КОД ИБ

ИТОГИ

БЕЗОПАСНОСТЬ ЧЕРЕЗ ДОВЕРИЕ: КУЛЬТУРА КАК ПЕРВАЯ ЛИНИЯ ЗАЩИТЫ

АНТОН ТЕРЕШОНКОВ
CSO
RIS group

КОД ИБ

ИТОГИ

Цифры, которые должны заставить задуматься:

Кибератак в России (2025)
105K+
+46% за год | Пик август: 17K
(Red Security SOC)

50%+ атак используют социальную инженерию
(Positive Technologies)

Ущерб от человеческого фактора
60%
(Allianz Risk Barometer)

КОД ИБ

ИТОГИ

Две модели построения культуры безопасности:

Модель контроля

Сотрудники — потенциальная угроза

Жёсткие ограничения и запреты

Страх наказания

Скрытие инцидентов

Низкая вовлечённость

Реактивная позиция функции ИБ

Модель доверия

Сотрудники — первая линия защиты

Обучение и поддержка

Открытая коммуникация

Быстрое реагирование

Высокая вовлечённость

Проактивная позиция функции ИБ

КОД ИБ

ИТОГИ

В ряде инцидентов такой подход существенно сокращает время реакции:

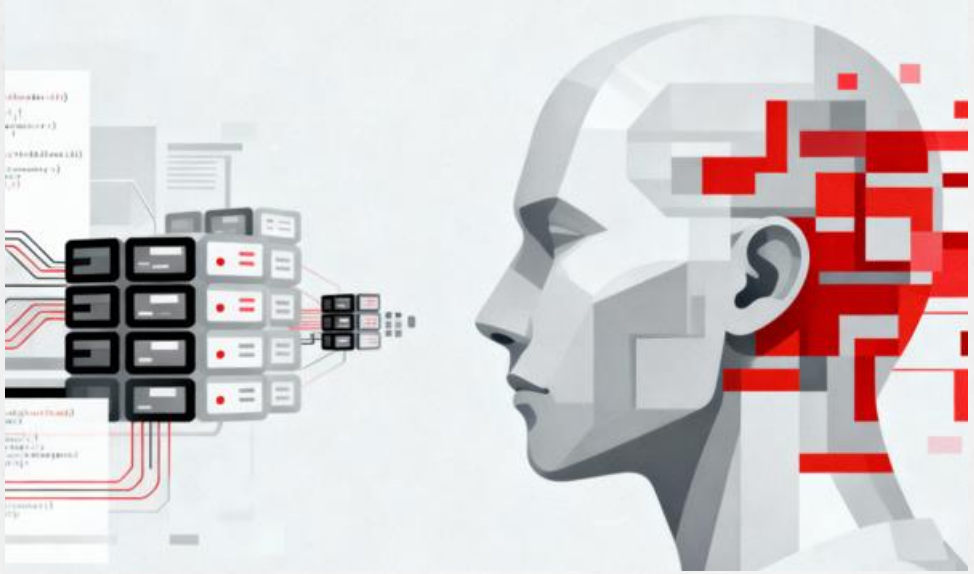
Автоматика SOC

10-15

минут

Среднее время от возникновения угрозы до алерта аналитику.

Атакующий получил начальный доступ



Обученные люди

5

минут

Время от начала очевидной подозрительной активности до обращения в ИБ

Инцидент заблокирован на входе

КОД ИБ

ИТОГИ

Культура команды обеспечения защиты и реагирования:

- Осознание факта, что при данной модели культуры безопасности в компании полный ZeroTrust не возможен
- Основной уклон на скорость реагирования, не забываем и о проактивности, но…
- SaaS в сочетании с MSSP, фокус на синергию с подрядчиком при четком SLA для управления ожиданиями
- Учить, лечить, но не мочить
- Благодарить обратившегося, с чем бы он не обратился. Только так будет поддерживаться принцип «открытой двери»

*Если компания относится к КИИ или основа бизнес-процессов работа с ЗГТ – увы, это не про Вас

КОД ИБ

ИТОГИ

Люди

Социальная инженерия
Фишинг
Ошибки и халатность сотрудников
Инсайдеры (намеренные и ненамеренные)
Невежество о политиках безопасности
Перегрузка информацией (информационная усталость)
Неправильное обращение с учётными данными
Использование слабых паролей

Процессы

Нарушения бизнес-процессов
Отсутствие понимания назначения процедур
Обход «неудобных» элементов процессов
Слабое разделение ответственности и доступа
Недокументированные процедуры
Отсутствие процедур инцидент-менеджмента
Неправильное управление жизненным циклом доступа

Технологии

Технические уязвимости (известные и неизвестные)
APT
Слабое шифрование или его отсутствие
Устаревшее ПО и оборудование
Неправильная конфигурация систем
Отсутствие сегментации сети
Слабые механизмы аутентификации
Отсутствие резервного копирования и восстановления

Реальность распределения рисков

КОД ИБ

ИТОГИ

История «До»

Страх
Сотрудники боялись сообщать об ошибках или подозрительных действиях, опасаясь наказания

Незнание
Низкая осведомлённость о современных угрозах. Формальные тренинги раз в год не работали и
забывались через неделю

Дистанция
Безопасность компании воспринималась как неясный процесс, ИБ как «надзорный орган», а не партнеры в общем деле

Факт: Инциденты обнаруживались поздно, расследования затягивались

КОД ИБ

ИТОГИ

Реальность рынка

ИИ-генерируемый фишинг становится неотличим от реальных писем

Дефицит специалистов ИБ — автоматика не справляется одна

Средний ущерб от одного инцидента растёт

Усиливаются санкции со стороны регуляторoа за инциденты связанные с утечками данных

Традиционный подход больше не работает

Больше технологий ≠ больше защиты

Формальные тренинги раз в год неэффективны

«Карательная» модель функции безопасности создаёт культуру замалчивания

«Безопасность с человеческим лицом»

Инвестиции в культуру и доверие как технологическое преимущество.

Люди не проблема — они решение.

КОД ИБ

ИТОГИ

Решение 1: Принцип открытой двери

Любой сотрудник может обратиться в службу ИБ в любое время
Никаких наказаний за "глупые вопросы" или ложные тревоги
Помощь, а не допрос
Анонимность гарантирована при необходимости

«Лучше 100 ложных тревог, чем один пропущенный инцидент,

До: 5 обращений/месяц, 20% — реальные угрозы
После: 20-25 обращений/месяц, 85% — реальные угрозы
Логика: больше сигналов, но выше качество

Результат: в 3 раза выросло количество обращений от сотрудников. Большинство — реальные угрозы.

КОД ИБ

ИТОГИ

Решение 2: Геймификация. Соревнования и вовлечённость

Ежеквартальные чемпионаты

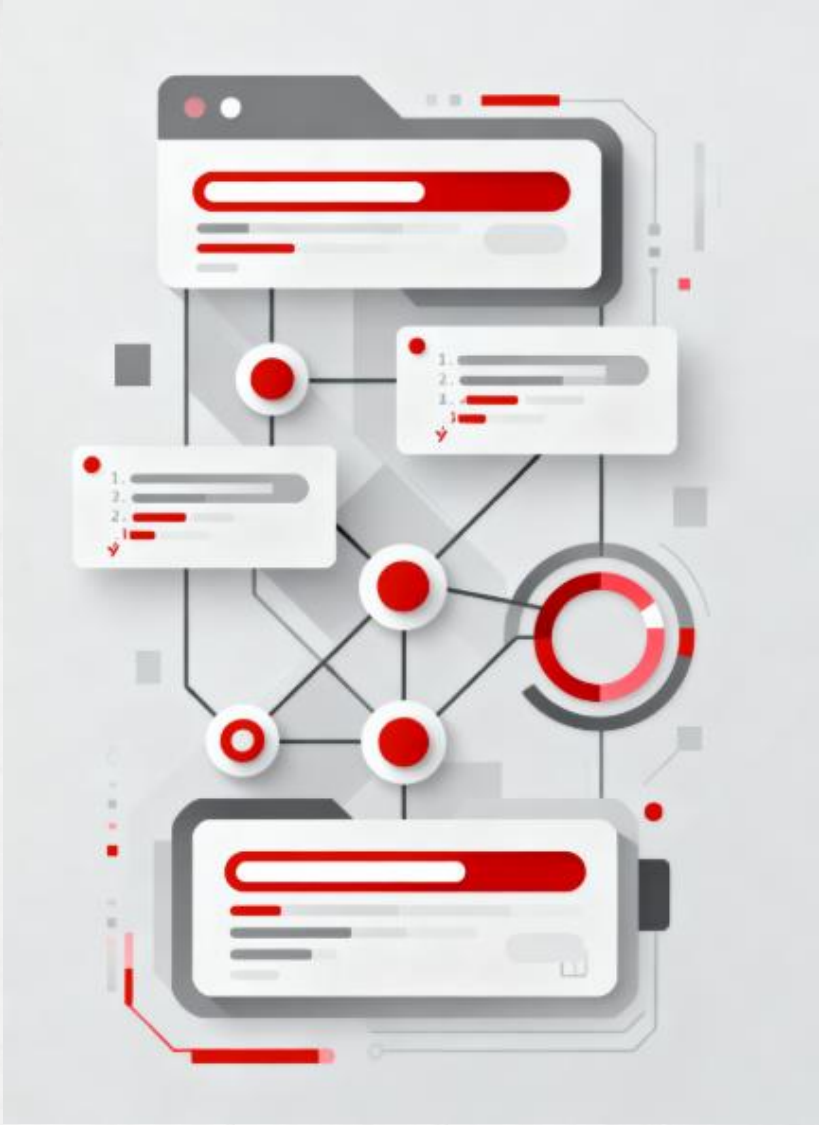
Соревнования между отделами: кто быстрее обнаружит учебные фишинговые письма, подозрительные файлы. Реальные призы.

Security Feedback Loop

Сервис получения обратной связи от сотрудников на прямую. ИБ не только слушает но и действует. Сотрудник получает ОС. Это создаёт доверие и открытость.

Рейтинги и достижения

Публичные дашборды с анонимизированными результатами. Здоровая конкуренция без стыда.



Эффект: Из рутинной обязанности безопасность превратилась в общую цель и объект интереса сотрудников.

КОД ИБ

ИТОГИ

Решение 3: Прозрачность, открытость процессов
СЗИ и информация.
Компания объясняет, какие данные как классифицируются, и почему их нужно защищать.
Сотрудники не враги системы, а её участники. Система не шпионит за личной жизнью, а:

- Фиксирует перемещение «бизнес-информации» — документы, которые имеют статус «конфиденциально/для служебного пользования/коммерческая тайна» и этот статус согласован со всеми отделами.
- Предупреждает об ошибках: если сотрудник случайно отправит конфиденциальные данные на личный email, система заблокирует и предупредит
- Безопасность избегает дисциплинарной работы, все риски митигируются по средствам изменения процессов
- Безопасность и HR работают вместе, чтобы обеспечить справедливость и отсутствие злоупотреблений

Security Day — ежеквартально
Открытая встреча всей компании. Отчёты о инцидентах новые угрозы, статистика, Q&A сессия «Зачем мы это делаем?». Все видят реальную картину. Обучение новых сотрудников, «стареньким» - расширение кругозора, прикольные кейсы.

Цель: коллеги понимают «почему» и следуют правилам осознанно.

КОД ИБ

ИТОГИ

Результаты: цифры говорят

×3

Рост обращений от сотрудников

Из 5-7 в месяц до 20-25

85%

Обращения — реальные угрозы

Качество вместо количества

-60%

Время расследования

Быстрое обнаружение = быстрое решение

0

Успешных BEC-атак

Все попытки обнаружены

Дополнительные эффекты:

Повышение общей цифровой грамотности сотрудников

Улучшение репутации службы ИБ внутри компании

Снижение стресса: сотрудники знают, что помощь всегда рядом

КОД ИБ

ИТОГИ

Вызовы, с которыми мы столкнулись

честно о сложностях трансформации

Скептицизм руководства

"Зачем нам это? У нас есть СЗИ и аналитики!»
Доказали ROI культуры через пилотные проекты и метрики.

Инерция сотрудников

Первые месяцы — низкая активность. Старые привычки сильны. Потребовалось время, чтобы люди поверили, что "открытая дверь" — это всерьёз.

Необходимость гибкости и изобретательности при построении культуры

Нельзя за один день изменить культуру, нельзя резко перестроить бизнес под задачи ИБ, нельзя добавить сотрудникам +X часов рабочего времени на бесконечные инструктажи

КОД ИБ

ИТОГИ

СПАСИБО ЗА ВНИМАНИЕ!

С РАДОСТЬЮ ОТВЕЧУ НА ВОПРОСЫ

Антон Тершонков
Itereshl