УПРАВЛЕНИЕ КИБЕРБЕЗОПАСНОСТЬЮ – ПОНИМАНИЕ ЧЕРЕЗ ОПЫТ

Kaspersky Interactive Protection Simulation – , БАНК

ПОПУЛЯРНЫЕ АТАКИ: ФИНАНСОВЫЙ СЕКТОР

Кибератаки на финансовые организации не теряют свою актуальность

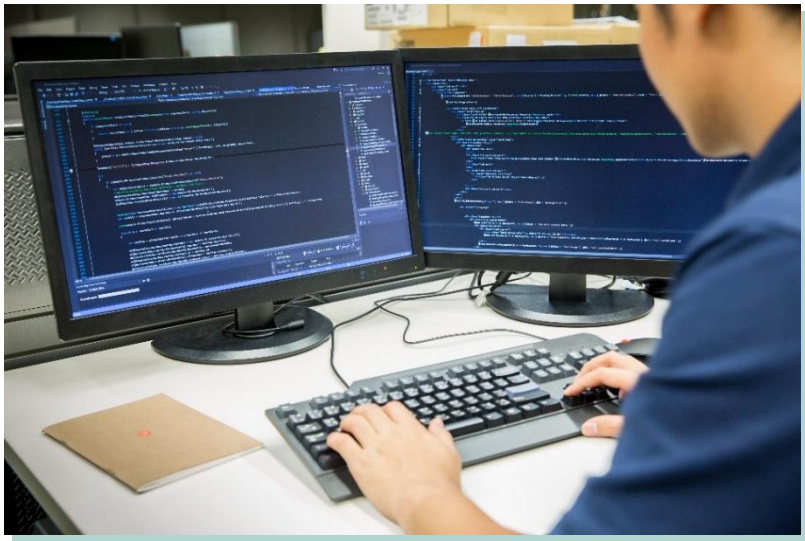
Тюпкин – кибератаки, направленные против нескольких десятков банкоматов в Восточной Европе

В результате деятельности группировки **Carbanak** пострадало около 100 финансовых организаций. Убытки каждого из банков составляют от 2,5 примерно до 10 миллионов долларов.

Black Energy атакуют банки Восточной Европы и США начиная с 2007

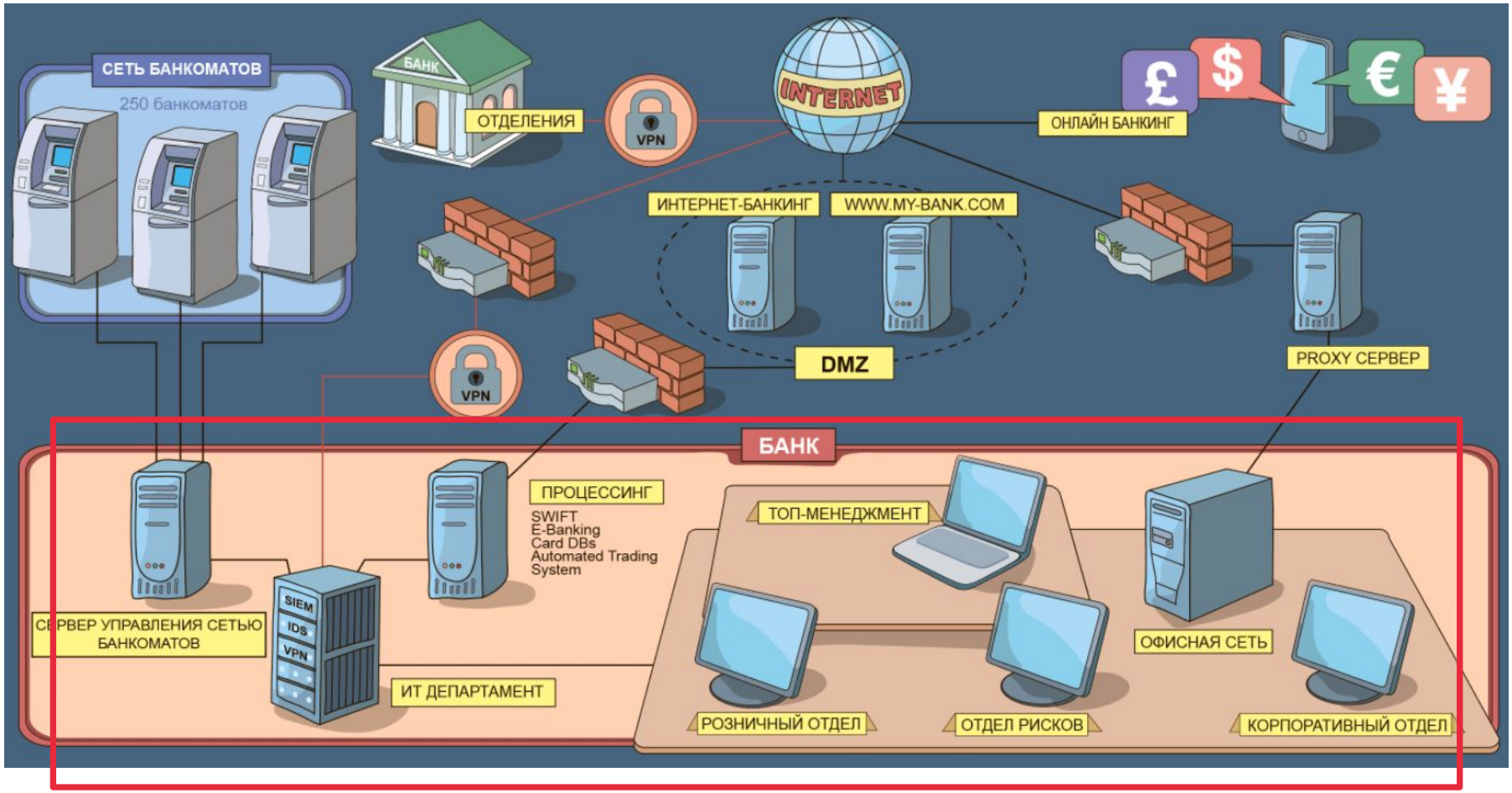
ВВЕДЕНИЕ

- Вы – специалисты по IT-безопасности в банке

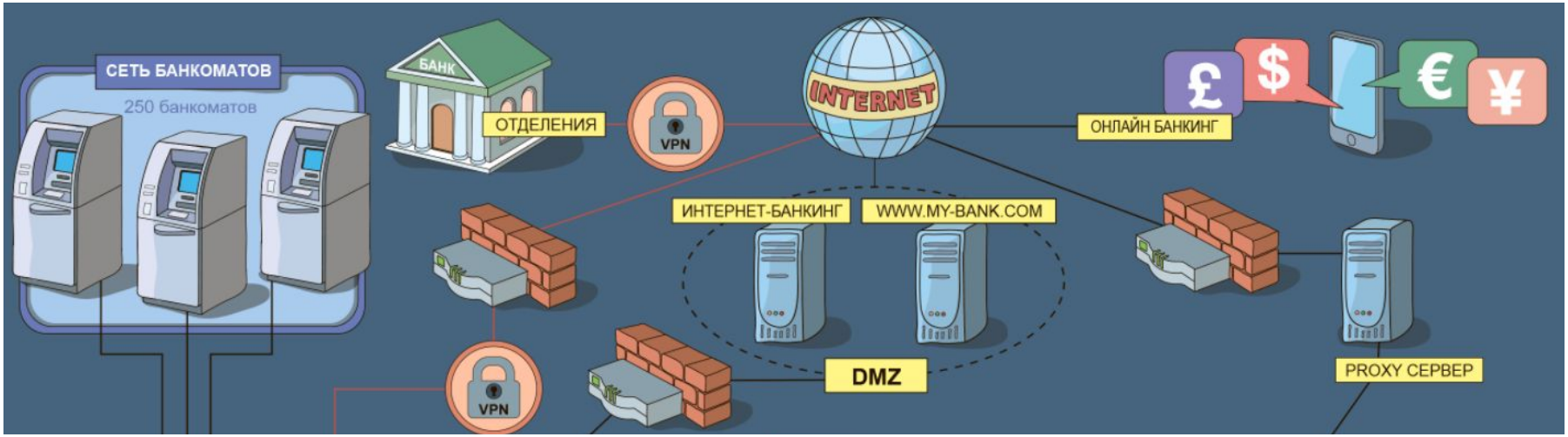


- Ваша главная задача – обеспечивать кибербезопасность для защиты активов банка

ПОЛЕ СИМУЛЯЦИИ



ПОЛЕ СИМУЛЯЦИИ

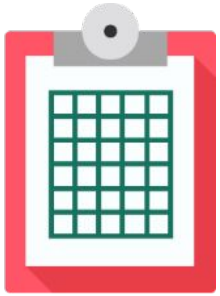


ЦЕЛЬ СИМУЛЯЦИИ

В идеальных условиях доход банка за ход составляет

$500,000 + **$4,500,000** = **$5,000,000**

Сеть банкоматов | Банковские операции | Доход за каждый ход



Длительность игры — 2 хода

Успех команды определяется совокупным доходом в конце симуляции

ПУБЛИЧНЫЕ НОВОСТИ

ХОД 1

ПРОИСШЕСТВИЕ НЕДЕЛИ

"True Investment Bank" вызвал сегодня переполох на биржевых торгах – он скупал акции нескольких компаний по всем заявкам в течение 30 минут. Убытки банка оцениваются примерно в $2,000,000.

Анонимный источник заявил, что причиной данного происшествия банк считает сбой в автоматизированной биржевой системе, отвечающей за все операции трейдеров.

ПУБЛИЧНЫЕ НОВОСТИ

ХОД 2

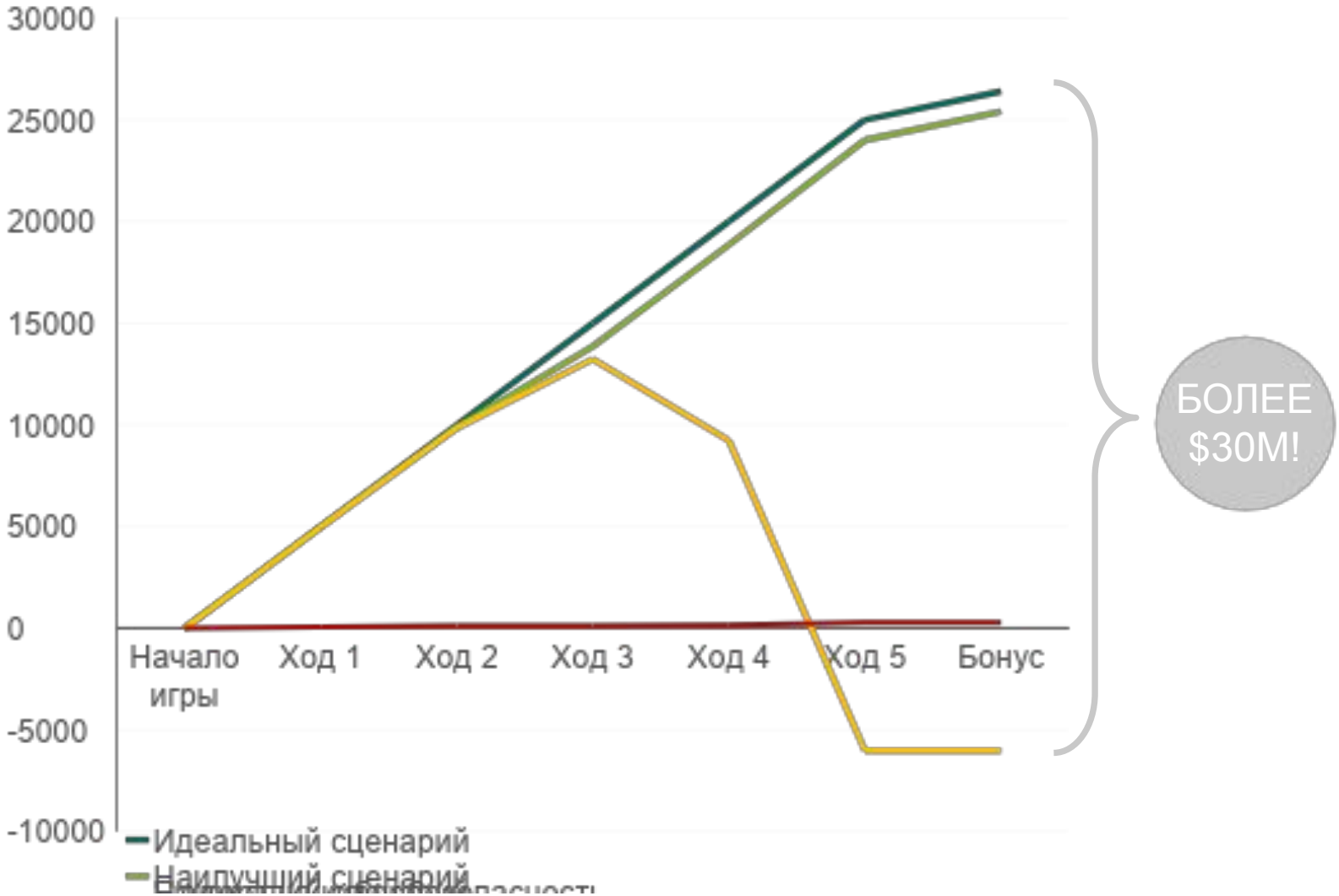
НОВОСТИ ИНДУСТРИИ

ИТ департамент сообщает, что согласно публикациям в СМИ в "True Investment Bank" установлено такое же ПО для работы трейдеров, как и в нашем банке.

АТАКИ И УГРОЗЫ

1. «TYUPKIN» – ВИРУС ДЛЯ БАНКОМАТОВ
2. «CARBANAK» - ФИНАНСОВАЯ APT
3. «BLACK ENERGY» - НЕОБЫЧНЫЙ ВИРУС
4. «CRYPTOR» - ПРОСТОЙ, НО ЭФФЕКТИВНЫЙ

СРАВНЕНИЕ СЦЕНАРИЕВ



ПОНИМАНИЕ СТРАТЕГИЧЕСКОГО ЦИКЛА КИБЕРБЕЗОПАСНОСТИ

ПРЕДОТВРАЩЕНИЕ УГРОЗ

- Анализ и оценка рисков кибербезопасности
- Планирование мероприятий по обеспечению защиты информации
- Информирование и обучение пользователей

ВОССТАНОВЛЕНИЕ

- Проведение аудита и оценки рисков, пересмотр политик кибербезопасности для предотвращения будущих угроз

ОЦЕНКА ИНЦИДЕНТА

- Обнаружение и анализ инцидента

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- Немедленное реагирование на инцидент для уменьшения его последствий

РЕЗУЛЬТАТЫ, РАБОТАЮЩИЕ В РЕАЛЬНОЙ ЖИЗНИ

В процессе игры участники сами приходят к важным и применимым в их каждодневной работе выводам:

- Кибератаки влияют на доход предприятия, и поэтому такие случаи должны выводиться на уровень высшего руководства,
- Взаимодействие между IT-специалистами и профессионалами, ответственными за операционную деятельность, крайне важно для поддержания безопасности АСУ,
- Выделяемый на кибербезопасность бюджет намного меньше, чем доход, который вы рискуете потерять. И этот бюджет не исчисляется миллионами,
- Сотрудники легко привыкают к разумным мерам безопасности и хорошо понимают важность как тренингов и аудита, так и просто установки антивируса.

В ЦЕРНе огромное число IT- и инженерных систем, с которыми работают тысячи сотрудников. Именно поэтому информировать людей и вовлекать их в заботу о кибербезопасности – это не менее важно, чем совершенствовать методы технического контроля. Тренинг, проведенный Kaspersky Lab, был действительно вовлекающим, ярким и эффективным.

Stefan Luders, CISO, ЦЕРН

KASPERSKY INTERACTIVE PROTECTION SIMULATION (KIPS)

- Увлекательный и вовлекающий формат
- Продолжительность – всего 2 часа
- Командная работа, помогающая создавать эффективное сотрудничество
- Атмосфера соревнования, способствующая проявлению инициативы и развитию навыков ситуационного анализа
- Сценарий разработан таким образом, чтобы способствовать лучшему пониманию мер информационной безопасности
- От участников не требуется глубокая экспертиза в области безопасности

ДОСТУПНЫЕ СЦЕНАРИИ

Промышленная компания

Защита АСУ ТП и критически важной инфраструктуры. Существует два варианта сценария – «Электростанция» и «Станция водоочистки».

Электронное правительство

Защита государственных электронных ресурсов от атак и эксплойтов.

Корпорация

Защита предприятия от программ-вымогателей, целевых атак и нарушений безопасности автоматизации.

Банк

Защита финансовых учреждений от специализированных целевых атак, направленных на банкоматы, управляющие серверы и бизнес-системы.

Транспорт

Защита логистической компании от серии кибератак, включая целеву атаку, проникновение инсайдера, ошибку Heartbleed.

Нефтегазовая компания

Защита компании, осуществляющей поставку сырой нефти, от целевых атак.

KASPERSKY SECURITY AWARENESS

Игровые тренинги для повышения кибербезопасности корпоративной среды

- Автоматизация/ самонастраивающаяся траектория обучения
- Тренинги для разных уровней
- Реальная геймификация
- Конкуренция и дух соревнования

ЭФФЕКТИВНЫЙ МЕТОД УКРЕПЛЕНИЯ КОРПОРАТИВНОЙ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ

93%

Вероятность применения навыков в повседневной работе

90%

Сокращение количества инцидентов до 10 раз

50-60%

Снижение рисков кибербезопасности в денежном выражении

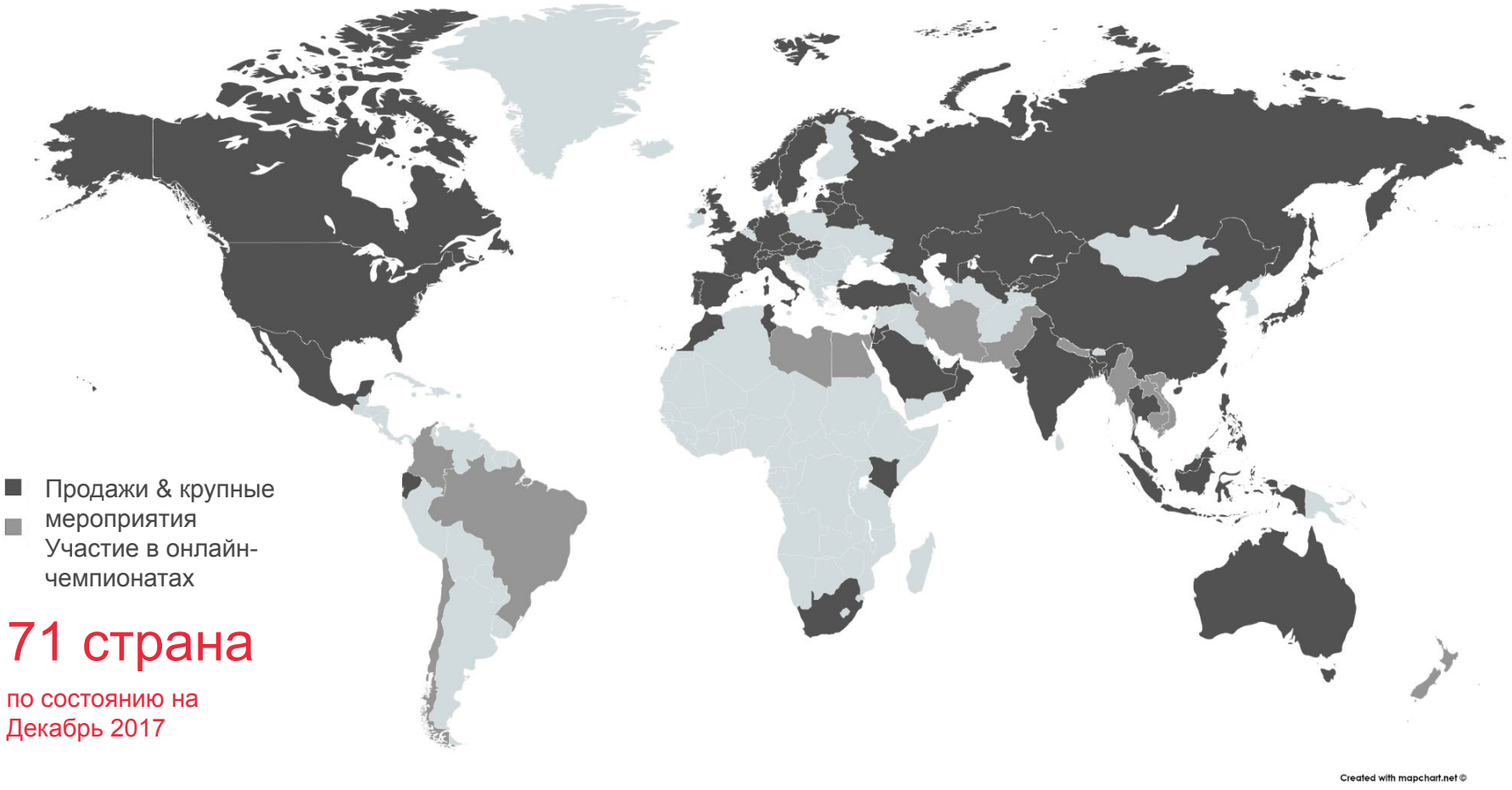
30x

Более чем 30-кратная окупаемость вложений в повышение осведомленности

86%

Готовность рекомендовать программу

KASPERSKY SECURITY AWARENESS В МИРЕ



71 страна

по состоянию на
Декабрь 2017