

ТЕОРИЯ РАЗБИТЫХ ОКОН В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

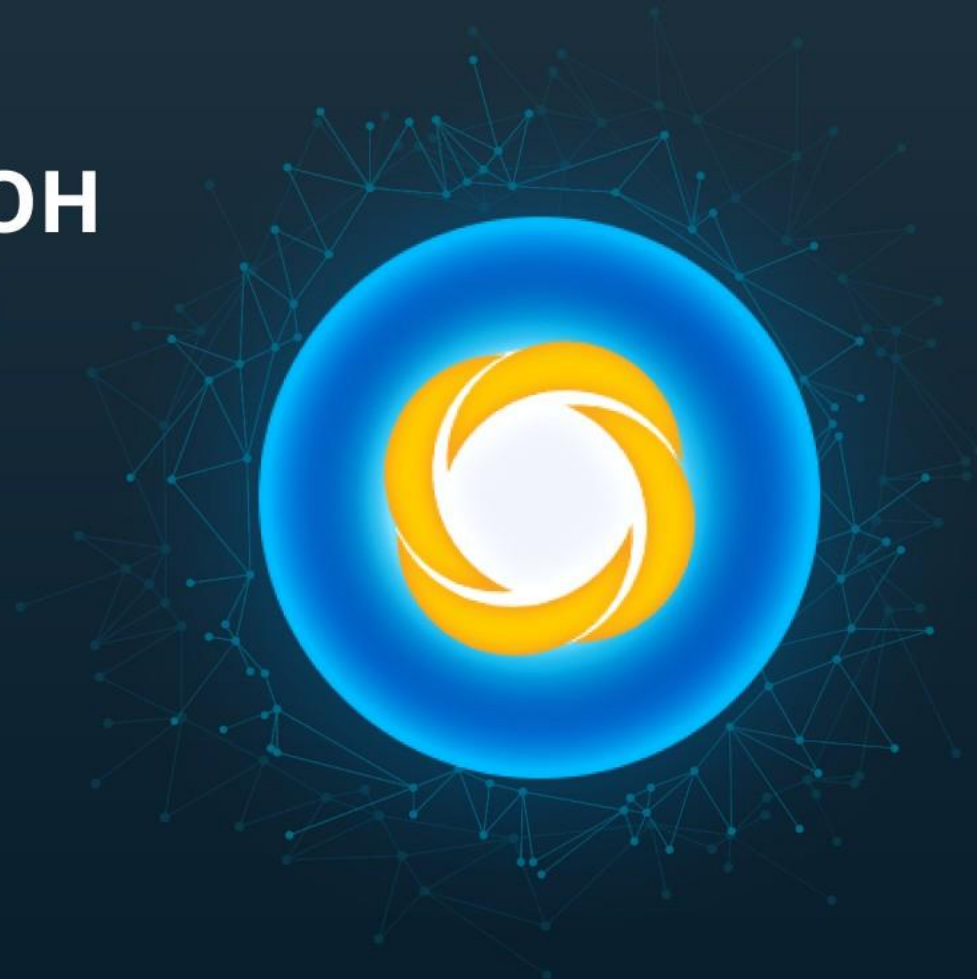
ДМИТРИЙ ХОМУТОВ

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ПО РАЗВИТИЮ
КОМПАНИЯ «АЙДЕКО»

+7-922-200-8230

D.HOMUTOV@IDECO.RU

IDECO.RU





ТЕОРИЯ СФОРМУЛИРОВАНА
КРИМИНОЛОГАМИ ДЖЕЙМСОМ УИЛСОНОМ И
ДЖОРДЖЕМ КЕЛЛИНГОМ В 1982 ГОДУ.

**«ЕСЛИ В ЗДАНИИ РАЗБИТО ОДНО СТЕКЛО
И НИКТО ЕГО НЕ ЗАМЕНЯЕТ, ТО ЧЕРЕЗ
НЕКОТОРОЕ ВРЕМЯ В ЭТОМ ЗДАНИИ НЕ
ОСТАНЕТСЯ НИ ОДНОГО ЦЕЛОГО ОКНА.
ВОКРУГ НАЧИНАЕТ ЦАРИТЬ ХАОС И
БЕСПОРЯДОК, РАСТЕТ УРОВЕНЬ
ПРЕСТУПНОСТИ»**





**ЧТО ТАКОЕ «РАЗБИТЫЕ ОКНА»
ИЛИ ОТ ЧЕГО НЕ СПАСЕТ
МЕЖСЕТЕВОЙ ЭКРАН?**



Уязвимости в ОС
оборудовании, протоколах



Спам



Вирусы



Эксплоиты



Сайты, распространяющие
вредоносное ПО



Атаки на веб-приложения



КАКИЕ РИСКИ НЕСУТ В СЕБЕ «РАЗБИТЫЕ ОКНА»?



Выведение из строя серверов,
ПО и промышленного оборудования



Кража пользовательских
данных



Кража коммерческой
информации



Нецелевое использование
вычислительных средств предприятия



Тайный сбор
информации



Нецелевое использование
рабочего времени



**ЕСЛИ КОМПАНИЯ НЕ СЛЕДИТ ЗА «РАЗБИТЫМИ ОКНАМИ», ТО
РАНО ИЛИ ПОЗДНО ЭТИМ ВОСПОЛЬЗУЮТСЯ
ЗЛОУМЫШЛЕННИКИ.**

**ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА КОМПАНИИ БУДЕТ
ПОВРЕЖДЕНА ИЛИ УНИЧТОЖЕНА, ЧТО ПРИВЕДЕТ К
СЕРЬЕЗНЫМ ФИНАНСОВЫМ ПОТЕРЯМ ИЛИ БАНКРОТСТВУ.**



12 МАЯ 2017 ГОДА — WANNA CRY

27 ИЮНЯ 2017 ГОДА — ЕХРЕТУА

24 ОКТЯБРЯ 2017 ГОДА — BAD RABBIT





АПРЕЛЬ 2018: АТАКА НА МАРШРУТИЗАТОРЫ CISCO

- БОЛЕЕ 170 000 ПОСТРАДАВШИХ УСТРОЙСТВ
- ИСПОЛЬЗУЯ ЭКСПЛОИТ, ЗЛОУМЫШЛЕННИКИ МОГЛИ ПОЛНОСТЬЮ ПЕРЕХВАТИТЬ УПРАВЛЕНИЕ МАРШРУТИЗАТОРОМ, ИЗМЕНЯТЬ ФАЙЛЫ КОНФИГУРАЦИИ И ПРОШИВКУ УСТРОЙСТВА





МАЙ 2018: АТАКА VPNFILTER

- БОЛЬШЕ 500 000 ЗАХВАЧЕННЫХ УСТРОЙСТВ
- ПОСТРАДАЛИ УСТРОЙСТВА MIKROTIK, D-LINK, TP-LINK, LINKSYS, NETGEAR, UBIQUITI, ZTE, ASUS И ДРУГИХ ПРОИЗВОДИТЕЛЕЙ





ПЛОХОЙ ТРАФИК

- **WINDOWS 10 ПРИ ОТКЛЮЧЕННОЙ ТЕЛЕМЕТРИИ СОВЕРШАЕТ БОЛЕЕ 200 ОБРАЩЕНИЙ НА СЕРВЕРА ТЕЛЕМЕТРИИ В СУТКИ**
- **В СРЕДНЕМ КОМПЬЮТЕР ОТПРАВЛЯЕТ В РЕКЛАМНЫЕ И БАННЕРНЫЕ СЕТИ 900 ЗАПРОСОВ В ДЕНЬ**
- **ЕЖЕДНЕВНО КОМПЬЮТЕР ПОЛУЧАЕТ ОКОЛО 1300 ЗАПРОСОВ ИЗ СТРАН АЗИИ, АФРИКИ И ЮЖНОЙ АМЕРИКИ**
- **БОЛЕЕ 300 ЗАПРОСОВ В СУТКИ КОМПЬЮТЕР ОТПРАВЛЯЕТ НА РЕСУРСЫ, СОБИРАЮЩИЕ ИНФОРМАЦИЮ О ПОЛЬЗОВАТЕЛЯХ: ВЕБ-ТРЕКЕРЫ, SPYWARE, ADWARE**

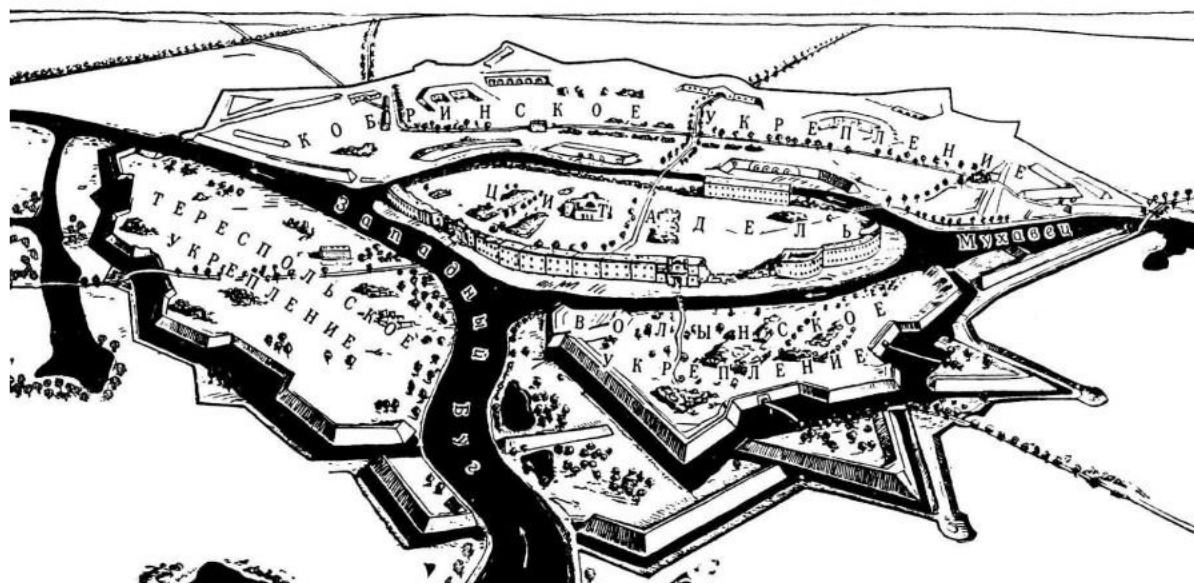




ЧТО ДЕЛАТЬ?



ЭШЕЛОНИРОВАННАЯ ОБОРОНА



- СЕТЕВОЙ ПЕРИМЕТР: UTM ИЛИ NGFW РЕШЕНИЕ ДЛЯ ЗАЩИТЫ ПЕРИМЕТРА СЕТИ И БЕЗОПАСНОГО ВЫХОДА В ИНТЕРНЕТ
- СЕГМЕНТИРОВАНИЕ СЕТИ (ПРОВЕРКА МЕЖСЕГМЕНТНОГО ТРАФИКА)
- ЗАЩИТА КОНЕЧНЫХ РАБОЧИХ СТАНЦИЙ (ПЕРСОНАЛЬНЫЙ АНТИВИРУС И СРЕДСТВА ЗАЩИТЫ ОС, АЛЬТЕРНАТИВНЫЕ ОС)
- ЗАЩИТА ОТ УТЕЧЕК ИНФОРМАЦИИ (DLP)
- РЕГУЛЯРНЫЕ БЭКАПЫ



IDECO UTM





IDECO UTM

- **МЕЖСЕТЕВОЙ ЭКРАН**
- **СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ**
- **КОНТРОЛЬ ПРИЛОЖЕНИЙ**
- **КОНТЕНТ - ФИЛЬТР (HTTP И HTTPS)**
- **WEB APPLICATION FIREWALL**
- **АНТИВИРУСНАЯ ПРОВЕРКА ТРАФИКА**
- **АНТИСПАМ И ПРОВЕРКА ПОЧТОВОГО ТРАФИКА**
- **ЗАЩИТА ОТ DOS И БРУТФОРС-АТАК**
- **ЗАЩИЩЕННЫЙ УДАЛЕННЫЙ ДОСТУП ПО VPN**



**КОМПАНИЯ «АЙДЕКО» — РОССИЙСКИЙ РАЗРАБОТЧИК
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.
НА РЫНКЕ С 2005 ГОДА.**

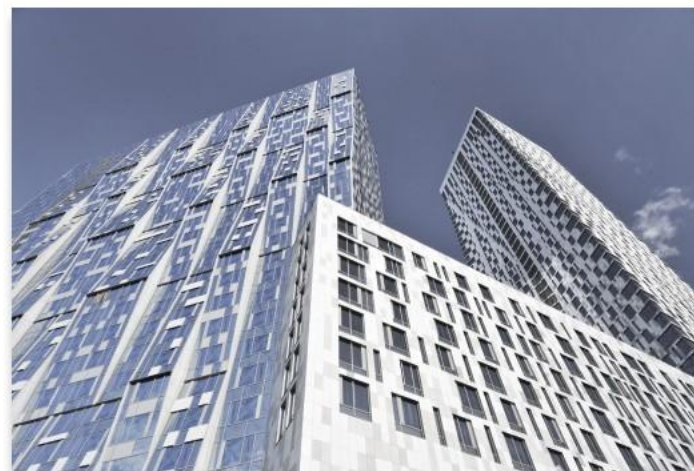
**РАЗРАБАТЫВАЕМ ПРОГРАММНЫЕ РЕШЕНИЯ ДЛЯ ЗАЩИТЫ
ПЕРИМЕТРА СЕТИ,
КОНТЕНТНОЙ ФИЛЬТРАЦИИ И ПОСТРОЕНИЯ БЕСШОВНЫХ
WI-FI СЕТЕЙ.**

**ПРОДУКТЫ «АЙДЕКО» ВКЛЮЧЕНЫ В «ЕДИНЫЙ
РЕЕСТР РОССИЙСКИХ ПРОГРАММ ДЛЯ ЭЛЕКТРОННЫХ
ВЫЧИСЛИТЕЛЬНЫХ МАШИН И БАЗ ДАННЫХ», ПРИНЯТЫХ
МИНИСТЕРСТВОМ ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ
КОММУНИКАЦИЙ РФ.**

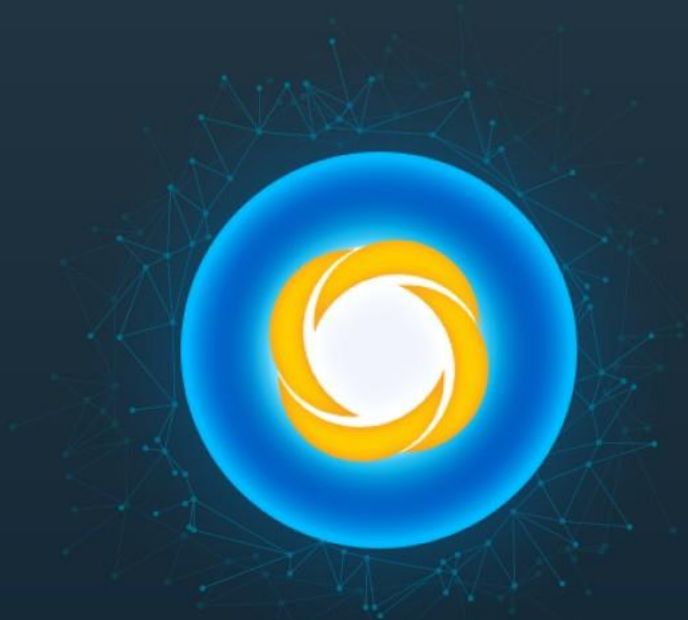
СЕРТИФИКАТ ФСТЭК ПО ТИПУ А5/Б5.

**НАШИ КЛИЕНТЫ — ТЫСЯЧИ КОМПАНИЙ В РОССИИ И СТРАНАХ
СНГ ИЗ ВСЕХ ОТРАСЛЕЙ ЭКОНОМИКИ.**





**А КАК ВЫГЛЯДИТ ВАША ИНФОРМАЦИОННАЯ
ИНФРАСТРУКТУРА?**



СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

ДМИТРИЙ ХОМУТОВ

D.HOMUTOV@IDECO.RU

+7-922-200-8230

8 800 555 33 40

Отдел продаж