

ВВЕДЕНИЕ В КУРС

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ



[СПИКЕР]

КРИВОНОС ИГОРЬ

- Белый хакер, пентестер, апсек и просто хороший человек (иногда)
- Старший специалист ИБ в RWB
- Ключевые навыки:
 - БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ АНДРОИД & IOS
 - РАЗРАБОТКА ПОД АНДРОИД (JAVA/KOTLIN, C/C++)
 - РАЗРАБОТКА НА PYTHON

CyberED



КТО ТАКОЙ "МОБИЛЬЩИК" И ЗАЧЕМ ОН НУЖЕН?

- МОБИЛЬНЫЕ ПЛАТФОРМЫ ИМЕЮТ СВОИ ОСОБЕННОСТИ И ОТЛИЧИЯ СПЕЦИФИЧНЫЕ ДЛЯ КАЖДОЙ ОС, КОТОРЫЕ НАДО ЗНАТЬ
- УЯЗВИМОСТЬ В КЛИЕНТЕ ЭТО УЖЕ ДАВНО НЕ "ПОДУМАЕШЬ ПРОБЛЕМА У ОДНОГО ПОЛЬЗОВАТЕЛЯ"
- МОБИЛЬНЫЕ ОС ПОСТОЯННО РАЗВИВАЮТСЯ В НИХ ПОЯВЛЯЮТСЯ НОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ, А ВМЕСТЕ С НИМИ И НОВЫЕ "ДЫРЫ"

КТО ТАКОЙ "МОБИЛЬЩИК" И ЗАЧЕМ ОН НУЖЕН?

- УРОВЕНЬ ЗНАНИЙ В ОБЛАСТИ БЕЗОПАСНОЙ РАЗРАБОТКИ СРЕДИ РАЗРАБОТЧИКОВ ДО СИХ ПОР НИЗОК
- ИНСТРУМЕНТЫ АВТОМАТИЗАЦИИ ПОИСКА УЯЗВИМОСТЕЙ НЕ ТАК РАСПРОСТРАНЕНЫ КАК ДЛЯ ВЕБА И ИМИ ВСЕ РАВНО НАДО УМЕТЬ УПРАВЛЯТЬ

А КАК ЧЕРЕЗ КЛИЕНТА МОЖНО АТАКОВАТЬ?

01 УГОН АККАУНТА В 1 КЛИК (ИЛИ СТАВИТ СТОРОННЕЕ ПРИЛОЖЕНИЕ)

ПОЛЬЗОВАТЕЛЬ КЛИКАЕТ НА ССЫЛКУ (ДИПИЛИНК) – ТОКЕН ОТПРАВЛЯЕТСЯ НА СЕРВЕР ЗЛОУМЫШЛЕННИКА

02 СТОРОННЕЕ ПРИЛОЖЕНИЕ ПОЛУЧАЕТ ДОСТУП К ДАННЫМ ПОЛЬЗОВАТЕЛЯ/ПРИЛОЖЕНИЯ

АНДРОИД → ЭКСПОРТИРОВАННЫЙ КОМПОНЕНТ → ДОСТУП К ДАННЫМ

03 БАЙПАС МЕХАНИЗМОВ ЗАЩИТЫ ПРИЛОЖЕНИЯ И ОС

- ОБХОД ПИНКОДА И ДРУГИХ МЕХАНИЗМОВ ЗАЩИТЫ
- ИЗВЛЕЧЕНИЕ ДАННЫХ ИЗ ПЕСОЧНИЦЫ ПРИЛОЖЕНИЯ
- ПРОСМОТР ПРИВАТНЫХ ФАЙЛОВ

04 КРАЖА СЕКРЕТОВ СЕРВЕРА ИЛИ АТАКА НА СЕРВЕР ПРИ МИСКОФНИГЕ

- АТАКА FIREBASE
- ПРИВАТНОЕ АПИ O_O?
- СЕКРЕТНЫЕ-СЕКРЕТЫ В КОДЕ ПРИЛОЖЕНИЕ

РЫНОК MOBILE SECURITY 💡 В РОССИИ

+24%

ИБ-вакансии растут: год к году в I квартале 2026

~3x

AppSec / DevSecOps специалистов меньше,
чем нужно бизнесу

4,8% vs 1,5%

вакансии DevSecOps/AppSec

резюме

Разрыв спроса и предложения

РЫНОК MOBILE SECURITY

В РОССИИ

Mobile security прячется в AppSec:

роли часто называются не “мобильщик”, а AppSec, Security Engineer, безопасность клиентских приложений

Ценится не базовый перехват трафика, а глубина:

reverse, client-side vulnerabilities, API security, SSL-pinning bypass, Frida / MobSF

Android + iOS = отдельная экспертиза:

общий безопасник часто не закрывает глубокий анализ клиента

Сильный мобильщик = редкий профиль на стыке AppSec, пентеста, реверса и мобильной разработки

ПЛАН КУРСА



1. Введение в ОС Android
2. Работа с Android OS и пакетами APK
3. Разработка Android приложения
4. Реверс-инжиниринг Android приложений
5. Типовые уязвимости мобильных приложений Android
6. Типовые уязвимости мобильных приложений Android 2
7. SSL-pinning и Frida-tools
8. Инструменты автоматизации анализа
9. Проведение работ по анализу защищенности мобильного приложения Android
10. Введение в iOS
11. Архитектура безопасности iOS
12. Jailbreaking iOS
13. Динамический анализ приложений iOS
14. Типовые уязвимости приложений iOS
15. BugBounty, CTF, Проектная деятельность

ДОСТАТОЧНО ЛИ КУРСА И ЧТО И КАК ЕЩЕ ИЗУЧАТЬ?

ПОЧЕМУ MOBILE SECURITY — ОТДЕЛЬНАЯ СПЕЦИАЛИЗАЦИЯ

КОМПАНИИ ЧАСТО ИЩУТ “ПРОСТО БЕЗОПАСНИКА”, НО НА ПРАКТИКЕ ИМ НУЖЕН СПЕЦИАЛИСТ ПО МОБИЛЬНЫМ ПРИЛОЖЕНИЯМ.

- ▶ Мобильная безопасность — это не только веб, API и инфраструктура
- ▶ Android и iOS — две отдельные платформы, которые нужно изучать глубоко
- ▶ Общий ИБ-специалист часто умеет перехватывать трафик и обходить SSL-pinning, но поверхностно смотрит клиентскую часть



ПОЧЕМУ MOBILE SECURITY — ОТДЕЛЬНАЯ СПЕЦИАЛИЗАЦИЯ

- ▶ На рынке есть дефицит людей, которые полноценно анализируют мобильные приложения: код, хранение данных, логику, защитные механизмы и поведение приложения
- ▶ Такие вакансии могут называться по-разному: AppSec, безопасность клиентских приложений, mobile security, пентестер мобильных приложений

ВЫВОД: СИЛЬНЫЙ MOBILE SECURITY-СПЕЦИАЛИСТ ЗАКРЫВАЕТ ЗАДАЧУ, С КОТОРОЙ ОБЫЧНЫЙ БЕЗОПАСНИК ЧАСТО НЕ СПРАВЛЯЕТСЯ.



КЕЙСЫ

MOBILE SECURITY

АТО – ACCOUNT TAKE OVER ПО КЛИКУ НА ССЫЛКУ

- Приложение принимало deeplink и извлекало из него параметр url=<host> далее без всякой проверки отправляло запрос на этот хост добавив в запрос токен.

КЕЙСЫ

MOBILE SECURITY

БАЙПАС ПИНК-КОДА ЧЕРЕЗ IPC

- Прямой вызов экспортированного компонента в обход активности с пинкодом
- Уязвимая навигация в Jetpack navigation или jetpack compose navigation (https://habr.com/ru/companies/swordfish_security/articles/830338/)
- Мисконфиги и ошибки в бизнес-логике приложения

КЕЙСЫ

MOBILE SECURITY

ИЗВЛЕЧЕНИЕ ДАННЫХ ИЗ ПЕСОЧНИЦЫ ПРИЛОЖЕНИЯ БЕЗ РУТА И ПОВЫШЕНИЯ ПРИВИЛЕГИЙ

- Уязвимые контент-провайдеры
- Доступ к файлам через webview
- Ошибки в валидации путей (path traversal)
- Мисконфиг в fileprovider
- Шаринг файлов и данных без проверки недоверенным приложениям

MOBILE SECURITY

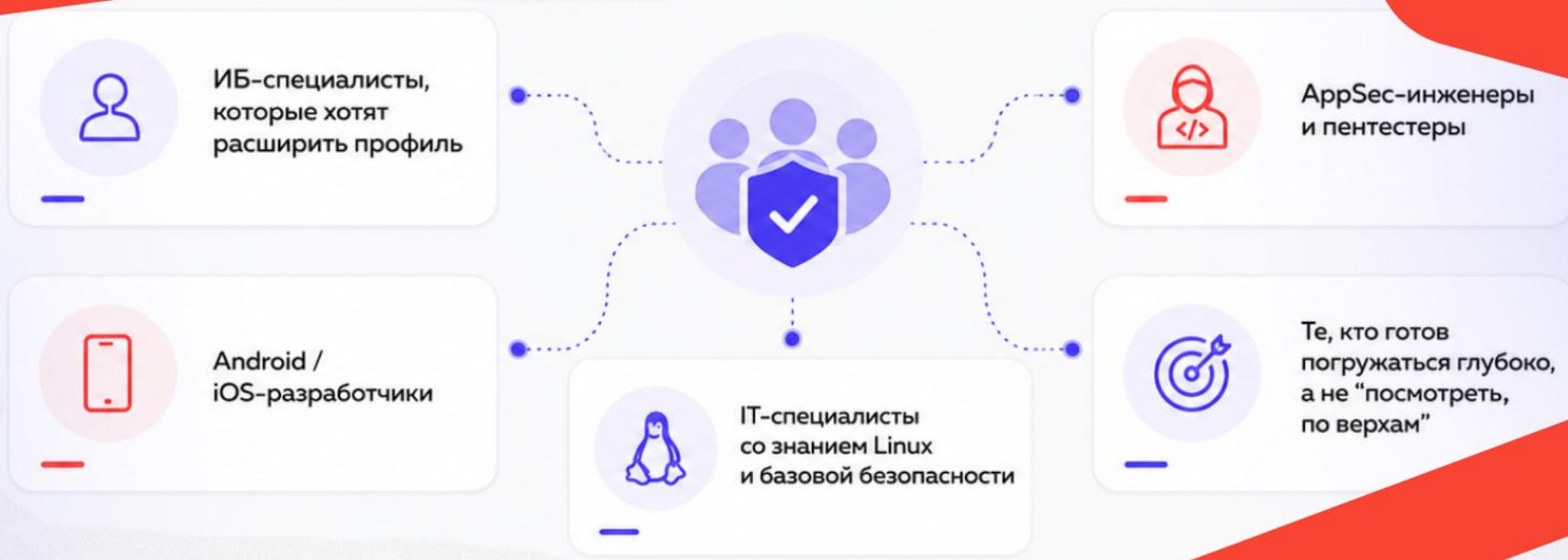


MUST-HAVE

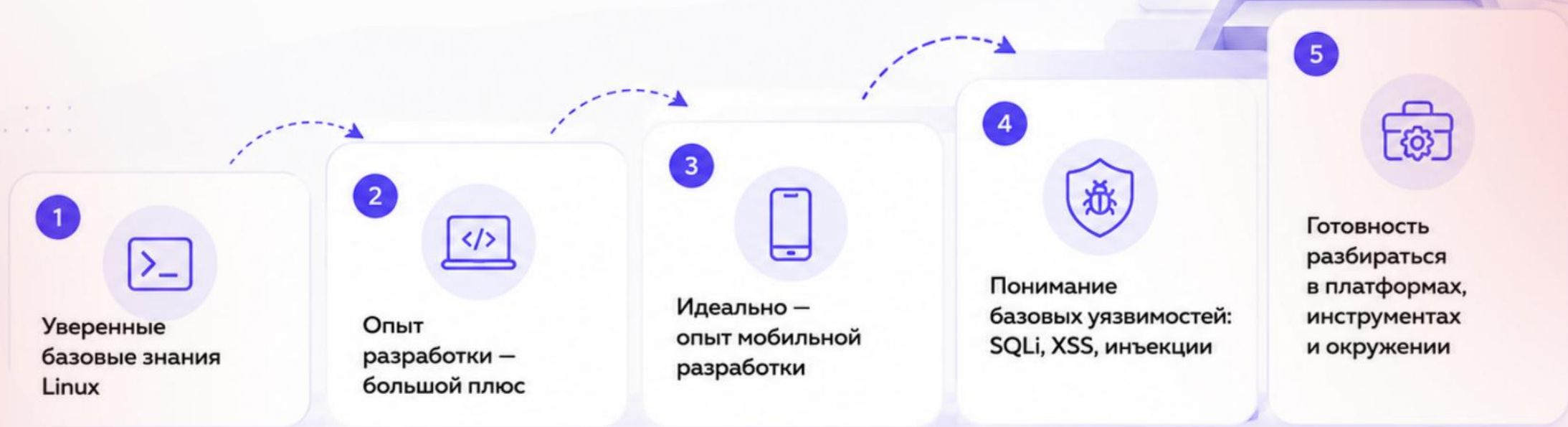
ДЛЯ APPSEC

- 01 Большинство клиентских приложений сегодня — это мобилка
- 02 Люди чаще взаимодействуют с бизнесом через смартфон, а не десктоп
- 03 AppSec-инженеру важно понимать мобильные уязвимости
- 04 Навык помогает адекватно оценивать риски клиентской части
- 05 Mobile security усиливает профиль любого безопасника

КОМУ КУРС ПОДОЙДЕТ ЛУЧШЕ ВСЕГО



КАКОЙ БЭКГРАУНД НУЖЕН НА ВХОДЕ



MOBILE SECURITY — ЭТО УЖЕ НЕ “ДОПОЛНИТЕЛЬНЫЙ НАВЫК”



РАНЬШЕ

- Мобилка часто была дополнением к AppSec



СЕЙЧАС

- Это самостоятельная область знаний
- Специалисту нужно понимать не только уязвимости, но и устройство платформ



ПЛАТФОРМЫ



Android

Большая и сложная экосистема устройств



iOS

Закрытая платформа со своими особенностями



HarmonyOS и другие

Появляются новые ОС и экосистемы

КУРС КАК ВХОД В ПРОФЕССИЮ И UPSKILL

МОЖНО ЗАЙТИ В
НАПРАВЛЕНИЕ С НУЛЯ

но потребуются добирать базу ИБ

ДЛЯ ДЕЙСТВУЮЩЕГО
БЕЗОПАСНИКА

курс работает как усиление профиля

ДЛЯ МОБИЛЬНОГО
РАЗРАБОТЧИКА

быстрый мост в mobile security

Навык можно использовать как основную специализацию
Или как дополнительную экспертизу внутри AppSec / пентеста

ЧТО СТУДЕНТ СМОЖЕТ ДЕЛАТЬ ПОСЛЕ КУРСА

Практические результаты обучения



Анализировать
защищенность
мобильных приложений



Работать с клиентской
частью Android и iOS



Делать реверс, патчинг
и динамический анализ



Настраивать окружение
и использовать
индустриальные инструменты



Работать с учебными
и open-source
приложениями



Писать собственные
скрипты и тестовое
приложение



ПРАКТИКА ВМЕСТО СУХОЙ ТЕОРИИ

- Основной фокус — практика, переплетенная с теорией
- Работа на стендах, виртуалках и учебных приложения
- Разбор реальных кейсов и типовых небезопасных реализаций
- Упор на устройство приложений и атаки на них
- Курс следует логике OWASP Mobile

ЧЕМ КУРС ОТЛИЧАЕТСЯ ОТ САМОСТОЯТЕЛЬНОГО ОБУЧЕНИЯ



САМОСТОЯТЕЛЬНО



В YouTube можно найти почти всё, но без маршрута



Самостоятельно легко потратить время на лишнее

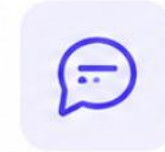
VS



С КУРСОМ



Курс дает структуру и последовательность



Живое общение с экспертом ускоряет вход



ВЫБОР ПРОСТОЙ: либо долго собирать самому, либо **быстрее войти** через готовую программу

СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ

При покупке одного
из курсов:

- Атаки на Active Directory
- Анализ безопасности мобильных приложений
- Программирование на Python для пентестеров

+



В подарок

**2 МИНИ-КУРСА
НА ВЫБОР В
ПОДАРОК**

из трека R301 и
курса DETA

+



Скидка

**скидка 10% за
покупку в
течение недели**



@CYBERED_RUSSIA

ДАВАЙТЕ РАЗБЕРЕМ
ВАШИ 
ВОПРОСЫ

