Курсы Академии

54 программы · 310 занятий и модулей · Редакция от 19 ноября 2026 года



Основы кибербезопасности с нуля

Занятий · 9

1. Компьютер, файлы и папки: первые правила безопасности
2. Как работает браузер: интернет и безопасные границы
3. Обновления программ и безопасность: ошибки и уязвимости
4. Пароли и двухфакторная аутентификация: второй шаг входа
5. Резервная копия, версия и проверка восстановления
6. Виртуальная машина: второй компьютер в окне
7. Журнал событий: как замечать события и сохранять историю
8. OSI и TCP/IP: путь запроса от кабеля до HTTP
9. VLAN, транк 802.1Q и проверка TLS



Основы сетей и сетевая безопасность

Занятий · 8

1. Как работает DNS: адреса и путь от браузера к серверу
2. Межсетевой экран: разрешить нужное и проверить запрет
3. Как работает VPN: защищённый путь и права удалённого доступа
4. DNS, SSL/TLS, SNI и CDN: что происходит после ввода адреса
5. Прокси, SOCKS5, V2Ray/Xray и REALITY: собираем путь запроса
6. IDS/IPS: от сетевого события к проверенному выводу
7. Безопасность Wi-Fi: гостевой доступ и похожие названия сетей
8. Маршруты, виртуальные сети и SDN: кто решает, куда идёт пакет



Linux для начинающих: терминал, Bash и безопасность

Занятий · 9

1. Первый рабочий каталог: Linux, файлы и терминал
2. Редактор, копии и доказательство изменения
3. Готовые пакеты, репозитории и проверенное обновление
4. Права доступа Linux: пользователи, группы и свой файл
5. Процессы и службы Linux: systemctl и своя служба
6. Сеть своего Linux и журнал проверяемого события
7. Bash для начинающих: текстовые утилиты и повторяемый разбор
8. Резервная копия, восстановление и границы снимка VM
9. Итог: проверка своей Linux-среды и ретест



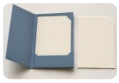
Безопасность Windows для начинающих: администрирование и защита

Занятий · 8

1. Первый файл в Windows: Проводник, загрузки и доступ NTFS
2. От чьего имени работает программа: пользователи, группы и UAC
3. PowerShell с нуля: ограниченная опись и проверяемый CSV
4. Службы Windows и тип запуска: процессы и встроенная защита
5. Сеть Windows: соединение, DNS и встроенная диагностика
6. Журнал событий Windows: поля, фильтр и экспорт
7. Резервная копия и восстановление: вернуть нужную версию текста
8. Итог по Windows: рабочая baseline, ретест и следующий шаг

Курсы Академии

Темы приведены в порядке прохождения.



Безопасность macOS для начинающих

Занятий · 12

1. Первый день: Finder, пути и простой текст
2. Терминал: команда, путь и безопасная ошибка
3. Приложение, окно и процесс в Activity Monitor
4. Пользователь, группы и права собственного файла
5. TCC, SIP и FileVault: три разные границы
6. Gatekeeper и quarantine: источник и подпись приложения
7. Фоновые задачи: plist, launchd и элементы входа
8. Своя сеть: localhost, HTTP и отрицательный контроль
9. Console: событие, фильтр и пределы журнала
10. Резервная копия и восстановление собственного файла
11. Учебная VM: Apple Silicon, Intel и изоляция
12. Итог: проверяемая карта учебного Mac



Основы Active Directory: домен, LDAP, Kerberos и GPO

Занятий · 7

1. Первый стенд AD: две машины и знакомые окна
2. Домен, контроллер и DNS: клиент находит редакцию
3. Каталог как адресная книга: объекты, OU и LDAP
4. Группы и права: Анна читает, Борис получает отказ
5. Kerberos без магии: вход, билет и доступ к службе
6. Group Policy: область, применение и проверка
7. Итоговая практика: базовый аудит домена



Пентест с нуля: методология тестирования на проникновение

Занятий · 8

1. Правила проведения пентеста, scope и план разведки
2. Инфраструктурные гипотезы и цепочка доказательств
3. WEB-гипотезы: объект, действие и доверие
4. Облачные проверки и границы общей ответственности
5. Отчёт, ограничения и независимый ретест
6. Первичный доступ: фишинг, вишинг и учётные данные приложений
7. Wi-Fi и первичный доступ подрядчика: проверка границ
8. Первичный доступ через подрядчика: проверка границ допуска



Веб-пентест: уязвимости веб-приложений по OWASP Top 10

Занятий · 14

1. Burp Suite Community: браузер, Proxy, Repeater и Decoder
2. A02:2025 — поверхность, конфигурация и debug-страницы
3. IDOR и контроль доступа (A01, A07:2025): права, вход и второй фактор
4. SQL-инъекции и другие инъекции (A05:2025): граница данных
5. Браузерные границы: A05 XSS и A01 CSRF/CORS
6. SSRF и XXE (A01, A02:2025): серверные границы
7. HTTP-кэш и согласованность обработки сообщений
8. A03 и A08:2025 — поставка ПО и целостность данных
9. A04:2025 — TLS, пароли, токены и ключи
10. A06:2025 — проектирование и правила бизнес-процесса
11. A09 и A10:2025 — журналы, сигналы и исключения
12. WEB-отчёт: все A01–A10:2025 и проверка исправлений
13. ClickFix: как связать веб-событие с действием на компьютере
14. Новая уязвимость в веб-стеке: от бюллетеня до приёмки исправления

Курсы Академии

Темы приведены в порядке прохождения.



Безопасность API: уязвимости, авторизация, OAuth и JWT

Занятий · 6

1. API-контракт: OpenAPI, типы и границы операции
2. API-авторизация и mass assignment: права на объект и поле
3. OAuth и JWT: полномочия, подпись и контекст токена
4. GraphQL: стоимость, глубина и права resolver
5. Race condition в API: атомарность и идемпотентность
6. Итоговая API-практика: контракт, доверие и состояние



Пентест инфраструктуры и аудит безопасности сети

Занятий · 16

1. Первая сеть: изолированный GOAD и понятный вывод Nmap
2. DNS, SMB и LDAP: превратить порты в понятную карту
3. Аудит учётных записей — политика, состояние и граница доказательства
4. Linux: почему файл открыт, а путь к нему закрыт
5. CVE ядра 2026: применимость, пакет и загруженная версия
6. Windows: токен пользователя, NTFS и общая папка
7. macOS: права файла, разрешение приложения и защита системы
8. Сегментация: проверить разрешённую связь и закрытую границу
9. INFRA-практикум: доказательство, решение владельца и ретест
10. Veeam: как принять восстановление сервиса
11. CrowdStrike Falcon и SentinelOne Singularity Endpoint: границы видимости EDR
12. L2. ARP, петли и контроль VLAN на магистрали
13. L3. Подлинность источника и асимметричная маршрутизация
14. L4. Состояния TCP, перегрузка и границы лимитов
15. Cisco IOS XE и MikroTik RouterOS. Границы управления и применимость обновлений
16. FortiGate и FortiGuard. Применимость PSIRT, охват веб-фильтра и журналы



Аудит безопасности Active Directory: атаки на AD и защита

Занятий · 10

1. GOAD: изолированный домен и доказательства
2. Nmap, NetExec и Impacket: сначала понять вывод
3. BloodHound CE и Certipy: граф и конфигурация
4. LDAP и ACL: подтвердить право на конкретный объект
5. Kerberos: SPN, делегирование и границы вывода
6. NTLM relay: проверить signing, binding и защиту endpoint
7. AD CS: шаблон, CA и подтверждение применимости
8. dMSA и BadSuccessor: применимость, права и патч
9. Certighost 2026: CA trust boundary и итоговый ретест
10. Active Directory: изменение привилегий и приёмка AD CS



OSINT с нуля: разведка по открытым источникам

Занятий · 5

1. OSINT с нуля: поисковые запросы и досье организации
2. Домены, WHOIS и Telegram: проверяем связи через готовые сервисы
3. GEOINT с нуля: EXIF-метаданные фото, обратный поиск и карта
4. Проверка контрагента: Wayback, публикации, суды и доказательный отчёт
5. Публичный мониторинг: Google Alerts, RSS и Telegram без кода

Курсы Академии

Темы приведены в порядке прохождения.



C2: анализ трафика и разработка модели состояний

Занятий · 3

1. Откуда взялся сигнал о C2
2. Модель состояния и независимые подтверждения
3. Контрольная выборка и цена ложного совпадения



Фишинговые шаблоны: разработка безопасных макетов и их статическая проверка

Занятий · 3

1. Контракт инертной карточки и редакторских пометок
2. Диагностика HTMLParser и координаты находки
3. Регрессионные примеры и приёмка макета



Сетевые туннели: разработка анализатора записей сеансов

Занятий · 3

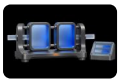
1. Контракт парсера записей потока
2. Сеанс подрядчика и границы допуска
3. Ретест видимости по двум точкам



Сокеты: разработка и тестирование локального протокола

Занятий · 3

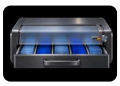
1. Граница записи в потоке байтов
2. Причины отказа и незавершённый хвост
3. Что видит приложение и что видит транзит



ClickFix: разработка модели событий и оценка защиты

Занятий · 3

1. ClickFix и границы наблюдения учебного интерфейса
2. Повторная доставка, порядок и конфликты событий
3. Охват регистратора и решение о выпуске



Инфостилеры: проверка утечек на синтетических данных

Занятий · 3

1. Контракт контрольной метки и граница совпадения
2. Квитанция приёмника и повтор доставки
3. Минимальный отчёт и проверка скрытых полей



SOC-аналитик: SIEM, триаж и расследование инцидентов

Занятий · 5

1. SIEM и корреляции: Sigma, контент-правила
2. Плейбуки и триаж L1/L2
3. Анализ логов, алертов, EDR
4. Эскалация и работа с IR
5. Отчётность, метрики SOC, threat hunting

Курсы Академии

Темы приведены в порядке прохождения.



Реагирование на инциденты информационной безопасности

Занятий · 5

1. Готовность и план IR, роли и SLA
2. Детектирование и триаж, SOC-плейбуки
3. Расследование и containment: Windows, Linux, облако
4. Восстановление, ретроспектива, метрики
5. Коммуникации, отчётность, tabletop



Цифровая криминалистика и форензика

Занятий · 5

1. Сбор и chain of custody, подготовка
2. Форензика дисков и памяти
3. Сетевой анализ и PCAP, TLS и HTTP
4. Логи и артефакты Windows, Linux, Cloud
5. Отчётность и подготовка к суду



Облачная безопасность: Yandex Cloud, AWS, Azure и Kubernetes

Занятий · 5

1. Разделённая ответственность и безопасные архитектуры
2. IAM и сети: AWS, Azure, сетевые контроли
3. Журналирование: CloudTrail, Defender, SIEM-интеграции
4. KMS, секреты, политика доступа
5. CI/CD и контейнеры: EKS и AKS hardening



Безопасная разработка и AppSec: безопасность веб-приложений

Занятий · 5

1. SDL и безопасность дизайна
2. OWASP Top 10 и ASVS: SSRF, IDOR, десериализация, auth
3. SAST, DAST, SCA в пайплайне
4. Код-ревью и архитектурные паттерны
5. Практика фикса и ретесты



DevSecOps: безопасность CI/CD и цепочки поставки

Занятий · 5

1. CI/CD: доверие к job, гейт и происхождение артефакта
2. Kubernetes: возможности Pod, admission и проверяемое правило OPA
3. Секреты и HashiCorp Vault: идентичность workload, lease и отзыв
4. SBOM и SCA: связать компонент, сборку и решение
5. IaC и Terraform: проверить plan, неизвестные значения и состояние

Курсы Академии

Темы приведены в порядке прохождения.



Безопасность ИИ и нейросетей: защита LLM-приложений

Занятий · 5

1. Данные ИИ: цель, происхождение, копии и приватность
2. Prompt injection, память агента и границы инструментов
3. RAG: отфильтровать права до контекста и не смешать кеш
4. Поставка ML/LLM: данные, код модели и проверенный артефакт
5. LLM-наблюдение: качество, нарушения прав и управляемый инцидент



Защита персональных данных по 152-ФЗ: основы и практика

Занятий · 5

1. 152-ФЗ с нуля: персональные данные, цель обработки и согласие
2. Уведомление Роскомнадзора, документы оператора и запросы субъекта
3. Уровни защищённости ИСПДн: роли, угрозы и меры по приказу ФСТЭК № 21
4. Категорирование КИИ, ГИС и ИСПДн: применимость без угадывания
5. Утечка персональных данных: 24/72 часа, инцидент и итоговый privacy-проект

Прикладные программы

Темы приведены в порядке прохождения.



Основы кибербезопасности

Занятий · 5

1. Что потеряет предприятие при инциденте
2. Каким системам действительно нужна связь
3. Очередь исправлений для небольшой команды
4. Жизненный цикл доступа и восстановление учётной записи
5. От записей журнала к решению дежурного



Этичный хакинг (Pentest)

Занятий · 5

1. Границы проверки и качество исходных сведений
2. Рецензия прав в каталоге учётных записей
3. Проверяемые требования к веб-приложению
4. Облачная часть аудита по выгрузкам владельца
5. Закрытие работ и приёмка исправлений



Управление инцидентами (IR)

Занятий · 5

1. План реагирования для критичного сервиса
2. Триаж сигнала и первичная карточка расследования
3. Временная шкала и выбор меры локализации
4. Возврат сервиса и измерение результата
5. Штабное учение и разбор решений



Безопасность в облаках

Занятий · 5

1. Облако и границы ответственности
2. Доступ к облачной операции из разрешённого сегмента
3. Какие действия видны в облачных журналах
4. Ключи шифрования и секреты приложения
5. Решение о выпуске контейнера в облако



OSINT и расследования

Занятий · 5

1. Проверяемый вопрос и досье источников
2. Официальный профиль, домен и представительство
3. Фотография площадки и след расчёта
4. Граф деловых связей и проверка альтернатив
5. Воспроизводимая сверка и выдача заключения



Цифровая криминалистика

Занятий · 5

1. Приём материалов и цепочка хранения
2. Сопоставление образа диска и снимка памяти
3. Что доказывает фрагмент сетевой записи
4. Единая шкала Windows, Linux и облачного журнала
5. Воспроизводимое техническое заключение

Прикладные программы

Темы приведены в порядке прохождения.



Secure Coding / AppSec

Занятий · 5

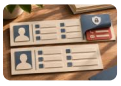
1. SDL: проектирование сервиса согласования
2. OWASP Top 10 и ASVS: требования на границах приложения
3. SAST, DAST и SCA: разбор отчётов сборки
4. Код-ревью: полномочия и безопасное хранение результата
5. Исправление и повторная проверка перед релизом



DevSecOps и автоматизация

Занятий · 5

1. CI/CD: от исходного изменения до артефакта
2. Контейнеры и Kubernetes: минимальные права, проверяемые политики
3. Vault и Secrets Manager: жизненный цикл машинного доступа
4. SBOM, SCA и оповещения по реально поставленным версиям
5. Terraform: изменение инфраструктуры и политика как код



AI Security и защита моделей

Занятий · 5

1. Источники данных и приватность в ML
2. Риски для модели: недоверенные указания, извлечение модели и изменение выборки
3. RAG: разграничение доступа и доверие к документам
4. Кто может выпустить модель: доступ и целостность пайплайна
5. Инциденты ИИ-сервиса: наблюдение, разбор и восстановление



SOC-аналитик (L1/L2)

Занятий · 5

1. SIEM и Sigma: от события к обоснованному сигналу
2. Триаж первой и второй линии
3. Журналы, EDR и временная линия события
4. Эскалация в IR и передача смены
5. Отчёт смены, метрики SOC и проверка гипотез



MLOps и продакшн ML

Занятий · 5

1. Данные, признаки и реестр моделей
2. Проверки данных и критерии допуска модели
3. Выпуск в эксплуатацию: batch, online, shadow и canary
4. Наблюдение за дрейфом и отложенным качеством
5. Инцидент в ML: SLO, резервный прогноз и переобучение

Прикладные программы

Темы приведены в порядке прохождения.



Разработка ИИ/LLM-продуктов

Занятий · 5

1. Архитектура помощника: задача, источники, интеграции
2. Промпт-дизайн и оценка качества на размеченном наборе
3. RAG: подбор фрагментов, качество поиска и кэш
4. Безопасность LLM-продукта: права и действия помощника
5. Экономика, задержка и решение о пилоте



Автоматизация работы СБ и SOC с ИИ-агентами

Занятий · 5

1. Поручение агенту и границы доступа
2. Как извлечь факт и сохранить ссылку на документ
3. Очередь инструментов и повторная доставка
4. Что согласует человек и какие данные получит модель
5. Приёмка пилота, стоимость ошибки и остановка

Продвинутые направления

Темы приведены в порядке прохождения.



Aegis для аналитика и руководителя смены

Занятий · 5

1. Кто и в каком контуре ведёт дело
2. Connect и CA: происхождение сигнала и пробелы сбора
3. От актива и версии пакета к решению по CVE
4. AEV: что означает пустой граф и наблюдение защиты
5. Сдача смены и приёмка полного комплекта



Веб-разработка: контракты, границы данных и выпуск

Занятий · 5

1. Контракт операции и совместимость клиентов
2. Авторизация объекта от HTTP до хранилища
3. Повтор запроса, конкуренция и побочный эффект
4. Персональная страница, кеш и журнал
5. Выпуск с миграцией и остановкой раскатки



Аудит веб-приложений: от задания до ретеста

Занятий · 6

1. Задание, границы и правила остановки
2. От требования к доказательству дефекта
3. NGINX2Root: приоритет узла и подтверждение обновления
4. Nodejs2Shell: где декодируются внешние данные
5. ClickFix: решение смены по браузеру и конечной точке
6. Отчёт, остаточный риск и приёмка ретеста



Инфраструктура: защита резервных копий, AD и рабочих станций

Занятий · 4

1. Какие серверы затронуты бюллетенем Veeam
2. Восстановление приложения из доверенной копии
3. PetitPotam и приёмка защиты выдачи сертификатов
4. Возврат станции с Falcon и антивирусом в работу



Сетевые расследования: туннели и удалённый доступ

Занятий · 4

1. Прокси V2Ray и границы согласованного подключения
2. Reverse SOCKS и Chisel в журналах двух систем
3. Neo-reGeorg и гипотеза о веб-оболочке
4. Локализация и возврат удалённого доступа



Радиосети и социальная инженерия: расследование обращения

Занятий · 4

1. Собственные точки Wi-Fi и границы обследования
2. Фишинг в почте и первичное обращение
3. Вишинг и происхождение номера обратной связи
4. Подтверждение изменений платёжной операции



SOC в России: гипотезы и проверка телеметрии

Занятий · 4

1. Нормализация в KUMA и сверка с источником
2. MaxPatrol SIEM и контекст актива во времени
3. R-Vision SIEM и проверка переносимости правила
4. Восстановление наблюдаемости после сбоя

Продвинутые направления

Темы приведены в порядке прохождения.



Прикладная криптография и управление ключами

Занятий · 4

1. AEAD и уникальность nonce при повторной обработке
2. Конвертное шифрование и вывод версии KEK
3. Проверка подписи и доказательства времени
4. Учебное восстановление архива и разделение ролей



Инженерия ИИ-систем, OpenCode и системные инструкции

Занятий · 4

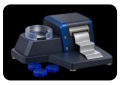
1. Системная инструкция и договорённости репозитория
2. Разрешения инструментов OpenCode и граница процесса
3. Контекст ответа и полномочия поиска
4. Повторные испытания агента и решение о выпуске



MLOps и DevOps: проверка и выпуск автоматизаций

Занятий · 4

1. Временная граница признаков и проверочная выборка
2. Происхождение сборки и контракт модели
3. Пробный выпуск и сопоставимые метрики
4. Откат автоматизации и проверка побочных действий



Red Team: разработка инструментов проверки защиты

Занятий · 4

1. Генератор синтетических журналов
2. Парсер и очистка записей перед передачей
3. Испытание детектора на границе окна
4. Воспроизводимая сборка и приёмка выпуска

Программы для сотрудников

Темы приведены в порядке прохождения.



Базовая для всех сотрудников

Занятий · 4

1. Какие данные и действия требуют защиты
2. Пароль, второй фактор и восстановление
3. Письмо с просьбой изменить платёж
4. Рабочее место и первое сообщение об инциденте



Продвинутая для ИТ

Занятий · 16

1. Требование безопасности в задаче разработки
2. Ревью изменений и защитные тесты
3. Зависимости и состав поставки
4. Секреты и журнал приложения
5. Учёт систем и владельцев
6. Права администраторов
7. Безопасное изменение конфигурации
8. Резервные копии и восстановление
9. Первичная оценка сообщения об инциденте
10. Хронология и часовые пояса
11. Сохранность цифрового материала
12. От восстановления к улучшениям
13. Что подтверждает сертификат
14. Жизненный цикл ключа
15. Продление и отзыв сертификатов
16. Приёмка технических контролей



Для руководителей

Занятий · 3

1. Риск, бизнес-цель и решение владельца
2. Данные, применимые требования и показатели
3. Бюджет и управленческая записка



OSINT/GeoINT интенсив

Занятий · 4

1. Проверяемый вопрос и план источников
2. Переход между организациями и документами
3. Сверка площадки по карте и снимку
4. Отчёт и проверка альтернативной версии