



Как вовлечь бизнес в обучение и прокачать навыки сотрудников в киберзащите

Леонид Петров

Positive Education

**«Большинство инцидентов
происходят из-за человеческого
фактора. Мы вкладываем
миллионы в технологии,
но забываем про знания»**



Недостаточно внедрить СЗИ — необходимо
обучать сотрудников пользоваться
внедренными инструментами

Дефицит компетенций



Ежегодно компании сталкиваются с дефицитом специалистов по ИТ и ИБ. Спрос на них продолжает расти, при этом уровень квалификации многих остается недостаточным

на 26%

увеличилось число
вакансий ИБ в 2025
году

в 1,3 раза

спрос на специалистов по
ИБ опережает их приток



Актуальные тренды



В последние годы работодатели из ИТ-сферы сместили фокус найма с junior- на middle- и senior-специалистов. В 2026 году рынок ИБ подхватывает этот тренд



Фокус найма
смещается на
специалистов
с опытом в ИБ от трех
лет



Укрепляются
требования к кросс-
функциональному
опыту



Растет важность
практико-
ориентированной
подготовки кадров

Что важно для каждой роли



CISO, CIO, CTO

Фокус:

управление рисками и защита компании

Что важно:

- Выстраивать стратегию безопасности с учетом бизнес-приоритетов
- Обосновывать бюджеты для руководства
- Вести управление инцидентами и координировать ответственные подразделения

Команды ИБ и ИТ

Фокус:

реализация и поддержка технологий

Что важно:

- Практические навыки реагирования на инциденты
- Интеграция решений (DevSecOps, настройка защиты)
- Совместная работа команд ИТ и ИБ без конфликтов

Что важно для каждой роли



Топ-менеджеры (CEO, CFO и др.)

Фокус:

стратегические решения и инвестиции

Что важно:

- Понимать, как киберриски влияют на бизнес-модели и финансы
- Принимать решения на основе данных: во что инвестировать, чтобы минимизировать ущерб
- Оценивать эффективность вложений в ИБ на уровне бизнеса

HR

Фокус:

культура безопасности и вовлечение сотрудников

Что важно:

- Встраивание обучения в адаптацию и регулярные процессы
- Форматы, которые вовлекают: микрообучение, геймификация
- KPI по обучению: не просто пройти курс, а изменить поведение сотрудников

Наш подход — не универсальный ключ



Программы, закрывающие
потребности каждой роли



Практико-
ориентированные курсы
для профильных
сотрудников



Опыт экспертов Positive
Technologies



Security awareness

Основа устойчивости компании к киберинцидентам

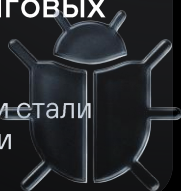
HR

pt

72%

рост числа фишинговых атак

Благодаря ИИ рассылки стали персонализированными и правдоподобными



79%

фишинговых сообщений

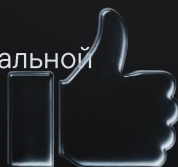
маскировались под финансовую и кадровую документацию



60%

успешных атак

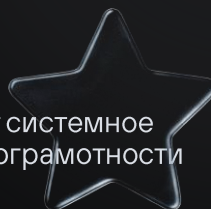
происходят из-за социальной инженерии



48%

компаний

не обеспечивают системное повышение киберграмотности сотрудников



Сотрудник — главное звено в защите организации

Курсы по эксплуатации продуктов Positive Technologies



CISO

NEW



Применение MaxPatrol VM
в процессе управления
уязвимостями



Миграция на PT NGFW:
полное руководство



Защита конечных устройств
с MaxPatrol EDR



MaxPatrol SIEM:
от настройки до
расследования инцидентов



Защита веб-приложений
на базе PT AF PRO



Обнаружение
кибератак
в трафике при
помощи
PT NAD



Возможности PT Sandbox:
от настройки до
интеграций

Программы повышения компетенций специалистов

CIO, CISO

pt

Мы не обучаем отдельным навыкам, а показываем, как построить процессы и подходы, которые делают защиту системной и управляемой

Построение и мониторинг защищенной сети

Практикумы:

- «Архитектура сетевой безопасности» 17.08
- «Анализ сетевого трафика: искусство обнаружения атак» 05.10

Повышение защищенности промышленных предприятий

Практикум «Предотвращение атак на АСУ ТП» 20.04

Построение системного процесса управления уязвимостями

Практикум «Управление уязвимостями: от теории к практике» 25.05

Повышение защищенности инфраструктуры

Практикум «Харденинг ИТ-инфраструктуры: от дизайна до настроек» 09.11

Внедрение подхода безопасной разработки в ИТ-процессы

- Практикум «Безопасность приложений: курс для инженеров» 07.09

Создание зрелой и устойчивой SOC-функции

Практикумы:

- «Мониторинг и реагирование на инциденты» 28.09
- «Построение SOC 2.0: от концепции до реализации» 14.09

Программы для команд ИТ и ИБ

СІО, СІSO

pt

Все программы сформированы на основе опыта экспертов Positive Technologies и гибко подстраиваются под бизнес-задачи организации

Задачи, которые мы поможем решить

- Устранить разрыв между знаниями и действиями в критически опасных ситуациях
- Выстроить понимание между подразделениями ИТ и ИБ
- Сформировать единую систему взаимодействия между подразделениями

Программы

- «Архитектура и защита корпоративной инфраструктуры и сети»
- «Харденинг ИТ: от дизайна до настроек»
- «Мониторинг и реагирование на инциденты для команд ИБ и ИТ»
- «Безопасная разработка: внедрение практик»

Платформа развития практических навыков

СІО, СІSO

pt

Платформа для интенсивной подготовки специалистов по ИБ. Сочетает практику на реальных кейсах с автоматизированным контролем прогресса на основе тренажера PT EdTechLab и онлайн-симулятора Standoff Cyberbones

Объективная оценка уровня подготовки команды

Встроенная статистика по решению кейсов и прохождению обучения

Результат: прозрачная картина компетенций, понятные зоны роста

Непрерывное развитие специалистов по ИБ

Три уровня сложности для отработки навыков: low, medium, hard

Результат: уровень готовности к атакам стабильно высокий

Отработка навыков на реальных сценариях атак

Более 80 кейсов для команд ИБ

Результат: команда быстрее выявляет и предотвращает атаки

Глубинное понимание формирования атак

В сценарии заложены навыки для red team

Результат: специалисты понимают не только то, как распознавать кибератаки, но и то, как развиваются векторы

Адаптация под задачи бизнеса

Модульная архитектура позволяет собирать тренажер под нужды компании

Результат: обучение релевантно профилю угроз и задачам компании

Автономный процесс обучения

Ментор не нужен, кейсы всегда запущены, автоматическая проверка результатов

Результат: минимизация времени и затрат на организацию обучения

CISO 3.0: путь от эксперта к управленцу

CISO, CIO, CTO



Программа поможет сделать кибербезопасность стратегической функцией, критически важной для устойчивости бизнеса

- > Старт: март 2027
- > Длительность: шесть недель
- > Для кого:
 - CISO, CIO, CTO
 - Тимлиды и руководители направлений в области ИТ и ИБ
- > Состав программы:
 - **Модуль 1.** Кибербезопасность и бизнес: стратегическая функция и результаты
 - **Модуль 2.** Бизнес-мышление и бизнес
 - **Модуль 3.** Организационный дизайн и управление изменениями

Что получают участники

- Переосмыслят роль кибербезопасности в компании, научатся формировать **значимый для бизнеса результат** и поймут способы его достижения
- Разберутся в моделях управления компанией, научатся разрабатывать стратегии **на основе бизнес-показателей**
- Научатся вести **диалог с бизнесом**, стейкхолдерами и командой
- Смогут **под разным углом** взглянуть на технологические компании и их подходы к развитию бизнеса

Программы для топ-менеджмента

CEO/CIO/CISO



Как повысить уровень устойчивости к кибератакам и не допустить нанесения ущерба

Трек 1

Личная и корпоративная
кибербезопасность: как
защитить себя, семью
и сотрудников

Трек 2

Киберсоревнования для
специалистов по ИБ

**Трансформация
подходов к
защите
организации**

Фокус на комплексе



Мы выстраиваем **обучение как систему**: от стратегических решений топ-менеджмента до повседневного поведения сотрудников. Это помогает внедрять безопасность в бизнес-процессы на всех уровнях



Обучение топ-менеджмента и руководителей

Погружение в кибербезопасность и повышение осведомленности о ключевых аспектах киберугроз, выработка стратегии управления для обеспечения безопасности на уровне компании

Профильное обучение команд ИБ и ИТ

Углубленное изучение методов защиты и повышения уровня киберустойчивости с фокусом на практику, современные подходы и выстраивание результативной кибербезопасности

Обучение сотрудников основам кибербезопасности

Повышение уровня киберграмотности, рекомендации по настройке параметров рабочих устройств, чек-листы для проверки своей защищенности и инструкции, как действовать в случае киберугроз

Дальнейшие шаги



1

Сформулируйте цели обучения

Определите внутри команды приоритеты, роли, направления обучения

2

Обратитесь к нам

Мы поможем подобрать формат обучения под ваши цели

3

Пройдите обучение

Мы обучим вашу команду в формате, который не мешает бизнес-процессам компании

Описание программ на сайте



edu.ptsecurity.com

Задай
вопрос
спикеру



Спасибо!



Леонид Петров

Менеджер по работе
с ключевыми клиентами Positive
Education



LPetrov@ptsecurity.com



+7 985 704 81 41



edu.ptsecurity.com