

CyberED

СПЕЦИАЛИСТ

ПО БЕЗОПАСНОЙ  
РАЗРАБОТКЕ  
ПРИЛОЖЕНИЙ



# О ЧЁМ ПОГОВОРИМ НА ЭФИРЕ?

- 01 Знакомство
- 02 Какое место занимают DevSecOps/AppSec на рынке ИБ?
- 03 Суть работы, ключевые навыки и траектория развития специалистов
- 04 Требования работодателей и рынка
- 05 Как устроена программа и почему именно так
- 06 Почему именно CyberED?
- 07 Как мы обучаем безопасной разработке: разбор на кейсах



[ О СПИКЕРЕ ]

# ИВАН АФАНАСЬЕВ



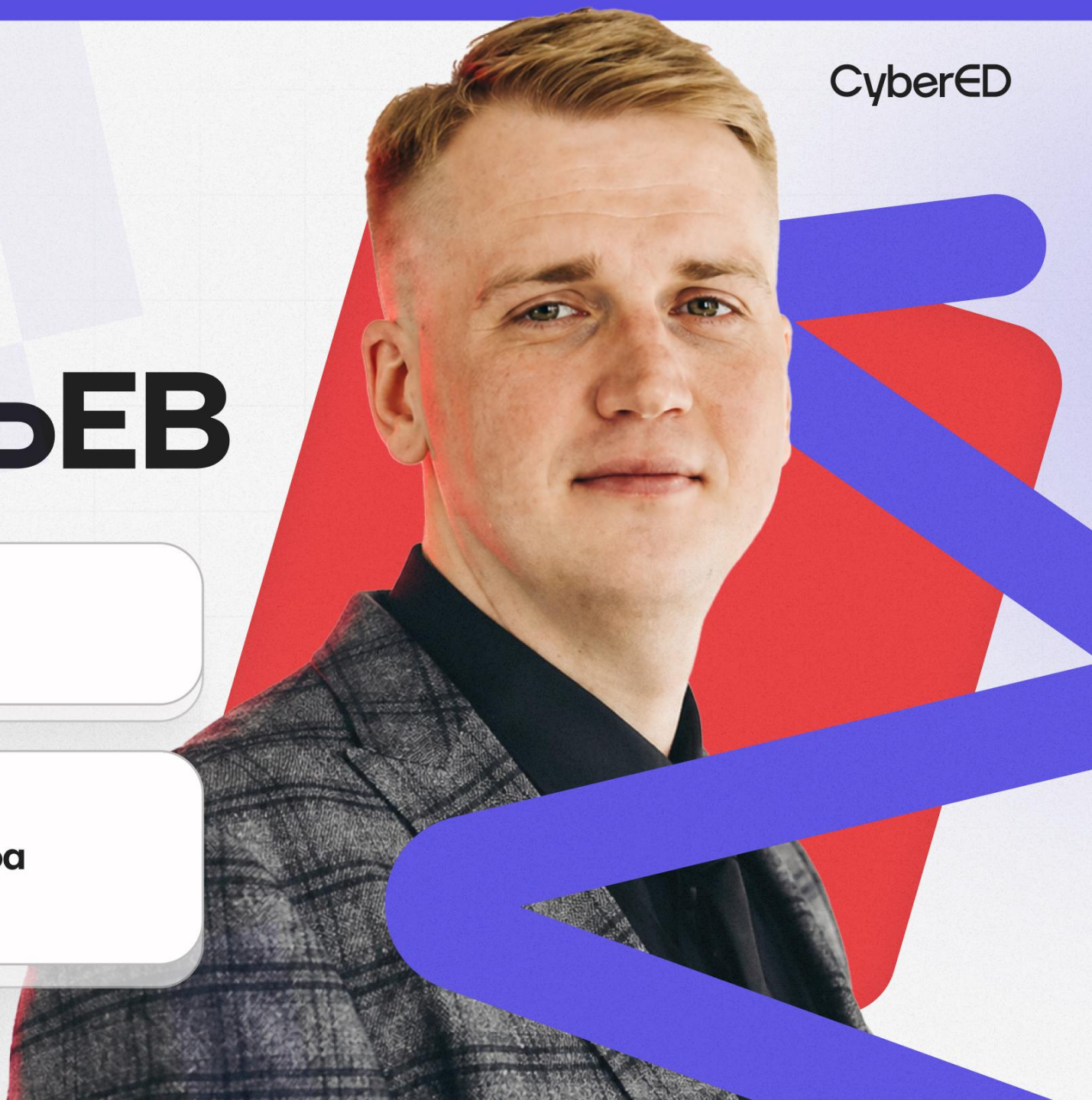
Текущая должность и место работы:

**AppSec Lead в Лесте**



Опыт работы:

**Самокат, AliExpress, bi.zone, Альфа банк, positive technologies**



# ДАВАЙТЕ ПОЗНАКОМИМСЯ

А)

ОТМЕТЬТЕ, КТО ВЫ  
И ОТКУДА ПРИШЛИ:

- 01 Новичок: без ИТ / ИБ бэкграунда
- 02 Новичок с ИТ-бэкграундом
- 03 Работаю в ИТ
- 04 Работаю в ИБ

Б)

КАКИЕ У ВАС ЦЕЛИ  
НА ВСТРЕЧУ?



# КАРТА НАПРАВЛЕНИЙ

## [ В КИБЕРБЕЗОПАСНОСТИ ]



### BLUE TEAM

Защита систем от атак, мониторинг и реагирование на инциденты.

■ Тип мышления:  
аналитический, с фокусом на расследование.

■ Верхние роли:

Аналитик SOC

Incident Responder / DFIR

Аналитик киберугроз

Аналитик BPO

### INFRA SEC

Обеспечение безопасности IT-инфраструктуры, включая сети, серверы и операционные системы.

■ Тип мышления:  
технический, системный.

■ Верхние роли:

Инженер по безопасности инфраструктуры

Сетевой инженер безопасности



Кибербезопасность —  
это не набор направлений.

Это цикл защиты, в котором у каждой роли есть своё место и своя функция. Вам важно понять, какие проблемы/боли вам интереснее решать.

### APP SEC

Безопасная разработка и тестирование приложений.

■ Тип мышления:  
креативный и технический, с акцентом на анализ кода.

■ Верхние роли:

AppSec-инженер

Специалист по анализу кода

Аналитик по безопасности приложений

DevSecOps

### RED TEAM

Имитация кибератак для тестирования систем на проникновение и оценки уязвимостей.

■ Тип мышления:  
творческий, наступательный.

■ Верхние роли:

Внешний пентест

Red Teaming

Внутренний пентест

Исследование уязвимостей

### GRC / ARCH

Проектирование архитектуры безопасности, управление рисками и обеспечение соответствия нормам.

■ Тип мышления:  
стратегический, управленческий.

■ Верхние роли:

Управление рисками

Архитектор безопасности

Безопасность поставщиков

Аудитор

[ СПЕЦИАЛИСТ ]

# ПО БЕЗОПАСНОЙ РАЗРАБОТКЕ ПРИЛОЖЕНИЙ



# ВОСТРЕБОВАННОСТЬ НА РЫНКЕ ИБ

- Доля вакансий DevSecOps/AppSec:  
**~4.8% всех ИБ-вакансий**
- Доля кандидатов:  
**~1.5%**
- Соотношение (критический дефицит)  
**≈ 1 кандидат на 3 вакансии**



В целом специалистов безопасной разработки требуется в 3 раза больше, чем есть на рынке



в инженерию → **DevSecOps**  
в глубину → **Product Security**  
в атаки → **Offensive**  
в управление → **Governance**

# DevSecOps / SECURITY ENGINEERING

— САМЫЙ ВОСТРЕБОВАННЫЙ ТРЕК ▲



**DevSecOps / Security Engineering**  
(самый востребованный трек)



**Суть:**  
встраивание безопасности в CI/CD и разработку

**Чем занимаешься:**

- ▶ внедрение SAST/DAST/SCA
- ▶ security gates в пайплайнах
- ▶ threat modeling
- ▶ работа с IaC и контейнерами

**Стек:**

- ▶ CI/CD (GitLab CI, Jenkins)
- ▶ SAST (Checkmarx, SonarQube)
- ▶ контейнеры (Docker, Kubernetes)
- ▶ облака

# ТРЕБОВАНИЯ [АНАЛИЗ ВАКАНСИЙ] РАБОТОДАТЕЛЕЙ



## Чем предстоит заниматься:

- ✓ Оценка архитектурных и бизнес-решений на ранних этапах разработки для выявления и предотвращения рисков информационной безопасности.
- ✓ Обеспечение безопасности на ранних этапах разработки в рамках Secure SDLC (SAST, SCA):
- ✓ проведение триажа уязвимостей, включая консультирование команд разработки по устранению уязвимостей и/или минимизации рисков;
- ✓ сопровождение выявленных уязвимостей от регистрации до закрытия: включая ревью предложенных исправлений и подтверждение их принятия в основную ветку разработки;
- ✓ проведение исследований и оценка новых инструментов безопасности при необходимости их внедрения.
- ✓ Внедрение, улучшение и сопровождение практик AppSec в процессах проектирования разработки, а также продвижение принципа «Security by design».
- ✓ Участие в реагировании на инциденты.



## От успешного кандидата мы ожидаем:

- ✓ Опыт работы в качестве специалиста по безопасности приложений (AppSec) от 3 лет.
- ✓ Умение писать и читать код на популярных языках (Java, Kotlin, Python, JS, Go) — для анализа уязвимостей, автоматизации и совместной работы с разработчиками.
- ✓ Знание архитектуры веб- и мобильных приложений с фокусом на типичные векторы атак и защитные механизмы.
- ✓ Опыт работы с инструментами автоматизированного анализа безопасности:
- ✓ SAST: Sspace\ Semgrep\CodeQL;
- ✓ Secret Scanning (сканирование на наличие секретов в коде): TruffleHog;
- ✓ OSA\SCA (анализ уязвимостей в зависимостях): Codescoring;
- ✓ ASOC (управление результатами сканирования): DefectDojo.
- ✓ Опыт работы с инструментальным стеком разработки: Jira, Gitlab, Harbor, Nexus, Rancher, Kubernetes, Vault, FreeIPA, Keycloak.
- ✓ Опыт работы с системами автоматической сборки: Maven, Gradle, Sbt, Bazel.
- ✓ Знание ключевых рисков безопасности веб-приложений (OWASP Top 10, CWE Top 25) и практик безопасной разработки (Secure SDLC, threat modeling, defense in depth).

## Чем предстоит заниматься:

- Участвовать в проработке задач на всех этапах жизненного цикла проекта от предпроектных исследований, до внедрения и контроля выполнения необходимых задач после внедрения
- Проводить анализ архитектуры решений на **безопасность** и участвовать в согласовании проектной документации (Включая организационно-распорядительную, архитектурную и техническую документацию)
- Моделировать сценарии угроз и участвовать в согласовании новых и пересмотре существующих рисков
- Анализировать планы и бэклог команд разработки, предъявлять требования и рекомендации к новым фичам
- Участвовать в расследованиях при выявлении инцидентов ИБ
- Оказывать экспертную поддержку командам разработки по вопросам ИБ, практикам написания **безопасного** кода, построения архитектуры ИС и выполнения требований **безопасности**
- Проводить Code Review по результатам автоматизированного и ручного анализа для выявления и устранения уязвимостей
- Проводить работу с результатами сканирования инструментов **безопасной** разработки для выявления и устранения уязвимостей
- Приоритизировать бэклог уязвимостей и контролировать их исправление

- Высшее образование со специализацией в области ИТ или ИБ
- Опыт работы в области практического анализа защищенности и анализа архитектурной документации от двух лет
- Уверенные знания в области основ информационной **безопасности** (протоколов, средств защиты информации, их предназначения, инфраструктуры PKI и понимания принципа работы криптографических алгоритмов)
- Уверенные знания в области **Application security**, умение находить и устранять веб-уязвимости из OWASP Top 10, OWASP Mobile Top 10, CWE Top 25
- Уверенные знания в области экспертизы архитектуры информационных систем, умение находить ошибки/уязвимости на уровне проектной документации, в т.ч. логике бизнес процессов и предлагать релевантные, аргументированные механизмы и средства защиты
- Уверенные знания в технологиях построения прикладных систем в т.ч. с использованием микросервисов и контейнеризации
- Глубокие знания в анализе кода и программировании
- Глубокое понимание принципов работы современных веб-приложений, процессов CI/CD и **безопасной** разработки SSDLC
- Глубокие знания типовых практик по повышению защищенности веб-приложений
- Глубокие знания регуляторных требований в области ИБ, умение соотносить область действия регуляторных требований к разрабатываемому или дорабатываемому функционалу, а так же трансформировать регуляторное требование в практическую плоскость
- Глубокие знания методологии риск-ориентированного подхода, умение проводить качественную оценку рисков и формировать сценарии угроз
- Профессиональное владение Burp Suite

**Что в задачах:**

- Разработка и внедрение процессов безопасной разработки (Secure SDLC);
- Разбор отчетов Bugbounty;
- Анализ уязвимостей и разработка рекомендаций по их устранению;
- Взаимодействие с разработчиками, DevOps и другими командами по вопросам безопасности;
- Разработка и внедрение политик AppSec, Secure Coding Guidelines и других стандартов безопасности;
- Проведение тестирования на проникновение в рамках продуктовых фичей в зоне ответственности (вручную и с использованием автоматизированных инструментов);
- Разработка и реализация технических решений для защиты приложений (WAF, CSP и др.);
- Консультирование по безопасной разработке для Security Champions и разработчиков.

**Что поможет попасть к нам в команду:**

- Понимание OWASP Top 10, CWE, SANS 25.
- От трёх лет опыта работы в роли AppSec.
- Опыт анализа уязвимостей и защиты веб-приложений, API(rate limiting, authentication, authorization, API Gateway security), мобильных приложений. Опыт работы с инструментами SAST, DAST, SCA и анализаторами инфраструктурного кода.
- Опыт работы с языками Java, Python, JavaScript, Go (чтение, анализ кода, выявление уязвимостей).
- Опыт проведения security code review и threat modeling.
- Знание современных методов защиты, включая CSP, JWT, OAuth2 и др.

# ГЛАВНЫЕ 💡 ВЫВОДЫ [ ИЗ АНАЛИЗА ВАКАНСИЙ ]



Ищут не “безопасника”, а инженера безопасности, встроенного в разработку



Dev background  
(или эквивалент)



Способность мыслить  
на уровне архитектуры



Понимание SDLC  
как системы



Умение балансировать  
безопасность и delivery

# ГЛАВНЫЕ ВЫВОДЫ [ ИЗ АНАЛИЗА ВАКАНСИЙ ]

## Безопасность приложений

- + OWASP Top 10 / CWE / SANS
- + Secure SDLC
- + Моделирование угроз
- + Жизненный цикл уязвимостей

## Средний уровень (ожидается у сильного кандидата)

- + DevSecOps практики (Работа с Kubernetes / CI пайплайнами)
- + Тестирование безопасности (ручное + автоматизированное)

## Код и разработка

- + Чтение кода  
(Java / Python / JS / Go)
- + Понимание:
  - Backend/Frontend
  - API security
  - Аутентификация/Авторизация (JWT, OAuth2, OIDC)

## Продвинутый уровень

- + Риск-ориентированный подход
- + Работа с регуляторкой
- + Проектирование контролей безопасности
- + Offensive security (пентест / bug bounty)

## Архитектура

- + Микросервисы
- + Контейнеризация
- + Типовые уязвимости дизайна

## Инструменты

- + SAST / DAST / SCA
- + CI/CD интеграции

## Софт / мета навыки

- + Коммуникация с разработчиками
- + Умение аргументировать риски
- + Приоритизация уязвимостей
- + Системное мышление (архитектура + процессы)

# ТРАЕКТОРИЯ РАЗВИТИЯ В ПРОФЕССИИ



## AppSec Engineer

- ▶ Senior AppSec / DevSecOps Engineer
- ▶ Security Architect
- ▶ Head of AppSec / DevSecOps Lead



Карьерный рост:

## Product Security (глубокая работа с продуктом)

### Чем занимаешься:

- ▶ secure code review
- ▶ архитектурный анализ
- ▶ threat modeling (глубже, чем в DevSecOps)
- ▶ взаимодействие с разработчиками



**Суть:**  
безопасность конкретного продукта/системы



### Карьерный рост:

- ▶ AppSec Engineer
- ▶ Security BP
- ▶ Security Architect

# ТРАЕКТОРИЯ РАЗВИТИЯ В ПРОФЕССИИ



## ○ Offensive AppSec (атакующая сторона внутри компании)

### Чем занимаешься:

- ▶ pentest веб-приложений
- ▶ bug bounty внутри компании
- ▶ red teaming (частично)



**Суть:**  
поиск уязвимостей в приложениях



### Карьерный рост:

- ▶ Junior Pentester
- ▶ AppSec Pentester
- ▶ Red Team / Lead Offensive Security
- ▶ Security Researcher

# НА ЧТО СМОТРЯТ ПРИ ПРИЕМЕ НА РАБОТУ



Практические кейсы  
(умение “думать вслух”, честность)



Понимание **VS** зазубривание



Умение рассказать о себе



Знакомство с вакансией и компанией

# ЭТО ПРОГРАММА – МАРШРУТ



В интернете много материалов на год и больше. на курсе эксперт дает вспомогательные материалы: **книги, статьи, видео** – после всего этого, если их вобрать в себя, ты будешь крут. Самые глупые вопросы ты можешь задавать эксперту и быстрее расти.



Эксперт помогает в любых вопросах:  
я правильно вот сюда иду? а я правильно понял, что вот так?



# АРХИТЕКТУРА ПРОГРАММЫ

[ СПЕЦИАЛИСТ ПО БЕЗОПАСНОЙ РАЗРАБОТКЕ ПРИЛОЖЕНИЙ ]

**20**

ЗАНЯТИЙ

**254**

АК. Ч.

**80**

АК.Ч. ЗАНЯТИЯ С ПРЕПОДАВАТЕЛЕМ

**174**

АК.Ч. САМОСТОЯТЕЛЬНОЙ РАБОТЫ

# [S-224] БЕЗОПАСНОСТЬ ОКРУЖЕНИЯ ПРИЛОЖЕНИЙ

- 01 Окружение приложений
- 02 Безопасность на уровне ОС
- 03 Nginx - Описание, Настройка, Безопасность
- 04 Введение в Docker контейнеры
- 05 Безопасность Docker
- 06 Введение в Kubernetes
- 07 Безопасность в Kubernetes
- 08 Hashicorp Vault - Безопасное хранение секретов
- 09 Обеспечение безопасности облачных сред
- 10 Финальное занятие - сдача финального проекта



# [S-232] БЕЗОПАСНАЯ РАЗРАБОТКА ПРИЛОЖЕНИЙ В РАМКАХ SDL ЦИКЛА

## 01 Общие концепции безопасности.

Security на этапах сбора требований и проектирования инфраструктуры

## 02 SDLc:

базовые понятия и мероприятия ИБ на каждом из этапов.  
DevSecOps: базовые понятия и приемы. Практика

## 03 Security на этапе написания кода

Статические анализаторы кода. Инструменты анализа сторонних компонентов ПО (Software Composition Analysis).

## 04 Динамический анализ уязвимостей и фаззинг тестирование

## 05 Предрелизные проверки безопасности

## 06 Безопасность окружения на этапе разработки.

## 07 Security Education. Security Culture

## 08 Безопасность в продакшн.

## 09 Jenkins. Базовые приемы. Реализации security pipeline (SAST, DAST, SCA)

## 10 Дорожная карта SSDLc в организации Уровни зрелости AppSec процессов (DSOMM, BSIMM, SAMM)

# ЧЕМУ НАУЧИМСЯ?

01 ✓

Формулирование требований и процессов в цикле безопасной разработки ПО;

02 ✓

Разработка дорожной карты развития SSDLC;

03 ✓

Применение инструментов DAST, SAST, SCA в CI/CD;

04 ✓

Автоматизация анализа безопасности окружения приложений;

05 ✓

Обнаружение ряд типовых уязвимостей и угроз веб-приложений, входящих в список проекта OWASP Top 10, с использованием автоматизированных средств.

06 ✓

Познакомимся с технологиями и безопасностью:

- ▶ Linux
- ▶ Docker
- ▶ Kubernetes
- ▶ Hashicorp Vault
- ▶ Облачные среды



# ПОЧЕМУ ИМЕННО **МЫ?**

## МЫ ЗАКРЫВАЕМ РЕАЛЬНЫЙ ЗАПРОС РЫНКА

Рынку не хватает:

- ▶ AppSec-специалистов и DevSecOps-инженеров
- ▶ тех, кто понимает и код, и безопасность
- ▶ просто крутых специалистов

## МЫ ДАЁМ ТО, ЧТО ВЫ МОЖЕТЕ НАПИСАТЬ В РЕЗЮМЕ

Напишите:

- ▶ внедрение security-практик в SDLC (моделирование угроз, контроль уязвимостей)
- ▶ настройка CI/CD пайплайна с интеграцией SAST / DAST / SCA
- ▶ работа с безопасностью инфраструктуры (Docker, Kubernetes, управление секретами)
- ▶ участие в проектировании архитектуры с учётом рисков безопасности



# ПОЧЕМУ ИМЕННО МЫ?



## МЫ МАКСИМАЛЬНО БЛИЗКИ К РЕАЛЬНОМУ ПРОДАКШЕНУ

- ▶ реальные инструменты
- ▶ реальные пайплайны
- ▶ реальные практики

## МЫ ФОРМИРУЕМ ПРОФИЛЬ T-SHAPED СПЕЦИАЛИСТА

Глубина ▶ AppSec

Ширина: ▶ Dev + Infra + Security

# ФИЧИ ПРОДУКТА CyberED

## 01 End-to-end покрытие:

собираем целостную модель от требований и архитектуры до продакшена, от SDLC до DevSecOps пайплайнов

## 02 Мышление на уровне архитектуры:

учим моделировать угрозы, проектировать безопасность, строить roadmap SSDLC

## 03 Современный стек:

- ▶ Docker / Kubernetes
- ▶ Hashicorp Vault
- ▶ облака
- ▶ безопасность окружения

## 04 Практика встроена в каждую тему:

обучение через реальные сценарии внедрения

## 05 Делаем из вас DevSecOps, а не только AppSec:

шире профиль, больше возможностей на рынке

## 06 Соответствие требованиям рынка и регуляторов:

- даем практики, которые
- ▶ применимы в компаниях с требованиями к ИБ и аудиту
  - ▶ соответствуют современным стандартам безопасной разработки
  - ▶ позволяют работать в среде с формализованными процессами безопасности



# ЗАДАВАЙТЕ ВОПРОСЫ

И ПРЕДЛАГАЙТЕ ОБСУДИТЬ КЕЙСЫ

# СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ

CyberED

ЗАБРОНИРОВАТЬ  
МЕСТО В ГРУППЕ



Курс

**Специалист по  
безопасной  
разработке  
приложений**

+



В подарок

Курс

**AI-агент по  
безопасности**



@CYBERED\_RUSSIA