МОСКОВСКАЯ БИРЖА

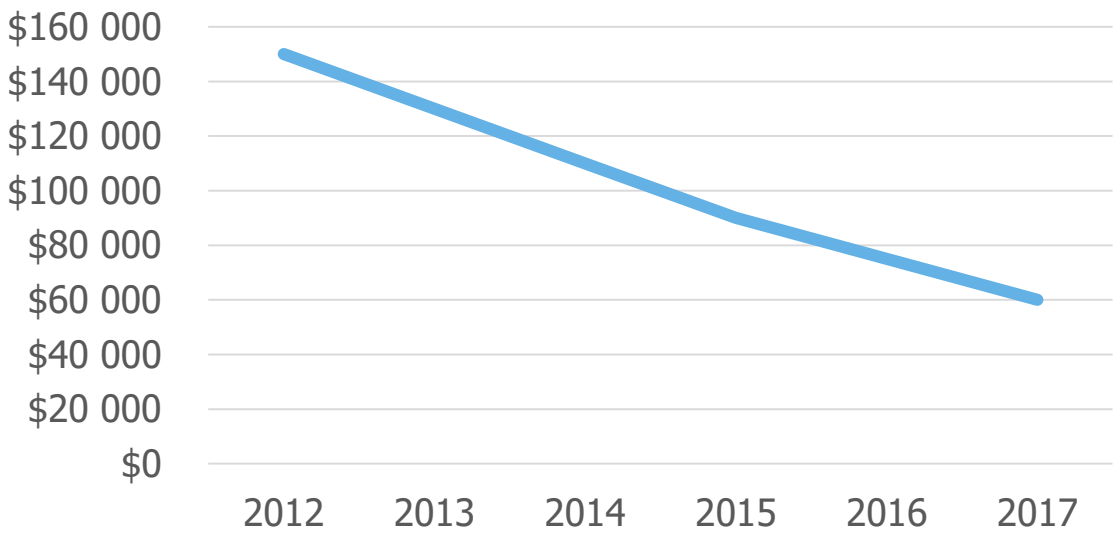
Сергей Демидов

Директор департамента операционных рисков,
информационной безопасности и непрерывности бизнеса

Новые угрозы безопасности vs новые требования регулятора: благодаря или вопреки?

Новые угрозы?

Удешевление стоимости «гарантированных» атак



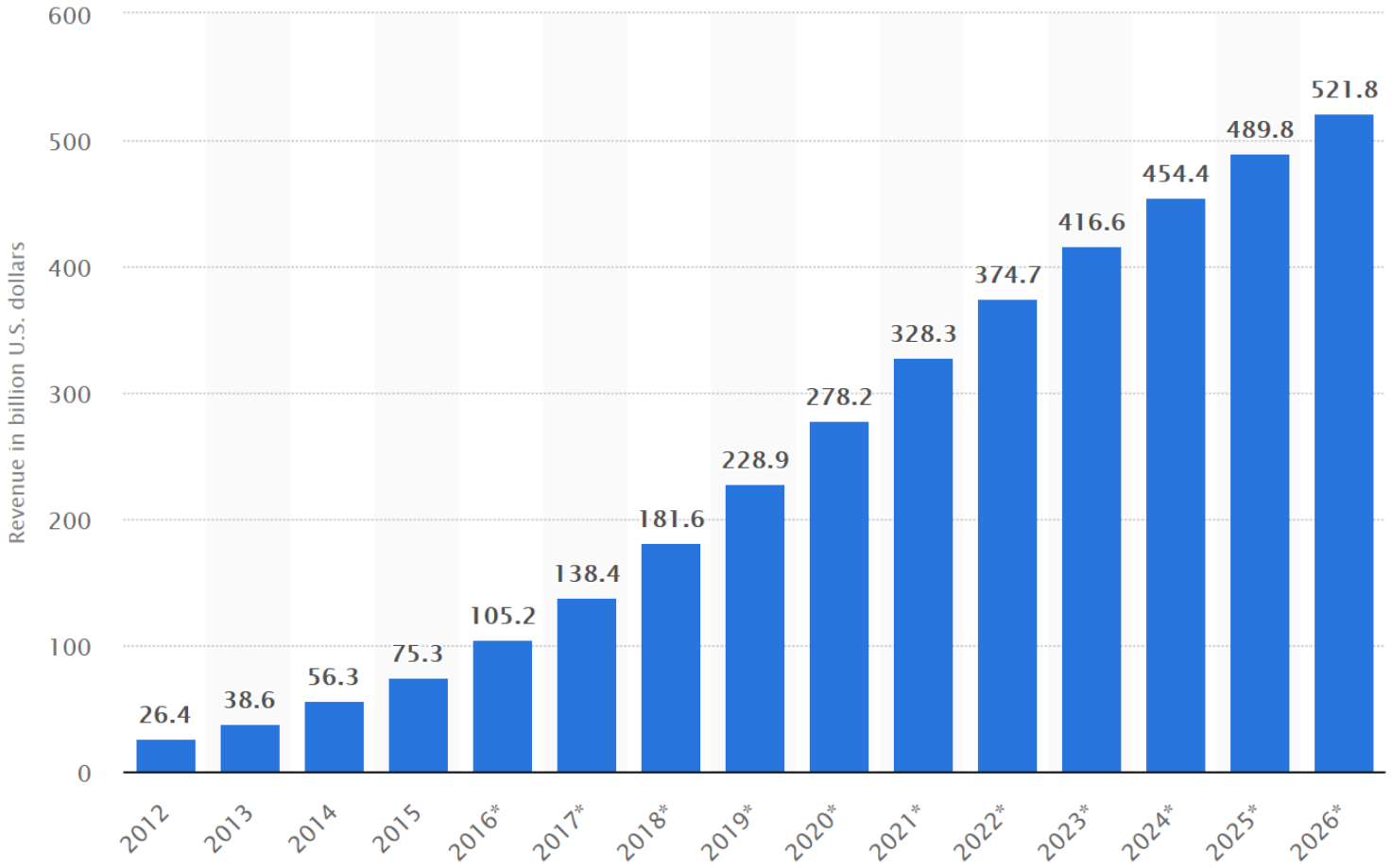
Снижение официальной стоимости 0-day

МОСКОВСКАЯ БИРЖА

Ускорение бизнеса, использование гибких методов в разработке продуктов

МОСКОВСКАЯ БИРЖА

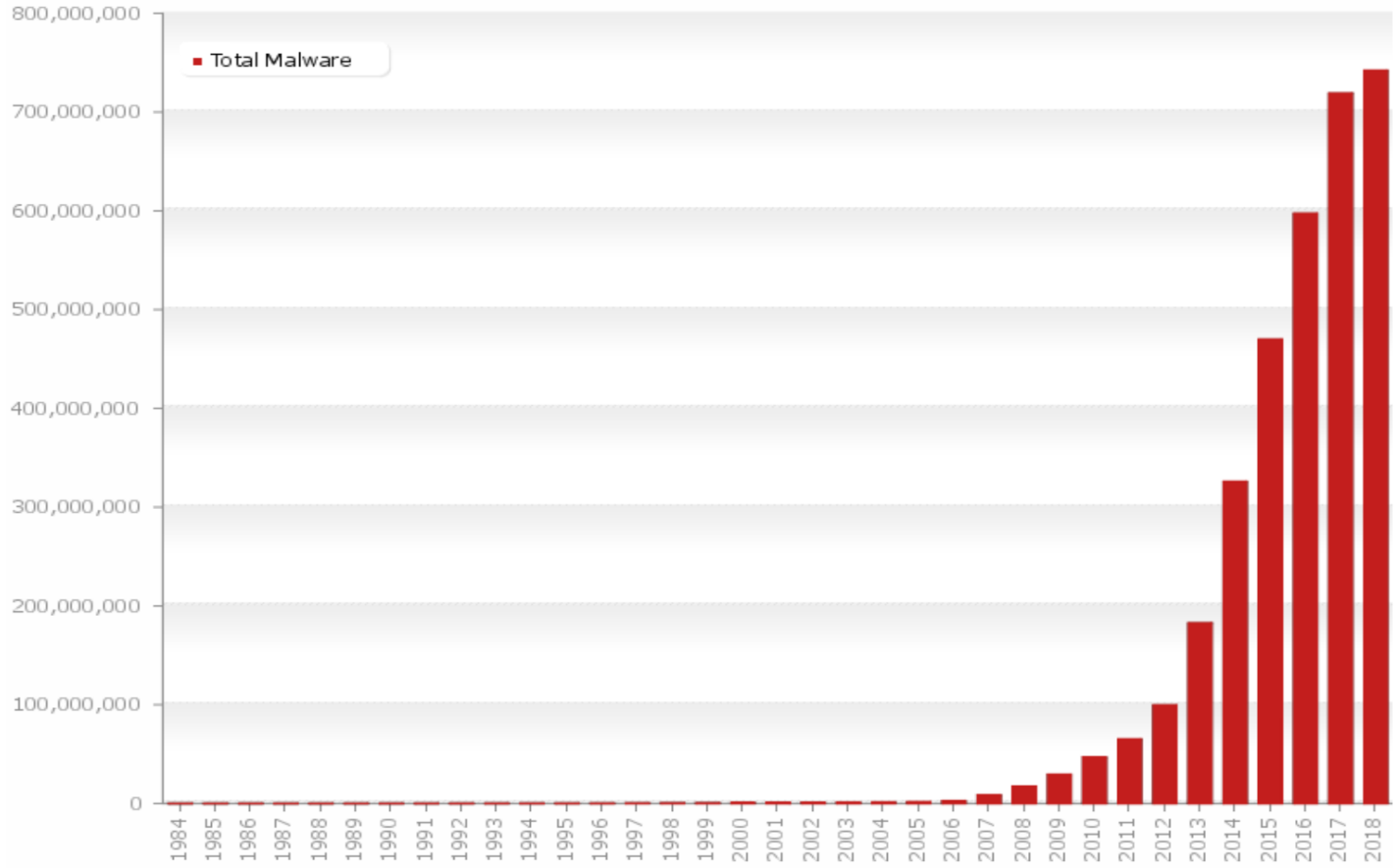
Использование облаков



Прогноз доходов рынка публичных облаков (в млрд. $)

МОСКОВСКАЯ БИРЖА

Устаревание средств безопасности и отсутствие готовых решений ИБ для новых технологий



МОСКОВСКАЯ БИРЖА

Отсутствие кадров и неготовность CISO адаптироваться под новые реальности бизнеса

… к 2022 году недостаток квалифицированных кадров в области информационной безопасности достигнет 1.8 млн специалистов, что на 20% больше чем предполагалось в 2015 году …

Опрос проведенный The International Information System Security Certification Consortium среди 19 000 специалистов по кибер-безопасности по всему миру

Новое регулирование?

Какие стандарты по информационной безопасности затрагивают компании финансового сектора в РФ?

- СТО БР ИББС-1.0-2014
- Письмо Банка России от 24 марта 2014 г. №49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»
- Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств …»
- ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер».
- Закон о Критической информационной инфраструктуре
- 152-ФЗ «О персональных данных»
- PCI DSS
- ПП № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”
- Положение Банка России от 24 августа 2016-го года №552-П "О требованиях к защите информации в платежной системе Банка России"

И другие нормативные акты …

- Требования ФСБ (для обладателей лицензий на криптографию)
- 149-ФЗ «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»
- 63-ФЗ «Об электронной цифровой подписи»
- 98-ФЗ «О КОММЕРЧЕСКОЙ ТАЙНЕ»
- Гражданский кодекс
- Уголовные кодекс
- КоАП РФ

Критическая информационная инфраструктура

6) критическая информационная инфраструктура - объекты критической информационной инфраструктуры ….;
7) объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;
8) субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

МОСКОВСКАЯ БИРЖА

* Статья 2, 187-ФЗ от 26.07.2017

ГОСТ Банка России и требования ФСТЭК по персональным данным

ЦБ

МЕНЕДЖМЕНТ ИБ
АНТИВИРУСНАЯ ЗАЩИТА
СЛУЖБА ИБ КРИПТОГРАФИЯ
ДОКУМЕНТЫ АУДИТ
САМООЦЕНКА УЧЕТ РЕСУРСОВ
МОНИТОРИНГ РИСКИ ИБ
ЖИЗНЕННЫЙ ЦИКЛ РОЛИ ПРЕДОТВРАЩЕНИЕ УТЕЧЕК
УПРАВЛЕНИЕ ДОСТУПОМ ОБНОВЛЕНИЕ ПО
СЕГМЕНТИРОВАНИЕ
ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТ
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ
ДОСТУП К ПДН ПЕРЕДАЧА ПДН
УДАЛЕНИЕ ПДН УЧЕТ НОСИТЕЛЕЙ ПДН
ОБРАБОТКА ПДН В БАНКОВСКИХ ПРОЦЕССАХ
УДАЛЕННЫЙ ДОСТУП СЕРТИФИЦИРОВАННЫЕ СРЕДСТВА
МОНИТОРИНГ ТРАФИКА ВИРТУАЛЬНЫЕ СРЕДЫ
СЕТЕВЫЕ АТАКИ МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ
СЕТЕВЫЕ УСТРОЙСТВА БЕСПРОВОДНЫЕ СЕТИ
РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ
НЕПРЕРЫВНОСТЬ ИДЕНТИФИКАЦИЯ
МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ
АВТОРИЗАЦИЯ ФИЗИЧЕСКИЙ ДОСТУП
КОНТРОЛЬ ИЗВЕСТНЫХ УЯЗВИМОСТЕЙ
РЕГИСТРАЦИЯ СОБЫТИЙ

VS.

ФСТЭК

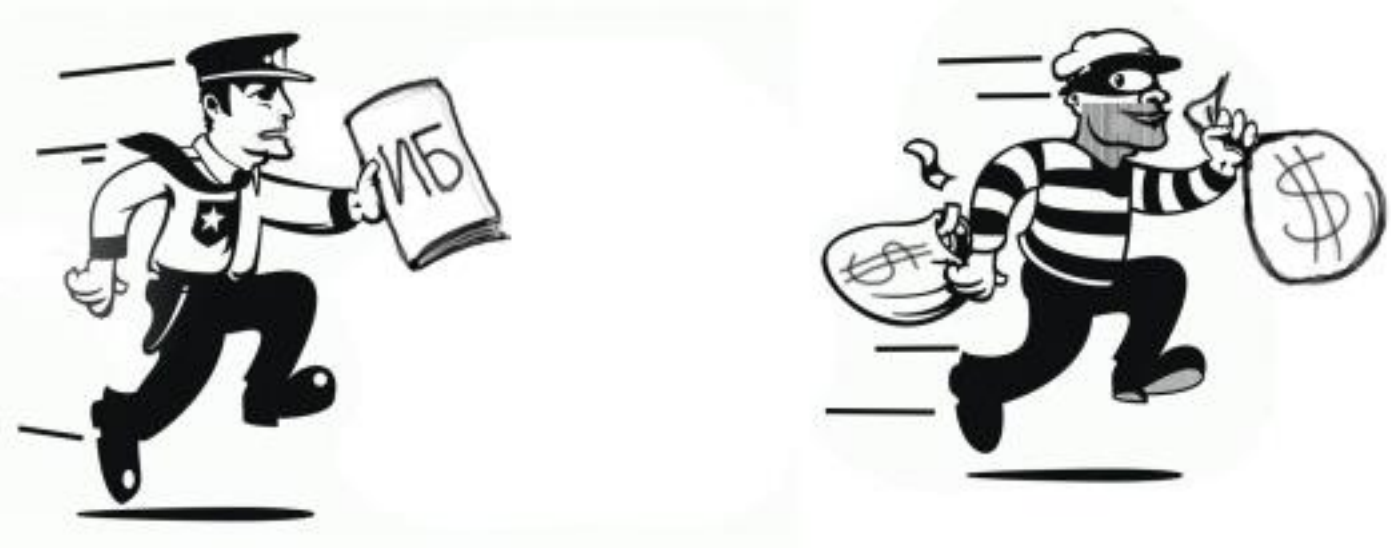
ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ
СОГЛАСИЕ ПЕРЕДАЧА ПДН
БИОМЕТРИЯ КАТЕГОРИИ ПДН
ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА
АУДИТ ПРАВА СУБЪЕКТА
ОТВЕТСТВЕННОЕ ЛИЦО ТИПЫ УГРОЗ
УПРАВЛЕНИЕ ДОСТУПОМ
ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ
АНТИВИРУСНАЯ ЗАЩИТА
ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ
УПРАВЛЕНИЕ КОНФИГУРАЦИЯМИ УЧЕТ НОСИТЕЛЕЙ
СЕРТИФИЦИРОВАННЫЕ СРЕДСТВА
ВОССТАНОВЛЕНИЕ ДАННЫХ
ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ
ЦЕЛОСТНОСТЬ ДОСТУПНОСТЬ
ВИРТУАЛЬНЫЕ СРЕДЫ
АНАЛИЗ ЗАЩИЩЕННОСТИ
ИНЦИДЕНТЫ ИБ РЕГИСТРАЦИЯ СОБЫТИЙ
ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ
БЕЗОПАСНОСТЬ ПОМЕЩЕНИЙ СЕТЕВАЯ ЗАЩИТА
ЗАЩИТА ТЕХНИЧЕСКИХ СРЕДСТВ

Учитывает ли регулирование новые угрозы ИБ?

Распоряжения Правительства РФ от 28.07.2017 г. №1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»

5.4.12. Приняты национальные стандарты информационной безопасности в системах, реализующих облачные, туманные, квантовые технологии, системах виртуальной и дополненной реальности, и технологии искусственного интеллекта	II квартал 2020 г.

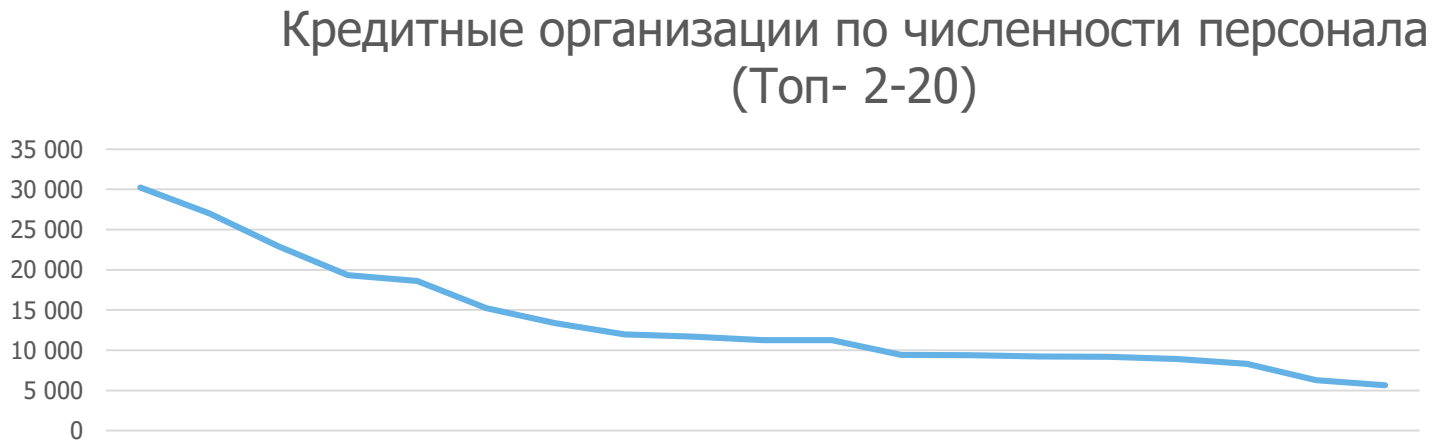
Учитывает ли регулирование новые угрозы ИБ?



… подожди, куда ты?! … я сделал новый стандарт по информационной безопасности …

«Проблема регулятора»

Действующих кредитных организаций (на 01.03.2018) = 551



МОСКОВСКАЯ БИРЖА

А что делать?

А что делать?

Распоряжения Правительства РФ от 28.07.2017 г. №1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»

5.4.1. Создан совет по вопросам безопасности новых технологий, включающий представителей центров компетенций в сфере цифровой экономики, нормативно определены его подчиненность, функции, полномочия	I квартал 2018 г.

СПАСИБО!

МОСКОВСКАЯ БИРЖА