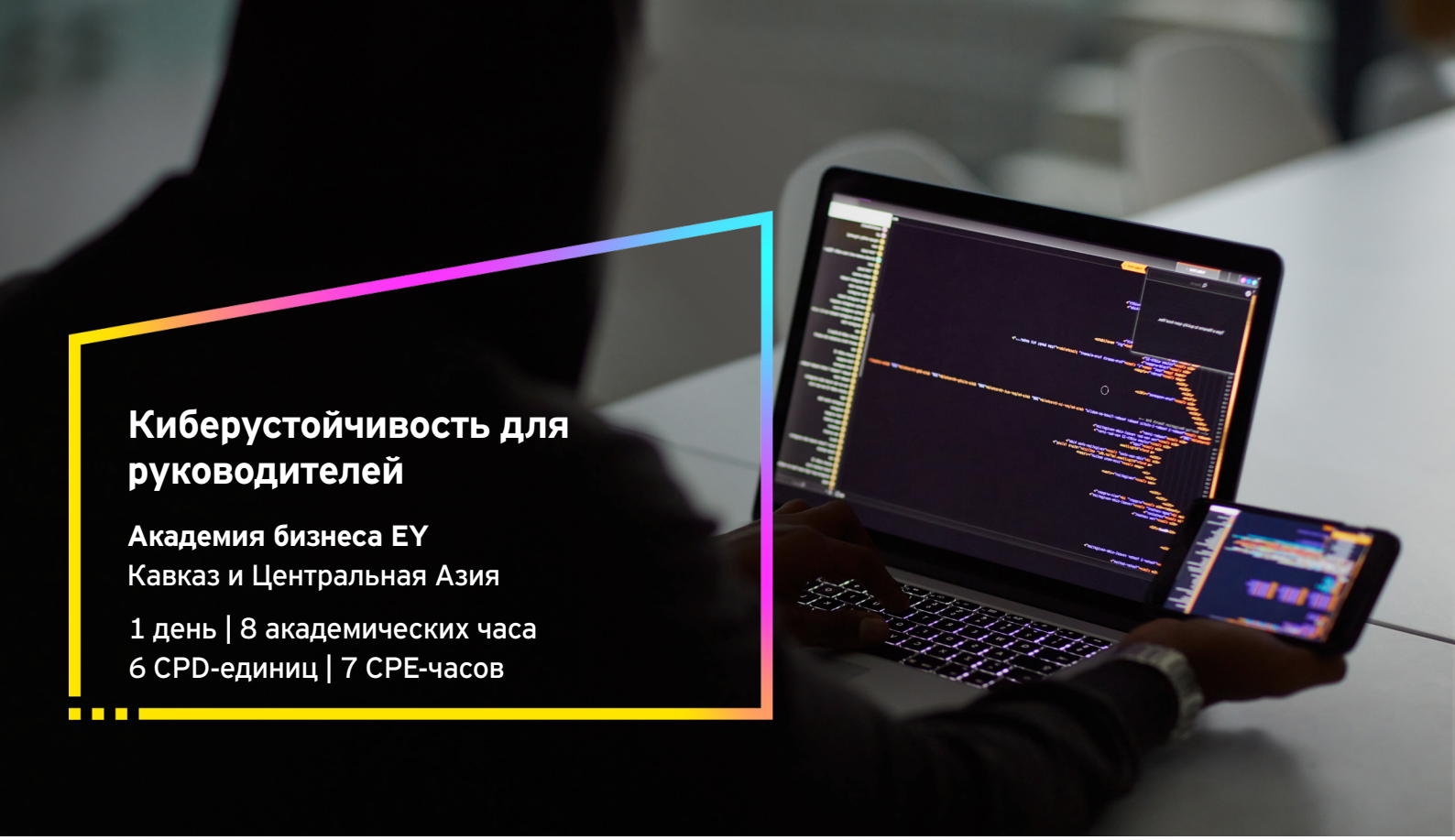

Киберустойчивость для руководителей

Академия бизнеса EY
Кавказ и Центральная Азия

1 день | 8 академических часа
6 CPD-единиц | 7 CPE-часов

Программа тренинга

Ландшафт киберрисков

- Эволюция киберугроз: как атаки смещаются с IT-инфраструктуры на людей, концепция Human-as-a-Vector, почему человеческий фактор становится критическим риском для бизнеса
- Социальная инженерия и манипуляции: распознавание Spear Phishing и других способов обмана сотрудников, влияние на бизнес-процессы и управленческие решения
- Публичная информация и OSINT: какие данные о компании и сотрудниках могут быть использованы злоумышленниками и как это отражается на стратегических рисках
- Риски третьих лиц (Third-Party Risks): как уязвимости подрядчиков, партнеров и цепи поставок (Supply Chain) влияют на безопасность основной компании

Продвинутые векторы атак

- Компрометация переписки (BEC & VEC): признаки атак, направленных на финансовое мошенничество, влияние на операционную деятельность и принятие решений руководителем
- GenAI и синтетические угрозы: Deepfakes и поддельные документы глазами бизнеса, оценка рисков для корпоративных процессов
- Риски Shadow AI: влияние публичных нейросетей и генеративного контента на конфиденциальность корпоративной информации, базовые меры защиты

Практическая часть

- Анализ стратегического кейса: оценка рисков и последствий киберинцидента для бизнеса
- Кризисная симуляция: принятие решений, разработка коммуникаций и защита выбранной стратегии

Операционная киберустойчивость и экономика ИБ

- Оценка операционных киберрисков: критичные процессы, данные и каналы коммуникаций. Анализ угроз критического уровня (Ransomware/шифровальщики, деструктивные атаки) и их последствия для непрерывности бизнеса
- Современные концепции защиты: на примере архитектуры Zero Trust – поиск баланса между требованиями безопасности и эффективностью бизнеса, влияние защитных мер на операционную гибкость и продуктивность сотрудников
- Экономика кибербезопасности: оценка эффективности инвестиций в защиту, метрики защищенности и выстраивание прозрачного, конструктивного диалога между бизнесом и функцией информационной безопасности (CISO)
- Правовой контекст и комплаенс: регуляторные требования, защита персональных данных и корпоративная ответственность первых лиц за последствия инцидентов

Протоколы реагирования и кризисное управление

- Первый час после инцидента (Golden hour): определение приоритетов действий, координация бизнес-подразделений и IT-функции
- Кризисные коммуникации и правовое реагирование (Crisis PR & Legal): управление репутационными рисками, стратегии информирования клиентов, СМИ и регуляторов, юридическое сопровождение инцидентов
- Учимся на ошибках: выявление уязвимостей в корпоративных процедурах (Lessons Learned), формирование управленческой отчетности и адаптация процессов

Цели обучения

- Понимать как киберинциденты влияют на бизнес-решения, финансовые показатели, репутацию и непрерывность операций
- Применять управленческие критерии для распознавания подозрительных коммуникаций, документов и цифровых сигналов
- Анализировать слабые места в процессах, каналах коммуникации и цепочках принятия решений, которые могут усилить последствия киберинцидента
- Оценивать варианты реагирования и меры защиты с точки зрения риска, стоимости, скорости восстановления и влияния на бизнес
- Применять полученные знания при разборе реальных бизнес-кейсов и моделировании киберинцидентов

Подробнее

Что вы получите в результате обучения

- Понимание влияния киберинцидентов на бизнес-решения, финансовые показатели, репутацию и непрерывность деятельности компании
- Практический опыт оценки вариантов реагирования и мер защиты с точки зрения рисков, стоимости, скорости восстановления и влияния на бизнес
- Практический опыт принятия управленческих решений в условиях хаоса при ограниченном времени, неполной информации и меняющихся вводных
- Навыки разработки кризисных коммуникаций для сотрудников, клиентов, партнеров, СМИ и регуляторов
- Понимание алгоритма действий в первые часы киберинцидента и при последующем восстановлении бизнеса
- Материалы тренинга в электронном виде
- Профессиональные рекомендации тренера-эксперта
- Сертификат Академии бизнеса EY

Как проходит обучение

- Обучение построено вокруг практических бизнес-ситуаций и Management Simulation. Участники работают с кейсами, в которых нет единственно правильного решения, и оценивают последствия своих решений для бизнеса
- Участники определяют критичный бизнес-процесс или управленческую проблему, анализируют вводные по киберинциденту, выявляют риски и оценивают возможные последствия для бизнеса

Тренеры

Тренинг проводит команда бизнес-тренеров Академии бизнеса EY. Тренеры обладают богатым практическим опытом, а также международными квалификациями ACCA, ACCA DipIFR(Rus), CFA®, CIA®, CIMA®, DipIPSAS, IPMA®, MBA, MBTI®, PMP® и др.

Запросить CV тренера и задать вопросы о тренинге: academy@kz.ey.com

Для кого этот тренинг

- Руководители всех уровней, принимающие решения по рискам
- Лидеры функций: финансы, юриспруденция, HR, закупки, маркетинг
- Владельцы бизнеса и ключевые лица, влияющие на стратегические решения
- Команды, заинтересованные в киберустойчивости и снижении операционных и репутационных рисков

Форматы участия

Для участия необходим ноутбук

Открытый формат

Тренинг проводится по расписанию Академии бизнеса EY с 10:00 до 17:00 с перерывом на обед и двумя кофе-брейками.

Корпоративный формат

Программа может быть адаптирована и проведена специально для Вашей компании.

- Предварительный анализ потребностей в обучении, определение целей и задач
- Гибкий подход к выбору места, сроков и времени проведения тренингов
- Адаптация тренинга с учетом отраслевой специфики
- Отчет о результатах обучения по запросу клиента

EY Shape the future with confidence