Киберучения как превентивные меры

Как подготовить сотрудников к противостоянию?

Абуталип Асель

Менеджер по развитию сектора SMB

KASPERSKY

Сколько компании тратят на безопасность?

Коммерческие организации по всему миру потратили:

- 2017 год - 87 миллиардов долларов $ (gartner.com)

  прирост 7% к 2016 году

- 2018 год – 114 миллиардов долларов $
- 2019 год – 124 миллиарда долларов $
- Россия: от 150 тысяч $ до 5 млн $
  (крупные предприятия)
- Казахстан: от 10000> 1млн $
  (крупные предприятия)

SYDNEY, Australia, August 15, 2018

Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019

Detection, Response and Privacy Driving Demand for Security Products and Services

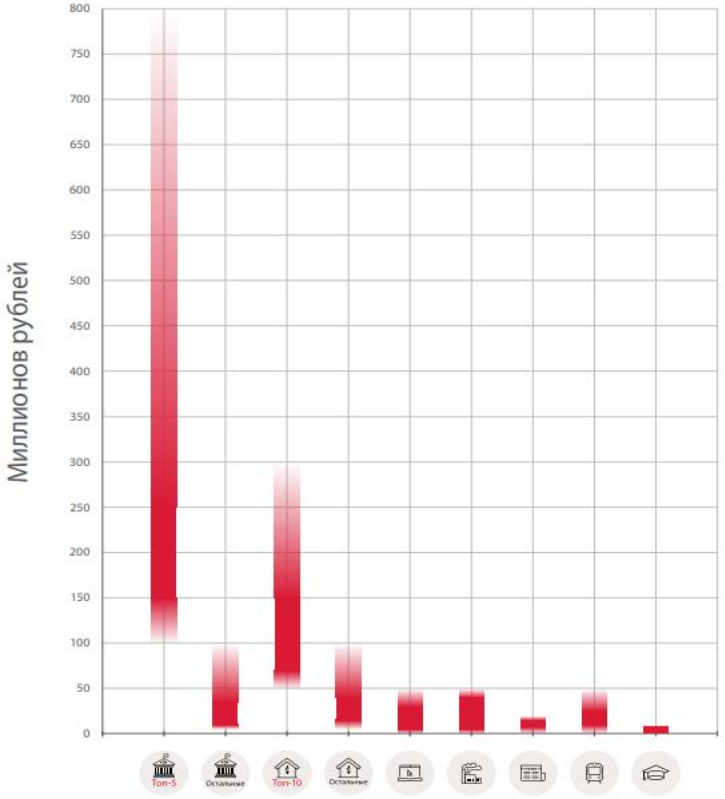
Worldwide spending on information security products and services will reach more than $114 billion in 2018, an increase of 12.4 percent from last year, according to the latest forecast from Gartner, Inc. In 2019, the market is forecast to grow 8.7 percent to $124 billion.

"Security leaders are striving to help their organizations securely use technology platforms to become more competitive and drive growth for the business," said Siddharth Deshpande, research director at Gartner. "Persisting skills shortages and regulatory changes like the EU's Global Data Protection Regulation (GDPR) are driving continued growth in the security services market."

A 2017 Gartner survey* revealed that the top three drivers for security spending are (1) security risks; (2) business needs; and (3) industry changes. Privacy concerns are also becoming a key factor. Gartner believes privacy concerns will drive at least 10 percent of market demand for security services through 2019 and will impact a variety of segments, such as identity and access management (IAM), identity governance and administration (IGA) and data loss prevention (DLP).

Mr. Deshpande said highly publicized data breaches, like the recent attack on SingHealth that compromised the personal health records of 1.5 million patients in Singapore, reinforce the need to view sensitive data and IT systems as critical infrastructure.

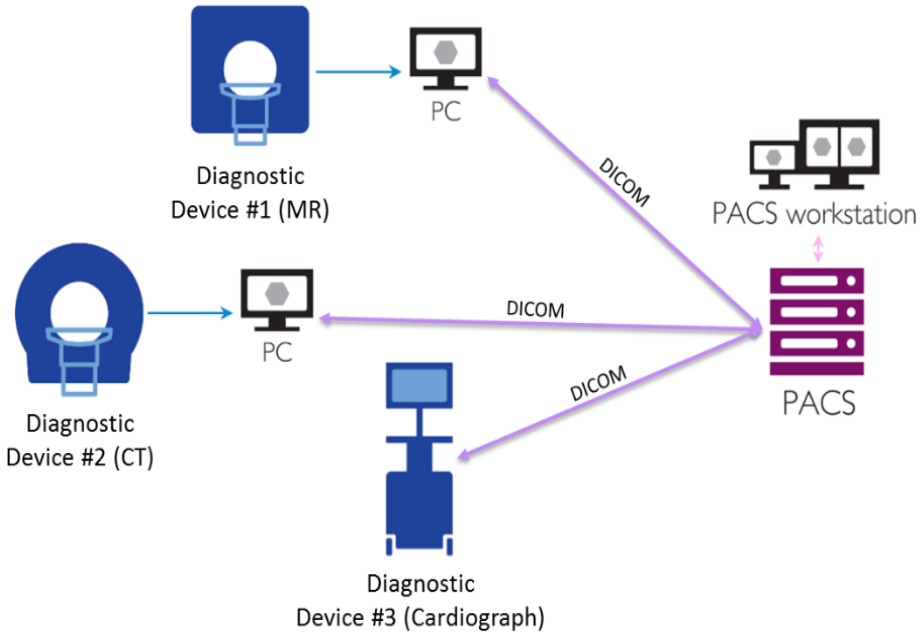
Бюджетирование ИБ по секторам в России



Бюджеты выделяемые ежегодно на ИБ по разным отраслям

- Топ 5 крупных банков от 100 млн руб до 800 миллионов руб.
- Банки не вошедшие в топ 5: от 1млн руб до 100 млн руб.
- Государственный сектор: от 50 млн руб до 300 млн руб.
- Промышленность: от 1 млн руб до 50 млн руб.
- Транспорт: 1 млн руб до 50 млн руб.
- Образование: до 1 млн руб.

Подключенная медицина



Топология сети «подключенной медицины»

Информационные системы в медицине:

- Базы данных: сервера, рабочие станции
- Медицинские порталы: удаленный доступ к личному кабинету
- Медицинские оборудования подключающиеся к корпоративной сети.
- Носимые устройства пациентов: фитнес браслеты, кардиостимуляторы, инсулиновые помпы
- Прочие информационные системы: мобильные приборы изменения подключаемые по Wi-fi, Bluetooth, RF)

Как происходит атака на корпоративную информационную систему?

Ущерб киберинцидента учреждения:

- Утечка данных о пациентах
- Судебные иски
- Простой работы учреждения от 1 дня до 2 месяцев
- Ошибка врачей из за неверных данных
- Выплата шантажистам
- Потеря репутации учреждения

Ущерб в денежном эквиваленте:

- От 100 000 до миллионов долларов США
- Wanna Cry – нанес ущерб по всему миру около 1 млрд долларов США

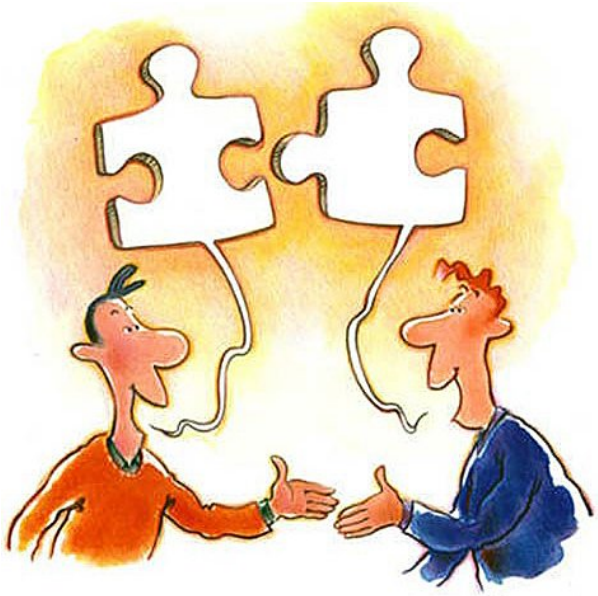
Какими должны быть действия сотрудников при киберинциденте?

- Действия сотрудников при киберинциденте должны быть так же отработаны как эвакуация при пожаре
- Сотрудники IT-отдела не всегда могут быстро справиться с ситуацией, не говоря уже о рядовых сотрудниках

Какие проблемы существуют между бизнесом и ИБ?

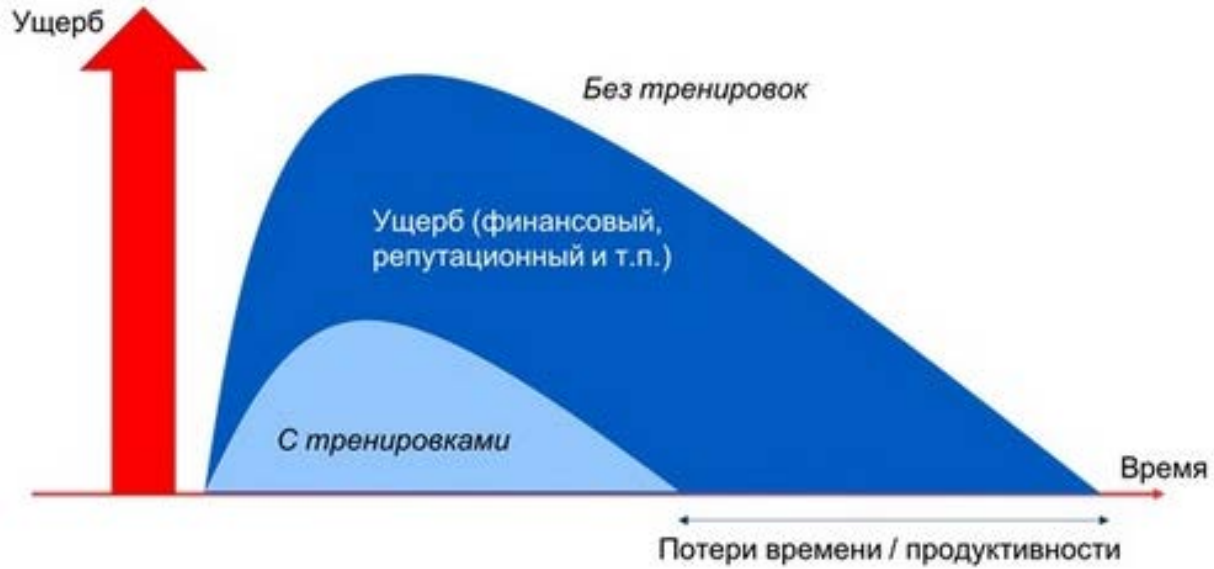
- На что жалуются руководители по ИБ чаще всего?
- Всегда ли руководители компании видят работу отдела ИБ?
- Почему возникают непонимания между бизнесом и ИБ?
- Как трансформировать отношение бизнеса к деятельности ИБ максимально эффективно?

В чем отличие киберучения для топ-менеджмента



- Проверка и выработка правильных коммуникаций между всеми участниками
- Устранение слабых мест
- Понимание роли кибербезопасности в деятельности компании
- Роль руководителя в обеспечении кибербезопасности
- Действия в нештатных ситуациях
- Что нужно делать для поддержания кибербезопасности в компании?

Почему необходимо проводить киберучения?



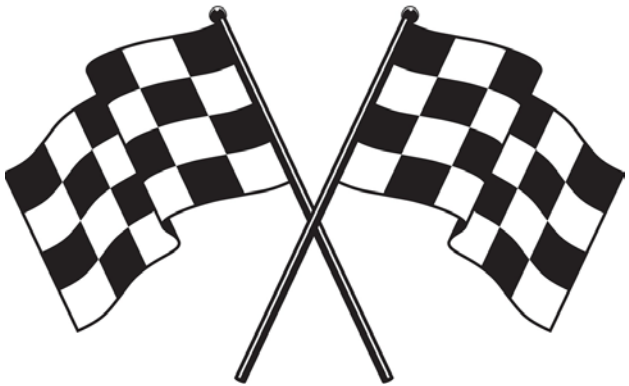
Сценарии киберучении

- Утечка важной для бизнеса информации
- Шантаж со стороны мошенников/хакеров
- Публикация в СМИ об инциденте
- Массовое заражение шифровальщиком
- «Злой айтишник» оставляет закладки в критические системы
- DDoS атака web сервисов компании
- Обнародование данных клиентов в открытом доступе

Цель киберучений:

- Получение обратной связи
- Определение ответственности
- Идентификация ролей
- Расширение навыков и знаний
- Оценка возможностей
- Оценка тонких и слабых мест
- Оценка требуемых ресурсов
- Мотивация сотрудника
- Вовлечение топ менеджмента

Ожидаемые результаты киберучений



- Ситуационная осведомленность сотрудников
- Повышение ответственности за кибербезопасность компании
- Определение плана непрерывности бизнеса
- Скорость реагирования
- Облегчение процесса принятия решении
- Обмен информацией
- Улучшение взаимодействия с отделом ИБ

Тренинги Kaspersky Security Awareness

Навыки, а не только знания

Тренинги для **всех уровней и функций** организации

Компьютеризированные учебные программы – легко проводить, управлять обучением и измерять эффективность

Эффективность через **соревнование**, обучение на практике (**learning-by-doing**) и использование **реальных рабочих ситуаций**

Оценка культуры кибербезопаности

Позволяет проанализировать повседневное поведение сотрудников и их отношение к кибербезопасности

Онлайн-исследование на основе кратких кастомизированных опросников для сотрудников и менеджеров. Развитая система отчетов.

KASPERSKY lab

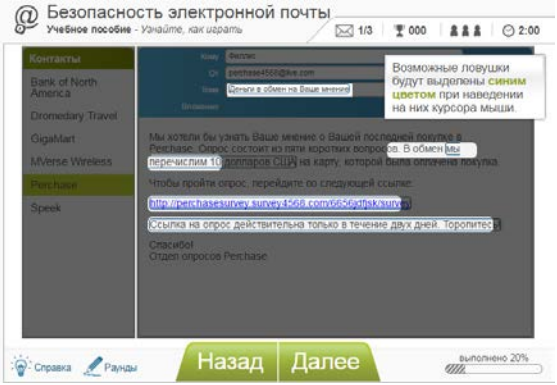
Подходы к обучению кибербезопасности

Стандартный подход

Инструкции, ежегодные презентации, постеры, тренинги

Низкая эффективность
Мало возможностей для измерения результата

Интерактивный подход + инструменты геймификации

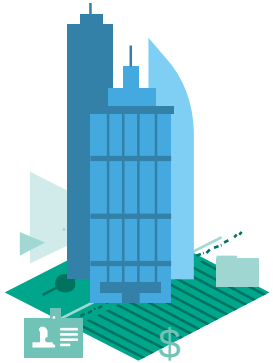


- 93% – вероятность применения полученных знаний в повседневной работе
- 90% – сокращение числа ошибок
- 50-60% – снижение рисков кибербезопасности в денежном эквиваленте
- Более чем 30-кратная окупаемость вложений (ROI)

Kaspersky Interactive Protection Simulation

ДЕЛОВАЯ ИГРА ДЛЯ ВЫРАБОТКИ СТРАТЕГИИ
РЕАГИРОВАНИЯ НА КИБЕРУГРОЗЫ

КОМАНДНАЯ РАБОТА ДЛЯ СОЗДАНИЯ НАВЫКОВ СОТРУДНИЧЕСТВА



ДЛЯ ТОП – МЕНЕДЖЕРОВ И РУКОВОДИТЕЛЕЙ ОТДЕЛОВ IT И ИБ

АТМОСФЕРА СОРЕВНОВАНИЯ

РАЗБОР ОШИБОК И АНАЛИЗ ОПТИМАЛЬНЫХ СТРАТЕГИЙ

СЦЕНАРИИ:

Corporation **E-Government** **Bank**

Transportation **Power station + Water plant**

Oil & Gas

KASPERSKY lab

Kaspersky Cybersafety Management Games

Понимание важности ИБ

Умение принимать бизнес – решения
С учетом принципов ИБ

Мониторинг

Убеждение и вдохновение

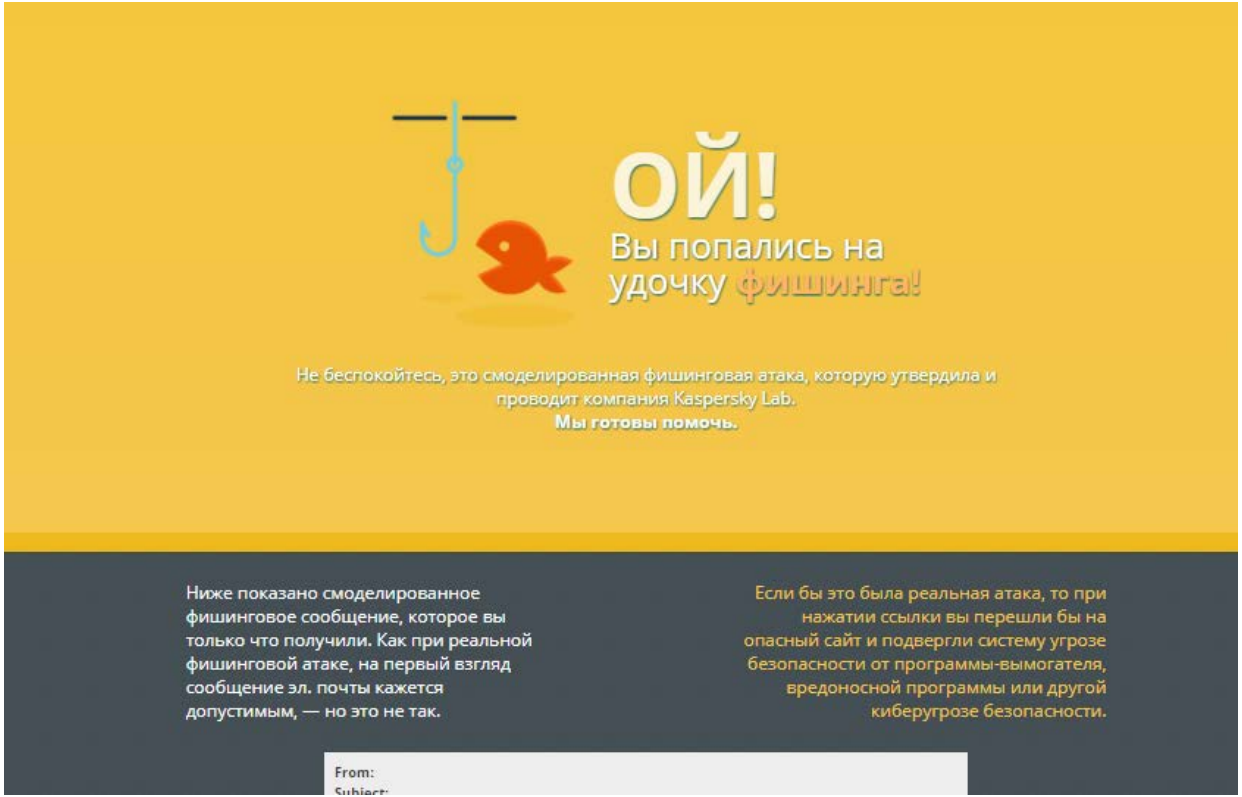
ДЛЯ МЕНЕДЖЕРОВ

KASPERSKY lab

Симуляция фишинговых атак

- Библиотека шаблонов фишинговых писем
- Большой список поддельных фишинговых доменов
- Библиотека шаблонов Обучающих страниц (которые видит пользователь, попавшийся на фишинг)
- Фишинговые письма и обучающие страницы полностью кастомизируются
- Отчётность по фишингу с возможностью экспорта
- Авто-назначение обучения тем, кто попался на фишинговое письмо

Мгновенная обратная связь



- Обучающая страница
- Авто-назначение обучения «попавшимся»

KASPERSKY lab

ВОПРОСЫ?

Assel.abutalip@kaspersky.com

Лаборатория Касперского
Центральная Азия и Монголия

KASPERSKY