Учебный план
Кибербезопасность

АНО ВО «Институт государственного администрирования»
Центр дополнительного профессионального образования

Программа профессиональной переподготовки

Квалификация: Специалист по безопасности компьютерных систем и сетей.
Продолжительность: 3 месяца. **Объём:** 362 академических часа.
Форма: заочная с применением дистанционных образовательных технологий и электронного обучения.
Требования: среднее профессиональное или высшее образование.
Режим занятий: не более 6 часов в день.

Распределение учебной нагрузки

№	Модуль	Всего, ч	Лекции ч	Практика ч	Самостоятельная работа, ч
1	Основы информационной безопасности	40	4	8	28
2	Нормативно-правовое регулирование в области защиты информации	40	4	8	28
3	Управление информационной безопасностью и оценка рисков	40	4	8	28
4	Криптографические методы защиты информации	40	4	8	28
5	Безопасность сетевой инфраструктуры	40	4	8	28
6	Безопасность веб-приложений и защищённая разработка	40	4	8	28
7	Защита данных: персональные данные, облака и резервирование	40	4	8	28
8	Управление инцидентами информационной безопасности	40	4	8	28
9	Современные технологии в обеспечении информационной безопасности	40	4	8	28
	Всего по модулям	360	36	72	252
	Итоговая аттестация	2	—	—	—
	Общая трудоёмкость	362	36	72	252

По каждому модулю — зачёт методом тестирования. Итоговая аттестация — экзамен методом тестирования (2 часа). Внеаудиторные занятия — 108 часов, включая 36 часов лекций и 72 часа практических занятий. Самостоятельная работа — 252 часа.

Данные приведены по исправленной программе, принятой и утверждённой 26 февраля 2026 года. Подробное содержание и оценочные материалы — в полной программе.

Содержание модулей 1–3

1. Основы информационной безопасности

Модуль формирует понятийный аппарат дисциплины: свойства безопасности информации (конфиденциальность, целостность, доступность), модель угроз и модель нарушителя, классификацию актуальных атак. Слушатели знакомятся с историей отрасли, ключевыми векторами угроз современности и ролями участников рынка ИБ.

Темы: Предмет, цели и задачи информационной безопасности; Модель угроз и модель нарушителя; Актуальный ландшафт киберугроз; Участники отрасли и инфраструктура безопасности.

40 часов: лекции — 4, практические занятия — 8, самостоятельная работа — 28. Контроль — зачёт методом тестирования.

2. Нормативно-правовое регулирование в области защиты информации

Рассматривается российская и международная правовая база: № 149-ФЗ, № 152-ФЗ, № 187-ФЗ, № 98-ФЗ, требования и методические документы ФСТЭК и ФСБ России. Отдельное внимание уделяется обязанностям операторов персональных данных и субъектов критической информационной инфраструктуры.

Темы: Правовая база защиты информации в РФ; Требования ФСТЭК и ФСБ России; Персональные данные: права субъектов и обязанности операторов; Международное регулирование и отраслевые стандарты.

40 часов: лекции — 4, практические занятия — 8, самостоятельная работа — 28. Контроль — зачёт методом тестирования.

3. Управление информационной безопасностью и оценка рисков

Модуль посвящён построению системы менеджмента ИБ по ISO/IEC 27001: разработке политики безопасности, организации процессов СУИБ, проведению внутреннего аудита. Слушатели осваивают методики оценки рисков и учатся обосновывать выбор мер защиты.

Темы: Система менеджмента ИБ по ISO/IEC 27001; Политика безопасности и организационно-распорядительная документация; Оценка и управление рисками ИБ; Внутренний аудит и анализ защищённости.

40 часов: лекции — 4, практические занятия — 8, самостоятельная работа — 28. Контроль — зачёт методом тестирования.

Содержание модулей 4–6

4. Криптографические методы защиты информации

Изучаются основы криптографии: симметричное и асимметричное шифрование, хэширование, электронная подпись, управление ключами и сертификатами. Практическая часть включает применение российских криптостандартов (ГОСТ) и сервисов ЭП в реальных задачах.

Темы: Основы криптографии и симметричное шифрование; Асимметричная криптография и электронная подпись; Хэширование, целостность и аутентификация данных; Управление ключами и инфраструктура открытых ключей.

40 часов: лекции — 4, практические занятия — 8, самостоятельная работа — 28. Контроль — зачёт методом тестирования.

5. Безопасность сетевой инфраструктуры

Разбирается архитектура защищённых сетей: сегментирование, межсетевые экраны, системы обнаружения и предотвращения вторжений (IDS/IPS), VPN-технологии. Слушатели получают навыки администрирования средств сетевой защиты и анализа сетевого трафика.

Темы: Архитектура защищённых сетей и сегментирование; Межсетевое экранирование и контроль трафика; Обнаружение вторжений и анализ сетевого трафика; VPN-технологии и защищённый удалённый доступ.

40 часов: лекции — 4, практические занятия — 8, самостоятельная работа — 28. Контроль — зачёт методом тестирования.

6. Безопасность веб-приложений и защищённая разработка

Модуль охватывает типовые уязвимости веб-приложений (SQL-инъекции, XSS, CSRF) и практики безопасной разработки (SDLC, OWASP Top 10:2025). В ходе практикума слушатели выявляют уязвимости в учебных приложениях и устраняют их средствами защищённого программирования.

Темы: Типовые уязвимости веб-приложений; Методы защищённой разработки ПО; Аутентификация, сессии и управление доступом в веб; Практикум: поиск и устранение уязвимостей.

40 часов: лекции — 4, практические занятия — 8, самостоятельная работа — 28. Контроль — зачёт методом тестирования.

Содержание модулей 7–9

7. Защита данных: персональные данные, облака и резервирование

Рассматриваются управление доступом, шифрование данных в покое и при передаче, построение систем резервного копирования и восстановления. Отдельные темы — обеспечение безопасности облачных сервисов (IaaS, PaaS, SaaS) и требования к обработке персональных данных.

Темы: Управление доступом и разграничение прав; Шифрование данных в покое и при передаче; Резервное копирование и восстановление систем; Безопасность облачных сервисов и ПДн.

40 часов: лекции — 4, практические занятия — 8, самостоятельная работа — 28. Контроль — зачёт методом тестирования.

8. Управление инцидентами информационной безопасности

Модуль формирует навыки выявления, классификации и регистрации инцидентов ИБ, планирования реагирования и восстановления систем после атак. Включает основы цифровой криминалистики, противодействие социальной инженерии и организацию обучения персонала.

Темы: Организация процесса реагирования на инциденты; Инструменты мониторинга и SIEM; Основы цифровой криминалистики; Человеческий фактор и обучение персонала.

40 часов: лекции — 4, практические занятия — 8, самостоятельная работа — 28. Контроль — зачёт методом тестирования.

9. Современные технологии в обеспечении информационной безопасности

Модуль знакомит с перспективными направлениями отрасли: применением искусственного интеллекта и машинного обучения в защите, блокчейн-технологиями и квантовой криптографией. Слушатели оценивают новые технологии с точки зрения рисков и возможностей и осваивают средства автоматизации процессов ИБ.

Темы: Искусственный интеллект и машинное обучение в ИБ; Блокчейн-технологии и безопасность распределённых систем; Квантовая криптография и постквантовые алгоритмы; Автоматизация процессов ИБ и итоговая подготовка проекта.

40 часов: лекции — 4, практические занятия — 8, самостоятельная работа — 28. Контроль — зачёт методом тестирования.

Итоговая аттестация

Экзамен методом тестирования — 2 часа. Общая трудоёмкость программы — 362 часа.