации через LDAP и MFA*		2	
Тема 1.13. Правовые и комплаенс-аспекты ИБ	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	13	***Правовые и комплаенс-аспекты ИБ*** *Уголовная и административная ответственность (статьи 272, 273 УК РФ). Персональные данные (152-ФЗ). Международные стандарты (GDPR, PCI DSS детально).*	2	
	в том числе, практических занятий		**2**	
	***ПЗ №13.** Анализ соответствия системы требованиям GDPR/152-ФЗ*		2	
Тема 1.14. Инструменты цифровой криминалистики	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	14	***Инструменты цифровой криминалистики*** *Форензика ОС Windows/Linux. Восстановление удалённых данных. Анализ памяти и дисков.*	2	
	в том числе, практических занятий		**2**	
	***ПЗ №14.** Форензический анализ образа диска*		2	
Тема 1.15. Безопасность беспроводных сетей и IoT	**Содержание учебного материала**		**4**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	15	***Безопасность беспроводных сетей и IoT*** *Угрозы Wi-Fi (WEP, WPA2-атаки), Bluetooth. Безопасность IoT (слабые пароли, отсутствие обновлений).*	2	
	в том числе, практических занятий		**2**	
	***ПЗ №15.** Анализ безопасности Wi-Fi и эмуляция IoT-устройства*		2	
Тема 1.16. DevSecOps и безопасность CI/CD	**Содержание учебного материала**		**6**	ПК.1.5., ПК.3.3., ОК.01, ОК.02, ОК.09
	16	***DevSecOps и безопасность CI/CD*** *Безопасное управление конфигурациями. SAST, DAST, сканеры уязвимостей в конвейере.*	2	
	17	***Решение комплексного кейса по расследованию инцидента*** *Повторение, разбор кейсов. Оценка последствий действий в реальных инцидентах. Этапы: обнаружение, анализ, сдерживание, восстановление.*	2	
	в том числе, практических занятий		**2**	
	ПЗ №16. Внедрение сканера уязвимостей в CI/CD (GitLab CI)		2	
***Дифференцированный зачет (ПЗ №17)**			**2**	
ВСЕГО:			**68**	

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Лаборатория «Компьютерных сетей и основ информационной безопасности»

оснащена оборудованием:

− рабочее место педагога (преподавательский стол (1 шт.), стул (1 шт.))

− рабочие места обучающихся (парты ученические (13 шт.), стулья ученические (25 шт.))

− доска учебная (меловая трех-секционная) (1 шт.)

− книжный шкаф – 1 шт.;

− учебно-методическая литература по дисциплине;

− комплект учебно-наглядных пособий;

техническими средствами обучения:

− персональный компьютер, подключение к сети Интернет с модулем контентной фильтрации Traffic Inspector, NetPolice и YandexDNS, возможность трансляции на экран аудио и видео информации (1 шт.)

− программное обеспечение на ПК – Microsoft Windows 10 или аналог, Microsoft Office (Word, Excel, PowerPoint) или аналог, 7Zip, 24PDF, Яндекс Браузер (1 шт.)

− программное обеспечение Android Studio, Visual Studio, Visual Studio Code или налоги

− монитор (1 шт.)

− клавиатура (1 шт.)

− мышь (1 шт.)

− телевизор (1 шт.)

− кабель для подключения HDMI (1 шт.)

3.2 Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд института имеет печатные и электронные образовательные и информационные ресурсы, в том числе рекомендованные ФУМО, для использования в образовательном процессе. Список дополнен новыми изданиями.

3.2.1 Основные источники

1. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Профессиональное образование). — ISBN 978-5-534-20645-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590435

2. Козырь, Н. С. Аудит информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь. — Москва : Издательство Юрайт, 2026. — 36 с. — (Профессиональное образование). — ISBN 978-5-534-20505-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590434

3. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587457

4. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458

5. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584372

6. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588374

3.2.2 Дополнительные источники

7. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547

8. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950

9. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510

10. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Методы оценки
Уметь: − распознавать задачу и/или проблему в профессиональном и/или социальном контексте; − анализировать задачу и/или проблему и выделять её составные части; − определять этапы решения задачи; − выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; − определять необходимые ресурсы; − владеть актуальными методами работы в профессиональной и смежных сферах; − оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); − определять задачи для поиска информации; − определять необходимые источники информации; − структурировать получаемую информацию; − выделять наиболее значимое в перечне информации; − оценивать практическую значимость результатов поиска; − оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; − использовать различные цифровые средства для решения профессиональных задач; − шифровать данные и обеспечивать их конфиденциальность; − анализ требований безопасности информационных систем; − *распознавать задачу в контексте ИБ;* − *выявлять и эффективно*	правильно идентифицирует наличие проблемы, формулирует её в терминах ИБ; выделяет составные части проблемы (источники угроз, уязвимости, активы, последствия); определяет логические этапы решения задачи и выстраивает их в правильной последовательности; разбивает сложную задачу на подзадачи и формулирует критерии перехода между этапами. самостоятельно определяет, какая информация необходима для решения задачи; выбирает релевантные и достоверные источники (включая специализированные базы уязвимостей, стандарты, документацию); использует корректные поисковые запросы и находит информацию в ограниченное время; структурирует полученные данные, выделяет наиболее значимое, отсекает второстепенное; оценивает практическую применимость найденной информации для конкретной задачи. определяет необходимые ресурсы (временные, программные, аппаратные, человеческие) для выполнения задачи; учитывает ограничения (права доступа, лицензии, бюджет); составляет реалистичный план действий с контрольными точками. использует актуальные методы ИБ (пентест, OSINT, анализ рисков, форензика, шифрование) применительно к контексту задачи; корректно работает с современными цифровыми инструментами (сканерами уязвимостей, криптоутилитами, анализаторами трафика, облачными консолями); обосновывает выбор конкретного метода или инструмента. выбирает подходящий алгоритм шифрования в зависимости от ситуации (симметричный/асимметричный, данные в покое/в транзите); применяет стандартные средства шифрования (GPG, OpenSSL, VeraCrypt) и корректно управляет ключами.	**Текущий контроль:** Оценка результатов выполнения практической работы Экспертное наблюдение за ходом выполнения практической работы (деятельностью студента) Оценка выполнения практического задания (работы) **Промежуточная аттестация:** дифференцированный зачет

искать информацию по угрозам; − *определять необходимые ресурсы для анализа.* − *анализировать задачу, выделять составные части, определять этапы решения;* − *анализ требований безопасности информационных систем, владение актуальными методами;* − *использовать различные цифровые средства для решения задач в облаке;* − *оформлять результаты поиска, применять средства ИТ для решения профессиональных задач*	сопоставляет текущее состояние системы с требованиями нормативных документов и стандартов; выявляет несоответствия и формулирует необходимые меры по приведению системы в соответствие. сравнивает достигнутый результат с требуемым; прогнозирует позитивные и негативные последствия выполненных действий; при обнаружении ошибок исправляет их самостоятельно или с обоснованной помощью наставника. создаёт структурированный отчёт (таблицы, диаграммы, чек-листы) с использованием средств ИТ; фиксирует источники информации и использованные инструменты; делает выводы о практической значимости полученных результатов.	
Знать: − основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; − алгоритмы выполнения работ в профессиональной и смежных областях; − структуру плана для решения задач; − приемы структурирования информации; − порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; − лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности − принципы криптографии и методов шифрования данных; − стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; − методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; − законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;	знает основные профильные ресурсы (CVE, NVD, CERT, официальные бюллетени) и назначение каждого; воспроизводит типовые алгоритмы (реагирование на инциденты, проведение пентеста, анализ рисков, настройка VPN); понимает структуру плана решения задачи (цель, этапы, ресурсы, ответственные, критерии успеха). правильно использует лексический минимум ИБ (угроза, уязвимость, риск, инцидент, конфиденциальность, целостность, доступность, аутентификация, авторизация) на русском и английском языке; не смешивает близкие понятия. объясняет разницу между симметричным и асимметричным шифрованием, хэшированием и цифровой подписью; называет примеры алгоритмов (AES, RSA, SHA) и сферы их применения. описывает назначение и базовую схему работы протоколов (TLS/SSL, SSH, Kerberos); называет методы аутентификации (пароли, сертификаты, биометрия, MFA) и факторы аутентификации. перечисляет основные законы РФ (149-ФЗ, 152-ФЗ, 187-ФЗ) и международные стандарты (GDPR, PCI DSS, HIPAA); называет регуляторов и понимает последствия несоблюдения требований. формулирует триаду CIA и дополнительные принципы (аутентичность, неотказуемость); объясняет современные подходы (Zero	**Текущий контроль:** Компьютерное тестирование по основным разделам программы. Решение задач по основным разделам программы **Промежуточная аттестация:** дифференцированный зачет

− принципов безопасности информационных систем; − современных методов и технологий в области безопасности информационных систем; − законодательных и нормативных актов в области безопасности информационных систем; − *основные источники информации для оценки угроз (ресурсы CVE, NVD, CERT);* − *лексический минимум для описания инцидентов и средств защиты, социальной инженерии, приемы структурирования информации об угрозах;* − *законодательные акты в области ИБ, структура плана управления рисками;* − *принципы безопасности ИС, современные методы защиты приложений;* − *стандарты безопасности для облаков (CSA, ISO 27017);* − *алгоритмы выполнения работ при расследовании инцидентов;* − *современные методы и технологии в области ИБ;* − *порядок применения протоколов и ПО*	Trust, DevSecOps, EDR, SOAR, Threat Intelligence); называет современные методы защиты приложений (SAST, DAST, RASP). воспроизводит этапы расследования (сбор доказательств → анализ → документирование); объясняет важность порядка действий и цепочки свидетельств. описывает модели IaaS/PaaS/SaaS и разделение ответственности; называет стандарты безопасности для облаков (CSA, ISO 27017). указывает, какое ПО используется для каких задач (OpenSSL, Wireshark, Nmap, Burp Suite, Autopsy); описывает порядок настройки протоколов и критически важные параметры.	