InfoWatch

Современные информационные угрозы и подходы к защите от них

Президент ГК InfoWatch
Наталья Касперская

Основные предпосылки угроз

- 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

Основные тенденции ИТ-угроз предприятиям

1. Рост числа утечек конфиденциальной информации и коммерческий шпионаж

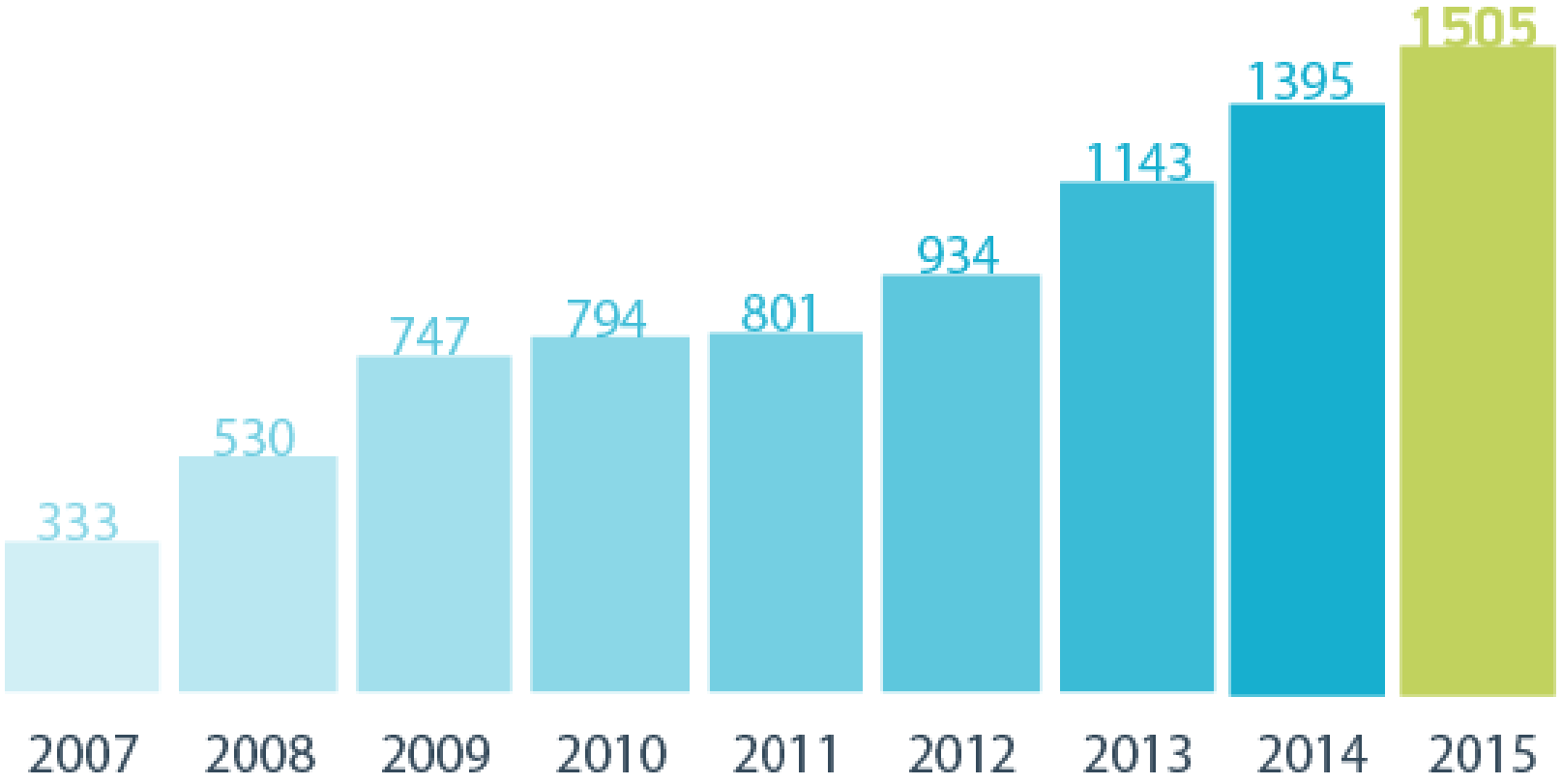
2. Развитие таргетированных (целевых) атак

3. Внедрение через уязвимости в имеющихся ИТ-продуктах

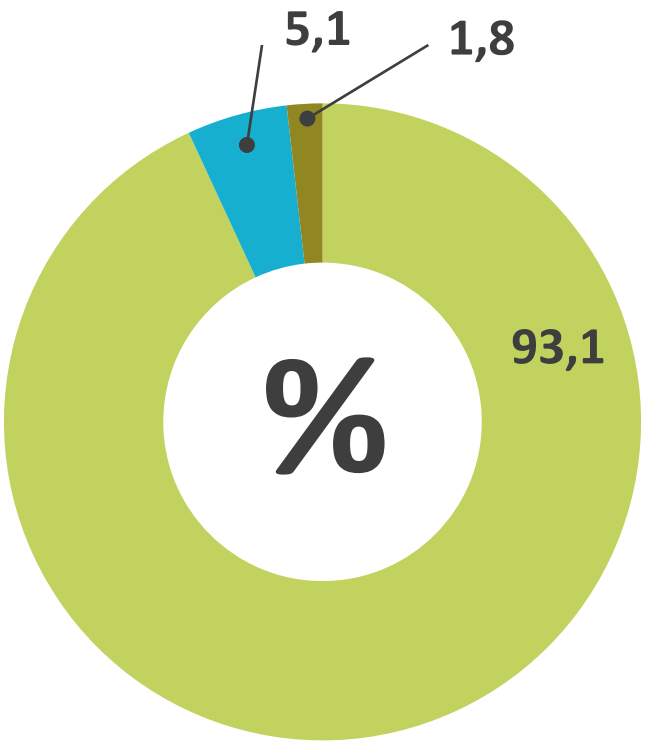
4. Угрозы АСУ ТП предприятий

5. Атаки на предприятия через социальные сети и блоги

Динамика утечек, 2006 – 2015



Распределение утечек по типам данных

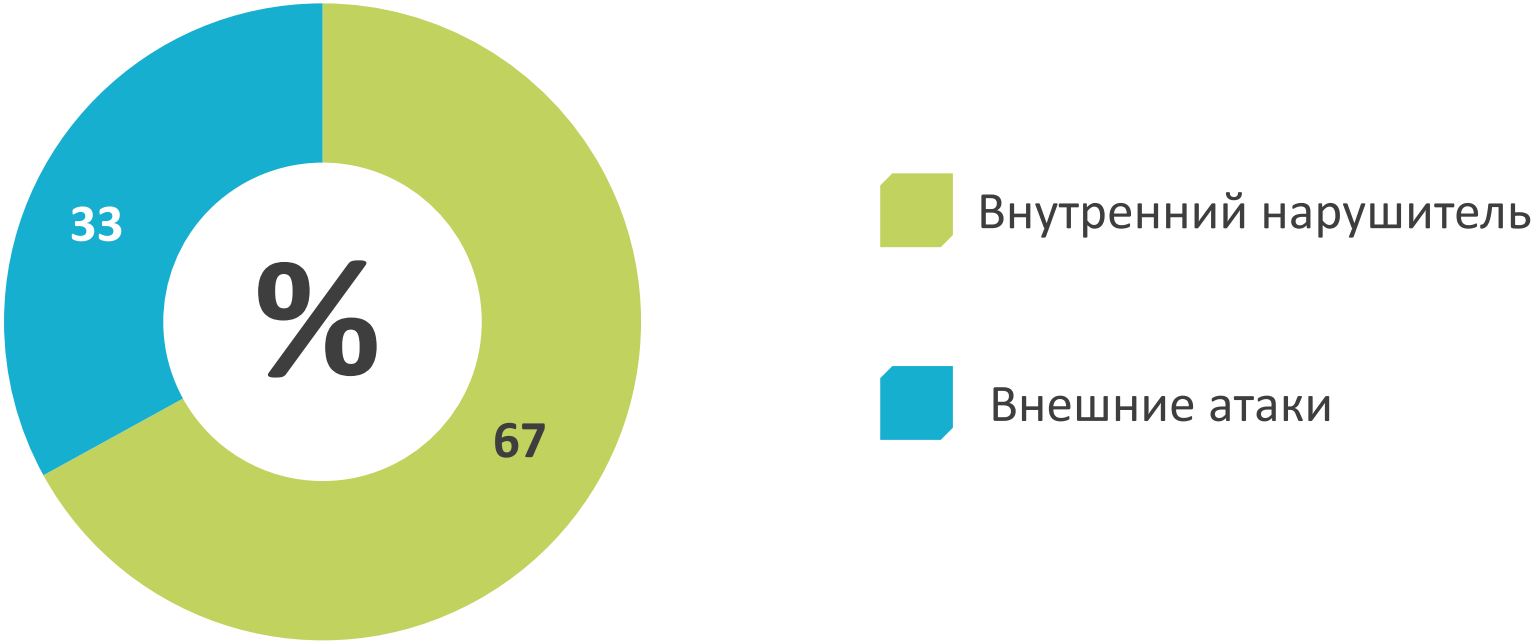


Персональные данные и платежная информация

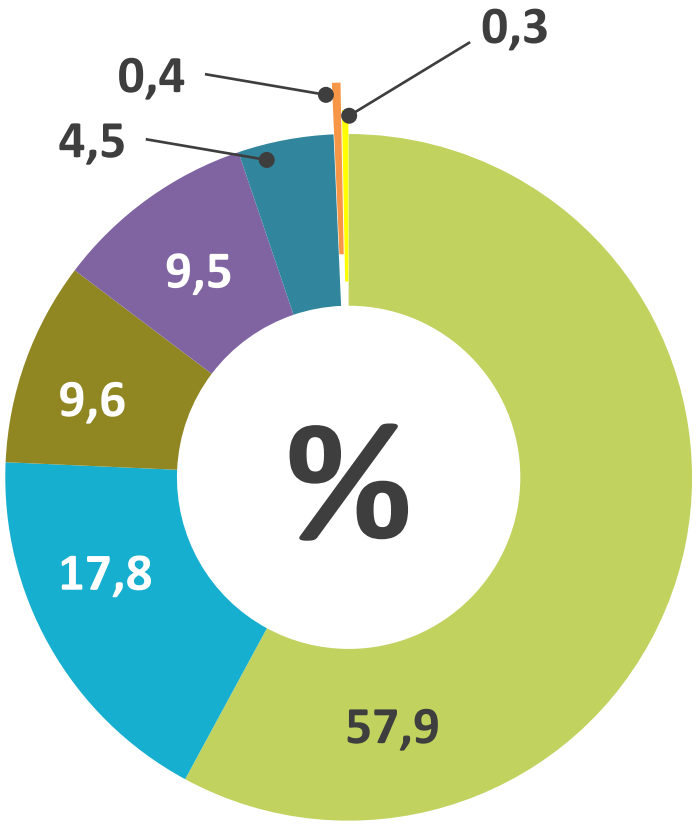
Коммерческая тайна, know-how

Государственная тайна

Распределение утечек по вектору воздействия

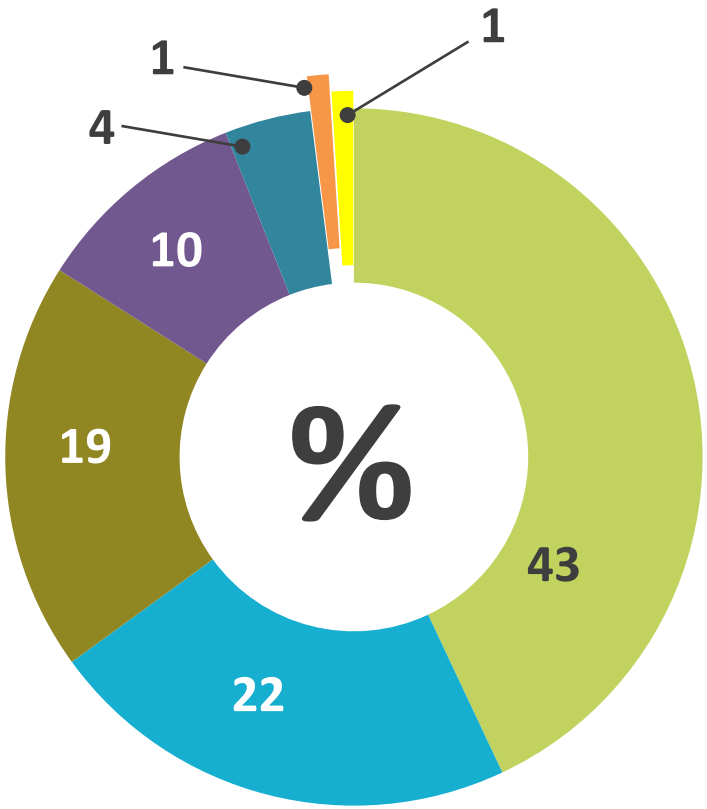


Распределение утечек по каналам, 2015



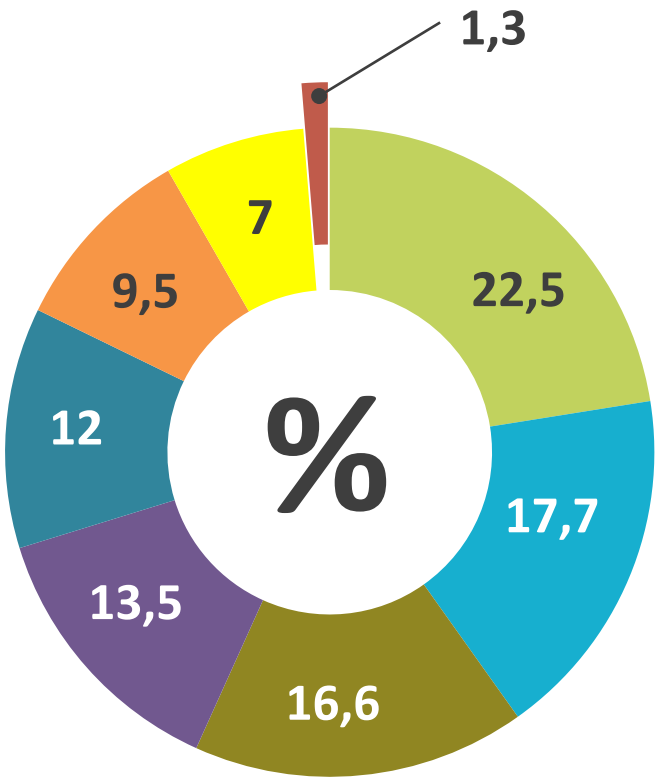
- Сеть (браузер, Cloud)
- Бумажные носители
- Кража/потеря оборудования
- Электронная почта
- Съемные носители
- Мобильные устройства
- IM (текст, голос, видео)

Распределение утечек по каналам, 2014



- Сеть (браузер, Cloud)
- Бумажные носители
- Кража/потеря оборудования
- Электронная почта
- Съемные носители
- Мобильные устройства
- IM (текст, голос, видео)

Распределение утечек по отраслям



- Медицина
- Госорганы и силовые структуры
- Образование
- Высокие технологии
- Торговля, HoReCa
- Банки и финансы
- Промышленность и транспорт
- Муниципальные учреждения

1. Как защищаться?

INFOWATCH®

Меры по защите предприятия

- Внедрение на предприятии режима коммерческой тайны
- Разработка и внедрение регламентов по защите информации
- Выбор и внедрение технических средств

Требования к техническим средствам

- Перехват значительного числа каналов передачи связи
- Возможность блокировки информации
- Обязательное наличие этапа pre-DLP, т.е. совместного с клиентом выбора объектов защиты и настройки политик

Задачи целевых атак на организации

INFOWATCH®

Целевая атака -

спланированная атака на ИС организации, организованная группой специалистов ради достижения конкретных целей

- Давление, демонстрация силы
- Получение информации ограниченного доступа
- Выведение из строя элементов ИТ-инфраструктуры и ИТ-сервисов, прерывание основных процессов
- Внесение изменений в обрабатываемую информацию (мошенничество, дезинформация, снижение качества производимой продукции и управленческих решений)
- Проверка защищенности объекта и др.

Пример: Целевая атака FakeCERT

Группировка хакеров, выдающая себя за FinCERT

Длительность атаки: с 15 марта по настоящее время

Этапы атаки:

1. Создание malware
2. Адресная email-рассылка по сотрудникам банков с вредоносным вложение
3. Сотрудники открывают вложение (вирус)
4. **Хакеры получают полный доступ к ИС банка**

Ущерб от целевых атак за Q4 2015 и Q1 2016

19 инцидентов, связанных с кредитными организациями

В основном пострадали банки среднего уровня

Общий ущерб **около 2 миллиардов рублей**

Источник: РИА Новости, согласно отчету ЦБ РФ

Как защищаться?

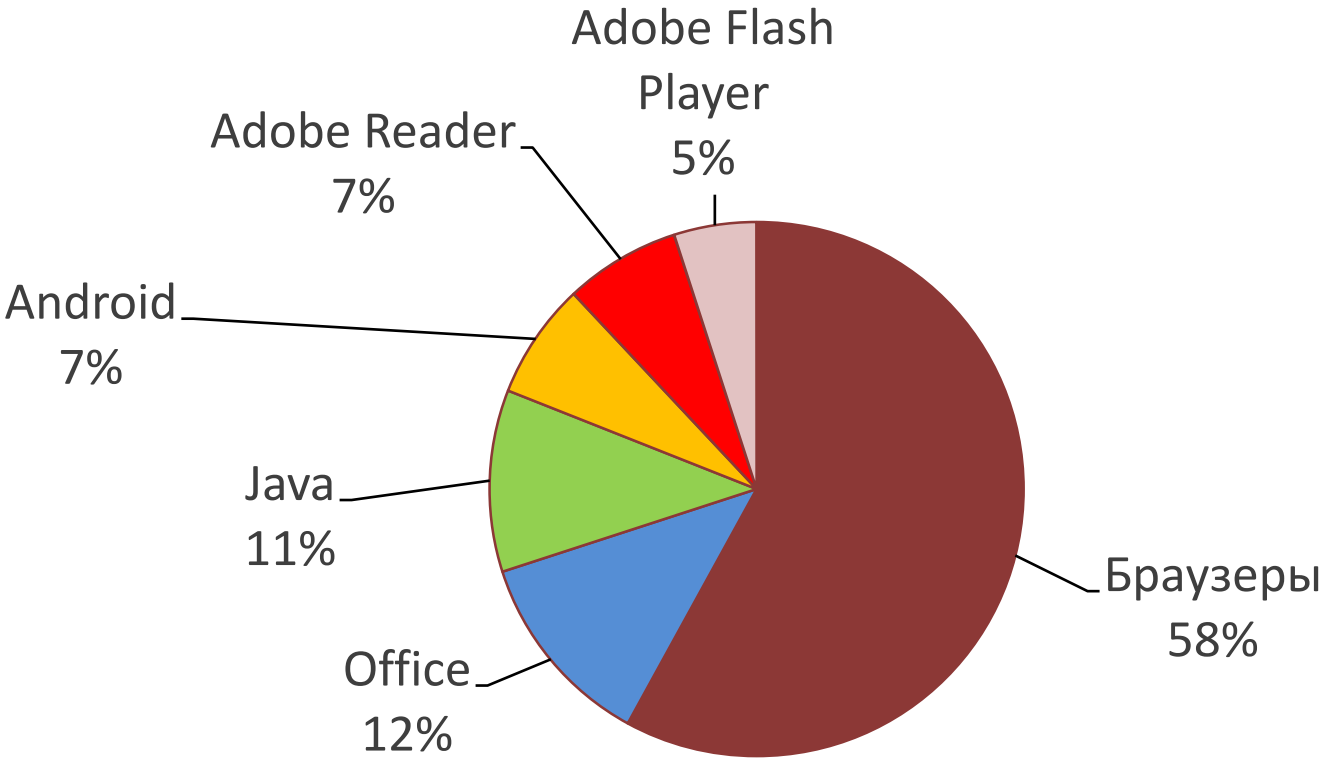
INFOWATCH®

АБСОЛЮТНОЙ ЗАЩИТЫ НЕ СУЩЕСТВУЕТ!

Однако, можно принять меры по снижению рисков:

- Выявление зон возможного вторжения в компанию
- Построение модели угроз
- Выбор технических средств
- Их внедрение и разработка концепции использования
- Разработка и внедрение процессов ИБ

Наиболее уязвимые системы, 2015



Источник: Лаборатория Касперского

Как защищаться?

INFOWATCH®

Существуют технические средства защиты от уязвимостей

- Системы типа Patch Management
- Системы анализа исходного кода приложений на уязвимости

Необходимо использовать обе составляющие!

4. УГРОЗА АСУ ТП

Целевая атака на немецкий сталелитейный завод

Группировка хакеров рассылала фишинговые e-mail + использовала социальную инженерию

Проникнув в сеть завода, злоумышленники получили доступ к компьютерам АСУТП – системам управления процессами

Системы управления получили команды, которые привели к физическим разрушениям в доменной печи

Угроза АСУ ТП на различных уровнях управления

SCADA (диспетчерское управление и сбор данных)	• Заражение СКУД извне с помощью вирусного ПО • Перехват и удаленное управление технологическим процессом • Ошибочные или намеренно неверные действия персонала • Закладки в оборудовании и ПО
Программируемые Логические Контроллеры (ПЛК)	• Подмена управляющих программ • Внедрение вредоносного ПО • Сетевые атаки • Закладки в оборудовании и ПО
Исполнительные устройства	• Врезка в канал связи • Атаки типа DDoS • Создание плацдарма для атак на вышестоящие уровни • Закладки в оборудовании

Последствия

- Нарушение **работоспособности** предприятия
- Аварии на **промышленных объектах**
- Аварии с **отложенным** результатом
- **Компрометация** информации
- **Кража информации** с целью шантажа
- **Шпионаж** и недобросовестная конкуренция

Методы защиты

- Регулярный аудит безопасности
- Встраивание функций защиты **на уровне вендоров**
- Разработка **дополнительных средств защиты** от независимых поставщиков
- Альтернатива. **Отказ от использования** сложных компьютеров и связи с Интернет на производстве

5. Атаки на предприятия через соцсети

- Вброс ложной информации и её дальнейшее распространение через соцсети или др. средства массовых коммуникаций
- Разглашение информации ограниченного доступа через соцсети
- Выступления сотрудников в блогах и соцсетях с рассказами о проблемах компании
- Информационный троллинг, шантаж, давление

ИНФОРМАЦИОННЫЕ ВОЙНЫ ЧЕРЕЗ СОЦСЕТИ

Пример информационной атаки

Две волны упоминаний возможности отзыва лицензии у Альфа-Банка
Пик – 25 сентября 2015

Более 700 сообщений в социальных сетях
Потенциальная аудитория - **более 600 тыс. чел.**

Последующая **массовая SMS-рассылка с подтверждением слуха**

Граждане бросились снимать денежные средства в размере до 15,6 млрд. руб. (оценка VC.RU)

Источники: Крибрум, vc.ru

Как защищаться?

1. Осознание проблемы
2. Использование сервиса автоматизированного мониторинга и анализа соцмедиа
3. Разработка модели поведения в случае атаки
4. Обучение руководства предприятия, PR-службы и отдела по работе с клиентами
5. Немедленное реагирование на начало атаки

Краткие выводы

Угрозы:

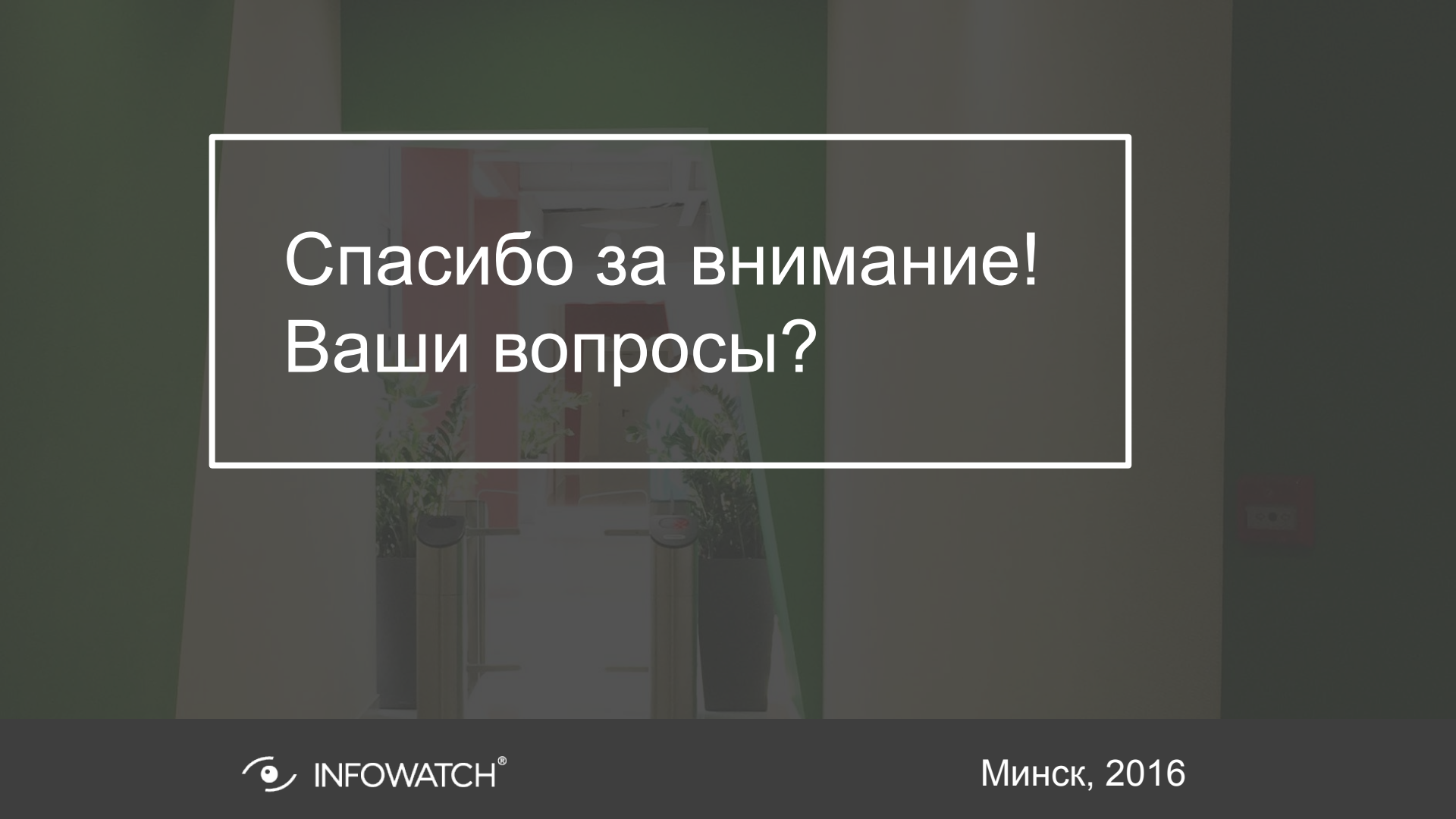
1. Новые технологии несут новые угрозы предприятиям

2. С ростом ценности и объёма информации возрастает значимость влияния на неё через информационные каналы => положение будет только ухудшаться

Защита:

1. Для многих новых видов угроз НЕТ готовых продуктов по защите
2. Требуется комплексный подход, позволяющий обеспечить допустимый уровень рисков ИБ

Бороться можно и нужно!


Спасибо за внимание!
Ваши вопросы?