Как компании противодействуют кибер рискам

Андрей Уколов
Дарья Богуш

IT Risk & Assurance, EY

Киев, 27 апреля, 2016

EY
Building a better working world

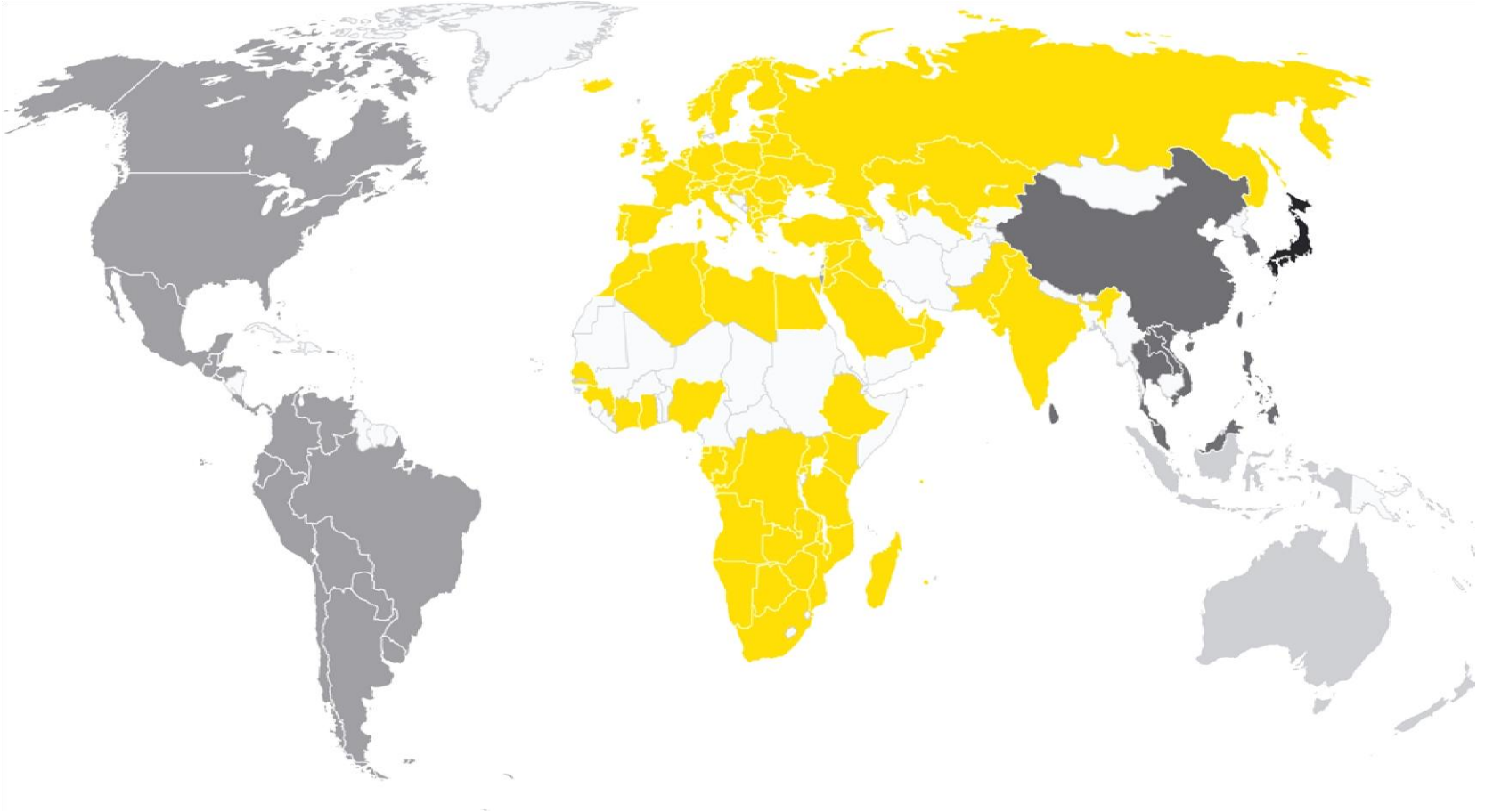
Программа

1. О компании EY
2. Что такое кибер риски?
3. Ландшафт кибер рисков
4. Технологии против кибер рисков
5. Кейс из практики EY

EY
Building a better working world

О компании EY

О компании EY



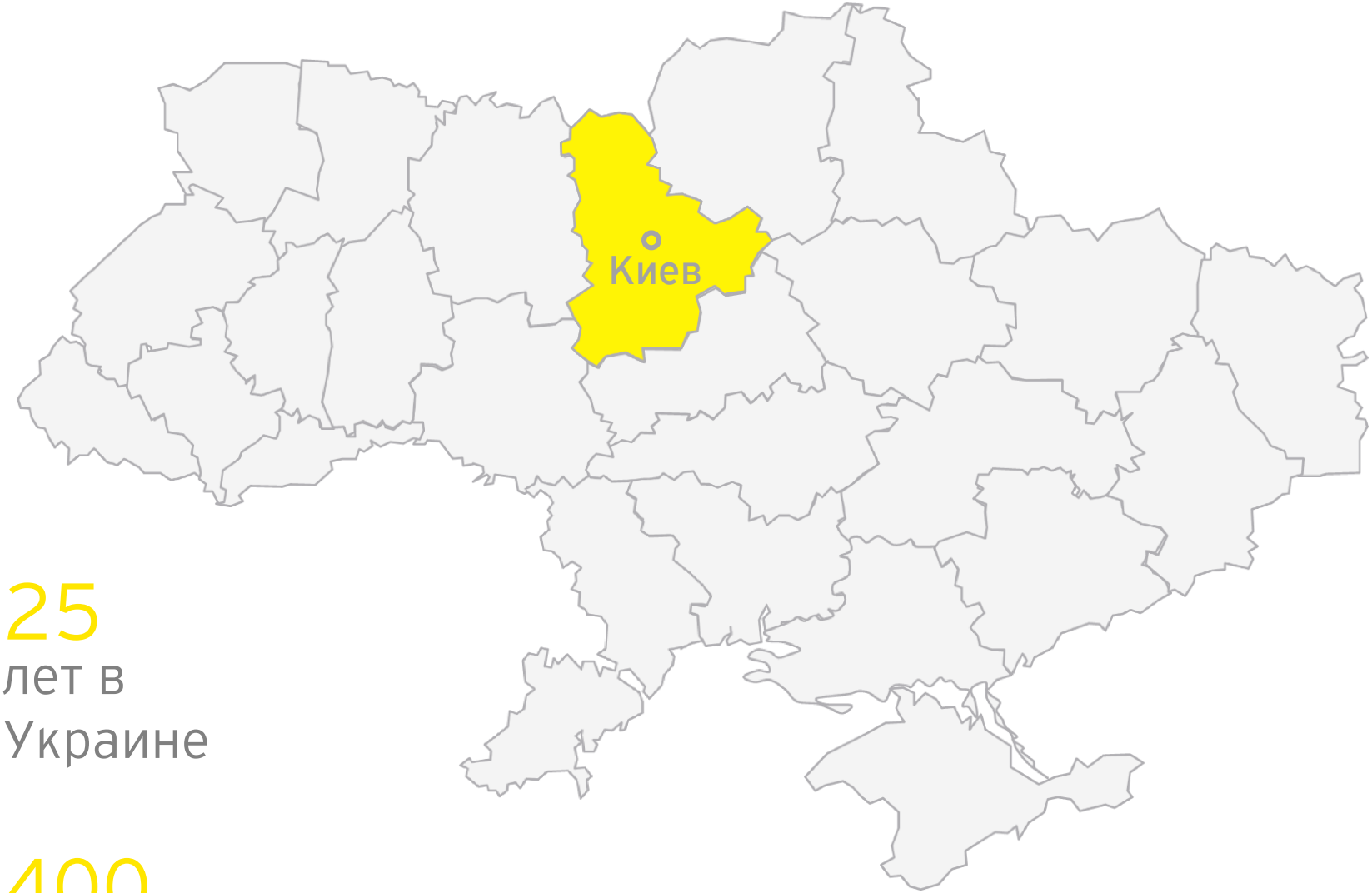
150
стран

212k
сотрудников

$28.7b
доход

EY
Building a better working world

EY в Украине



25
лет в
Украине

400
сотрудников

EY
Building a better working world

Услуги EY

Аудиторские услуги

- Аудит финансовой отчетности
- Расследование мошенничества
- Бухгалтерский учет
- Услуги в области чистых технологий и устойчивого развития

Консалтинг

- Повышение эффективности деятельности
- Услуги в области информационных технологий
- Управление бизнес-рисками
- Академия бизнеса

Налогообложение и право

- Корпоративное налогообложение
- Налогообложение физических лиц
- Управление персоналом
- Юридические услуги
- Трансфертное ценообразование

Сопровождение транзакций

- Сопровождение сделок
- Корпоративные финансы
- Оценка и бизнес-моделирование
- Консультационные услуги в области недвижимости

EY
Building a better working world

Услуги в области информационных технологий

Отдел по предоставлению услуг в области управления информационными технологиями и ИТ-рисками – IT Risk and Assurance (ITRA) – специализируется на независимых консультациях по оптимизации использования ИТ, а также аудиторских услугах.

Консультационные услуги

- Сопровождение внедрения информационных систем
- Организация/оптимизация процессов управления ИТ
- Стратегический ИТ консалтинг
- Разработка/оптимизация ИТ-контролей
- Консультации по организации компьютерных сетей

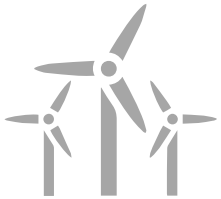
Аудиторские услуги

- Аудит информационных систем организации
- Аудит информационной безопасности
- Услуги по тестированию периметра безопасности (penetration testing)
- Аудит на соответствие требованиям ведущих стандартов (ISO 27001, PCI DSS, другие)

Наши клиенты

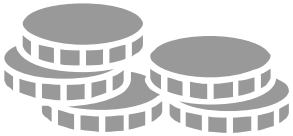
Государственные предприятия

ТЭК, химические и фармацевтические компании



Софтверные компании

Банки, страховые компании



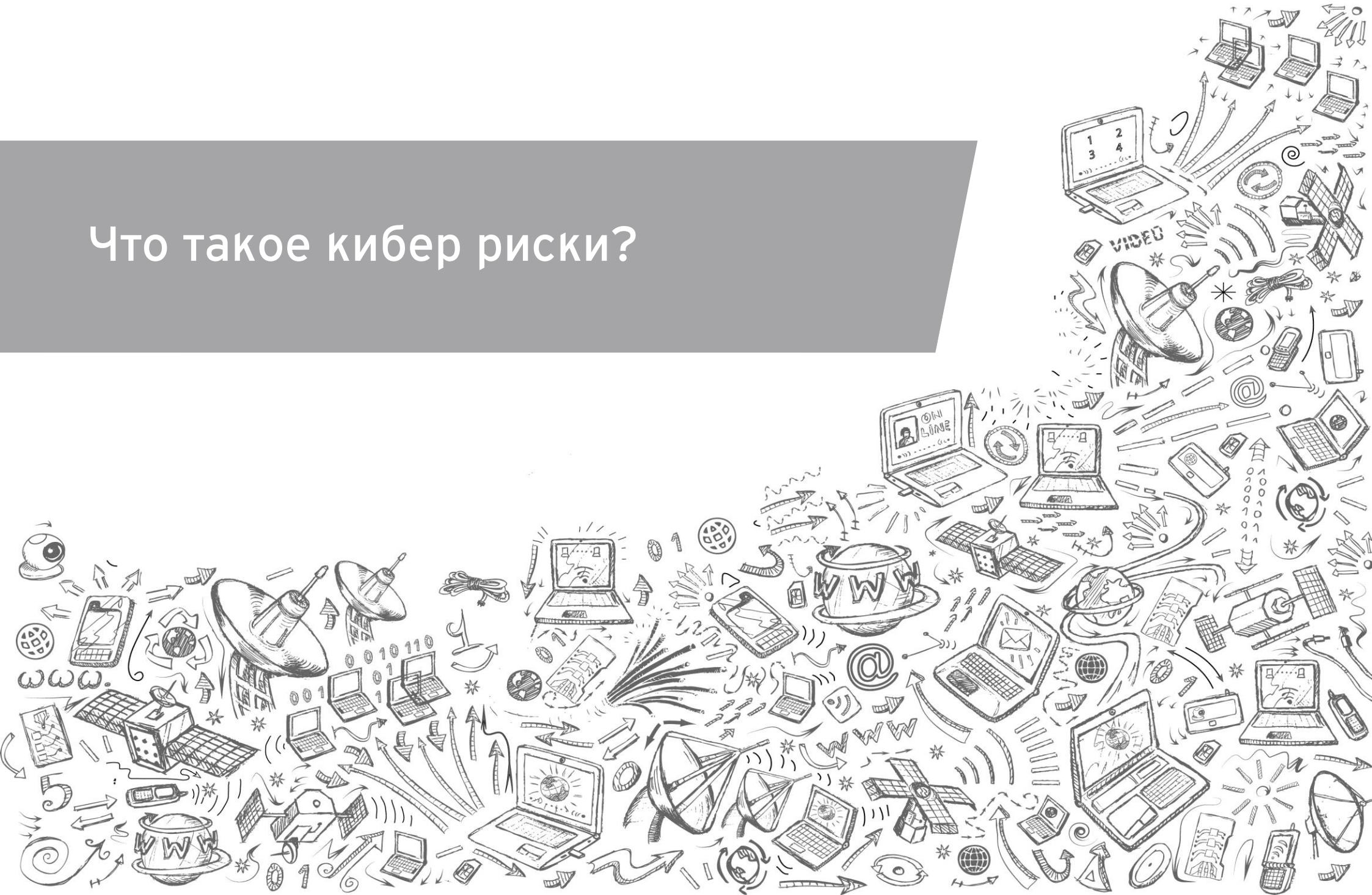
Телекомы

Ритейл

Недвижимость, гостиничный бизнес, строительство

EY
Building a better working world

Что такое кибер риски?



Что такое информационная безопасность?

Термины информационной безопасности

1. Уязвимость
2. Угроза
3. Источник угрозы
4. Риск
5. Воздействие
6. Защитные меры
7. Актив

- Люди
- Информация
- Оборудование
- Помещения
- Коммуникации
- Электроэнергия, водоснабжение

EY
Building a better working world

Взаимодействие между концептами ИБ

Базовые концепции ИБ: Сценарий

Антивирус не был обновлен

Уязвимость

Вирус попал в сетевой периметр

Угроза

Данные скомпрометированы

Воздействие

Установка антивируса с актуальными базами

Защитные меры

Какие примеры кибер угроз Вы знаете?

- **Зловредный код** - программное обеспечение, предназначенное для выполнения несанкционированных действий, которые оказывают неблагоприятное воздействие на конфиденциальность, целостность или доступность информационных систем. Примерами вредоносного кода являются вирусы, черви, троянские кони, логические бомбы и т.д

- **Распределенная атака типа «отказ в обслуживании»** (DDoS-атака) - атака на вычислительную систему путем многочисленных распределенных запросов, с целью довести её до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам)

- **Несанкционированный доступ** - обретение пользователем или злоумышленником прав доступа в ИТ-системе, которые не назначены ему явно.

Как определяется риск?

Риск

=

Вероятность реализации угрозы

×

Ущерб от реализации угрозы

- Следует различать риски, которые ведут к прямым и непрямым денежным потерям
- В первом случае довольно легко выразить ущерб в денежном выражении
- Во втором же - необходимо пользоваться качественной / экспертной оценкой величины ущерба

Кибер угроза может реализоваться множеством способов

Важно понимать, какую информацию стоит защищать

Корпоративная информация

- Внутренние прайс листы и политика скидок
- Предписания регулирующих органов
- Управленческая отчетность
- Интеллектуальная собственность
- Проектно-сметная документация

Экономическая информация

- Информация о себестоимости продукции
- Статистика по объемам продаж
- Финансовые транзакции
- Отчетность до ее публикации
- Информация о заработной плате
- Прогнозы производства

Критичная информация

Информация о клиентах

- Реестры клиентов
- Реквизиты партнеров
- Реестры потенциальных клиентов
- Информация о B2B операциях
- Корпоративные контакт-листы

Персональные данные

- Номера кредитных карт
- Паспортные данные
- Идентификационные коды
- Информация для доступа в системы (логины, пароли, ключи, настройки)

EY
Building a better working world

Инциденты кибербезопасности наносят огромный ущерб

МИР

- Катастрофическая уязвимость Heartbleed в протоколе OpenSSL до сих пор не устранена на 300 тысячах серверов по всему миру
- Verizon сообщил об утечке 1,5 млн аккаунтов корпоративных клиентов
- ЗАО "ФосАгро АГ" - незаконная передача конфиденциальной информации и убытки в размере 2 млн. долларов
- Наибольший известный ущерб от утечки данных (2 млрд долл. и падение акций на 17% - 2012 г.) своему работодателю нанес бывший менеджер американского банка, предав огласке планы финансового развития компании

Украина

- Кибер атака на инфраструктурные энергетические объекты Украины привела обесточиванию 220 000 потребителей электроэнергии (что составляет около 1% всего энергопотребителей страны)
- Одна из украинских компаний - ошибочная массовая рассылка зарплатной ведомости привела к оттоку ключевых специалистов.
- Две украинских медиакомпании - уничтожение видеоматериалов, вывод из строя рабочих мест операторов эфира

За последние 6 лет ущерб от кибератак вырос на 82%

Реализация киберугроз приводит к финансовому ущербу

Результат реализации киберугрозы	Влияние на бизнес	Финансовый ущерб
Утечка данных	Остановка и замедление бизнес-процессов	Потеря клиентов и дохода
Утрата доступности данных	Потеря конкурентного преимущества	Снижение акционерной стоимости
Нарушение целостности информации	Ущерб бренду и потеря репутации	Затраты на устранение последствий
	Судебные разбирательства	Штрафы и санкции регулирующих органов
	Санкции регулирующих органов	

EY
Building a better working world

Система управления ИБ должна быть комплексной

Система управления информационной безопасностью представляет собой набор взаимосвязанных стратегических и операционных компонент для создания надежной программы по безопасности. Каждый компонент - это набор процессов и практик, работающие вместе и направленные на один аспект безопасности компании. Компоненты направлены как на физическую так и на электронную безопасность.

Ожидания и требования руководства к использованию и защите технологических, физических и информационных активов

Разработка сервисов технической безопасности, соответствующих требованиям бизнеса

Процессы, процедуры и методы управления и выполнения программы по безопасности

Непрерывное тестирование соответствия требованиям и отчетность об эффективности программы безопасности

Корпоративные факторы развития бизнеса, отраслевая специфика, регуляторные требования и стратегические цели, определяющие требования к информационной безопасности

Инвентаризация, классификация и профили риска технологических, физических и информационных активов, которые поддерживают бизнес-процессы

Технологические процедуры и стандарты для обеспечения безопасности операционных систем, баз данных, приложений и сетевых устройств

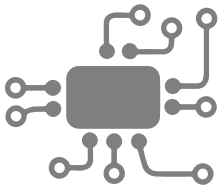
Организация, роли, ответственности и персонал сопровождающий и выполняющий программу безопасности

EY
Building a better working world

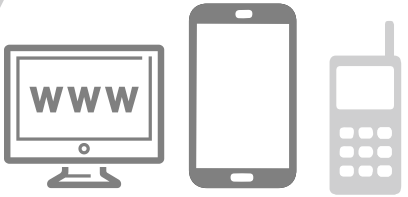
Ландшафт кибер рисков

Тенденции в информационной безопасности

Развитие технологий

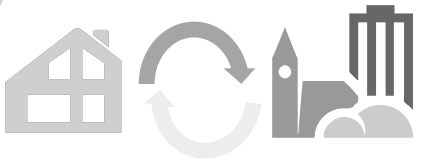


Информатизация окружающей среды



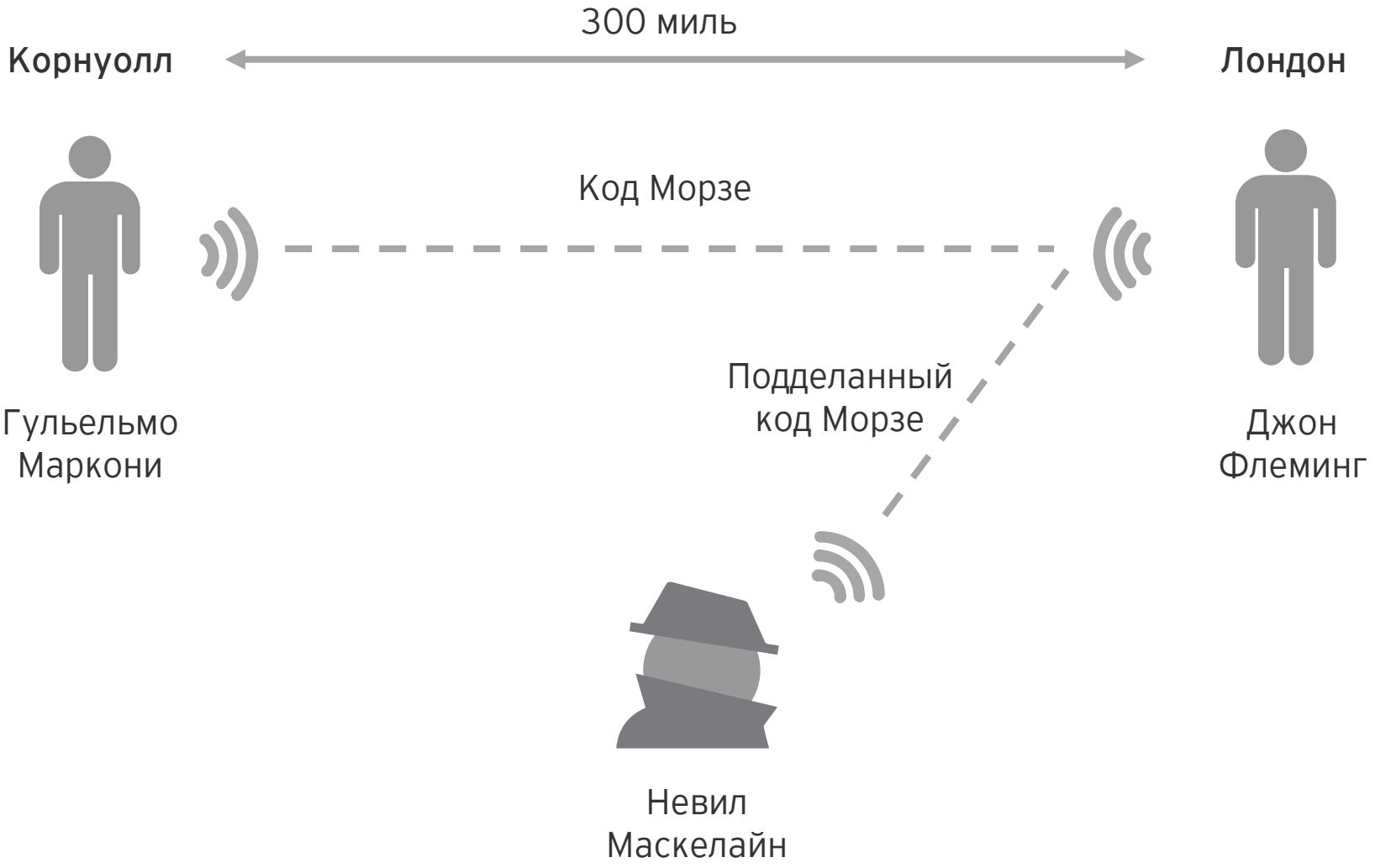
Популярность мобильных технологии

Облачные вычисления



Угрозы воздействующие на инфраструктуру

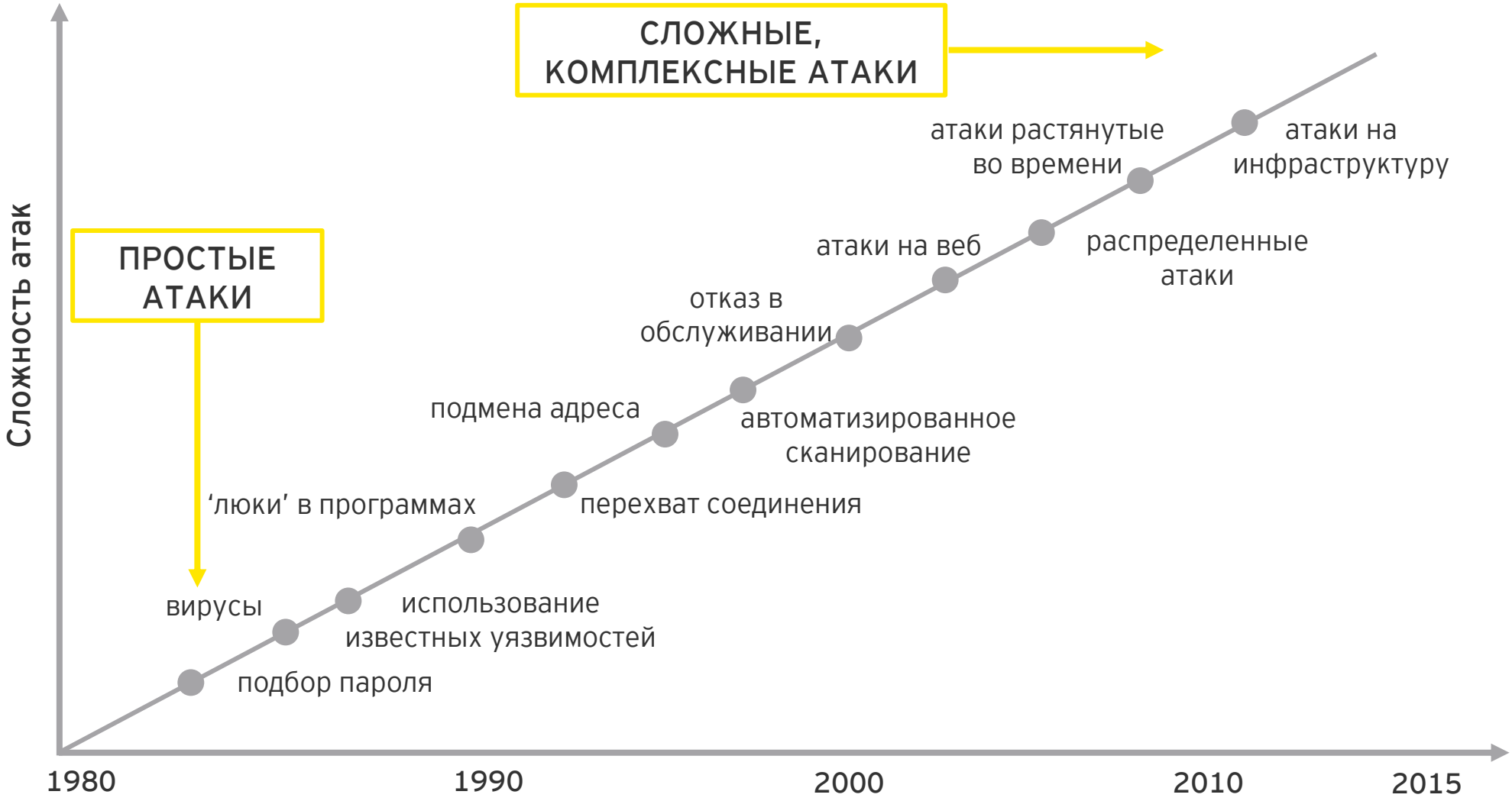
Первый взлом в истории



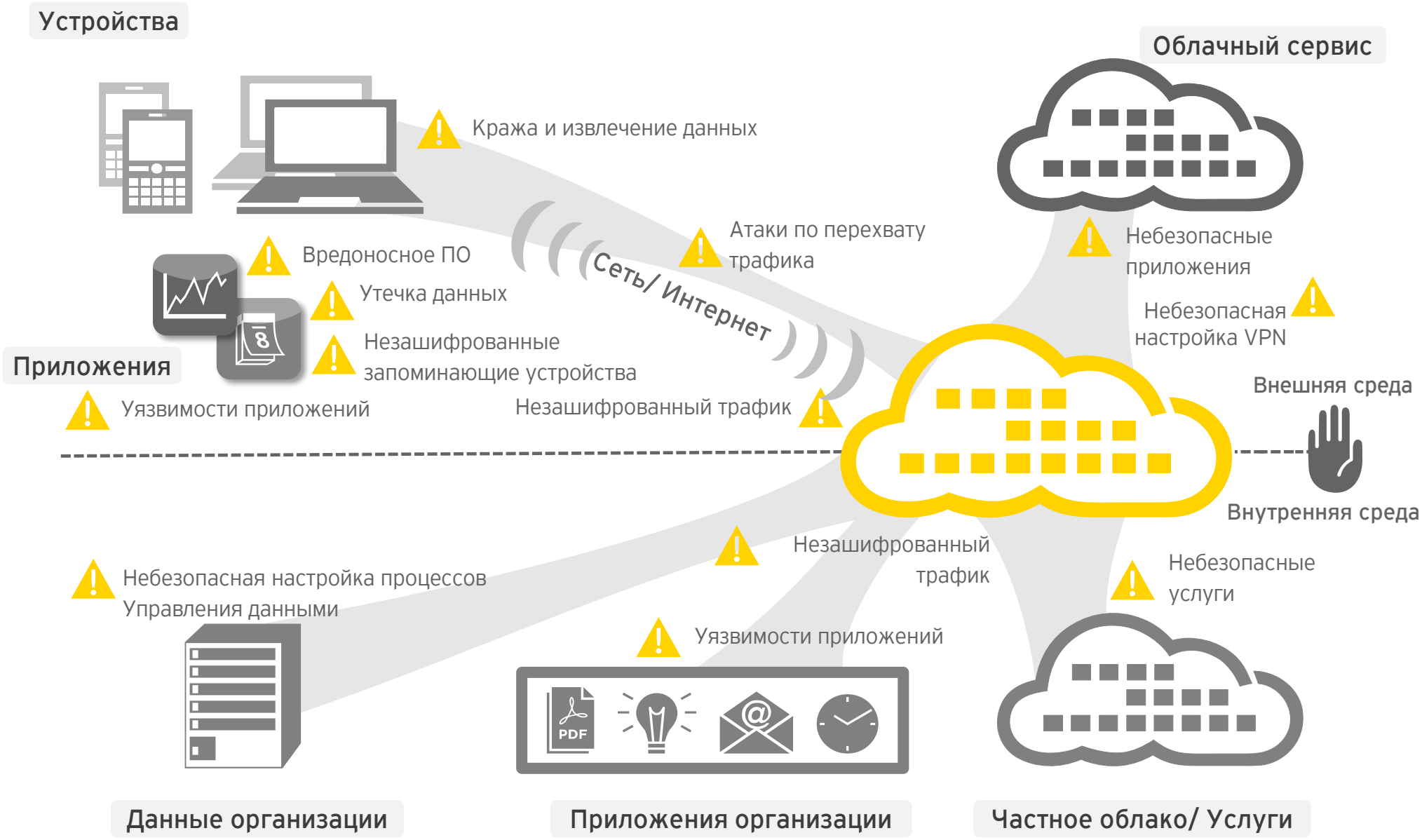
Хакеры и их мотивация

Тип хакеров	Основная мотивация
Этичные хакеры (White hats)	Улучшить защиту
Хакеры-дилетанты (Script kiddies)	Прославиться
Хакеры-одиночки	Развлечься
Группы хакеров (Хактивисты)	Продвинуть политические или религиозные идеи
Хакеры, поддерживаемые государством	Контролировать
Хакеры в криминальных структурах	Заработать
Кибер-террористы	Разрушить

Сложность хакерских атак постоянно растет



Облачные вычисления порождают новые риски



EY
Building a better working world

Кибер риски: факты и цифры (1/3)

Наиболее вероятные источники атак

Хакеры - наиболее вероятный источник атак

36% не способны обнаружить сложную атаку

88% респондентов считают, что их функция ИБ не соответствует нуждам бизнеса

Источник данных: EY GISS 2015

EY Building a better working world

Кибер риски: факты и цифры (2/3)

За 2015 год количество вредоносных программ для мобильных устройств выросло на 72%

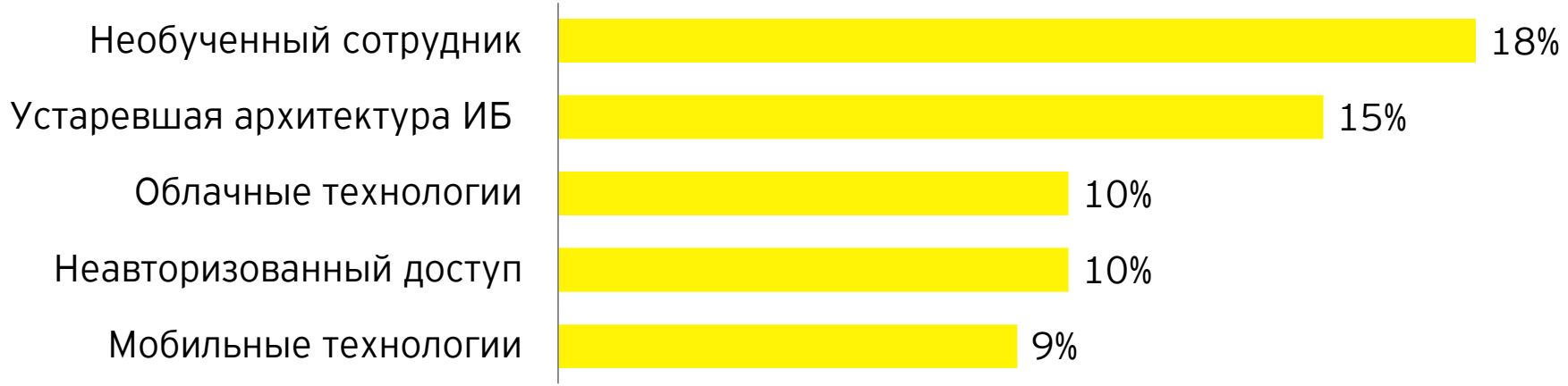
По статистике, 18% пользователей открывают полученное фишинговое сообщение и переходят на вредоносную ссылку

На 26% увеличилось количество программ, требующих выкупа

Источник данных: Отчет McAfee за Март 2016 года

Кибер риски: факты и цифры (3/3)

ТОП 5 уязвимостей по степени критичности



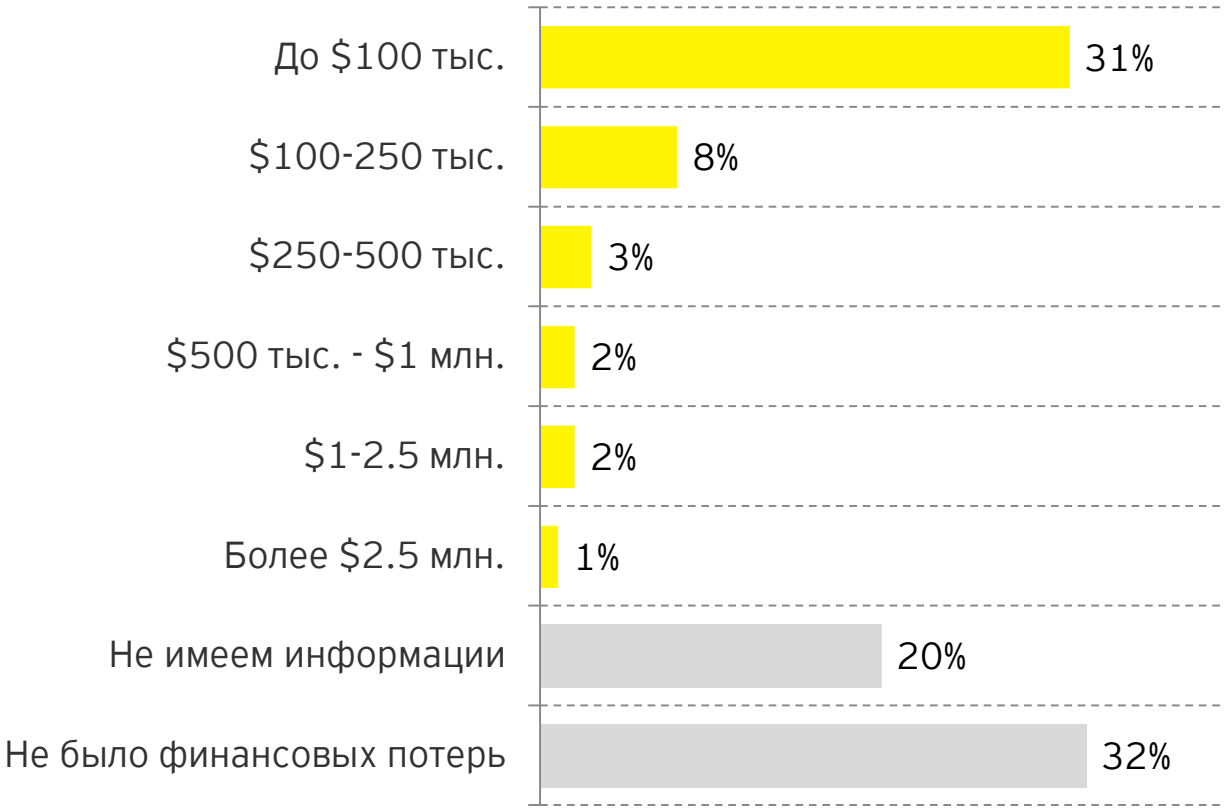
ТОП 5 угроз по степени критичности

Источник данных: EY GISS 2015

EY
Building a better working world

Цена реализации кибер рисков

Ущерб, который понесли организации от инцидентов ИБ



Общая сумма ущерба

$202 млн.
потеряли наши респонденты за последний год

При этом...

62%
респондентов отметили нехватку финансирования ИБ

- Около половины организаций понесли денежные потери от инцидентов ИБ. При этом, каждый пятый респондент не имеет информации о финансовом ущербе
- Организации на территории СНГ потеряли 4,1 млн долл. США, в то время как известный ущерб, нанесенный украинским компаниями не превышает миллион долларов США

EY
Building a better working world

Человек – самое слабое звено

Типы инцидентов, связанных с человеческим фактором

- Социальная инженерия
- Непреднамеренное разглашение
- Потеря оборудования
- Промышленный шпионаж

64% респондентов считают беспечность и неосведомленность сотрудников одной из наибольших уязвимостей

Примеры инцидентов, связанных с человеческим фактором

1 Передача коммерческой тайны

- Российская машиностроительная компания
- Передача ноу-хау конкурентам
- Ущерб в размере 50 млн. рублей

2 Ошибочная рассылка

- Одна из украинских компаний
- Ошибочная рассылка зарплатной ведомости
- Отток ключевых специалистов

3 Разглашение финансовых планов

- Американский банк
- Разглашение финансовых планов
- Ущерб 2 млрд долл. и падение акций на 17%
- Наибольший известный ущерб от утечки данных

EY
Building a better working world

Утечка данных: цифры и факты

$14 000 теряют малый и средний бизнес за один инцидент

$695 000 теряет крупный бизнес за один инцидент

В среднем, сотрудник небольшой компании (штатом до 500) отправляет 48 и получает 125 сообщений электронной почты в день

От 20% до 25% электронных писем содержат вложения, любое из которых может содержать конфиденциальную информацию

31% сотрудников в небольших компаниях и 16% в более крупных являются пользователями Facebook

15% пользователей в крупных компаниях и 29% в небольших используют службы мгновенный сообщений

Источники данных:
Лаборатория Касперского,SearchInform

EY
Building a better working world

Сложности, с которыми сталкиваются организации

Внешние

Внутренние

59% респондентов считают криминальные синдикаты наиболее вероятным источником атак (53% в 2014)

57% респондентов отметили нехватку навыков персонала в сфере ИБ (53% в 2014)

Смещение вектора атак

Нехватка навыков персонала в сфере ИБ

43% респондентов планируют потратить больше на облачные технологии (39% в 2014)

62% респондентов отметили нехватку финансирования ИБ (63% в 2014)

Расширение периметра защиты

Информационная безопасность

Недостаток бюджета

36% респондентов отметили низкую вероятность обнаружения атак (22% в 2014)

36% респондентов не используют программы актуализации данных об угрозах (36% в 2014)

Рост сложности атак хакеров

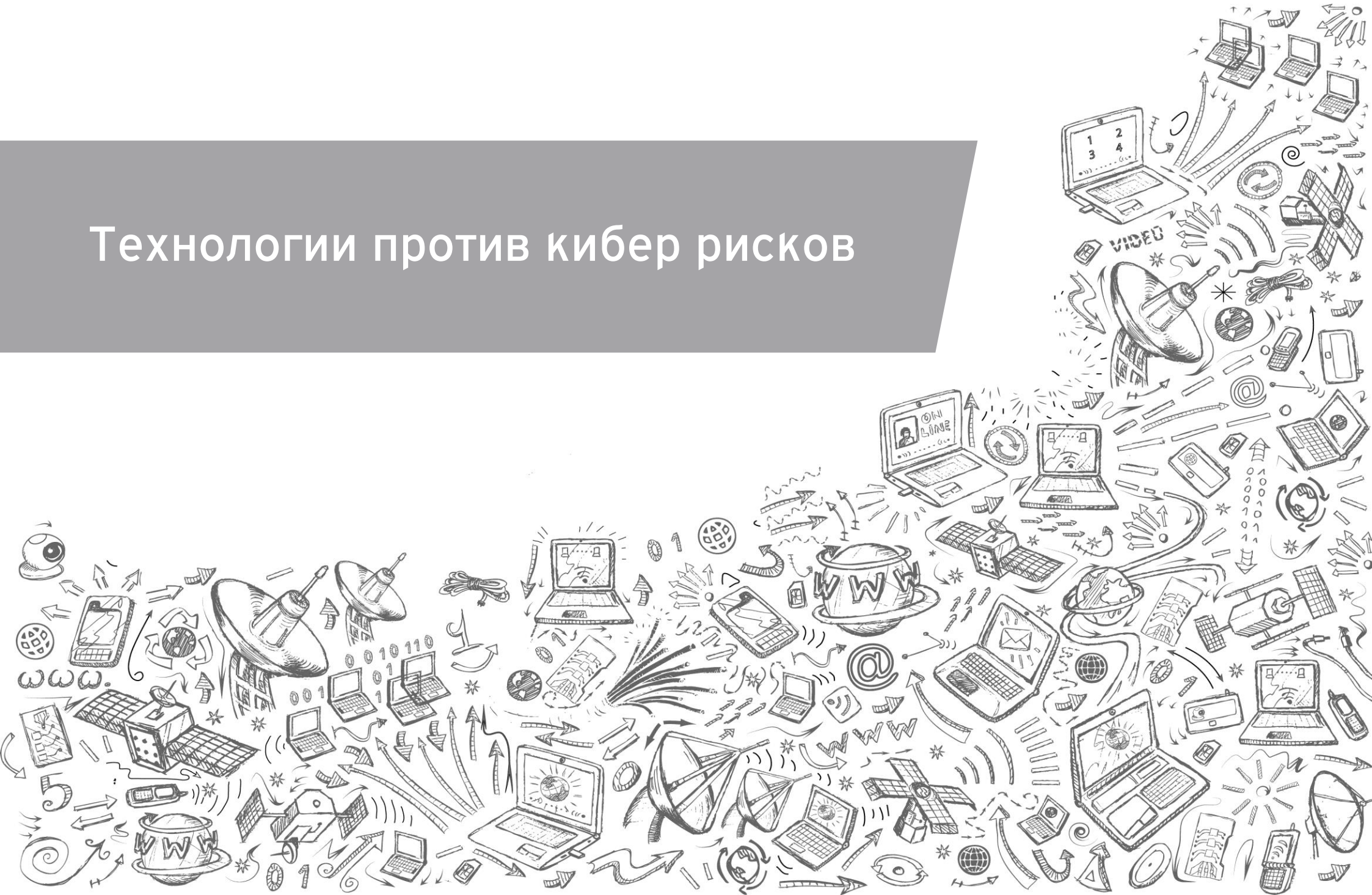
Недостаточная гибкость системы защиты

Источник данных: EY GISS 2015

Насколько хорош Ваш контроль безопасности?

“The boss is worried about information security, so he sends his messages one alphabet letter at a time in random sequence.’

Технологии против кибер рисков

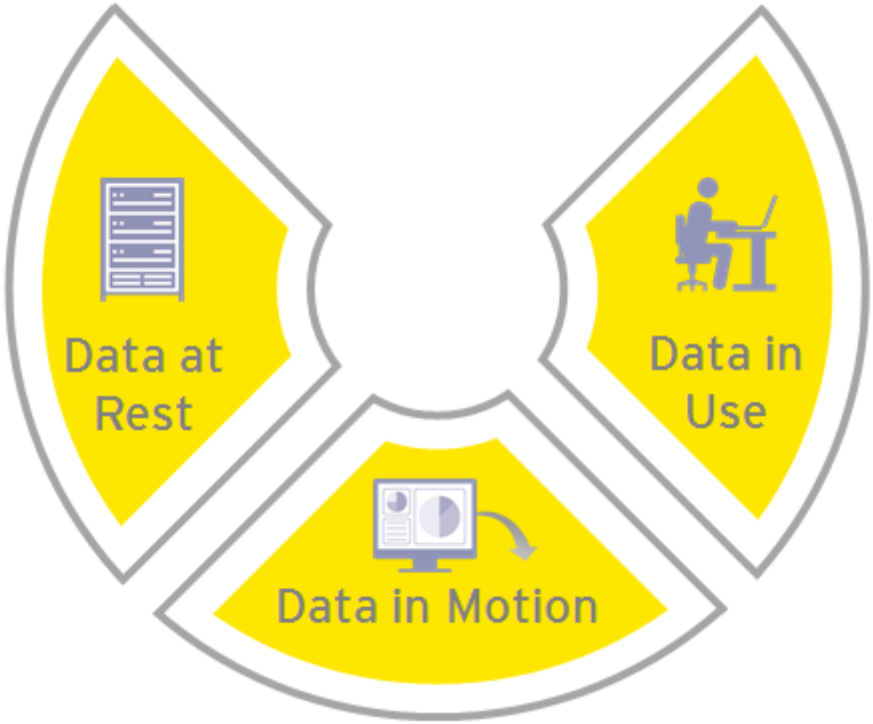


Информация может находится в различных состояниях

Современные подходы и решения по защите данных от киберугроз направлены на построение превентивных и детективных мер для защиты данных в различном состоянии.

С точки зрения утечки информации выделяют три состояния данных:

- Данные на файловых серверах, рабочих станциях, мобильных устройствах, в базах данных



- Файлы в оперативной памяти ПК, открытый отчет или запущенный запрос, черновик сообщения электронной почты

- Сообщения электронной почты, мгновенные сообщения

Система защиты должна быть комплексной

Управление данными

Политики и стандарты	Идентификация	Классификация	Оценка рисков	Архитектура	Качество

Контроль данных

Структурированная информация

Ключевые направления

Data in motion	Data in use	Data at rest
Безопасность периметра	Мониторинг доступа / использования	EndPoint защита
Сетевой мониторинг	Мониторинг привилегированных пользователей	Шифрование дисков
Контроль доступа во внешние сети	Обезличивание данных	Защита мобильных устройств
Обмен данными вне периметра	Использование тестовых данных	Контроль файловых хранилищ
Сообщения (эл.почта, чаты)	Редактирование данных	Контроль внешних носителей
Удаленный доступ	Контроль сохранения\экспорта данных	Утилизация и уничтожение данных

Неструктурированная информация

Процессы информационной безопасности

Управление доступом (IAM)	Управление событиями безопасности	Управление конфигурациями	Отношения с 3-ми лицами
Управление уязвимостями	Реакция на инциденты	Физическая безопасность	Повышение осведомленности
Управление активами	Защита персональных данных	Проверка сотрудников	Управление изменениями
Непрерывность бизнеса	Катастрофоустойчивость	Соответствие требованиям	Безопасная разработка

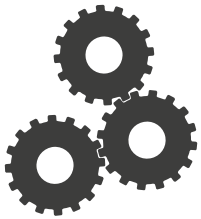
EY
Building a better working world

Различают организационные и технические меры защиты

Информационная безопасность

Меры организационного характера

- Управление рисками
- Разработка политик и процедур в области ИБ
- Управление доступом в информационных системах
- Управление инцидентами
- Ограничение физического доступа в помещения и к оборудованию
- Повышение осведомленности в области ИБ



Меры технического характера

- Разграничение доступа в информационных системах
- Управление паролями
- Настройки безопасности приложений, ОС, СУБД, сетевых устройств
- Системы обнаружения/ предотвращения вторжений, фаерволлы
- Резервное копирование

Инфраструктура ИТ системы состоит из 5 уровней

ИТ-система – это, как правило, 5-уровневый программно-аппаратный комплекс, состоящий из следующих компонентов:

- Приложение (пользовательская часть и серверная часть) - то, с чем контактирует пользователь (видимая часть) и то, что скрыто «за кадром»
- Операционная система - система, которая управляет ресурсами различных приложений
- База данных и система управления базой данных (логическое упорядоченное хранилище таблиц с информацией)
- Аппаратное обеспечение - сервера и персональные компьютеры, которые обрабатывают данные
- Сетевая инфраструктура - оборудование и каналы передачи данных

Каждый из этих уровней потенциально является подверженным угрозам информационной безопасности

Защита ИТ систем: Идентификация и аутентификация

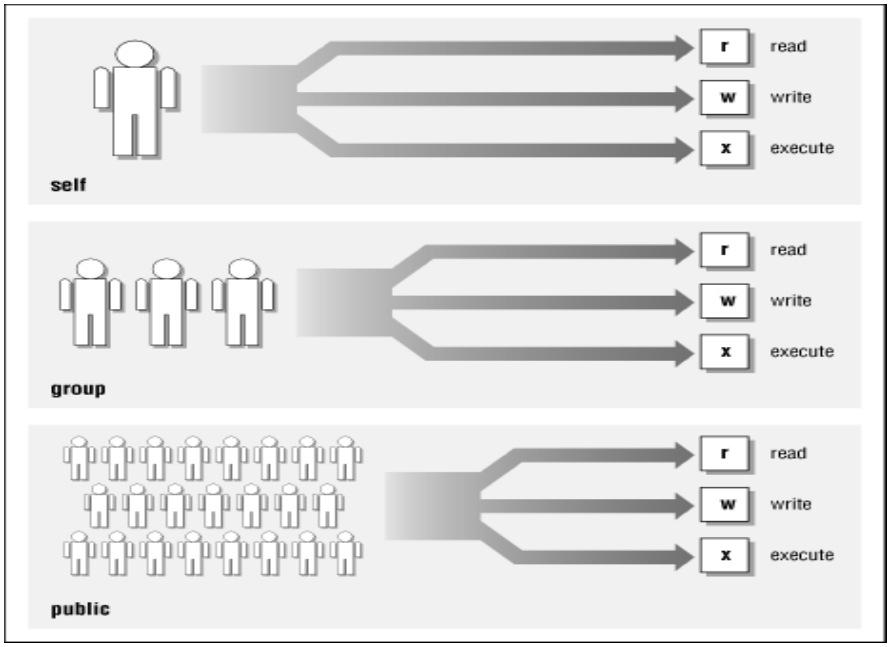
Идентификация - заключается в сообщении пользователем своего идентификатора. Для того чтобы установить, что пользователь именно тот, за кого себя выдает, то есть что именно ему принадлежит введенный идентификатор, в информационных системах предусмотрена процедура **аутентификации**.

- Пользователь аутентифицируется на основании:
  - того, чем пользователь владеет (ключ или магнитная карта)
  - того, что пользователь знает (пароль)
  - атрибуты пользователя (отпечатки пальцев, подпись, голос)

Защита ИТ систем: Разграничение доступа

Разграничение доступа

- После успешной регистрации система должна осуществлять авторизацию (authorization) - предоставление пользователю прав на доступ к объекту
- Зачастую разграничение доступа базируется на реализации ролевой модели управления доступом



	SUBJECTS \ OBJECTS	A	B	C	D	E	F	G	H	J	K	L
Group 1	Alex	W	W	W	R	R	R	R	R	R	R	R
	Brook	R	W	W	R							
	Chris	R	W	W	R	R						
	Denny	R	W	W	R	W	R					
Group 2	Eddie	R	R	R	W	W	W					
	Fran	R	R	R	R	W	W					
Group 3	Gabriel	R	R	R			R	W	W	R		
	Harry	R						W	W	R	R	R
	Jan							W	W	W		
Group 4	Kim	R									W	W
	Lee	R									W	W
	Meryl	R									W	W

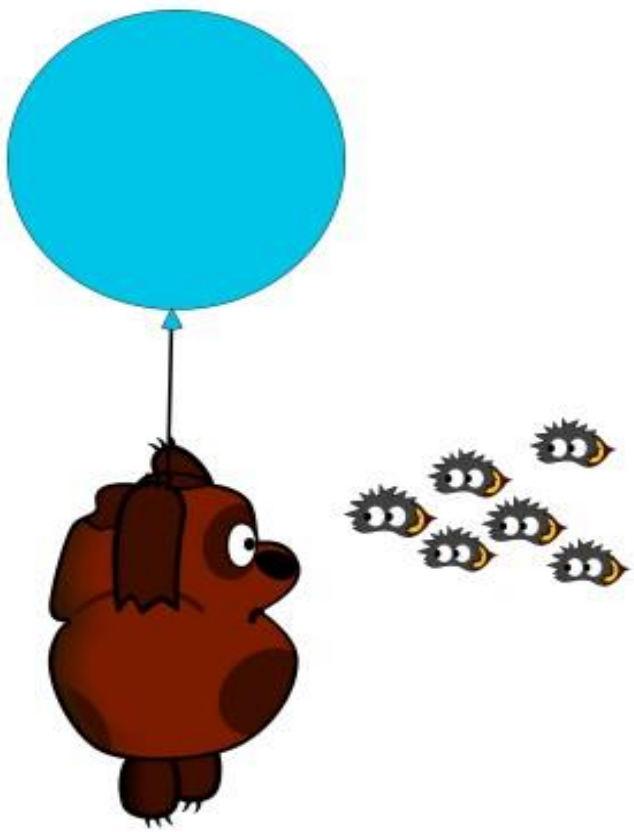
Notes:
R Read
W Write and read

Защита ИТ систем: Пароли

Наиболее простой подход к аутентификации - применение пароля.

- Парольные настройки включают в себя:
  - минимальную длину пароля
  - периодичность смены пароля
  - требования к сложности пароля (наличие в пароле цифр, букв, спецсимволов)
  - сохранение истории предыдущих паролей с невозможностью их повторного использования
  - блокировку учетной записи при определенных количествах неудачного входа

Защита ИТ систем: Пароли



В качестве примера возьмем стишок из известного мультфильма:

Кто ходит в гости по утрам,
Тот поступает мудро!
Тарам-парам, парам-тарам,
На то оно и утро!

Сложный пароль. Оставляем первые буквы каждого слова из песни в присущем им регистре (как они пишутся в куплете). В итоге получаем:

Кхвгпу
Тпм
Тппт
Нтоиу

Составим в одну строку: **КхвгпуТпмТпптНтоиу**. Это и есть наш пароль. Набранный в латинской раскладке, он дает нам 18-тисимвольное **R[dugeNgvNggnYnjbe**

Защита ИТ систем: Пароли (шифрование)

С хранением и передачей пароля связаны основные проблемы:

- Если передавать пароль в открытом виде, то его можно узнать, прослушивая пакеты по сети
- Хранить пароль на сервере в открытом виде тоже небезопасно, так как его можно подсмотреть

Шифрование – процесс преобразования сообщения из открытого текста (plaintext) в шифротекст (ciphertext) таким образом, чтобы:

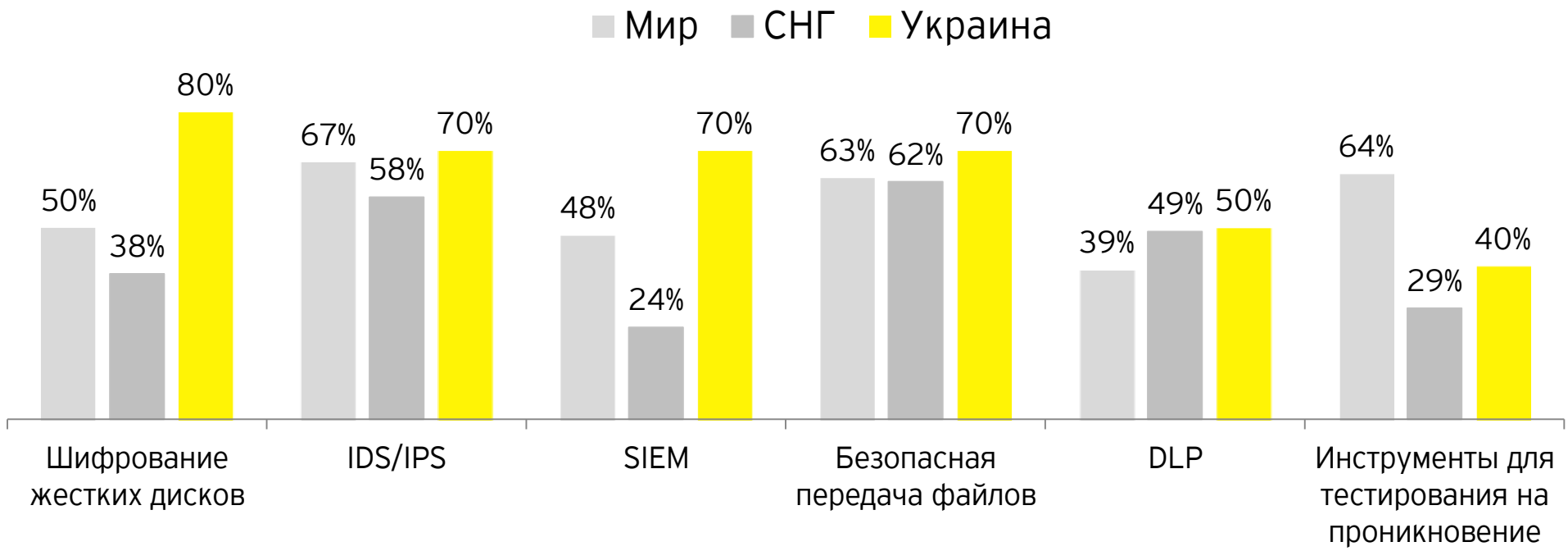
- его могли прочитать только те стороны, для которых оно предназначено
- проверить подлинность отправителя (аутентификация)
- гарантировать, что отправитель действительно послал данное сообщение

Наиболее распространенными методами шифрования являются:

- Алгоритмы одностороннего хеширования (MD4, MD5, SHA)
- Алгоритмы шифрования (DES, 3DES, AES)
- Криптографические протоколы (CHAP, S-HTTP, WPA2, etc.)

Наиболее приоритетные технологии ИБ

Наиболее приоритетные технологии ИБ



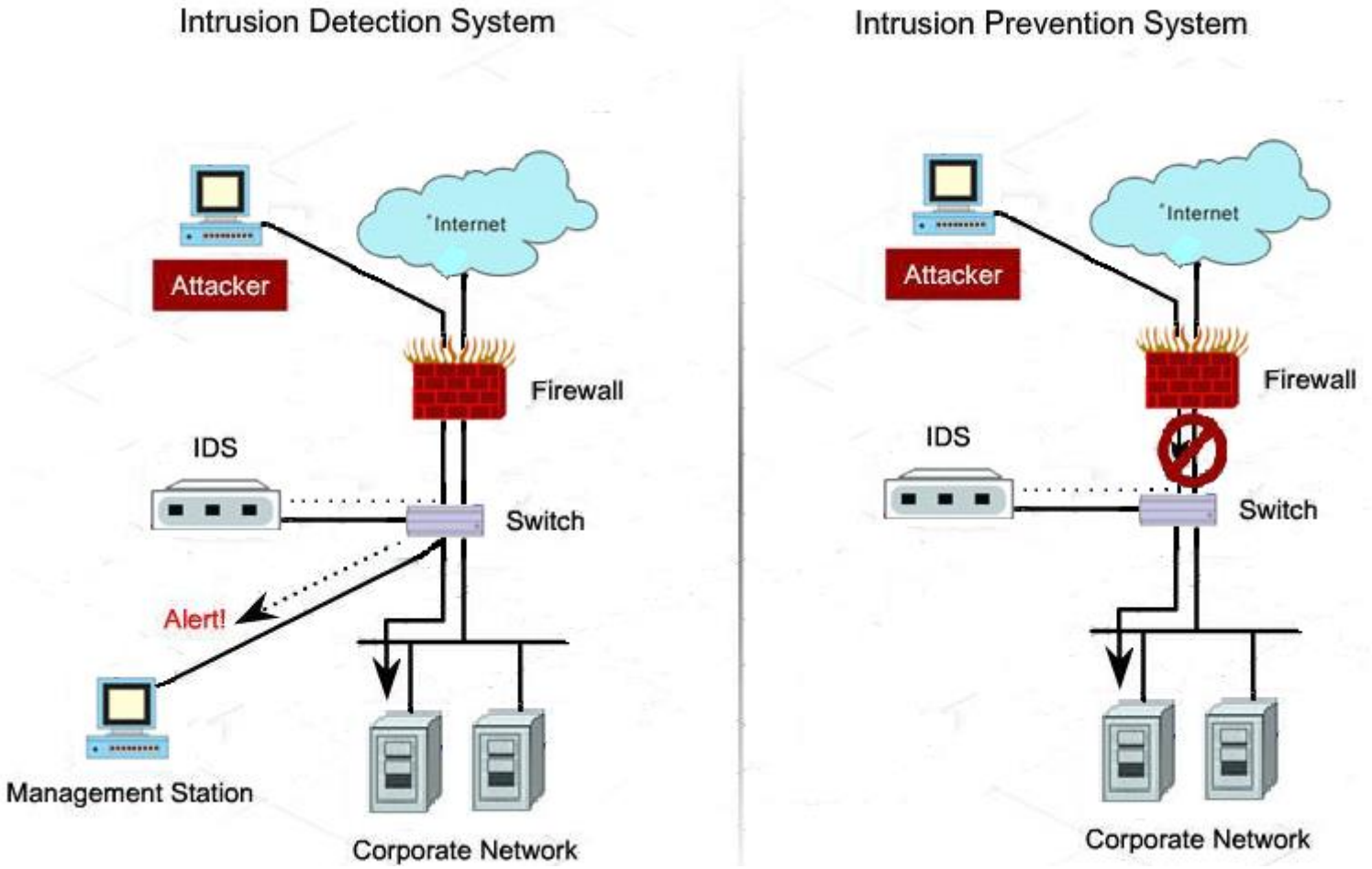
- Украинские компании уделяют довольно много внимания технологиям ИБ и идут в ногу с отраслевыми показателями
- Однако, украинские компании и компании СНГ уделяют гораздо меньше внимания тестированию на проникновение, чем это делают мировые компании

Источник данных: EY GISS 2015

EY
Building a better working world

Обнаружение и предотвращение вторжений

Система обнаружения и предотвращения вторжений (Intrusion Detection and Prevention System – IDS/IPS) – программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.



Пример работы DLP системы

Система предотвращения утечек данных (DLP система – Data Leakage Prevention) – набор различных автоматизированных средств, позволяющих распознавать и блокировать несанкционированное использование или передачу конфиденциальных данных.

EY
Building a better working world

Управление информацией и событиями безопасности

Система управление информацией и событиями безопасности (Security information and event management, IDS/IPS) – система, которая предназначена для сбора и анализа в реальном времени событий безопасности, исходящих от сетевых устройств, приложений, систем безопасности, других систем и устройств.

Общий подход к тестированию на проникновение

Тестирование на проникновение (Penetration testing) – оценка безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника.

Тестирование на проникновение

Этап 1 Сканирование

- Сбор и анализ информации о периметре безопасности
- Анализ социальных сетей
- Сканирование периметра безопасности с помощью специализированных инструментов
- Идентификация уязвимостей

Этап 2 Планирование атак

- Разработка сценариев атак на основании целей атак и выявленных уязвимостей
- Определение и подготовка необходимых специализированных инструментов
- Оценка рисков реализации атак
- Планирование проведения атак (дата, время)

Этап 3 Проведение атак

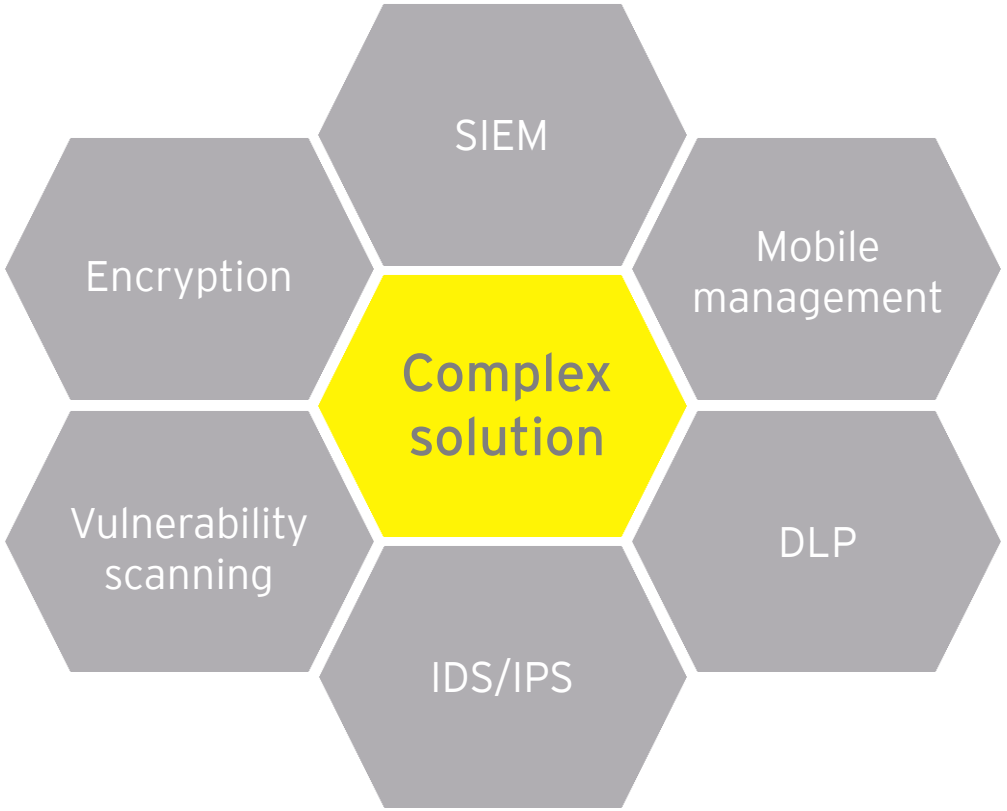
- Проведение атак в запланированное время
- Сбор информации об успешных и неуспешных атаках
- Подготовка отчетов и презентация их заказчику

Инструменты для тестирования на проникновение

Инфраструктурные компоненты	Веб-приложение	Клиент-серверные приложения	Операционные систем	Приложения	Беспроводные сети
Nmap/Amap/SuperScan	WebScarab	Wireshark	Ettercap-ng	Mercury script database	Airmon-ng
Whisker/nikto.pl	Metasploit	Eclipse IDE	Ernst & Young Mercury scripts	FX Cop	Airodump-ng
Netcat	Nessus	JAD	MS Baseline analyser	IBM Red Book Series	Aireplay-ng
Ophcrack	Cenzic Hailstorm	Boomerang	nmap	OWASP Code Review Guide	Aircrack-ng
Maltego	HP Web Inspect	sslcaudit	dnmap client	Alive6	Reaver
NBTscan/enum	Websmack	ssldump		DMitry	
Wininfo/walksam	Burp Suite Professional	sslscan		nbtscan	
Dsniff	Hydra	sslsniff		smtp-user-enum	
Metasploit	OWASP-ZAP	sslstrip		cisco-auditing-tool	
Wireshark	Wafw00f			cisco-torch	
Cain	smtp-user-enum			Bruteforce Exploit Detector	
Phonesweep (War dialling)	ssldump			hexorbase	
PSH toolkit	sslscan			sidguesser	
Stunnel	sslsniff				
OAT (Oracle Auditing Tool)	sslstrip				
SQL Ping	Nikto				
Nessus					
Cenzic Hailstorm					

Тенденции в технологиях обеспечения ИБ

Комплексные решения ИБ

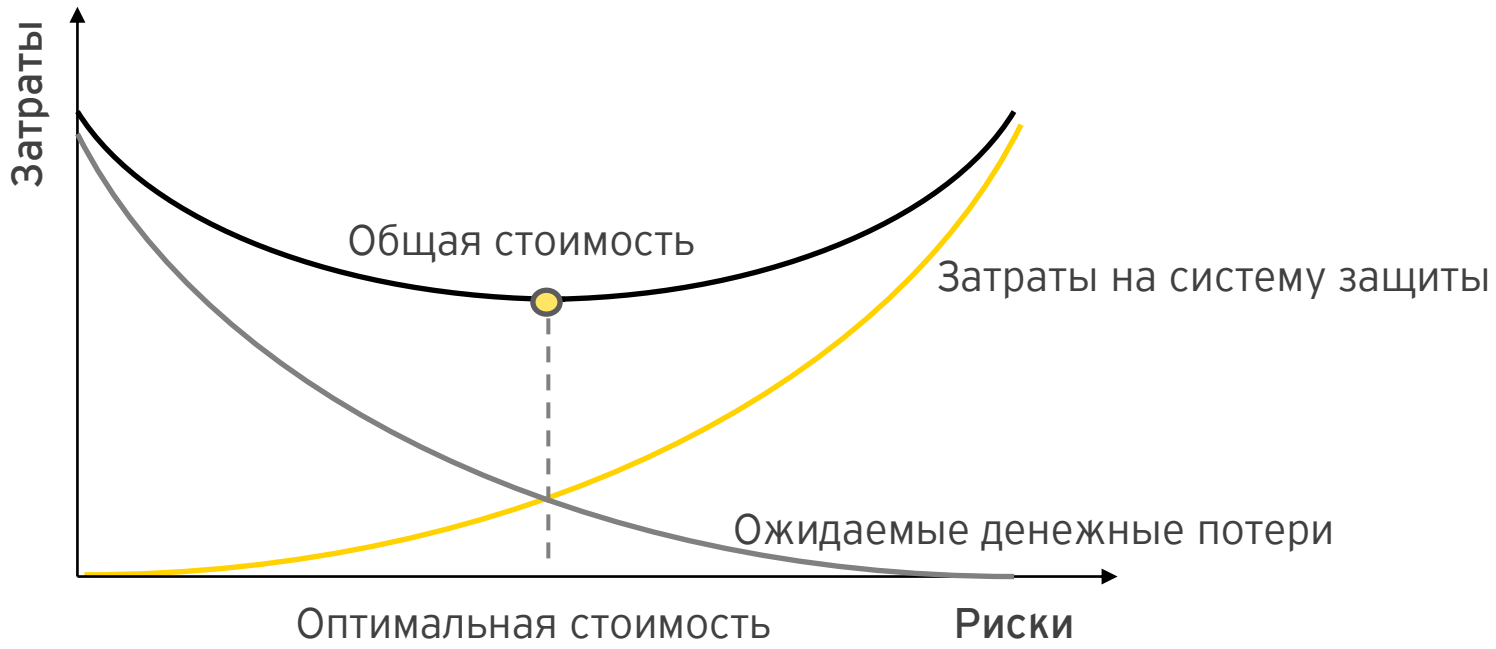


Аутсорсинг функции ИБ и перенос систем в облако

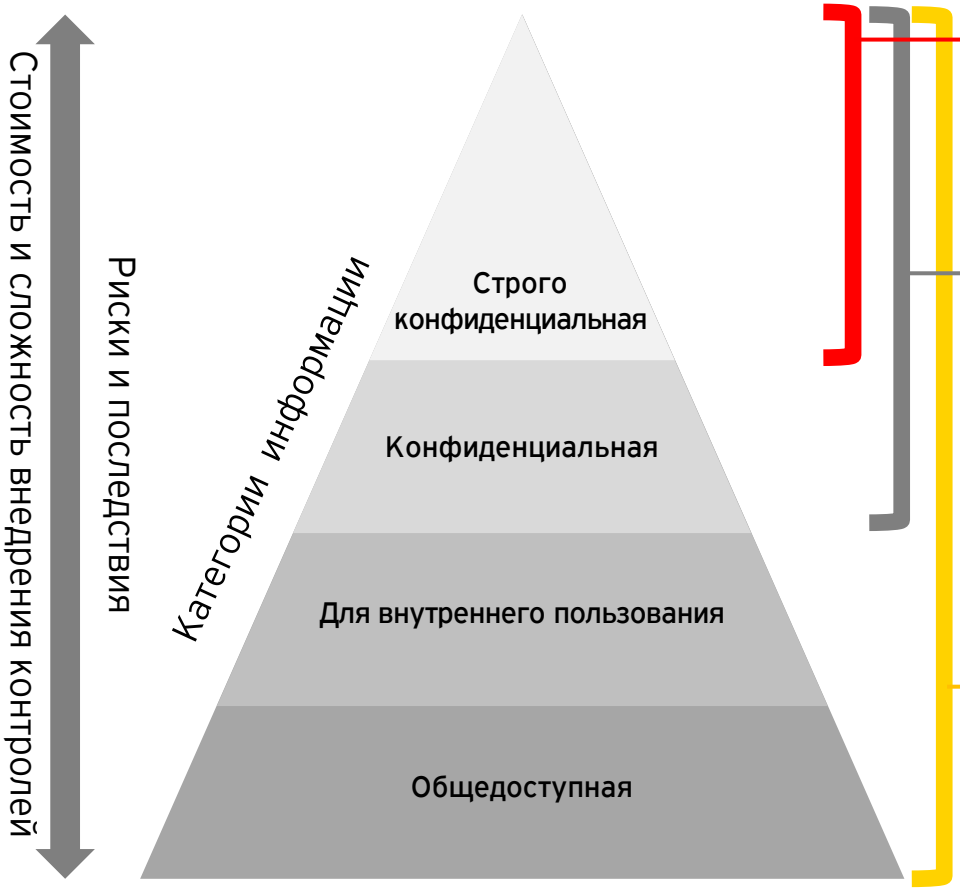
Строить систему защиты необходимо с умом

- Важно, понимать, что не кибер риски не могут быть полностью устранены:
  - Не все угрозы могут быть идентифицированы
  - Смягчение определенных рисков требует больших денежных затрат
  - Не всегда можно определить точный денежный ущерб от реализации риска

- Поэтому, систему защиты необходимо строить с умом, учитывая ее экономическую обоснованность:



Для разной информации – разные средства защиты



Наиболее строгие/дорогостоящие меры защиты

- Контроли наибольшей строгости как правило применяются не более чем к 10-15% данных компании (наиболее критическая информация с точки зрения конфиденциальности)

Целенаправленные меры защиты

- Шифрование
- Обеспечение безопасности сетевого периметра
- Правомерность пользовательского доступа
- Полная регистрация действий и мониторинг
- Многофакторные контроли доступа
- Способность быстрого реагирования
- Инфраструктура виртуальных рабочих столов

Базовые меры защиты

- Повышение осведомленности пользователей
- Управление доступом пользователей
- Управление изменениями
- Управление конфигурациями
- Антивирусная защита
- Физическая защита периметра
- Защита рабочих станций\ноутбуков
- Эвристическое обнаружение угроз и расследование инцидентов

Чем более конфиденциальна информация, тем более строгие и эффективные меры должны применятся для обеспечения ее защищенности

Кейс из практики EY

Основная информация о клиенте. Выявленная проблема

Профиль клиента

- Финансовый сектор
- Территория СНГ: Головной офис, сеть региональных офисов
- Количество персонала ~ 2 000 чел.
- Розничные и корпоративные клиенты

Утечка конфиденциальной информации:

- В открытом доступе выявлена информация о стратегии и планах развития бизнеса
- Непосредственно событие утечки компанией выявлено не было.

Места хранения, передачи и обработки информации

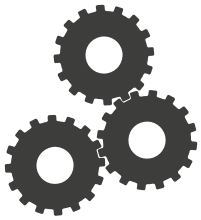
Data-at-rest	Data-in-motion	Data-in-use
Персональные компьютеры, ноутбуки	Сетевое оборудование	Персональные компьютеры, ноутбуки
Мобильные устройства	Коммуникации	Мобильные устройства
Базы данных	Оперативная память устройств	Оперативная память устройств
Хранилища данных		Кэш-память процессора
Резервные копии		Другие интерфейсы информационных систем
Внешние дисковые накопители и другие		Веб-клиенты приложений

Подходы к анализу возможных уязвимостей ИБ

Информационная безопасность

Меры организационного характера

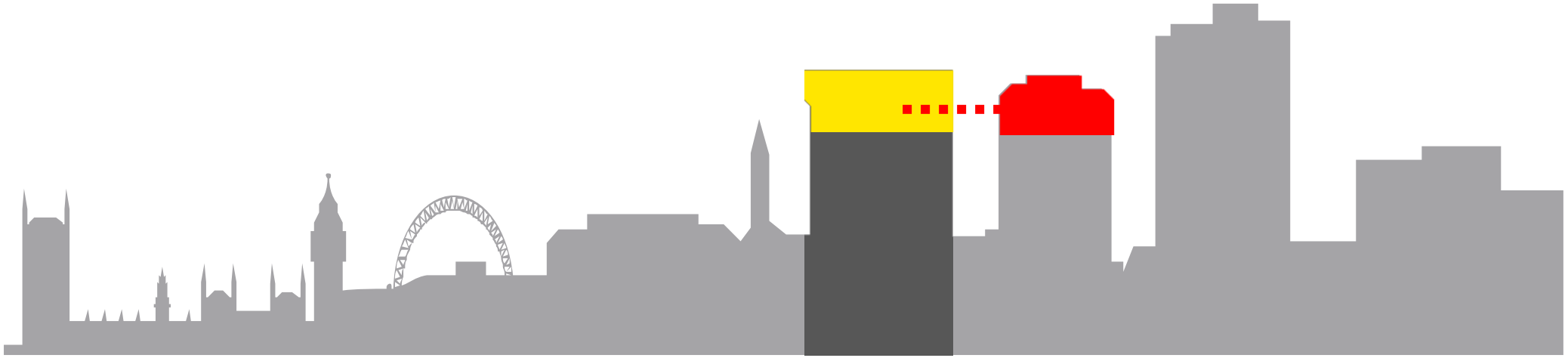
- Аудит основных ИТ-процессов
- Аудит системы управления информационной безопасностью
- Оценка дизайна контролей информационной безопасности
- Тестирование контролей ИБ организационного характера



Меры технического характера

- Тестирование контролей ИБ технического характера
- Анализ настроек безопасности приложений, ОС, СУБД, сетевых устройств
- Проведение тестирования на проникновение
- Анализ логов системы обнаружения/ предотвращения вторжений, фаерволов нового поколения

Современные атаки – комбинация из многих этапов



Первичный анализ цели

Оценка средств информационной безопасности

Выявление «узких мест»

Разработка плана взлома

Подготовка и организация средств и инструментов

Проведение атаки

Защита информации

Шаг 1. Определить что требует защиты

Ответить на вопросы:

- Какая информация существует в организации?
- Кто является ее владельцем?
- Какова ее ценность?
- Какие последствия понесет искажение, разглашение, или утрата информации?

Шаг 2. Разработать и внедрить меры защиты

Разработать и внедрить:

- Организационные меры:
  - Управление доступом в информационных системах
  - Управление инцидентами
  - Ограничение физического доступа в помещения
- Технические меры:
  - Настройки безопасности приложений, ОС, СУБД, сетевых устройств
  - Системы обнаружения/ предотвращения вторжений, фаерволлы
  - Резервное копирование
- Программа повышения осведомленности

Шаг 3. Поддерживать систему защиты

Регулярно проводить:

- Аудит системы управления информационной безопасностью
- Сканирование уязвимостей и тестирование на проникновение
- Актуализацию данных об угрозах ИБ
- Проверки уровня безопасности подрядчиков и облачных провайдеров

Пожалуйста, задайте Ваш вопрос!

Как компании противодействуют кибер рискам

Андрей Уколов
Дарья Богуш

IT Risk & Assurance, EY

Киев, 27 апреля, 2016

EY
Building a better working world