



«Мы считаем, что каждый – от пользователя домашнего компьютера до крупной компании и правительства – должен иметь возможность защитить то, что дорого для него. Неважно, идет ли речь о частной жизни, семье, финансах, бизнесе или критической инфраструктуре, мы работаем над тем, чтобы обеспечить защиту всего.»

Евгений Касперский,
генеральный директор

КИБЕРБЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ. Повышение осведомленности пользователей

Никитин Константин
Поликом Про
3258400
knikitin@polikom.ru

Санкт-Петербург, 2017 год

В 2015 году «Лаборатория Касперского» ежедневно детектировала 310000 новых вредоносных файлов

Создание нового вредоносного ПО обходится дорого

→ Киберпреступники поняли, что они могут получать те же результаты, используя назойливые рекламные программы или действительные цифровые подписи



Число вредоносных файлов, детектируемых «Лабораторией Касперского» каждый день

Добрые и толерантные люди



Тенденции киберпреступности



**ПРЕЖДЕ ВСЕГО
ПЫТАЮТСЯ ПОЛУЧИТЬ
БИЗНЕС ВЫГОДУ!**
Существенное снижение
затрат и массовый рост
предложений
(Кибератака-Как-Сервис)



**УМЕЮТ БЫТЬ
ТЕРПЕЛИВЫМИ И
НЕЗАМЕТНЫМИ!**
В среднем целевая атака
с момента её появления
остается необнаруженной
более 214 дней

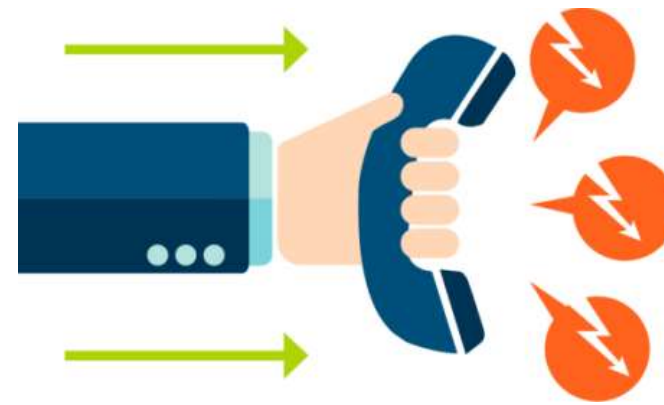


**НЕ БОЯТСЯ
ТРАДИЦИОННЫХ
АВТОМАТИЗИРОВАННЫХ
РЕШЕНИЙ ПО ИБ!**
Резкий спад эффективности
периметровой защиты

Последствия реализации угроз



Прямые финансовые
потери



Потеря клиентов



Потеря доли рынка



Затраты на
нейтрализацию последствий



Репутационные
потери



Потеря
конкурентного
преимущества

90%

инцидентов могли предотвратить сами пользователи

Клиенты и партнеры приносят вирусы и трояны на съемных носителях

Маркетологи и HR кликают на ссылки или открывают зараженные файлы в почте и получают заражение всей сети

Администратор тратит уйму времени, чтобы восстановить потерянную информацию и работоспособность системы

Секретарь хранит все документы на открытом файловом сервере

Пароли простые – «что бы не забыть!»
Давно ли Вы меняли пароль от почты **12345678**?

VIRUS

Типовое развитие целевой атаки

НЕГАТИВНОЕ ВОЗДЕЙСТВИЕ

- доступ к информации
- воздействие на бизнес процессы
- сокрытие следов
- тихий уход

РАСПРОСТРАНЕНИЕ

- кража идентификационных данных
- повышение привилегий
- налаживание связей
- легитимизация действий
- получение контроля

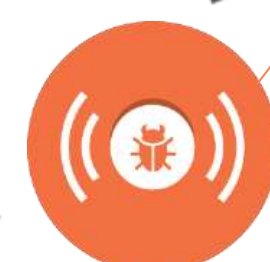


ЦЕЛЕВАЯ АТАКА
МОЖЕТ ДЛИТЬСЯ
МЕСЯЦЫ... И ГОДАМИ
ОСТАВАТЬСЯ
НЕОБНАРУЖЕННОЙ



ПОДГОТОВКА

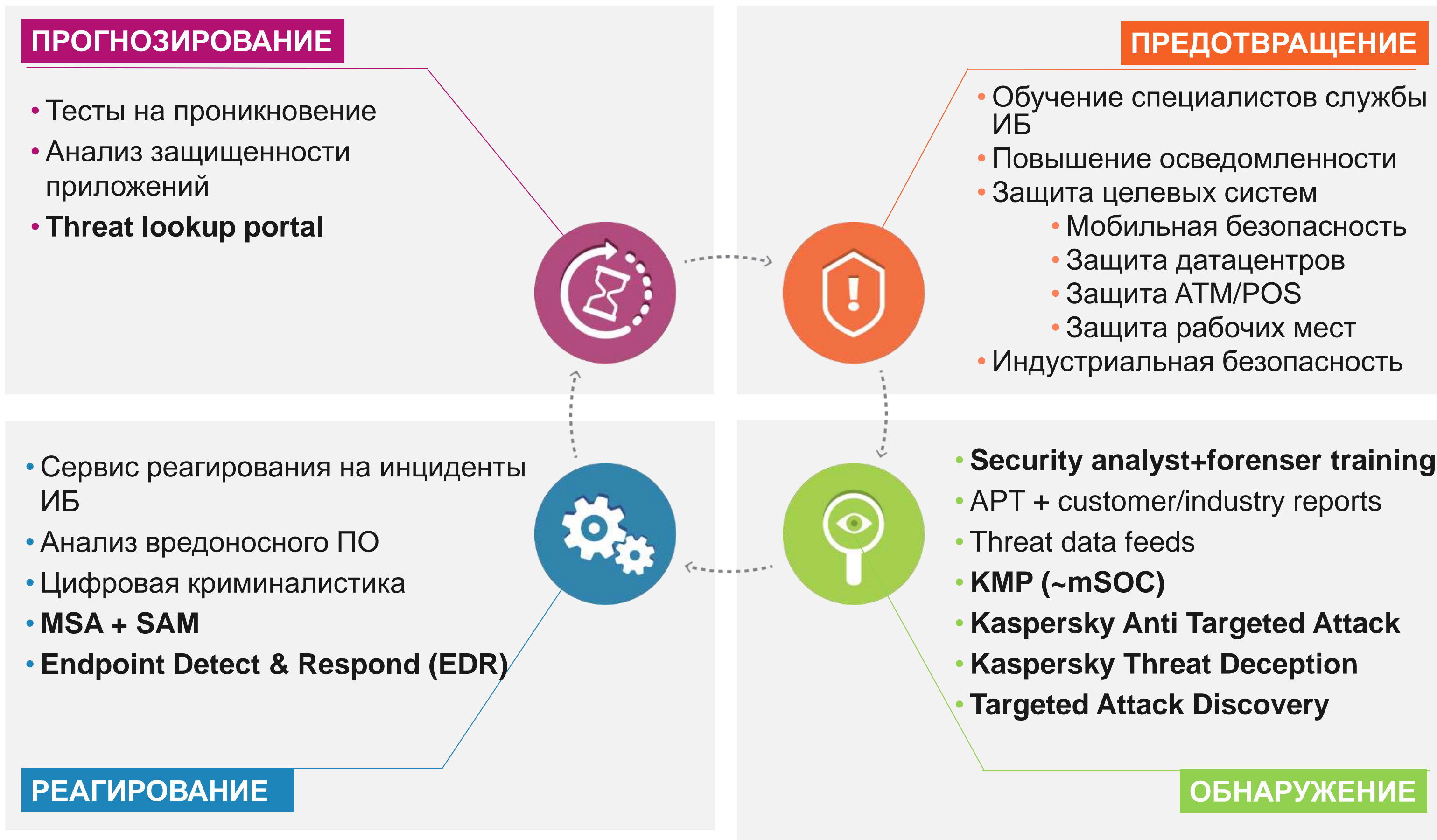
- анализ цели
- подготовка стратегии
- создание/покупка тулсета



ПРОНИКНОВЕНИЕ

- использование слабых мест
- проникновение внутрь инфраструктуры

Адаптивная стратегия корпоративной ИБ



Повышение уровня осведомленности в части ИБ



Структура тренингов «Лаборатории Касперского» по повышению осведомленности в области кибербезопасности

- Сокращение числа инцидентов до 90%
- Включение в процесс руководителей организации благодаря переводу требований кибербезопасности на понятный язык без IT-терминологии
- Измеримые результаты программы осведомленности

<https://kaspersky.securityeducation.com>



Обучение сотрудников

Все сотрудники – базовый уровень

ОНЛАЙН-ПЛАТФОРМА

ОСНОВЫ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ,
ПРАКТИЧЕСКИЙ КУРС

Базовые знания в области IT



Линейные руководители –
средний уровень

ИГРОВОЙ ФОРМАТ CYBERSAFETY

S E C U R E

Руководители

ОЦЕНКА УРОВНЯ ОСВЕДОМЛЕННОСТИ
В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Обучение продолжается в течение года, цикл за ЦИКЛОМ



Мы предоставляем руководство по рекомендованным практикам и техническую поддержку



Обучение экспертов ИБ

1 уровень БАЗОВЫЙ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ /ПРАКТИЧЕСКИЙ КУРС/
Требуются базовые знания в области IT

2 уровень СРЕДНИЙ

ЦИФРОВАЯ КРИМИНАЛИСТИКА
Требуются навыки системного администрирования

**АНАЛИЗ И ОБРАТНАЯ РАЗРАБОТКА
ВРЕДОНОСНОГО ПО**
Требуются навыки программирования

3 уровень ЭКСПЕРТНЫЙ

**ЦИФРОВАЯ КРИМИНАЛИСТИКА
(профессиональный уровень)**
Требуются экспертные навыки системного администрирования

**АНАЛИЗ И ОБРАТНАЯ РАЗРАБОТКА
ВРЕДОНОСНОГО ПО
(профессиональный уровень)**
Требуются навыки программирования на языке ассемблер



Спасибо!

Буду рад ответить на ваши вопросы

Константин Никитин

Поликом Про

325 84 00

knikitin@polikom.ru

ПОЛИКОМ ПРО

Просто работаем