

[ВЕБИНАР]

CyberED

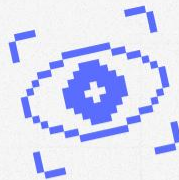
ПРОФЕССИЯ ИНЖЕНЕР ИБ



ТВОЙ СТАРТ В
КИБЕРБЕЗОПАСНОСТИ



[О СПИКЕРЕ]



CyberED

АНДРЕЙ ШАБАЛИН

- 2011-2022 - ТРЕНЕР, ИНСТРУКТОР АКАДЕМИЙ CISCO, HUAWEI
- 2022-2026- ИНСТРУКТОР “АКАДЕМИЯ ELTEX”, “АСТРО- УНИВЕРСИТЕТ”
- КАНДИДАТ НАУК, ДОЦЕНТ КАФЕДРЫ ИБ ТЮМГУ.

ДАВАЙТЕ ПОЗНАКОМИМСЯ

А)

**ОТМЕТЬТЕ, КТО ВЫ
И ОТКУДА ПРИШЛИ:**

- 1 Новичок: без ИТ / ИБ бэкграунда
- 2 Новичок с ИТ-бэкграундом
- 3 Работаю в ИТ
- 4 Работаю в ИБ

Б)

**КАКИЕ У ВАС ЦЕЛИ
НА ВСТРЕЧУ?**

В)

**ЧТО ВАС БОЛЬШЕ ВСЕГО
НАСТОРАЖИВАЕТ / ОСТАНАВЛИВАЕТ
В ВЫБОРЕ НАПРАВЛЕНИЯ?**



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



BLUE
TEAM

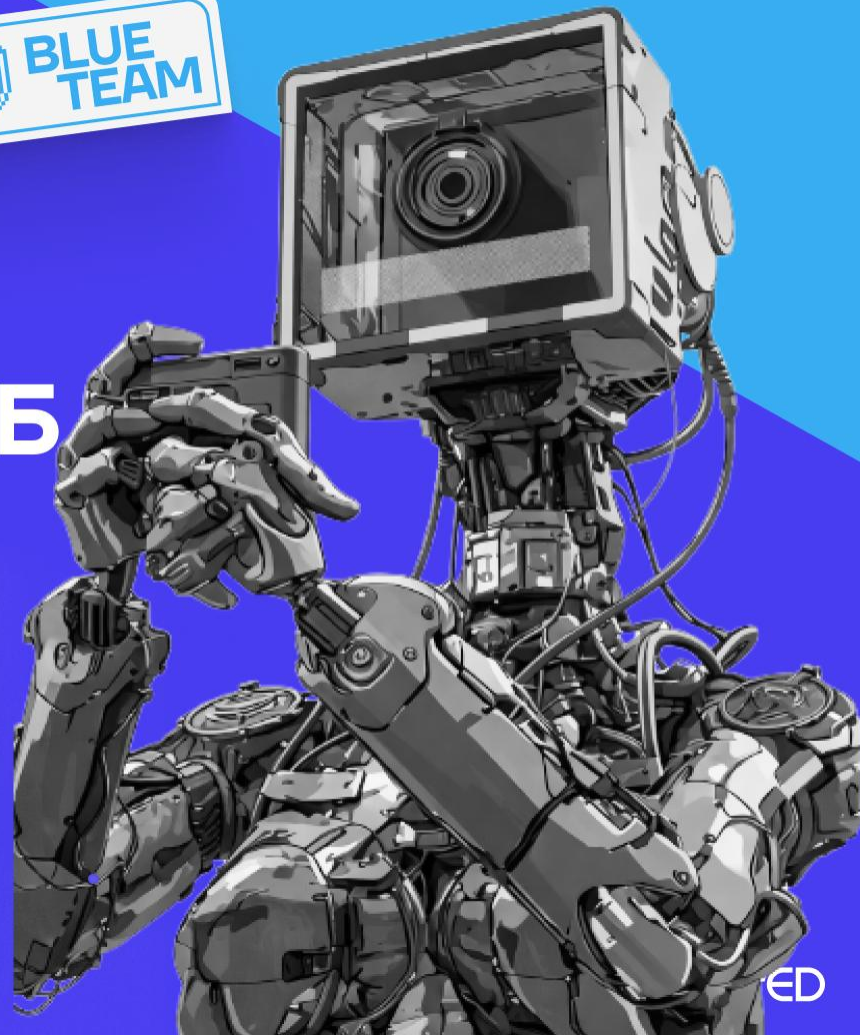
ИНЖЕНЕР ПО ИБ/ СПЕЦИАЛИСТ ПО ИБ

● С НУЛЯ

Программа где не нужно ничего уметь на старте .
Мы всему научим! Главное это ваша тяга к IT среде и отсутствие
страха обучаться новому

● ОТ ЛЕГКОГО К СЛОЖНОМУ

● ПОВТОРЯЕМ И ПОДСКАЗЫВАЕМ



СФЕРЫ ИБ

ВОЕННАЯ / СИЛОВАЯ ИБ

Что делает:

Контрразведка, радиоэлектронная борьба, защита государственной тайны и шифрования.

ГОСУДАРСТВЕННАЯ/ НАЦИОНАЛЬНАЯ ИБ

Что делает:

Направление по линии Минцифры, Банка России, ФСТЭК, МВД и других госструктур.

ЧАСТНАЯ/ БИЗНЕС ИБ

Что делает:

Частная деятельность, направленная на защиту от кибератак, соответствие требованиям регуляторов, расследование инцидентов внутри компании.

[ИНЖЕНЕР ПО ИБ]

СУТЬ РАБОТЫ И КЛЮЧЕВЫЕ ЗАДАЧИ

ИНЖЕНЕР ПО ИБ:



Специалист, который проектирует, внедряет и поддерживает защищенную сетевую инфраструктуру организации. Его основная цель – предотвратить несанкционированный доступ, хакерские атаки и утечки конфиденциальных данных с серверов и рабочих станций пользователей через корпоративную сеть.

Главные задачи:



Обеспечение непрерывной защищенности инфраструктуры организации.

КОМПАНИЯ ПЛАТИТ ИБ-ИНЖЕНЕРУ ЗА МИНИМИЗАЦИЮ РИСКОВ
ОСТАНОВКИ БИЗНЕС-ПРОЦЕССОВ

ИДЕАЛЬНЫМ РЕЗУЛЬТАТОМ РАБОТЫ ЯВЛЯЕТСЯ



Отсутствие успешных инцидентов:

Злоумышленники не смогли проникнуть в сеть, данные не утекли.



Минимальное время простоя:

Если инцидент произошел, система восстанавливается максимально быстро.



Актуальность:

Все СЗИ обновлены, настроены и не конфликтуют.

[СХОЖИЕ ДОЛЖНОСТИ С ИНЖЕНЕРОМ ПО ИБ]



Администратор ИБ



Администратор СЗИ (средств защиты информации)



Инженер по сетевой безопасности (Network Security Engineer)



Специалист поддержки по ИБ



Переходы – развитие

Системный администратор

Сетевой инженер

Аналитик SOC L1

[АНАЛИЗ ВАКАНСИЙ]

ВАКАНСИИ ДЛЯ НОВИЧКОВ

ТРЕБОВАНИЯ РАБОТОДАТЕЛЕЙ К КАНДИДАТАМ БЕЗ ОПЫТА

ПРИМЕРЫ ВАКАНСИЙ

- Младший специалист по ИБ
- Младший инженер по ИБ (сервисы РАР)
- Начинающий специалист по ИБ

ОСНОВНЫЕ ЗАДАЧИ

- Техническая поддержка сотрудников по вопросам ИБ
- Мониторинг событий безопасности и уязвимостей
- Настройка и обновление политик СЗИ
- Ведение технической документации
- Консультирование клиентов компании

КЛЮЧЕВЫЕ НАВЫКИ И ЗНАНИЯ

- Высшее или неоконченное высшее образование в сфере ИБ или ИТ
- Базовое администрирование Windows Server и Linux/Unix
- Понимание сетевых протоколов: TCP/IP, DNS, DHCP
- Знание моделей OSI и TCP/IP
- Понимание принципов работы СЗИ: антивирусы, SIEM, DLP, VPN, NTA
- Навыки составления инструкций и технической документации

БУДЕТ ПРЕИМУЩЕСТВОМ

- Знание продуктов класса CYBERARK
- Понимание требований 152-ФЗ «О персональных данных»

[АНАЛИЗ ВАКАНСИЙ]

ВАКАНСИИ ДЛЯ СПЕЦИАЛИСТОВ:

ТРЕБОВАНИЯ РАБОТОДАТЕЛЕЙ К КАНДИДАТАМ С ОПЫТОМ 1–3 ГОДА

ПРИМЕРЫ ВАКАНСИЙ

- Специалист по ИБ
- Инженер по информационной безопасности

ОСНОВНЫЕ ЗАДАЧИ

- Администрирование СЗИ: настройка политик, NAT, VPN, PKI
- Расследование инцидентов (IRT): анализ трафика, блокировка угроз
- Анализ уязвимостей, участие в Pen-тестах
- Разработка технической документации: схемы, политики, инструкции
- Обеспечение соответствия требованиям регуляторов (ФСТЭК, ЦБ, РКН)
- Обучение сотрудников правилам информационной безопасности

КЛЮЧЕВЫЕ НАВЫКИ И ЗНАНИЯ

- **Сети** : TCP/IP, DNS, DHCP HTTP/HTTPS, SSL/TLS VPN, VLAN, BGP, OSPF, Модели OSI и TCP/IP
- **Средства защиты**: NGFW: Check Point, UserGate, Континент, IDS/IPS: Cisco Firepower, Suricata, Snort, DLP, SIEM, WAF, NTA, СКЗИ, антивирусы (включая Sandbox)
- **Нормативная база**
- 152-ФЗ, 149-ФЗ, 98-ФЗ
- 757-П ЦБ, ГОСТ Р 57580.1
- 187-ФЗ (КИИ), приказы ФСТЭК

ДОПОЛНИТЕЛЬНЫЕ ТРЕБОВАНИЯ

- Опыт категорирования КИИ и подготовки документации по 187-ФЗ
- Опыт проведения работ по оценке соответствия 757-П
- Навыки написания скриптов для автоматизации (сбор логов, проверка конфигураций)
- Опыт взаимодействия с вендорами и контроля контрагентов

ПУЛ КЛЮЧЕВЫХ ИНСТРУМЕНТОВ

■ Сети и инфраструктура:

Linux / Windows

Active Directory

Cisco IOS

TCP/IP, DNS, DHCP, NAT, VLAN, ACL

SSH, RDP, HTTP(S), SMB

Kerberos, LDAP

■ Средства защиты:

NGFW \ IDS/IPS \ WAF

SIEM \ EDR

и др. СЗИ: DLP, NAC, NTA, UEBA, Sandbox, HoneyPot.

■ Виртуализация и практическая среда

VirtualBox

GNS3

■ Мониторинг и анализ

SOC

Syslog

SNMP

xFlow

WMI

xSPAN

Wireshark \ tcpdump

nmap

■ Контроль доступа и криптография

MFA

PKI \ Certificates

AES, SHA, RSA

SSL/TLS

IPsec \ VPN

SSH

[СПЕЦИАЛИСТ ИБ]

ЗАРПЛАТА



СТАЖЁР / ОПЛАЧИВАЕМАЯ СТАЖИРОВКА	JUNIOR (БЕЗ IT-ОПЫТА)	JUNIOR + (С ОПЫТОМ В IT)	MIDDLE	SENIOR
0 мес.	0-1 года	0-1 года	1,5-3 года	3-5 лет
50 – 70 ТЫС.	70 - 110 ТЫС.	110-180 ТЫС.	150-350 ТЫС.	ОТ 350 ТЫС.

Примечание: Данные являются ориентировочными и основаны на анализе рынка вакансий.

Фактический уровень дохода зависит от: региона, размера и типа компании, формата работы, уровня навыков и конкретной роли. Зарплаты указаны в российских рублях до вычета налогов.

КАК ОБЫЧНО ПРОИСХОДИТ НАЙМ ИБ ИНЖЕНЕРОВ

- 01 Скрининг (HR): проверка на адекватность и наличие базы (техническое образование или профильные курсы).
- 02 Технический пре-скрининг: короткий звонок от инженера. Могут попросить объяснить, что происходит, когда вы вводите google.com в браузере.
- 03 Техническое интервью: глубокий опрос по сетям и работе операционных систем.
- 04 Практическое задание: организация доступа к виртуалке, где нужно настроить или найти ошибку в конфигурации сети.

Наниматели Junior-инженеров смотрят не на знание «кнопок» в конкретном ПО, а на «инженерную мышление» и понимание того, как «данные ходят по проводам».

ПОЧЕМУ ДЖУНЫ ПРОВАЛИВАЮТСЯ

НА ОТБОРЕ В ИБ

05 Слабая фундаментальная база

Сети, протоколы, ОС, базовые принципы ИБ

06 Недостаток практических навыков

Linux/CLI, работа с логами, поиск ошибок в конфигурации

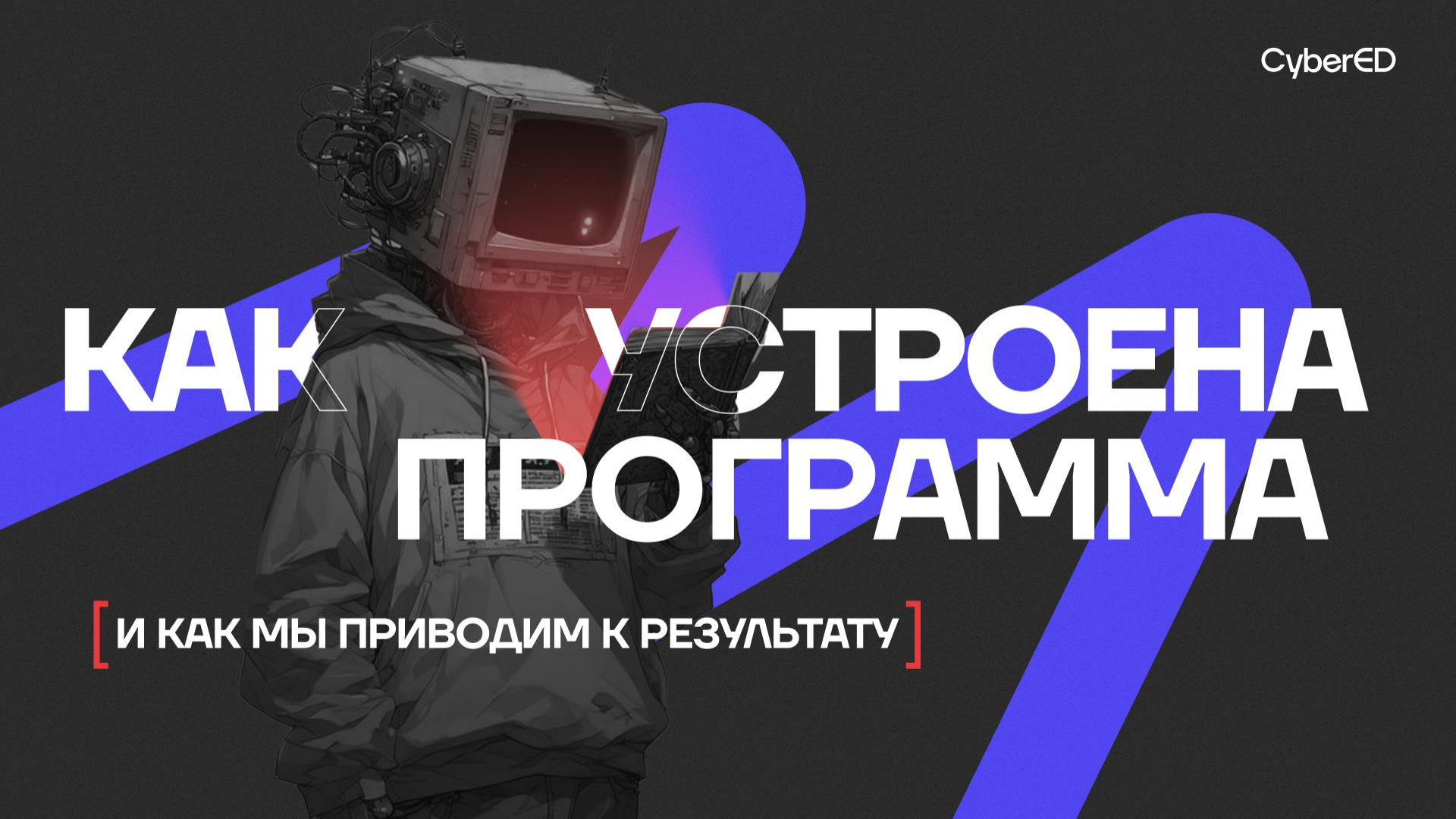
07 Нет подтвержденной практики

Проекты, лабораторные работы, кейсы в портфолио

08 На собеседовании нужно показать: база + логика + практика

Работодатели часто жалуются, что новички знают, как "нажимать кнопки" в условном «Касперском», но не знают, как работает, например, протокол DNS или права доступа в Linux.

На отборе junior-кандидата
проверяют на способность
**понимать, объяснять
и применять** базовые
инженерные принципы



КАК УСТРОЕНА ПРОГРАММА

[И КАК МЫ ПРИВОДИМ К РЕЗУЛЬТАТУ]

[ПРОГРАММА “ИНЖЕНЕРА ПО ИБ” ПОСТРОЕНА ПО ЛОГИКЕ РЕАЛЬНОЙ РАБОТЫ]

Понимание
инфраструктуры и её
проектирование сети, ОС

Требование рынка: понимание архитектуры сети и принципы её функционирования.

Результат обучения: программа делает нашего выпускника универсальным: он может быстро пересечь с Cisco на Eltex или с Debian на Astra Linux, потому что понимает базовую логику работы сетей и ОС.

Внедрение защиты СЗИ
и логика их применения

Требование рынка: умение осуществлять установку и настройку специального ПО.

Результат обучения: слушатель понимает, чтобы установить антивирус в сети, необходимо использовать механизм групповых политик.

Эксплуатация и
мониторинг логи,
мониторинг, уязвимости

Требование рынка: умение осуществлять поиск уязвимостей и расследовать инциденты.

Результат обучения: слушатель понимает, где смотреть логи серверов и как настроить их отправку в SIEM.



Результат программы: слушатель на выходе — не просто продвинутый «оператор софта», а инженер, который понимает архитектуру системы и может обосновать каждое изменение в настройках безопасности.

ПРОЕКТЫ В ПРОГРАММЕ - ЭТО
ГОТОВЫЙ ПЛАН РАЗВЕРТЫВАНИЯ
ЗАЩИТЫ В КОМПАНИИ "С НУЛЯ"

ПОСТРОИТЬ СЕТЬ

Тема 1. Подготовительное занятие

+

Тема 2. Сети с точки зрения информационной безопасности. Знакомство с инструментарием.
Сетевая модель OSI.

+

Тема 3. Уровень L2 модели OSI. Коммутация. Протокол ARP.

+

Тема 4. Уровень L3 модели OSI. IP сети. DHCP.

+

Тема 5. Уровень L4 модели OSI. DNS. NAT.

+

Тема 6. Практика построения сетевой инфраструктуры.

+

Тема 7. Безопасность локальной сети. Сегментирование.

+

Тема 8. Безопасность локальной сети. Защита сети.

+

Тема 9. Технология NAT. SSH.

+

Тема 10. Практика обеспечения безопасности сетевой инфраструктуры.

+

Тема 11. Корпоративный VPN.

+

ПРОЕКТЫ В ПРОГРАММЕ - ЭТО
ГОТОВЫЙ ПЛАН РАЗВЕРТЫВАНИЯ
ЗАЩИТЫ В КОМПАНИИ "С НУЛЯ"

ПОДНЯТЬ ДОМЕН И СЕРВЕРЫ

ДОМЕННАЯ ИНФРАСТРУКТУРА WINDOWS

Тема 1. Подготовительное занятие	+
Тема 2. Windows Server & Domain Services & Active Directory Management	+
Тема 3. Groups & Windows Authentication	+
Тема 4. Доменные сервисы (DHCP, DNS, GPO)	+
Тема 5. DNS, DHCP, GPO	+
Тема 6. Обмен данными в домене. Центр сертификации.	+
Тема 7. Доменное взаимодействие (Sites, Trust).	+

ОПЕРАЦИОННАЯ СИСТЕМА LINUX

Занятие 1. Подготовительное занятие	+
Занятие 2. Общие положения. Терминал и системные утилиты	+
Занятие 3. Привилегии, сеть и скрипты	+
Занятие 4. Управление сетью и менеджеры пакетов (Самостоятельное занятие)	+
Занятие 5. Управление сервисами. Часть 1	+
Занятие 6. Управление сервисами	+
Занятие 7. Общие вопросы безопасности OS	+

ПРОЕКТЫ В ПРОГРАММЕ - ЭТО
ГОТОВЫЙ ПЛАН РАЗВЕРТЫВАНИЯ
ЗАЩИТЫ В КОМПАНИИ "С НУЛЯ"

ВКЛЮЧИТЬ МОНИТОРИНГ И ФИЛЬТРАЦИЮ



Тема 1. Системы защиты информации



Тема 2. СЗИ: SIEM



Тема 3. СЗИ: SIEM



Тема 4. СЗИ: IDS/IPS



Тема 5. СЗИ: IDS/IPS



Тема 6. СЗИ: WAF



Тема 7. СЗИ: WAF



ОТЛИЧИЕ ПРОГРАММЫ “ИНЖЕНЕР ПО ИБ” ОТ ДРУГИХ

01 Акцент на «Hard Skills» системного уровня:

Сначала сети, ОС, AD и Linux – слушатель понимает и может устранить проблему (почему пакет не проходит через фаервол), а не жалуется, что “кнопка не работает”.

03 Актуальность для рынка РФ

наряду с классическими решениями Cisco, Linux, Windows для демонстрации преимуществ происходит знакомство с отечественными решениями (специфика РФ): Astra Linux, Eltex, Angie.

02 Сквозная инженерная логика

программа имитирует жизненный цикл ИТ-проекта: от проектирования топологии до эксплуатации. В результате у слушателя в голове не «каша из инструментов», а четкий алгоритм: Спроектировал – Настроил сеть – Развернул Домен – Добавил СЗИ – Проверил по MITRE

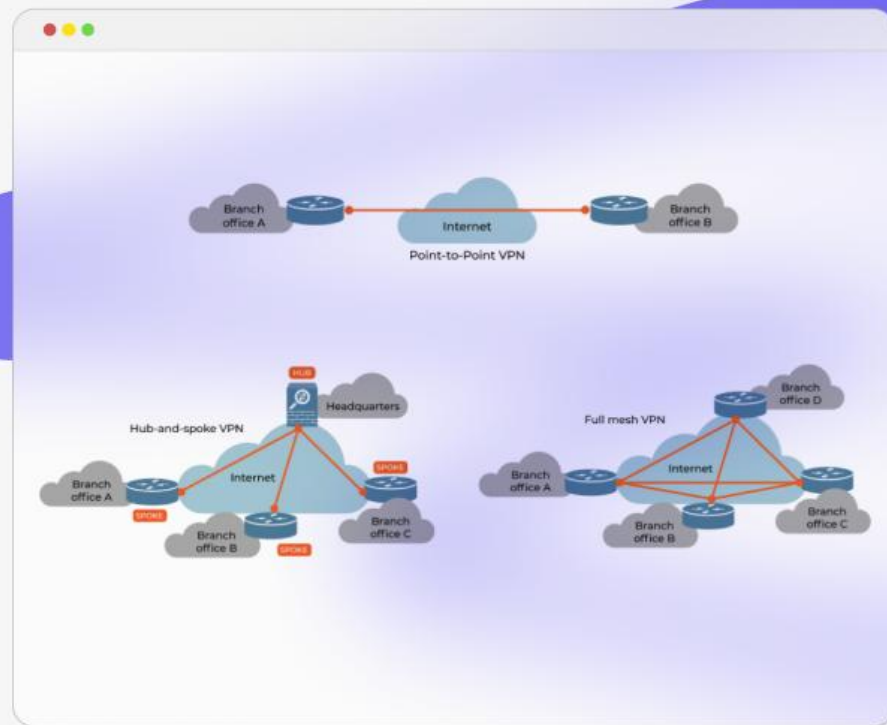
04 Классические фундаментальные технологии:

отсутствует привязка к “кнопкам”, изучается то, как работает технология \ служба. В результате конкретная имплементация какого-то вендора менее важна, так как, если ты понимаешь как работает внутри, то “кнопки” освоишь.

Многие конкуренты готовят «операторов мониторинга» (которые смотрят в экран). Мы готовим инженеров, которые этот экран (и всё, что за ним) создают, настраивают и защищают.

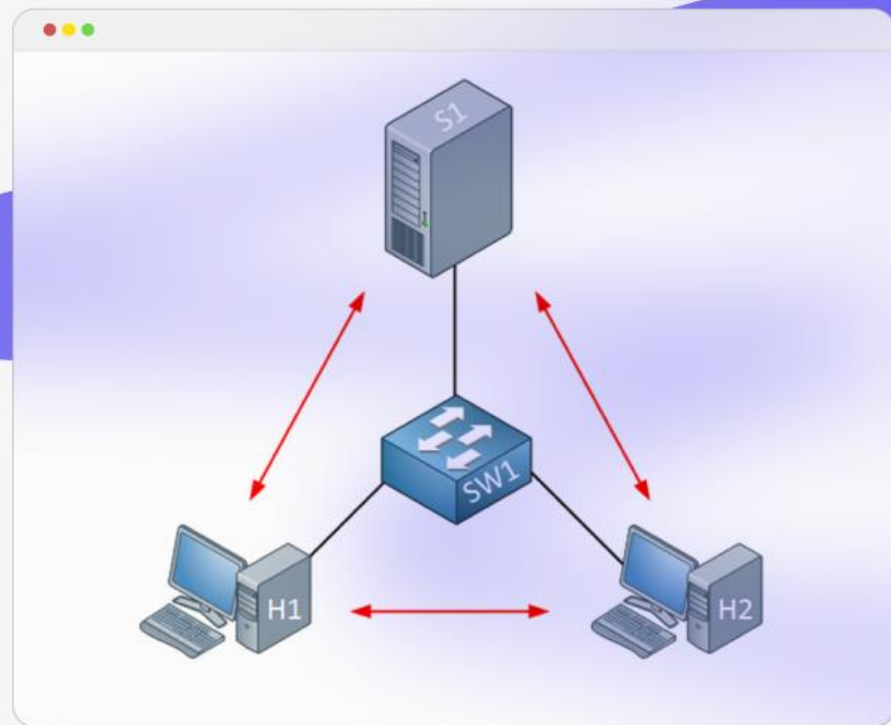
ПРАКТИЧЕСКАЯ ПРИМЕНИМОСТЬ ПРОГРАММЫ

- Спроектировал и развернул систему корпоративного VPN для безопасного объединения территориально распределенных офисов.
- Выполнил полную настройку криптографических параметров туннеля IPSEC, обеспечив конфиденциальность и целостность передаваемого трафика через публичные сети

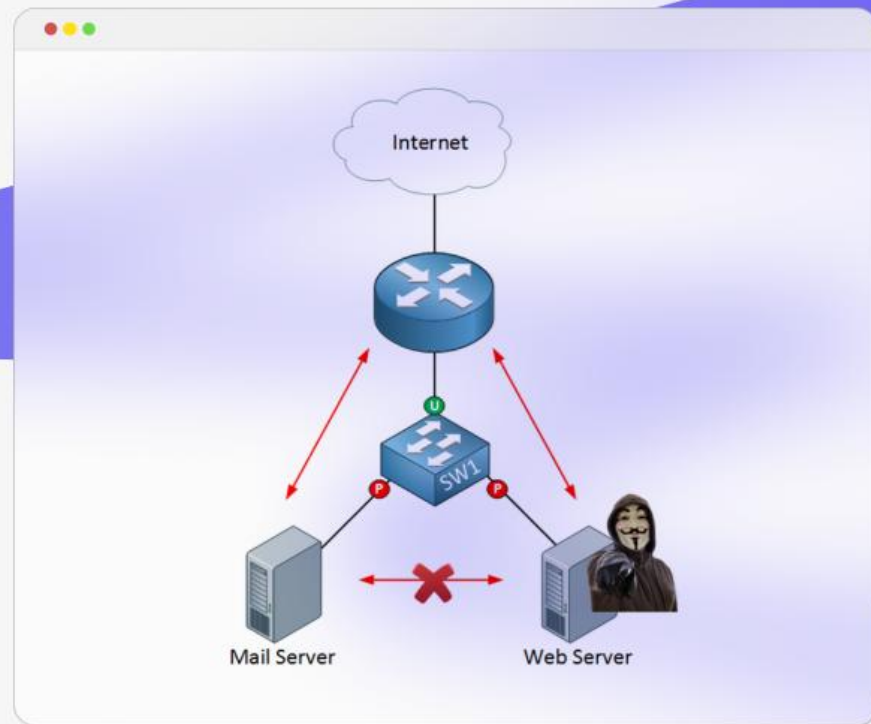
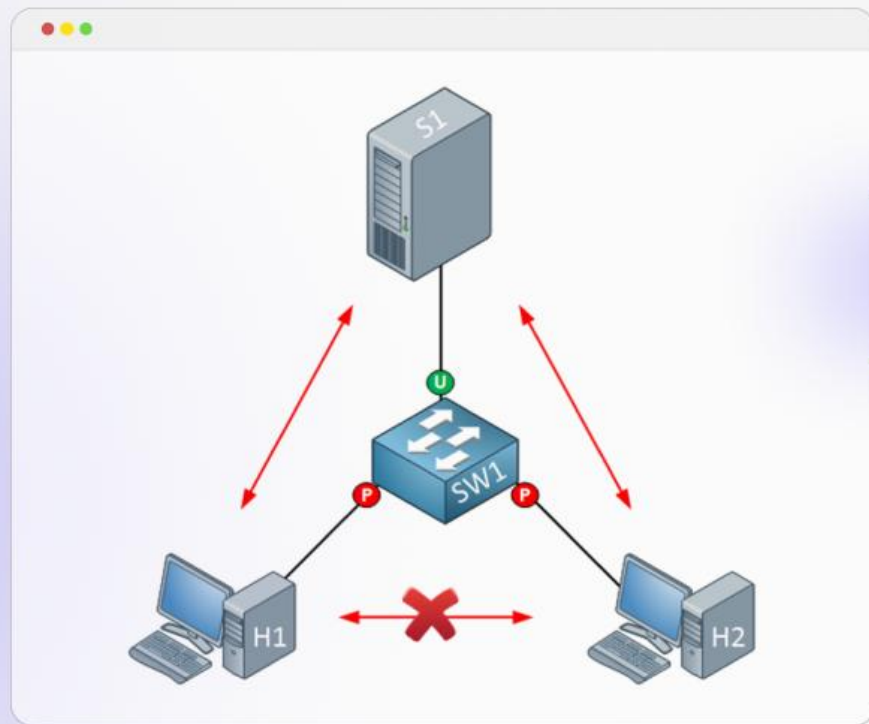


ПРАКТИЧЕСКАЯ ПРИМЕНИМОСТЬ ПРОГРАММЫ

- Спроектировал и реализовал логическую структуру сети с разделением отделов на виртуальные локальные сети (VLAN).
- Настроил протокол управления VTPv3 для синхронизации базы данных VLAN между коммутаторами, обеспечил безопасность протокола через парольную аутентификацию".



ПРАКТИЧЕСКАЯ ПРИМЕНИМОСТЬ ПРОГРАММЫ



[НОВЫЙ КУРС]

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ЗАДАЧАХ ИНЖЕНЕРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



КУРС ПОСВЯЩЁН ПРИНЦИПАМ РАБОТЫ И ПРАКТИЧЕСКОМУ ПРИМЕНЕНИЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАДАЧАХ ИНЖЕНЕРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

СОДЕРЖАНИЕ КУРСА

1. Промпт-инжиниринг для ИБ-специалистов

Точные и полезные ответы на запросы к ИИ

2. Автоматизация рутинных задач с помощью ИИ

Логи, инциденты, отчёты — делегируем ИИ

3. Облачные vs корпоративные vs локальные модели

Выбор модели под задачи и инфраструктуру

4. Безопасная работа с ИИ

Контроль доступа и защита конфиденциальных данных

5. Агенты и Model Context Protocol (MCP)

Подключение ИИ к внешним инструментам и данным

ОТЗЫВЫ ПО ПРОГРАММЕ [F402]

Лосев Александр, слушатель курса "Инженер ИБ"

Мне очень нравится обучение – много материалов полезных, преподаватель заинтересован в том, чтобы студенты усвоили материал. Так же нравится что есть поддержка в тг, где можно задать вопросы по дз и лекциям. Но хочу сказать что тем у кого нет базы будет нелегко – лекции занимают 8 часов в неделю, плюс домашние задания. Учиться нужно активно! Спасибо, что можно договориться о сдаче дз чуть позже срока. В общем обучение мне нравится, рекомендую!

Болотников Сергей, слушатель курса "Инженер ИБ"

Мне нравится формат обучения и что каждая лекция записана на видео. Очень удобно пересматривать и сразу же пробовать все то, чему обучает преподаватель.

Также поддержка при решении сложных задач. Быстро реагируют на твои трудности и помогают дойти до истины.

Павел Наседкин, слушатель курса "Инженер ИБ" Преподаватель ФГБОУ ВО ИРГУПС по направлению ИБ.

Мне 54 года, я кандидат технических наук (системный анализ, 2.3.1). И я очень рад, что академическая база находит применение в кибербезопасности. Моя цель — сразу после курса найти работу в ИБ, а в перспективе — выйти на докторскую по безопасности сложных систем

Сейчас я обучаюсь на курсе F-402 «Инженер по информационной безопасности» (группа F402-1). Уже прошли модули по основам ИБ и локальным сетям — было много практики с VLAN, ACL, VPN. Сейчас активно изучаю Linux (терминал, права, сеть, скрипты).

Преподаватель Андрей Шабалин — настоящий эксперт (CCNA, HCIP).

Курс даёт реальную инженерную базу. Рекомендую!

Юдина Евгения, слушатель курса "Инженер ИБ" Работает в сфере веб-разработки

Учусь на курсе «Инженер по ИБ», сейчас примерно в середине – заканчиваем блок по Linux. Пришла почти без базы по всем темам, поэтому могу оценить именно с позиции новичка.

Программа очень насыщенная, охватывает все необходимые темы, при этом не перегружает: домашние задания достаточно сложные чтобы хорошо подумать, где-то пересмотреть запись занятия, где-то погуглить, но не слишком сложные. Чувствуется, что курс выстроен методично и последовательно.

По содержанию – очень понравился блок по сетям, там все разобрали максимально подробно, от важных базовых вещей до интересных нюансов, которых в программе даже нет. И буквально каждую фишку в каждой теме рассматриваем с точки зрения безопасности – это именно то, чего ждешь от курса по ИБ, очень классно.

Отдельно хочу отметить преподавателя – это вообще огромный плюс курса. Объясняет увлеченно, на вопросы отвечает развернуто и в чате, и на занятиях. Уделяет много времени всем темам, все хорошенько объяснит, даже если времени потратит больше. Видно, что ему не все равно, как мы разбираемся в материале. Такой подход сильно мотивирует продолжать.

Пока мне все очень нравится.

ДАВАЙТЕ РАЗБЕРЕМ
ВАШИ
ВОПРОСЫ



НАЧНИ УЧИТЬСЯ И ПОЛУЧИ ДОПОЛНИТЕЛЬНЫЕ КУРСЫ В ПОДАРОК

CyberED

Курсы на выбор

Из направления “Пентестер”

- Исследование целей тестирования (Reconnaissance)
- Получение первичного доступа через атаки на аутентификацию (Authentication)
- Получение первичного доступа через атаки на веб-приложения (Web-applications)
- Получение первичного доступа через атаки социальной инженерии (Social Engineering)

Из направления “Аналитик SOC”

- Обнаружение атакующего на этапе работы с внешним периметром

Эти курсы бьют в самое слабое место любой инфраструктуры — внешний периметр. Вы осваиваете роль пентестера: разведка, атаки на аутентификацию, веб-приложения и социальная инженерия.

А курс по SOC-аналитике учит видеть ту же атаку с другой стороны — в логах, событиях и системах мониторинга. Таким образом, вы получаете двойную оптику: знаете, как проникают, как это заметить и как защититься до того, как атака состоится.



[ДЛ Я УЧАСТНИКОВ ВЕБИНАРА]

ТОЛЬКО ДО 30 ИЮНЯ

Инженер по информационной безопасности

Обычная цена 143 900 Р

за 115 000 рублей

Скидка 20 %

**Инженер по информационной безопасности +
3 мини-курса**

за 129 500 рублей

Уже со скидкой 10%

