

Старт в информационной безопасности в 2026 году

Как выбрать направление, оценить свои навыки и
построить первую карьерную траекторию на
сложном рынке

📅 22 октября

📅 четверг

🕒 19:00 МСК

📺 открытый эфир

РОЗЫГРЫШ

Поделись вопросом о
поиске работы в ИБ
и получи приз

Поделимся результатами
после эфира

t.me/cyberedrussia/2254



CyberED





Андрей Шабалин

Инструктор Академии Eltex и Астра Университета · кандидат наук

должность

Доцент кафедры информационной безопасности
Тюменского государственного университета

опыт

Инструктор Академии Eltex и Астра Университета с 2022 года, до этого тренер и инструктор академий Cisco и Huawei в 2011–2022 годах

экспертиза

Компьютерные сети и сетевая безопасность



Сообщество «Компьютерные сети и сетевая
безопасность»

vk.com/utmn_network

Кто вы и зачем пришли на вебинар?

1

Начинаю знакомиться с ИБ и хочу понять, подходит ли мне эта сфера.

2

Уже изучаю ИБ, но пока не могу выбрать специализацию.

3

Работаю в IT и рассматриваю переход в информационную безопасность.

4

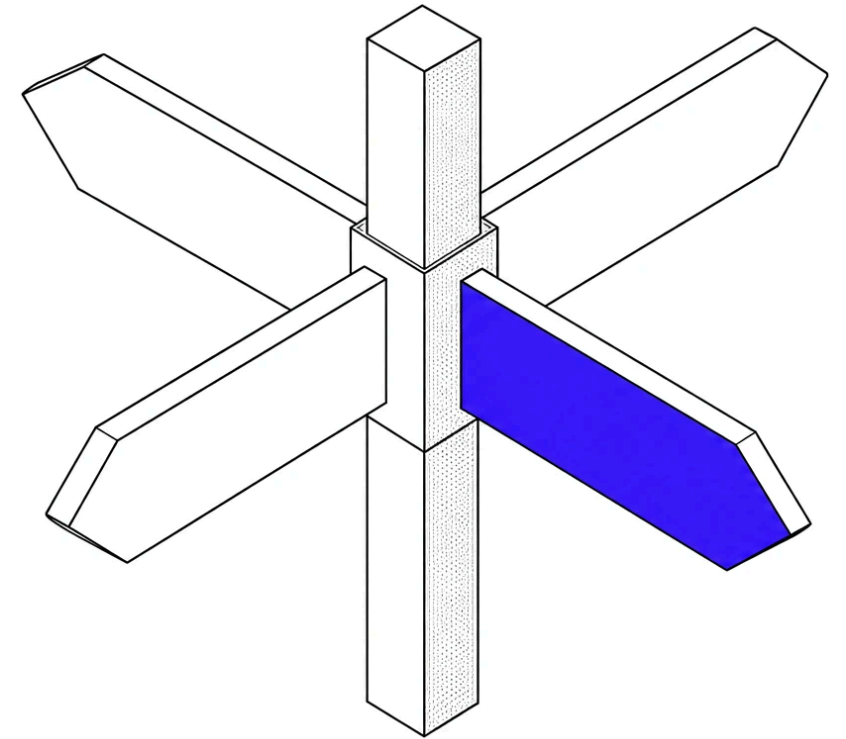
Хочу оценить навыки, найти пробелы и составить план развития.



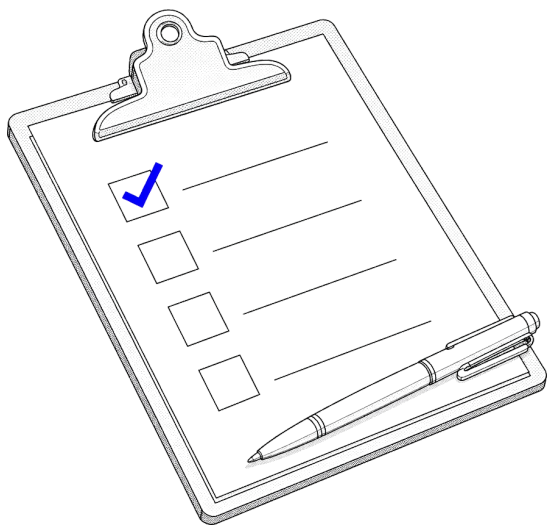
Напишите номер в чат.
Можно выбрать несколько вариантов.

О чём вебинар

- 01 Как изменился вход в информационную безопасность в 2026 году
- 02 Какие профессиональные направления и стартовые роли существуют
- 03 Как один инцидент выглядит глазами разных специалистов
- 04 Какие знания составляют общий фундамент в ИБ
- 05 Как оценить свою стартовую базу и учесть предыдущий опыт
- 06 Как выбрать направление и составить план следующих шагов



Что будет у вас к концу вебинара

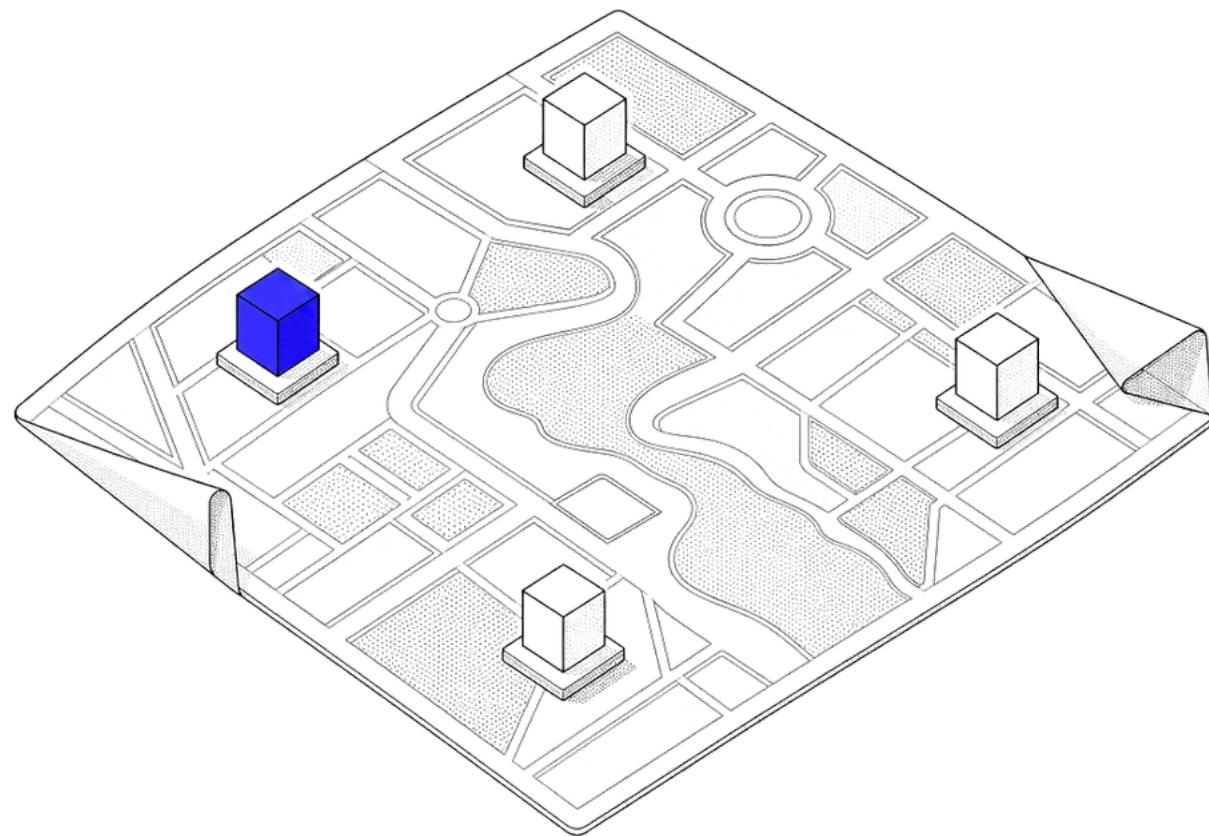


- ✓ Увидите работу в ИБ изнутри на примере одного инцидента
- ✓ Познакомитесь с разными типами профессиональных задач
- ✓ Оцените свой интерес к четырём направлениям
- ✓ Выберите основное и запасное направление
- ✓ Поймёте, какие навыки у вас уже есть
- ✓ Определите, что стоит изучать в первую очередь
- ✓ Получите доступ к открытой диагностике CyberED

Карта ролей в информационной безопасности



cybersecurity-roadmap.ru



В ИБ нужны люди. Почему тогда новичку сложно войти?

+24%

Столько прибавили вакансии в информационной безопасности год к году к концу марта 2026 года.

-18%

Настолько сократилось количество вакансий в IT в целом за тот же период.

80%

компаний испытывают потребность в специалистах по ИБ.

11%

компаний смогли полностью укомплектовать штат ИБ.

Что происходит на старте

Компании остро нуждаются в опытных и узкопрофильных специалистах. Среди начинающих ситуация обратная: кандидатов много, а стажёрских и младших позиций заметно меньше.

Что изменилось для начинающего специалиста

- 01 **Массового набора начинающих почти нет:** компании открывают точечные стажировки и младшие позиции под конкретные задачи.
- 02 **Стажировка или опыт в смежной IT-роли** обычно весит больше, чем ещё один сертификат.
- 03 **На первых этапах чаще появляются тестовые задания,** лабораторные задачи и разборы кейсов.
- 04 **Опыт системного администрирования, поддержки, сетей, разработки или тестирования** сокращает дистанцию до первой роли в ИБ.
- 05 **Домашняя лаборатория, CTF и учебный проект работают,** если кандидат может объяснить, что именно он делал.
- 06 **Рынок узкий:** профессиональные сообщества, конференции, стажировки и рекомендации часто дают больше, чем поток одинаковых откликов.
- 07 **Вакансию нужно читать через задачи.** Одно объявление может объединять мониторинг, настройку средств защиты, реагирование и документацию.

Как ИИ изменил требования к специалистам

Где ИИ уже помогает



Собрать и структурировать информацию

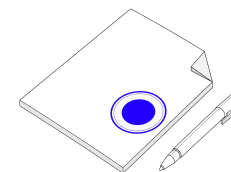
Ускорить первичный анализ

Подготовить черновик скрипта

Объяснить незнакомую технологию

Автоматизировать повторяющиеся операции

Что остаётся на специалисте



Проверить команды и выводы модели

Учесть контекст конкретной инфраструктуры

Заметить пропущенные риски

Выбрать безопасное действие

Объяснить решение команде

Отвечать за последствия

★ **ТОП-НАВЫК 2026 ГОДА**

Использовать ИИ и понимать, где ему нельзя доверять

// профессия · старт 28 октября

AI-native инженер по ИБ с нуля за 6 месяцев

306 ак. часов

11 воркшопов
с преподавателем

12 проектов
в портфолио

⚙️ Обучение ИИ — интенсивы на 270 900 ₽ уже включены

Карьерный трек

👤 Семь своих агентов за программу



Воркшопы с СТО Антоном Кузьминым

Задачи от компаний: поднять инфраструктуру после атаки

📄 Цифровое резюме

➡️ ИБ 360: атака и защита



Тренировочное интервью с HR-партнёром

Закрытые воркшопы по AI



Диплом за 6 месяцев

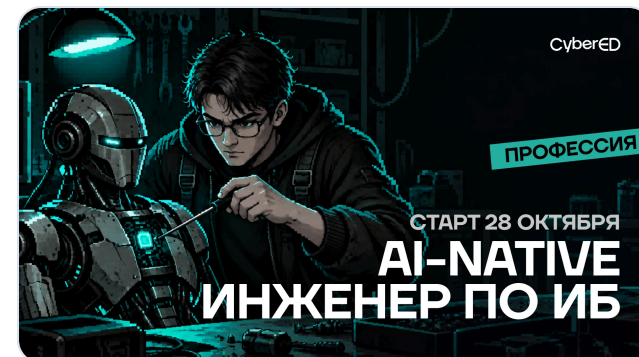
Закрыл программу — выходишь на стажировку

SINGLETON
SECURITY

ANGARA SECURITY

★ Старая цена для тех, кто сейчас в эфире

143 900 ₽ ~~153 900 ₽~~



Перейди и получи программу

new.cyber-ed.ru/inzhener-ib

От карты профессий — к реальной задаче

1

Познакомьтесь с компанией
и её инфраструктурой

2

Увидите первые сигналы

3

Выберете действие

4

Проследите за развитием
событий

5

Разберёте работу четырёх
специалистов

6

Заполните чек-лист

Как работать с чек-листом

Интерес к задачам

- 0 Такой тип задач мне неинтересен
- 1 Некоторые задачи показались интересными
- 2 Мне хочется заниматься такими задачами

Текущая база

- 0 Пока не знаком с необходимыми технологиями и задачами
- 1 Есть отдельные знания или смежный опыт
- 2 Уже есть заметная часть необходимой базы

Желание попробовать

- 0 Не хочу проверять это направление
- 1 Готов выполнить небольшую пробную задачу
- 2 Хочу сделать практический проект в этом направлении

Дополнительно
запишите



Что в работе вас заинтересовало



Какой полезный навык у вас уже есть



Чего пока не хватает

Компания «Север»

- > 250 сотрудников
- > Офисная и удалённая работа
- > Собственная IT-инфраструктура
- > Внутренние сервисы
- > Команда разработки
- > Небольшой отдел информационной безопасности

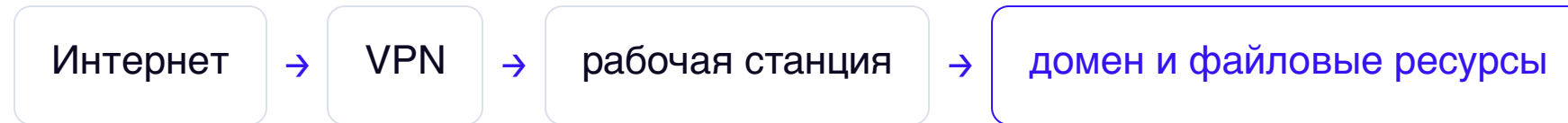
Вечер буднего дня

Средства защиты фиксируют несколько подозрительных событий. Они приходят из разных систем и пока выглядят несвязанными.



Как устроена инфраструктура

Путь пользователя



Контур разработки



Что ещё есть в системе

- > Учётные записи сотрудников
- > Секреты приложений
- > Сервисные учётные записи
- > EDR на рабочих станциях
- > Права доступа
- > Журналы VPN, домена, GitLab и API

Первые сигналы

18:47 Вход через VPN из нетипичной для сотрудника локации.

18:53 EDR фиксирует подозрительный процесс на его рабочей станции.



Дополнительный риск

Для группы пользователя не включена обязательная MFA.



Текущий статус

Сессия активна. Других подтверждённых данных пока нет.



Достаточно ли этого, чтобы объявить инцидент?

Ваше первое решение

- 1 Заблокируете учётную запись
- 2 Изолируете рабочую станцию
- 3 Соберёте и сопоставите события
- 4 Смените связанные сервисные секреты
- 5 Попытайтесь воспроизвести действия пользователя



Напишите номер в чат.

При выборе учитывайте



Насколько
достоверны текущие
данные



Продолжается ли
подозрительная
активность



Какой ущерб может
возникнуть



Что произойдёт с
рабочими системами
после вашего
действия

Появляются новые события

- 19:02 Обращение к служебной папке, которой сотрудник обычно не пользуется.
- 19:08 Чтение конфигурации проекта в GitLab.
- 19:14 Нетипичные запросы к внутреннему API от имени сервисной учётной записи.
- 19:20 Оповещения из разных систем поступают нескольким сотрудникам ИБ.

Рабочая версия

Доступ сотрудника могли скомпрометировать. Из конфигурации проекта могли получить сервисный секрет и использовать его для запросов к API.

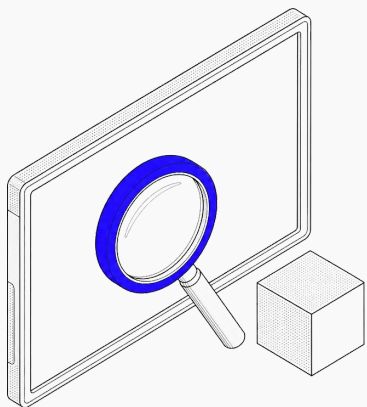
Нужно подтвердить

- > Кто выполнил вход
- > Какие ресурсы были затронуты
- > Какие данные могли быть доступны
- > Продолжается ли активность

Анализ событий и реагирование

главный вопрос

Что произошло и насколько
это опасно?



что делает специалист

- 01 Собирает события из VPN, EDR, GitLab и API
- 02 Связывает их по времени, пользователю и устройству
- 03 Отделяет подтверждённые факты от рабочих версий
- 04 Определяет затронутые системы
- 05 Оценивает критичность
- 06 Передаёт команде данные для локализации

что нужно на старте

Основы Windows и Linux

Сети и сетевые протоколы

Чтение журналов событий

Базовая работа с SIEM и EDR

Умение проверять гипотезы

Аккуратная фиксация результатов

Инженерная защита

главный вопрос

Как остановить атаку и
сохранить
работоспособность систем?

что делает специалист

- 01 Изолирует рабочую станцию
- 02 Ограничивает доступ учётной записи
- 03 Отзывает активные сессии
- 04 Организует замену сервисного секрета
- 05 Проверяет права доступа
- 06 Включает MFA
- 07 Добавляет правила обнаружения и контроля

что нужно на старте

Администрирование Windows и Linux

Сети и сетевые сервисы

Учётные записи и права доступа

VPN, MFA и механизмы аутентификации

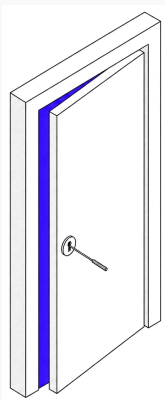
Настройка средств защиты

Базовая автоматизация

Анализ защищённости

главный вопрос

Можно ли повторить этот
путь атаки в контролируемых
условиях?



что делает специалист

- 01 Формулирует сценарий проникновения
- 02 Проверяет настройки VPN и MFA
- 03 Оценивает доступность служебных ресурсов
- 04 Проверяет возможность получить секрет
- 05 Подтверждает потенциальный ущерб
- 06 Описывает найденные проблемы
- 07 Проводит повторную проверку после исправлений

что нужно на старте

Сети и сетевые сервисы

Windows и Linux

Веб-технологии и API

Типовые классы уязвимостей

Инструменты анализа защищённости

Базовое программирование

Технические отчёты

Безопасность приложений

главный вопрос

Как секрет попал в конфигурацию и почему процесс разработки это пропустил?

что делает специалист

- 01 **Выясняет источник секрета**
- 02 **Организует его замену**
- 03 **Настраивает безопасное хранение**
- 04 **Проверяет доступы к проекту**
- 05 **Добавляет проверки в CI/CD**
- 06 **Пересматривает модель угроз**
- 07 **Помогает команде изменить процесс разработки**

что нужно на старте

Жизненный цикл разработки ПО

Архитектура веб-приложений и API

Чтение кода

Типовые уязвимости приложений

Управление секретами и зависимостями

Основы CI/CD

Что объединяет **разные роли**

Техническая база

- > Компьютерные сети
- > Windows и Linux
- > Устройство IT-инфраструктуры
- > Аутентификация
- > Учётные записи и права доступа

Работа с данными

- > Журналы событий
- > Источники телеметрии
- > Поиск связей
- > Проверка рабочих версий

Инженерные привычки

- > Базовая автоматизация
- > Чтение документации
- > Фиксация изменений
- > Понятная передача результатов команде

«У меня нет опыта» — так ли это?



Системное администрирование

Сети

Операционные системы

Доступы

Резервное копирование

Устранение сбоев



Техническая поддержка

Диагностика

Работа с пользователями

Анализ обращений

Соблюдение инструкций



Разработка и тестирование

Код

Приложения

API

Воспроизведение ошибок

Работа с Git и CI/CD



Аналитика и аудит

Требования

Риски

Данные

Отчёты

Интервью с владельцами процессов



Самостоятельная практика

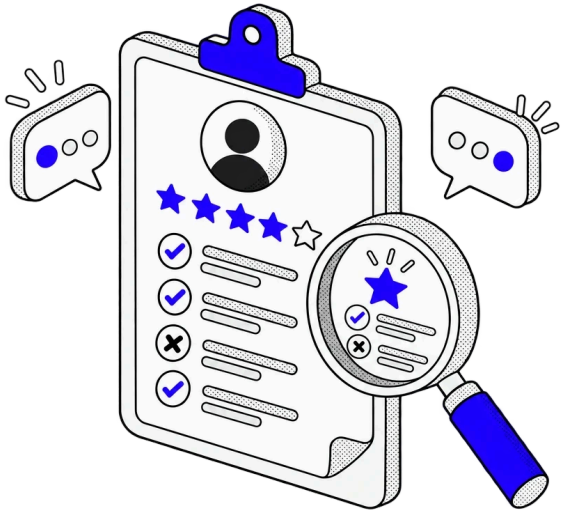
Домашние лаборатории

CTF

Скрипты

Технические разборы и учебные проекты

Чем подтвердить навыки до первой работы



Стажировку



Опыт в смежной IT-роли



Домашнюю лабораторию



Законченный учебный проект



CTF или практический тренажёр



Разбор учебного инцидента



Скрипт или автоматизацию

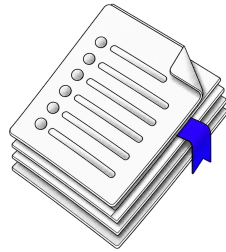


Технический отчёт

Открытая диагностика CyberED

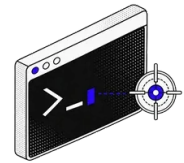
Чек-лист

Показывает ваш интерес к задачам, самооценку текущей базы и желание попробовать направление.



Диагностика

Проверяет технические знания, понимание инфраструктуры и подход к решению задач.



После прохождения сравните

01

Результаты по
разделам

02

Оценки в чек-листе

03

Навыки из
предыдущего опыта

04

Темы, которые вызвали
сложности

Ассессмент CyberED

Полная диагностика доступна после
вебинара



portal.cyber-ed.ru



Что мешает пройти путь обучения **самостоятельно**

01 Сети, операционные системы, доступы и средства защиты изучаются отдельными кусками.

03 Теория не закрепляется на инфраструктуре и лабораторных задачах.

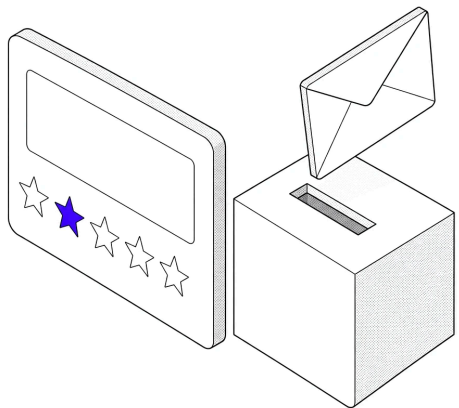
05 Сложно подобрать проект, который соответствует реальным задачам специалиста.

07 Прогресс оценивается по просмотренным материалам, а не по выполненным задачам.

02 Непонятно, какие темы нужны для старта, а какие пока можно отложить.

04 Ошибочное решение некому разобрать.

06 Без контрольных точек обучение легко растягивается на месяцы.



Оцените мероприятие

Анонимная анкета

8 вопросов

2 минуты

Ваши ответы помогают нам делать встречи качественнее.



new.cyber-ed.ru/events/feedback