INFOWATCH®

МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Риски и угрозы нового цифрового мира

Президент ГК InfoWatch

Наталья Касперская

Москва, 2017

Предпосылки современных угроз ИТ

- Зависимость от ИТ во всех сферах, «цифровой мир»
- Всеобъемлющий Интернет (подключение к сетям и оборудованию)
- Рост технологических возможностей атак с развитием ИТ
- Отставание средств защиты от новых ИТ-средств
- Ухудшение политической обстановки
- Нехватка квалифицированных кадров

АКТУАЛЬНЫЕ РИСКИ и УГРОЗЫ, связанные с информационными технологиями

Рассмотрим три группы угроз

Утечки и компрометация информации, в том числе, через смартфоны

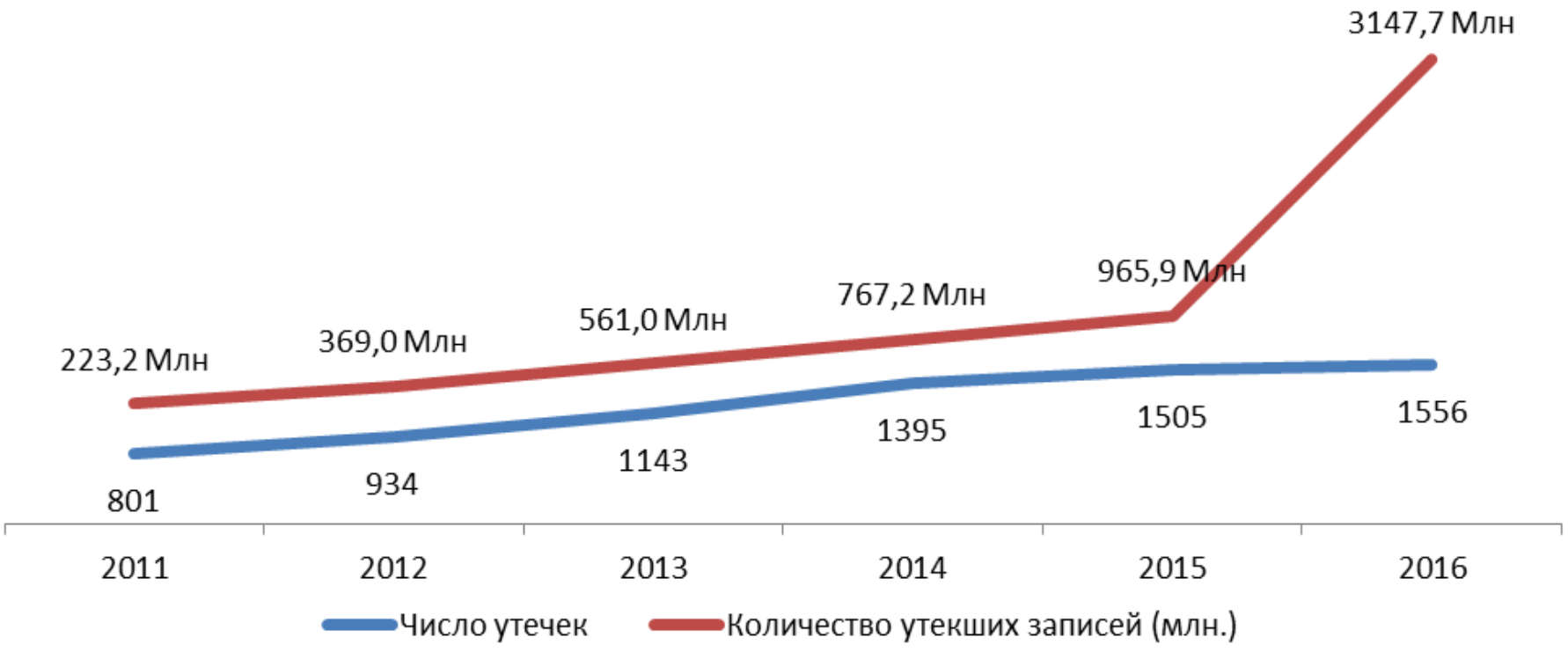
Атаки на АСУ ТП, в том числе с помощью «Интернета вещей» **(IIoT)**

Кампании по очернению и атаки на репутацию с помощью современных ИТ

УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Число утечек стремительно растет

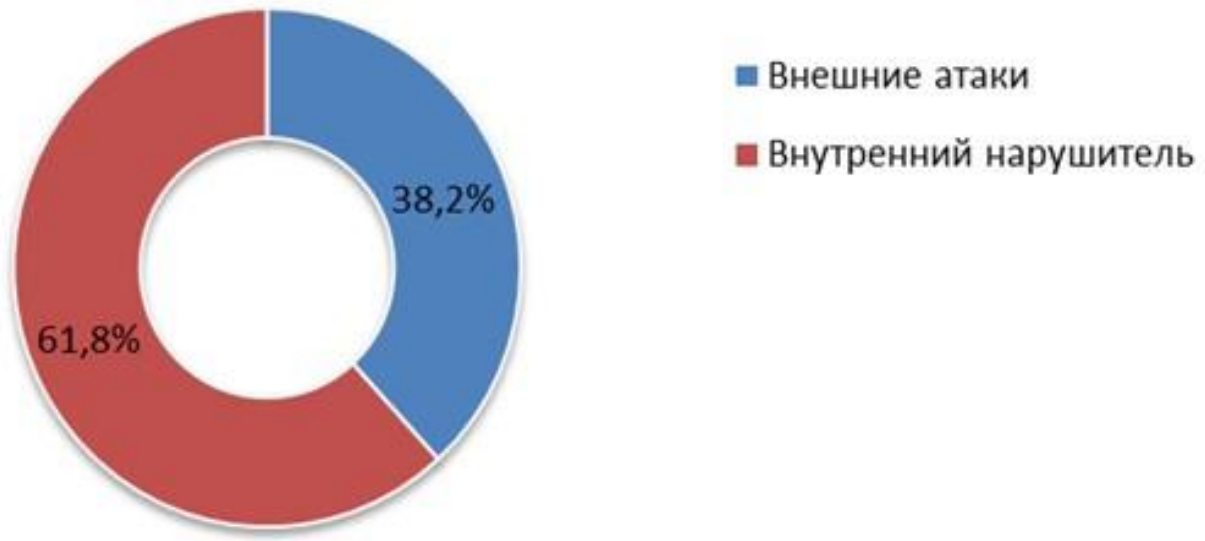
*За 2016 год утекло **в три раза больше** данных, чем в 2015 году!*



по данным Аналитического Центра InfoWatch, 2017

Часто виноваты сами сотрудники

Из зарегистрированных в 2016 году утечек информации **540** произошли по вине внешнего злоумышленника. В **873** случаях утечка произошла по вине внутреннего нарушителя



по данным Аналитического Центра InfoWatch, 2017

Случай Клинтон

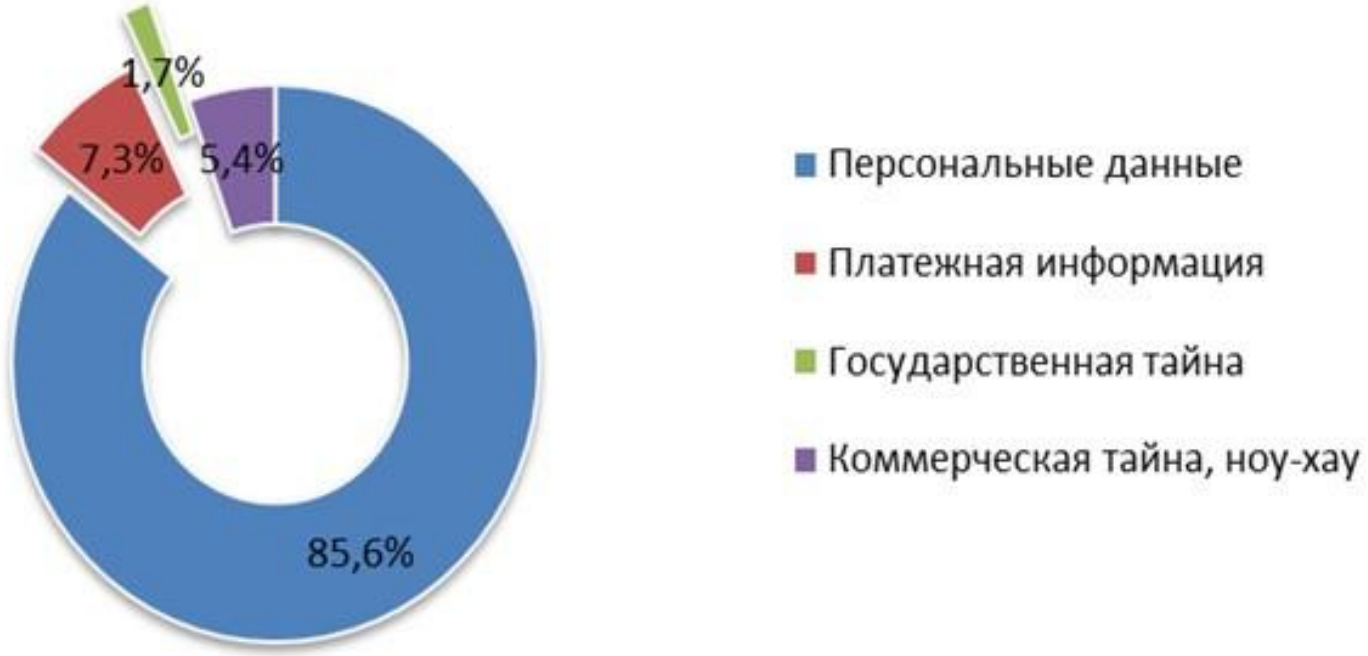
Как это было:

1. Из-за неудобств государственной почты пересылка документов по внешней
2. Передоверие другу писем, содержащих гостайну, чтобы работать дома

Результат:

1. Репутация подорвана
2. Информация об утечке всплывает в **самый неподходящий момент**
3. **Выборы проиграны**

Утечки информации



Распределение утечек по долям не изменилось
по сравнению с прошлым годом

* Утечка платежной информации = компрометация
реквизитов платежных карт

по данным Аналитического Центра InfoWatch, 2017

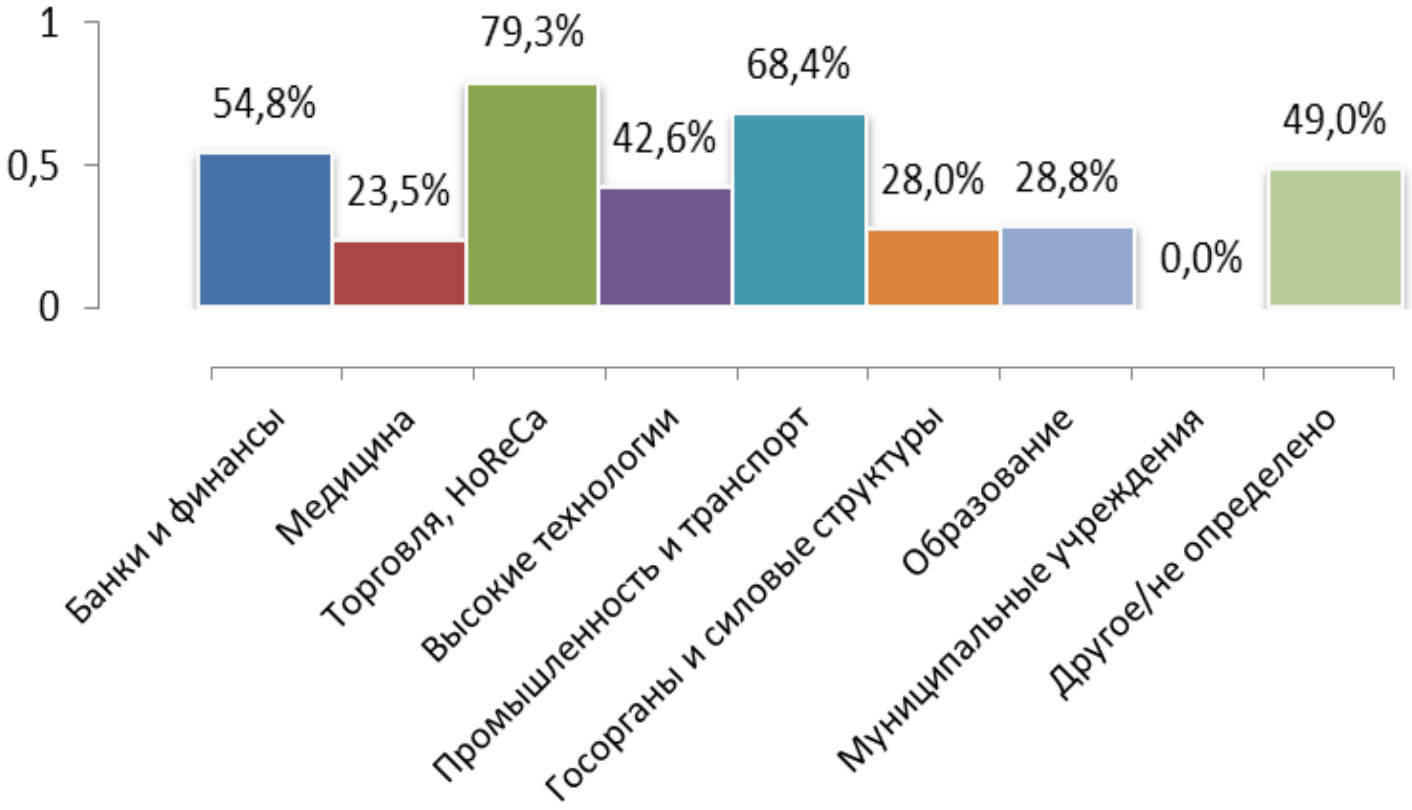
Распределение утечек по каналам

Сетевой канал лидирует как по объему скомпрометированных данных, так и по количеству утечек

по данным Аналитического Центра InfoWatch, 2017

Отраслевая карта утечек

В 2016 году «лидировали» торговые, транспортные и промышленные компании. В этих отраслях более половины утечек носили умышленный характер.

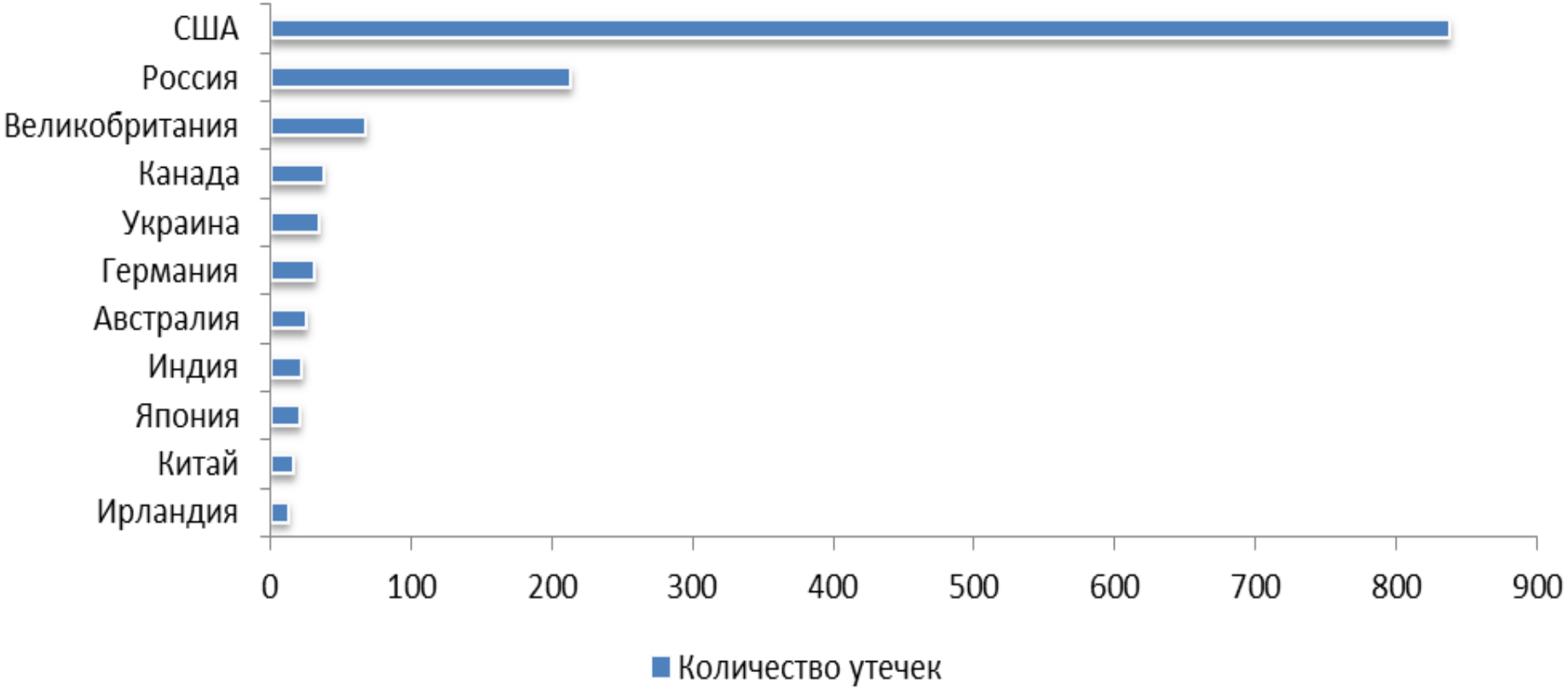


по данным Аналитического Центра InfoWatch, 2017

Распределение утечек по странам

В 2016 году на долю России пришлось 213 случаев компрометации данных – в 2 раза больше, чем годом ранее

Высокая позиция России объясняется, в частности, методикой подсчета



по данным Аналитического Центра InfoWatch, 2017

Пример: смартфон – устройство для утечек

Смартфон =
ШПИОН «ВСЕ В ОДНОМ»:

- Определение местонахождения
- Содержание переписки (смс, почта)
- Фото- и видеофайлы
- Контакты
- Связь с браузерами и поисковиками на десктопах
- Анализ предпочтений (политические взгляды, потребительские привычки, личная жизнь)
- + все возможности слежки от поисковиков, соцсетей, браузеров, операционной системы
- Встроенные в «железо» антенны

А в будущем…

«Интернет вещей»:

- Телевизор, воспринимающий всё, что происходит в комнате
- Медицинский браслет, отправляющий информацию о состоянии пациента
- Автомобили и другие самоходные устройства собирают и передают данные о передвижениях и состоянии
- Всевозможные датчики и домашние системы передают данные о состоянии объектов
- «Умный дом» – объединение различных устройств в единую систему управления зданием

ЦЕЛЕВЫЕ АТАКИ
НА ОРГАНИЗАЦИЮ или
ВЕДОМСТВО,
в том числе – на
Индустриальный
«Интернет вещей» (IIoT)

Возможные угрозы

- Нарушение конфиденциальности информации – кража, подслушивание, искажение, подмена информации и пр.
- Угрозы внешнего воздействия на устройства со стороны злоумышленников
- Угрозы программных уязвимостей и ошибок
- Обработка Больших Данных, собираемых с устройств, с целью атаки или компрометации
- Угроза жизни и здоровью людей и организаций
- Угроза атаки типа «отказ в обслуживании» (DDoS)
- Санкции производителей

ПРИМЕР атаки на АСУ ТП

Хакерская атака на автозаправки, 2015

Хакеры подключились к системе управления насосными механизмами топливного хранилища через Интернет.

В результате они могли контролировать уровень запасов бензина, отправлять сигналы об опасности, поломке и аварии.

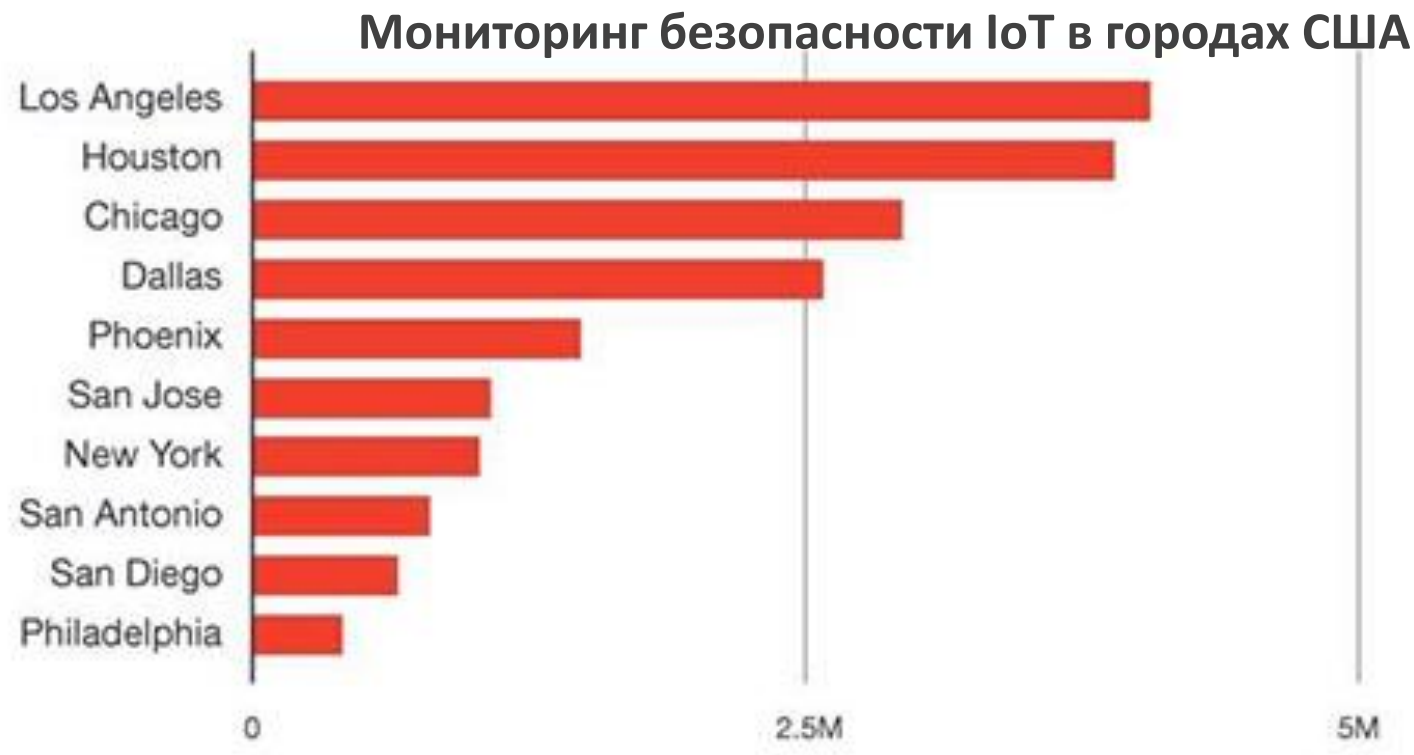
В настоящий момент в открытом доступе находятся не менее 5,8 тысяч ATG-датчиков, не имеющих даже парольной защиты.

ПРИМЕР атаки через «Интернет вещей» на интернет-сервисы, 24.10.2016

Мощная атака на время вывела из строя Twitter, Netflix, Paypal, Spotify и SoundCloud, сайты The New York Times и CNN.
Способ – DDoS.
Цель – компания Dyn (обслуживает службу DNS) и её клиенты.

Для атаки использовался «Интернет вещей»: сетевые роутеры, веб-камеры и др. устройства на скоростных каналах связи.

Безопасность АСУ ТП



по данным Trend Micro, 02.2017

Figure 1: Number of exposed cyber assets in the 10 largest US cities by population

«Среди найденных в Интернете компонентов АСУ ТП только 2/3 можно назвать «условно защищёнными». Самые распространённые в Интернете – системы автоматизации зданий Tridium/Honeywell и мониторинг управления энергией SMA Solar Technology. (данные Positive Technologies, 2017)

Сравнение безопасности АСУ ТП и ИТ

Вопросы безопасности	Для традиционных ИТ	Для АСУ ТП
Жизненный цикл технологии	3-5 лет	От 20 лет
Антивирус	Повсеместно	Сложно реализовать, редок
Аутсорсинг	Общая практика	Редко используется
Установка патчей	Регулярно	Долго и редко
Управление изменениями	Регулярно, по расписанию	Вместе с изменением системы
Доступность	Допустимы задержки	Задержки недопустимы
Обновление знаний персонала	Регулярно	Обычно слабо в вопросах ИБ
Аудит ИБ	Планируется регулярно	Время от времени
Физическая без-ть	Решается по-разному	Надёжно решена

Кому нужна защита?

- Нет стандартов защиты
- Нет требований к защите
- Нет понимания у потребителей
- Мало имеющихся наработок

Что делать?

Создавать единые стандарты через:

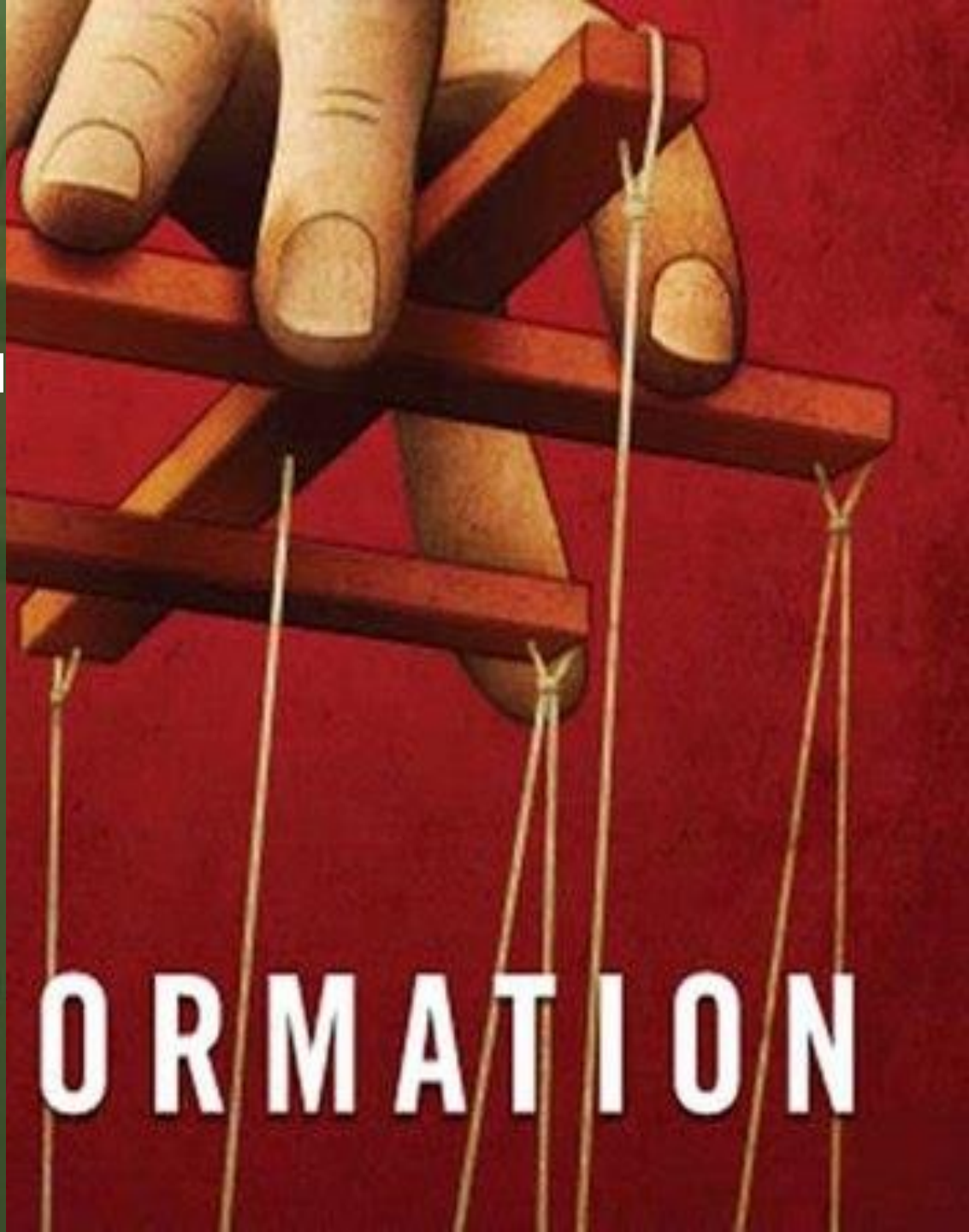
- Национальный консорциум Промышленного Интернета
- Национальную Ассоциацию Промышленной автоматизации (НППА)
- Российскую Ассоциацию «Интернета вещей»

Внедрять соответствующие законы

Обеспечивать импортозамещение:

- Разработка собственной компонентной базы
- Разработка российского программного обеспечения
- Разработка отечественных систем защиты

ИНФОРМАЦИОННЫЕ АТАКИ и КАМПАНИИ ДЕЗИНФОРМИРОВАНИЯ с помощью современных ИТ



Информационные атаки и медийные взрывы

INFOWATCH®

Атаки на руководство (происшествия, благосостояние, аморальное поведение, острая несправедливость)

Атаки на предприятие (сбои, ошибки, неудачные высказывания, жадность, фрод; сейчас часты вбросы про Крым, попадание под санкции, отнятие лицензии)

Длительные кампании очернения: серии вбросов, подбор негативных тем, вызывающих живой отклик и вирусный рост, подогревание темы в течение многих месяцев

Атака: как организовывают

- **Контент**: подбор темы и формы сообщений. Вброс должен соответствовать архетипам пользователей
- **Вброс**: первые размещения для создания «источника», места для ссылок, снятия ответственности за контент.
- **Место**: неизвестный аккаунт, «сливной бачок» (квазиСМИ), платный блогер, интернет-СМИ.
- **Цикл отмывки в ангажированных СМИ**: вброс –> подхват СМИ –> перепечатка в соцсетях –> снова в СМИ.
- **Снятие ответственности**: публикации в формате «в Интернете пишут, что».
- **Поддержка атаки**: новые вбросы, повторы и поддержка старых вбросов.
- **Естественность и бесплатность**: хорошая атака практически неотличима от естественного события, люди перепощивают и комментируют добровольно.

Пример информационной атаки в сети

INFOWATCH®

СБЕРБАНК
Всегда рядом

Дата: 18.12.2014

Предпосылка: Пиковый рост курса валют

Суть атаки: Активность около 80-300 аккаунтов в сети на тему *(большинство – украинские):*

- Visa прекращает операции по картам Сбербанка
- Сбербанк скоро прекратит выдачу депозитов
- Нельзя снять деньги из банкомата, это не технический сбой – денег нет

Последствия:

- Граждане бросились забирать деньги

- ЦБ и Правительство принимают беспрецедентные меры по снижению накала

Тенденции атак в сети

- **Резкий рост числа и изощренности информационных атак**
- **Их трудно отличать от естественных явлений**
- **Все больше доминирует политический контекст (пропаганда, ангажированная подача информации)**
- **Негатив доминирует и вытеснять его сложнее, чем вбрасывать**
- **Сеть злопамятна**
- **Неконкретность – детали не запоминаются, только ощущения**

Выводы:

- ✓ С появлением новых ИТ появляются и развиваются и новые угрозы
- ✓ Разрабатываемые технические средства быстро становятся неэффективными
- ✓ Предприятию нельзя надеяться только на производителя средств защиты. ИБ – это не состояние, а процесс
- ✓ Для решения некоторых проблем (угрозы АСУ ТП) технических средств недостаточно, нужно государственное регулирование
- ✓ Необходимо замещать импортные ИТ отечественными

Спасибо за внимание!