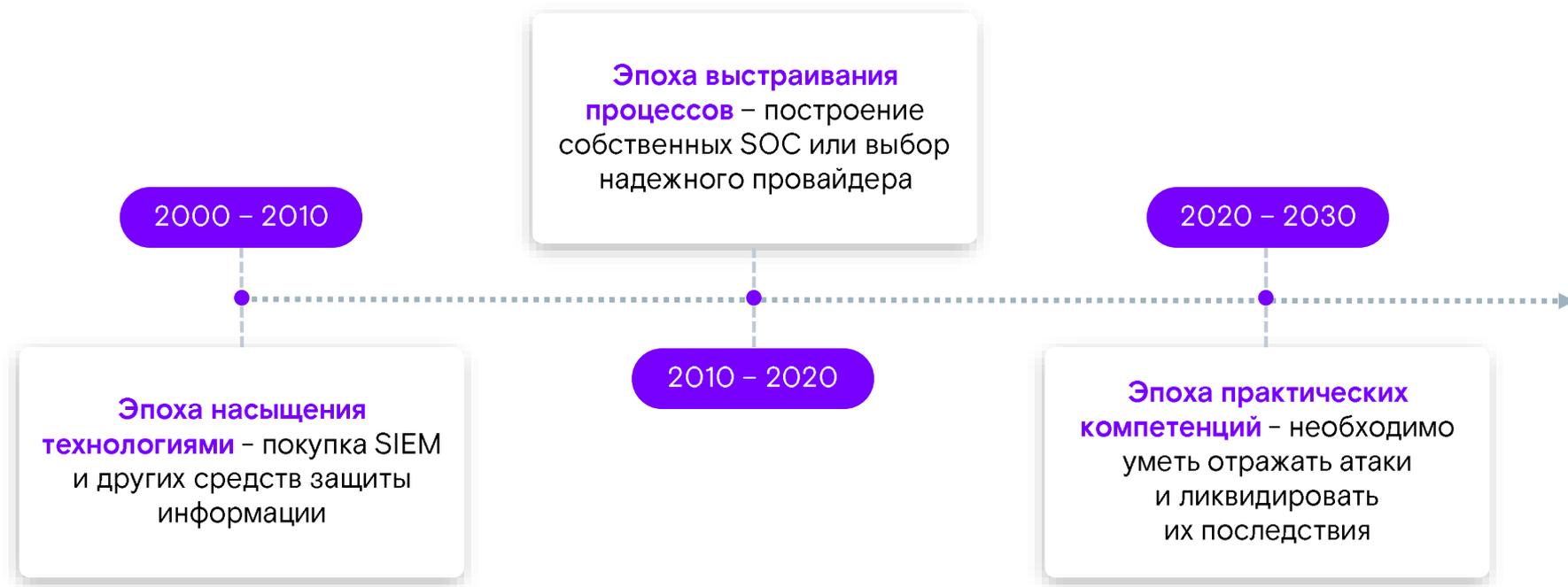


Успешная команда ИБ: как создать и развить высококвалифицированных профессионалов в области ИБ

Андрей Кузнецов, технический директор
Татьяна Кукарцева, аналитик-методолог
Национальной киберполигон, «Ростелеком-Солар»

Код ИБ, Красноярск
23 марта 2023 г.

Новый тренд в области кибербезопасности – фокус на повышение квалификации персонала



Типовые проблемы эпохи практических компетенций и их решение

1

Нехватка ИБ-персонала

Помощь в создании кадрового резерва службы ИБ внутри компании за счет непрерывного обучения практическим навыкам

2

Недостаточный уровень квалификации

Проверка навыков сотрудников информационной безопасности и повышение их квалификации за счет практической отработки на киберполигоне

3

Отсутствие практических навыков

Возможность эмулировать реальную атаку на киберполигоне с целью «своими руками» отработать процесс реагирования на инцидент

4

Отсутствие слаженности команд

Отработка планов реагирования и ликвидации последствий киберинцидентов за счет слаженности действий работы разных подразделений компании

5

Низкая скорость принятия решений

Предупреждающая проработка возможных векторов развития событий для оперативного реагирования на киберинциденты

6

Появление новых продуктов на рынке

Практическое обучение работе с новыми ИБ-продуктами с возможностью тестирования их взаимодействия с внедренными ИТ- и ИБ-решениями

Продукты киберполигона от «Ростелеком-Солар»

Киберучения

- Командно-штабные тренировки, направленные на теоретическую отработку сценариев реагирования
- Практические киберучения для проверки навыков защиты от киберугроз для технических специалистов
- Полномасштабные киберучения, сочетающие командно-штабные тренировки и практическую часть

Киберобразование

- Обучение и профессиональная подготовка по кибербезопасности с отработкой практических навыков

Киберучения

Сценарии проведения киберучений

1

Теория

Отработка сценариев реагирования на инциденты ИБ для всей компании

2

Практика

Оценка компетенций и навыков сотрудников службы ИБ

3

Улучшение

Повышение компетенций и отработка практических навыков специалистов службы ИБ

4

Развитие

Разработка программы развития сотрудников службы ИБ в компании

5

Тестирование

Тестирование при приеме на работу

Участники киберучений:

- ТОП-менеджеры компании
- Руководители ИТ- и ИБ- подразделений
- Сотрудники службы ИБ
- Сотрудники службы ИТ
- Эксперты АСУ ТП
- DevSecOps-эксперты
- Эксперты SOC
- Пентестеры

Варианты киберучений

Командно-штабные тренировки, направленные на теоретическую отработку сценариев реагирования

- Отслеживание правильности существующих процессов
- Выстраивание взаимодействия между смежными командами внутри компании
- Проверка существующих регламентов реагирования

Практические киберучения для улучшения навыков защиты от киберугроз для технических специалистов

- Проверка знаний участников киберучений по матрице MITRE ATT&CK
- Повышение компетенций сотрудников
- Разработка плана обучения сотрудника

Типы киберучений

- Стандартные киберучения на типовой учебной инфраструктуре с готовыми сценариями
- Кастомные киберучения с вариативностью СЗИ, инфраструктуры и сценариев

Полномасштабные киберучения, сочетающие командно-штабные тренировки с практической частью

Два этапа

- Командно-штабные тренировки, направленные на теоретическую отработку сценариев реагирования
- Практические киберучения для улучшения навыков защиты от киберугроз для технических специалистов

Примеры проведенных киберучений



Киберучения на SOC-Форуме



Командно-штабные тренировки для ТЭК



Red Team vs Blue Team на SOC-Форуме



Отраслевые практические киберучения



Полномасштабные киберучения



Скоринг результатов киберучений

Реализованный кейс.

Кастомные практические киберучения

Трубная металлургическая компания

Практические киберучения для улучшения навыков защиты от киберугроз для технических специалистов

Что было сделано:

- Проведение киберучений в течение 3 дней в офлайн формате
- Застройка площадки для проведения киберучений
- Кастомизированная для заказчика инфраструктура
- Отраслевые сценарии проведения киберучений
- Оценка работы и действий ИТ- и ИБ-подразделений в ходе киберучений
- Совместная отработка обнаружения и реагирования на атаки
- Составление индивидуальных рекомендаций для повышения навыков сотрудников

Результат киберучений:

- Обучены специалисты ИБ и ИТ
- Отработаны практические навыки обнаружения, реагирования и восстановления после атак
- Составлен план развития каждого сотрудника

Подробнее: <https://rt-solar.ru/events/news/2385/>

Реализованный кейс.

Стандартные практические киберучения

Региональные организации

Практические киберучения для улучшения навыков защиты от киберугроз для технических специалистов

Что было сделано:

- Проведение киберучений в течение 2 дней в онлайн-формате
 - Стандартная инфраструктура
 - Стандартные сценарии проведения киберучений
 - Оценка работы и действий ИТ- и ИБ-подразделений в ходе киберучений
 - Совместная отработка обнаружения и реагирования на атаки
 - Составление рекомендаций для ИТ- и ИБ-подразделений
-

Результат киберучений:

- Обучены специалисты ИБ и ИТ
- Отработаны практические навыки обнаружения, реагирования и восстановления после атак
- Составлен план развития ИТ- и ИБ-подразделений

Киберобразование

Варианты образовательных курсов

Практико-ориентированный учебный центр с отработкой навыков

Получение начальных знаний в области ИБ

Интенсивная программа обучения основам кибербезопасности Cyber Boost

- Интенсивная программа от 6 до 9 дней непрерывного обучения
- Теоретические и практические модули

Обучение для исследователей уязвимостей

Комплексная программа подготовки «Исследователь уязвимостей с нуля»

- Программа из 5 курсов для отработки навыков в практической безопасности
- Теоретические и практические модули

Переподготовка ответственных за ИБ

Программа «Указ 250»

- Программа для госслужащих (512 час.)
- Программа для сотрудников коммерческих компаний (360 час.)

Обучение пользователей ИБ-продуктов

Обучение по ИБ-продуктам с возможностью проверить работу СЗИ на киберполигоне

- Обучение по продуктам «Ростелеком-Солар»
- Обучение по продуктам российских вендоров по кибербезопасности

Реализованный кейс. Интенсив по кибербезопасности в Минске

Национальный центр обмена трафиком

Проведение интенсива по кибербезопасности CyberBoost

Что было сделано:

- Срок проведения – 6 рабочих дней
- Проведение интенсива Cyber Boost в офлайн-формате на площадке заказчика
- Программа состояла из 9 модулей, включая теорию, лабораторные работы и проведение финальных киберучений
- Темы интенсива от защиты инфраструктуры до реагирования на типовые хакерские атаки

Результат проекта:

- Обучено более 20 представителей белорусских компаний

Подробнее: <https://rt-solar.ru/events/news/3339/>

Не знаешь где взять квалифицированного
специалиста, так вырасти его сам!

Как воспитывать кадры со студенческой скамьи?

Делимся опытом:)



Начинать подбор с 2 и 3 курса

1

ВУЗы и кафедры ИБ

2

Стажировки

ВУЗЫ и кафедры ИБ



СибГУ им. М.Ф. Решетнева



СИБИРСКИЙ
ФЕДЕРАЛЬНЫЙ
УНИВЕРСИТЕТ

SIBERIAN
FEDERAL
UNIVERSITY

Проводить лекции про
компанию

Собеседования

Узнавать про программу
обучения

Заключать партнерство с
ВУЗами

Стажировки

«Не знаешь где взять квалифицированного специалиста, так вырасти его сам!»

Неизвестный автор



Показывать горизонты будущего

Построить программу стажировки в соответствии потребностями компании



Центральный офис

**125009, Москва, Никитский
переулок, 7с1**

+7 (499) 755-07-70
cybermir@rt-solar.ru

