DeviceLock DLP
Proactive Endpoint Security

Экспертный взгляд на DLP-технологии.

DeviceLock DLP.

СЕРГЕЙ ВАХОНИН

Директор по решениям

Смарт Лайн Инк / DeviceLock, Inc.

EMAIL SV@DEVICELOCK.COM

АО «Смарт Лайн Инк» - 20 лет на рынке информационной безопасности

Смарт Лайн Инк

ГОД ОСНОВАНИЯ

1996

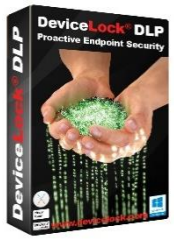
Отечественная компания с штаб-квартирой и офисом разработки в Москве,
офисами продаж в США, Канаде, Великобритании, Германии, Италии,
а также партнерской сетью по всему миру

FUJITSU EADS ING vodafone Tokyo Volkswagen Bank Taiwan Mobile US Army Corps of Engineers Raiffeisen BANK METRO JAXA SOCIETE GENERALE SAIC NORTHROP GRUMMAN POLICE Ministry of JUSTICE CITY of LONDON POLICE 防衛省・自衛隊 MINISTRY OF DEFENSE BEST BUY vodafone Fidelity

ВЫБОРКА ЗАРУБЕЖНЫХ ПОЛЬЗОВАТЕЛЕЙ

Миссия

Международный лидер разработки программных средств для защиты от утечек данных с корпоративных компьютеров (Endpoint DLP)



Продукт

Программный комплекс предотвращения утечек данных **DeviceLock DLP**

Более 90 000 пользователей при более чем 7 000 000 инсталляций

АО «Смарт Лайн Инк» - 20 лет на рынке информационной безопасности

Смарт Лайн Инк

ГОД ОСНОВАНИЯ

1996

Отечественная компания с штаб-квартирой и офисом разработки в Москве,
офисами продаж в США, Канаде, Великобритании, Германии, Италии,
а также партнерской сетью по всему миру

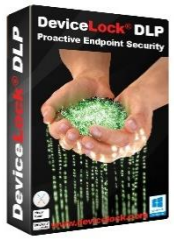
Банк России
Российская государственная библиотека
Дельта Банк
Атомэнергопроект
Лента
Новатэк
IRKUT Иркут
банк российский капитал
Газпром нефть
ОАО «ВНИПИгаздобыч»
Силовые машины
Гута Страхование
Сбербанк
Перекресток
РСХБ Управление активами
Челябинский механический завод Основан в 1942 году
Капитал Страхование
ВТБ24

ВЫБОРКА РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ

Миссия

Международный лидер разработки программных средств для защиты от утечек данных с корпоративных компьютеров (Endpoint DLP)

Продукт



Программный комплекс предотвращения утечек данных **DeviceLock DLP**

Более 90 000 пользователей при более чем 7 000 000 инсталляций

Внутренние угрозы
информационной безопасности

Проблемная область

Утечка данных

Инцидент информационной безопасности, при котором информация ограниченного доступа:

- Случайно или преднамеренно появляется в недоверенной среде или у неавторизованных пользователей вне информационной среды организации (*внешняя утечка данных*)
- Становится доступна неавторизованным пользователям внутри организации (*внутренняя утечка данных*)

Данные

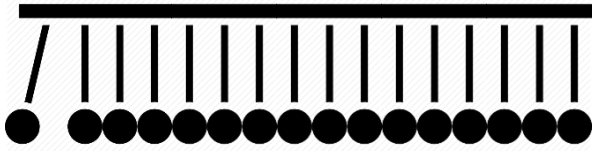
Данные платежных карт, персональные данные сотрудников и клиентов, сведения о пациентах, торговые секреты, сведения, составляющие государственную и коммерческую тайну, другие данные

Процесс

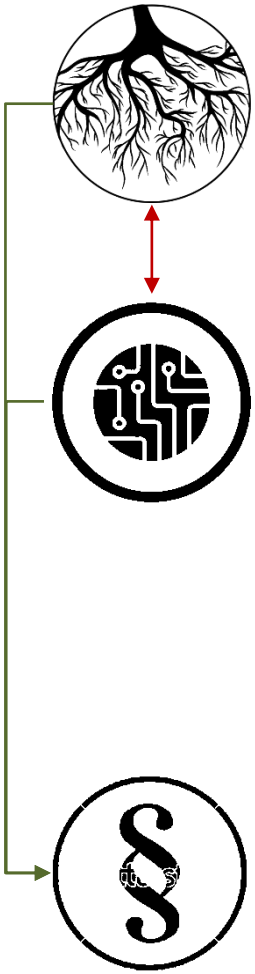
- Внешние атаки: проникновение вредоносного ПО (malware) через уязвимости защитного ПО, фишинг
- Внутренние утечки: инсайдерские ошибки, небрежность и халатность сотрудников, неправомерные действия и кража; системные сбои и некорректные настройки ПО

Последствия

- Финансовые и репутационные убытки вплоть до потери бизнеса
- Большие штрафы и дорогостоящие судебные процессы
- Ущерб национальной безопасности



Ключевые факторы в проблематике утечек данных



ЧЕЛОВЕЧЕСКИЙ

- Непреднамеренные утечки: ошибки и халатность
- Направленные утечки: злоумышленники, шпионаж
- Преднамеренные утечки: превышение полномочий, чрезмерное усердие («доработка на дому»)

ТЕХНОЛОГИЧЕСКИЙ

- Распределённость ИТ-процессов, «консьюмеризация» корпоративных ИТ, распространение скоростных беспроводных сетей
- Активное распространение модели BYOD
- Рост размеров памяти носителей и облачных хранилищ данных при снижении цены, габаритов и простоте использования
- Активное использование современных коммуникационных средств для решения бизнес-задач, в частности, переговоров с клиентами, субподрядчиками, партнерами и т.п.

НОРМАТИВНЫЙ

- ФЗ 152 «О персональных данных»
- Соглашение Basel II
- Стандарт PCI DSS
- Стандарт Банка России по ИТ-безопасности
- Законы Sarbanes-Oxley, HIPAA

Взаимосвязь человеческого и технологического факторов

Середина 2000-х

Взрывной рост емкости съемных PnP-устройств хранения данных, уменьшение габаритов, резкое снижение цен.

Технологии Web 2.0

Социальные медиа превратились в важный инструмент поддержки и ускорения как внутренних, так и внешних бизнес-процессов

Мгновенный обмен сообщениями

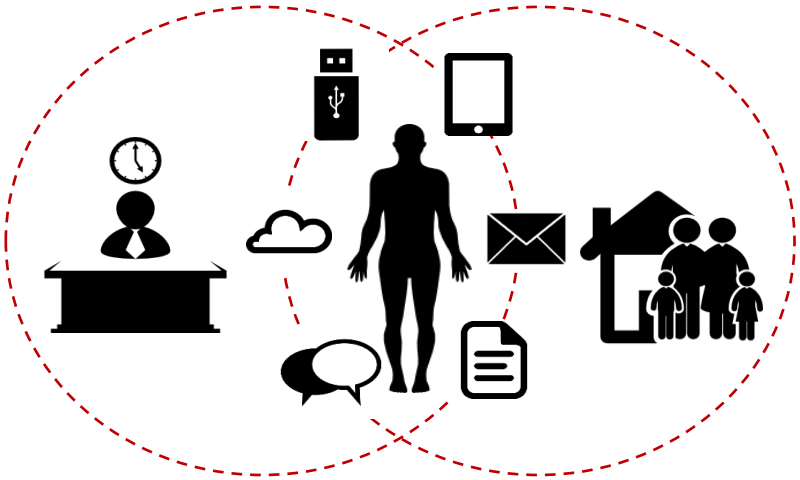
Незаменимое средство коммуникаций практически для любых организаций

2007-2009

Реинкарнация ультрапортативных устройств хранения данных в виртуальные диски, «живущие» в «облаке».

Последние годы

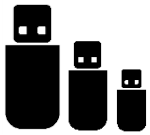
Модель BYOD («принеси свое собственное устройство») вызвала взрывной рост консьюмеризации корпоративных ИТ



МОДЕЛЬ BYOD СТАНОВИТСЯ НОРМОЙ

Одни и те же устройства и сервисы для личной жизни и рабочих процессов

Использование личных устройств в рабочих целях



Использование личных и рабочих съемных устройства хранения

Использование социальных сетей, веб-почты, IM, облачных хранилищ

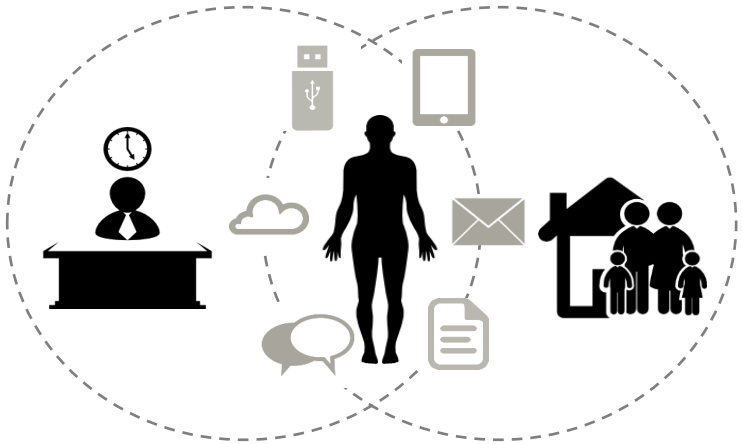
Сотрудники не разделяют часы личной и рабочей жизни

Эту возможность им дает использование одних и тех же технических средств и сетевых сервисов для коммуникаций в обоих измерениях их жизни: личном и бизнес-измерении

Удобство использования, ведущее к повышению эффективности деятельности…

…а также к росту количества и качества угроз и рисков ИБ

СЛЕДСТВИЯ



- Попадание в корпоративную ИС запрещенного и вредоносного контента
- Умышленные или непреднамеренные утечки конфиденциальной информации
- Неспособность традиционных решений обеспечить безопасность данных
- Частная собственность сотрудников на используемые устройства

Борьба с угрозами и деятельность по снижению рисков службами ИБ

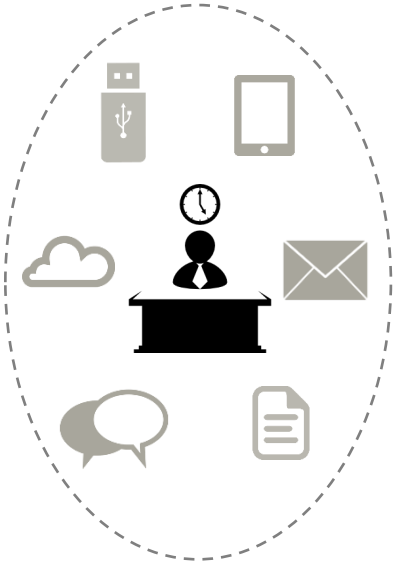
- **Должны производиться вне зависимости от личных интересов и пристрастий**
- **Не должны разрушать производственные процессы**

Наиболее примитивный сценарий утечки данных – наиболее вероятен

Использование сотрудниками любых ИТ-сервисов, доступных на персональном уровне и не требующих обслуживания корпоративными службами ИТ – наиболее простой и вероятный сценарий утечки данных

Отсутствие фокуса на безопасности

Практически все сетевые приложения (социальные сети, облачные хранилища, мессенджеры), созданные для удобства пользователей, для удовлетворения их социальных потребностей – функционируют абсолютно без какой-либо обратной связи с инструментарием корпоративной безопасности.



Решения принимаются пользователем

Модель информационной безопасности потребительских приложений основывается на том, что все решения о способах и уровне авторизации, аутентификации и уровне доступа к данным принимает конечный пользователь – который далеко не всегда является владельцем данных, будучи при этом сотрудником организации.

Угрозы становятся data-центричными

Внешние атаки на данные: механизмы современных атак на данные реализуются на уровне выше сетевого

Разделение внешних и внутренних угрозы целесообразно для обозначения класса применяемых для противодействия угрозам технических решений, но не для построения и модернизации системы информационной безопасности предприятия.

На многих предприятиях считается нормальным и правильным именно **противодействовать** внешним угрозам, отражать внешние атаки, не допускать компрометации учетных записей и т. д. К угрозам внутреннего характера зачастую подход **обратный** ☹.

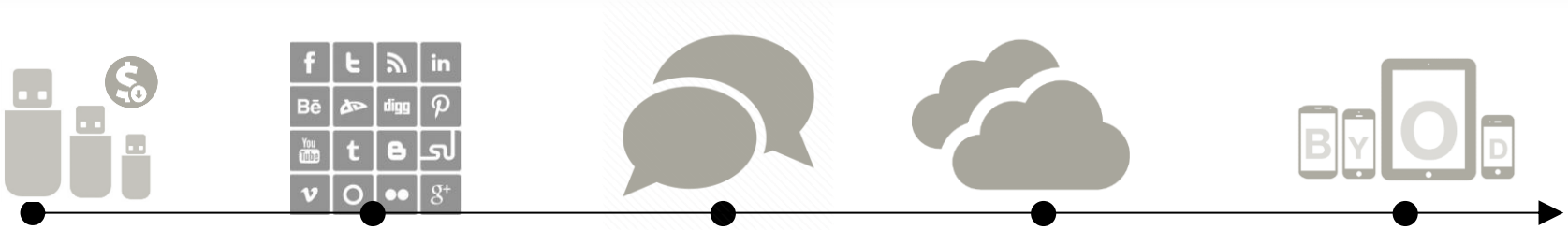
Внешняя атака, преодолев средства защиты корпоративного периметра, переходит в категорию внутренних угроз и использует внутренние каналы утечки.

Пользователь: активное использование современных коммуникационных средств для решения бизнес-задач

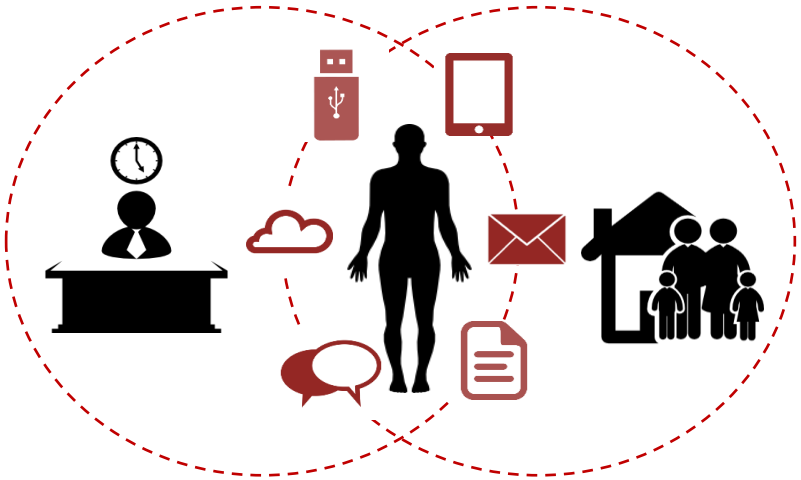
Практически все сетевые приложения (социальные сети, облачные хранилища, мессенджеры), созданные для удобства пользователей, для удовлетворения их социальных потребностей – функционируют абсолютно без какой-либо обратной связи с инструментарием корпоративной безопасности.

Предприятия чрезмерно доверяют своим сотрудникам.
Их защита напоминает яйцо: снаружи более или менее твердая скорлупа, а внутри мягкая среда, и как только злоумышленник попадает в нее, он может делать все, что хочет.

Консьюмеризация и модель информационной безопасности



Одни и те же устройства и сервисы для личной жизни и рабочих процессов



Пользователь становится “центром” в информационных процессах, используя персональные устройства и сервисы, что резко повышает значимость его дисциплины при использовании корпоративных данных.

Контроль нужен?

Контроль коммуникаций нужен, но не путем простых решений – примитивной блокировки или протоколирования

Сейчас в некоторых РФ решениях появляется функция блокировки каналов.
Но задача-то не примитивно блокировать, а интеллектуально контролировать!

Предприятию выгодно обеспечить сотрудникам максимально комфортный доступ к персональным коммуникациям, в том числе – в рабочее время, поскольку такие коммуникации повсеместно используются для бизнеса, а значит, повышается эффективность производственных процессов и результативность труда сотрудников.

Полный запрет личных устройств приводит к отказу от всех преимуществ консьюмеризации и BYOD как стратегии, стимулирующей сотрудников эффективно решать рабочие задачи с личных, удобных в использовании гаджетов.

Контроль? Да, контроль источника

Непрерывный контроль всех возможных каналов информационного обмена

Контроль =
избирательное **управление доступом** к каналу
+
регистрация событий и передаваемых данных
+
инспекция хранимых данных

Вы контролируете процесс, если можете точно определить, что и как будет происходить в этом процессе в определенное время при заданных вами условиях.

- Data In Use
- Data In Motion
- Data At Rest

- Равносильная DLP-защита внутри и вне корпоративной сети
- Анализ содержимого данных до их утечки, в целях предотвращения утечки

Наиболее эффективным способом ПРЕДОТВРАЩЕНИЯ утечек является КОНТРОЛЬ потоков данных именно на используемых сотрудниками оконечных устройствах (Endpoint) в любых сценариях их применения – как внутри, так и за пределами корпоративной сети.

Технологии DLP

для защиты от утечек данных

DLP = DATA LEAK (loss) PREVENTION (protection)

DATA LEAK PREVENTION =

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

Defining DLP

There is a lack of consensus on what actually compromises a DLP solution. Some people consider encryption or USB port control DLP, while others limit themselves to complete product suites. Securosis defines DLP as:

> *Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis.*

Thus the key defining characteristics are:

- Deep content analysis
- Central policy management
- Broad content coverage across multiple platforms and locations

- Data Loss Prevention/Protection
- Data Leak Prevention/Protection
- Information Loss Prevention/Protection
- Information Leak Prevention/Protection
- Extrusion Prevention
- Content Monitoring and Filtering
- Content Monitoring and Protection

Рекомендовано к чтению –
https://securosis.com/blog

'Understanding and Selecting a Data Loss Prevention Solution' –
https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf

DLP = DATA LEAK (loss) PREVENTION (protection)

DATA LEAK PREVENTION =

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

«Почтовые архивы» и «записывалки экранов»
на самом деле не являются DLP-системами.

Для чего нужны DLP-системы

Защита стратегически важной информации от утечки

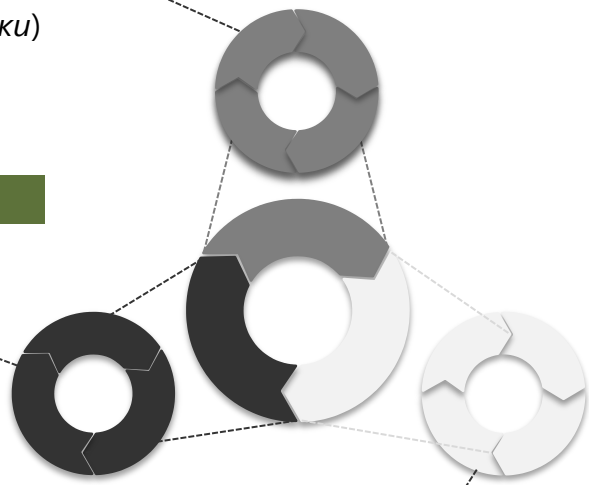
Непрерывный контроль всех возможных каналов информационного обмена

Контроль =
возможность **блокировки** канала (*предотвращение утечки*)
+
возможность **регистрации** инцидента (*мониторинг*)

Соответствие требованиям регуляторов

DLP-системы – инструмент обеспечения реальной безопасности

Обеспечения соответствия требования ФЗ-152, PCI DSS, СТО БР и другим требованиям за счет **контроля** каналов передачи данных и устройств хранения информации.



Контроль лояльности сотрудников

Анализ информационного обмена

Аудит журналов DLP-системы – попыток и/или фактов передачи данных, включая проверку содержимого переданных и/или заблокированных файлов и документов.

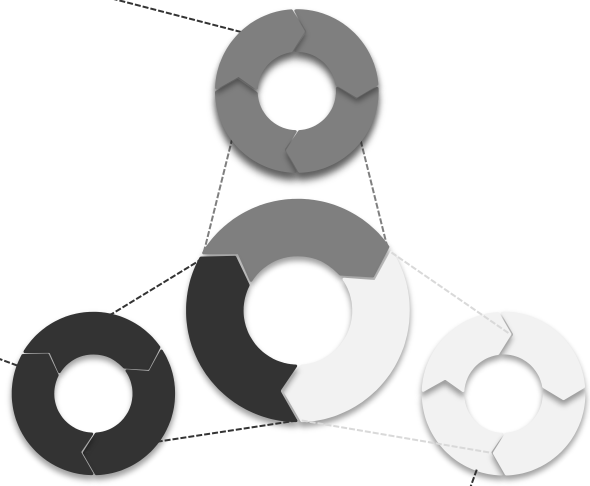
DLP как комплекс мер для обеспечения ИБ

ТЕХНОЛОГИЧЕСКИЕ МЕРЫ

Предотвращение утечек данных как защита корпоративной информации и персональных данных

Избирательная **блокировка**
каналов передачи данных и устройств,

Различные активные **действия**
с **хранимыми** и **передаваемыми** данными,
выполняемые для активного и проактивного
предотвращения утечек



Расследование и анализ инцидентов

Протоколирование событий доступа и передачи,
Работа с журналами, проверка теневых копий
(контроль инцидентов ИБ)

ОРГАНИЗАЦИОННЫЕ МЕРЫ

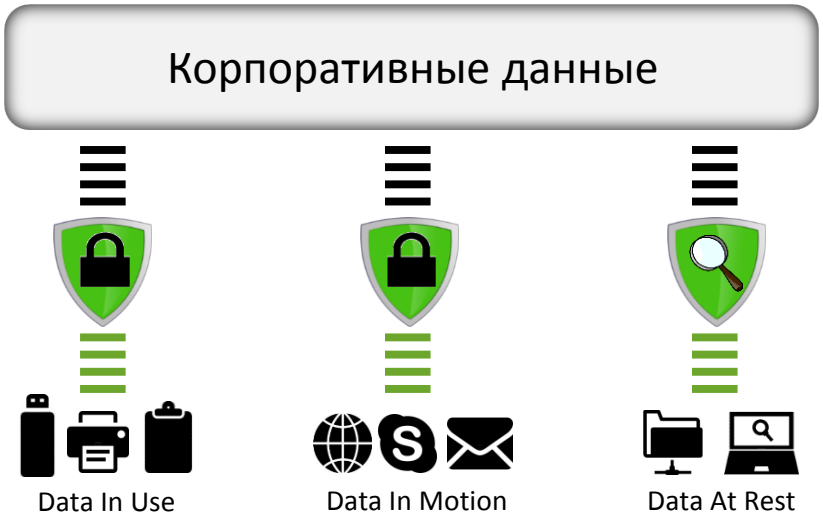
Тщательное проектирование. Регламентирующие документы.

Обеспечение организационных (административных и правовых) мер
по борьбе с утечками.
Личная ответственность **как сотрудников** *(за несанкционированную передачу данных),*
так и персонала служб ИБ *(за непринятие решения о снижении рисков или полное игнорирование рисков от использования каналов передачи данных)*.

Предотвратить утечки в любых сценариях

Мобильный сотрудник

Офисный пользователь



- ***Data In Use*** **(DIU)**
  - Локальные каналы – устройства сохранения, печати и передачи данных (съемные накопители, принтеры, буфер обмена, подключаемые устройства, включая мобильные, др.)
- ***Data In Motion*** **(DIM)**
  - Каналы сетевых коммуникаций – популярные коммуникационные приложения и протоколы, общие сетевые ресурсы (shares)
- ***Data At Rest*** **(DAR)**
  - Поиск и обнаружение документов со значимым для организации содержимым, хранимым в непредусмотренных для этого местах (файловые хранилища и файл-серверы, рабочие станции)
- **Равносильная DLP-защита для пользователей внутри и вне корпоративной сети**
  - Офисные пользователи
  - Мобильные сотрудники (в командировке, дома, …)
- **Сочетание контекстных и контентных механизмов для эффективной реализации принципа наименьших привилегий в DLP**
  - Сначала ограничить до минимума разрешенные каналы передачи данных – без нарушения бизнес-процессов
  - Затем использовать инспекцию содержимого (контента) для блокировки потоков данных, нерелевантных для бизнес-процессов

Технический аспект предотвращения утечек данных

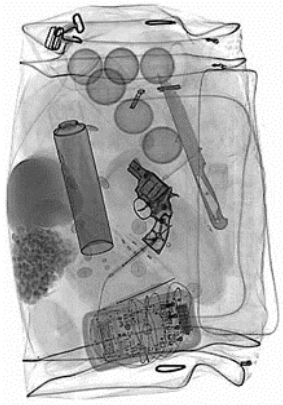
Автоматическое принятие решений на основе двух взаимодополняющих методов

Контекстный контроль

- Пользователь, его права, группы, в которых он состоит и т.п.
- Дата и время
- Местонахождение
- Источник / адресат
- Тип файла
- Направление передачи данных

Анализ и фильтрация содержимого (контентный контроль)

- Ключевые слова и сочетания слов, морфологический анализ, промышленные словари
- Встроенные шаблоны данных (номера карт страхования, кредитных карт, др.)
- Пользовательские шаблоны
- Проверка архивов и вложенных архивов, встроенных в файлы-контейнеры
- Возможность проверки как сообщений, так и вложений почты и мессенджеров
- Прочие критерии проверки



Взаимозависимость контентной фильтрации и контекстного контроля

КОНТЕКСТНЫЙ КОНТРОЛЬ

- Опосредован: контролируется доступ к портам, устройствам, другим интерфейсам
- Надежен, но неинтеллектуален: не может работать с информацией, содержащейся в формах данных

КОНТЕНТНАЯ ФИЛЬТРАЦИЯ

- Эффективный анализ информации возможен только в рамках её контекста
- Эффективная контентная фильтрация невозможна без сопутствующих данных о её передаче, отвечающих на вопросы: «кто», «откуда/куда», «когда» и т.п.
- Для того, чтобы отфильтрованная информация была содержательной и применимой к конкретным задачам обеспечения информационной безопасности, методы контентной фильтрации должны включать обработку контекстных параметров

Для полноценного DLP контроля требуется интеграция контекстных механизмов контроля с системой контентного анализа и фильтрации

Сочетание контекстных и контентных механизмов для эффективной реализации принципа наименьших привилегий в DLP:

- Сначала ограничить до минимума разрешенные каналы передачи данных – без нарушения бизнес-процессов
- Затем использовать инспекцию содержимого (контента) для блокировки потоков данных, нерелевантных для бизнес-процессов

Схема принятия решения DLP-системой при контентной фильтрации

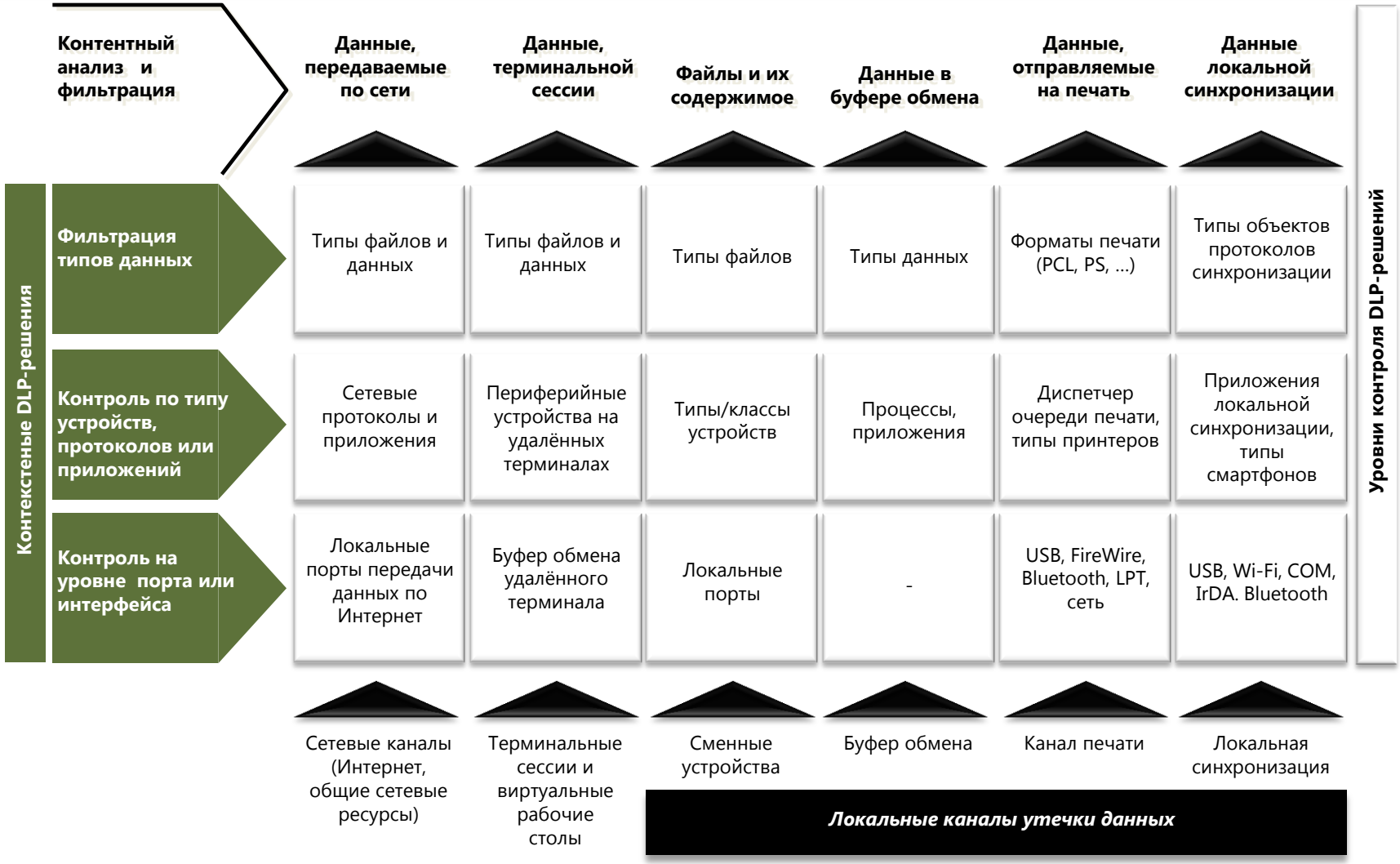
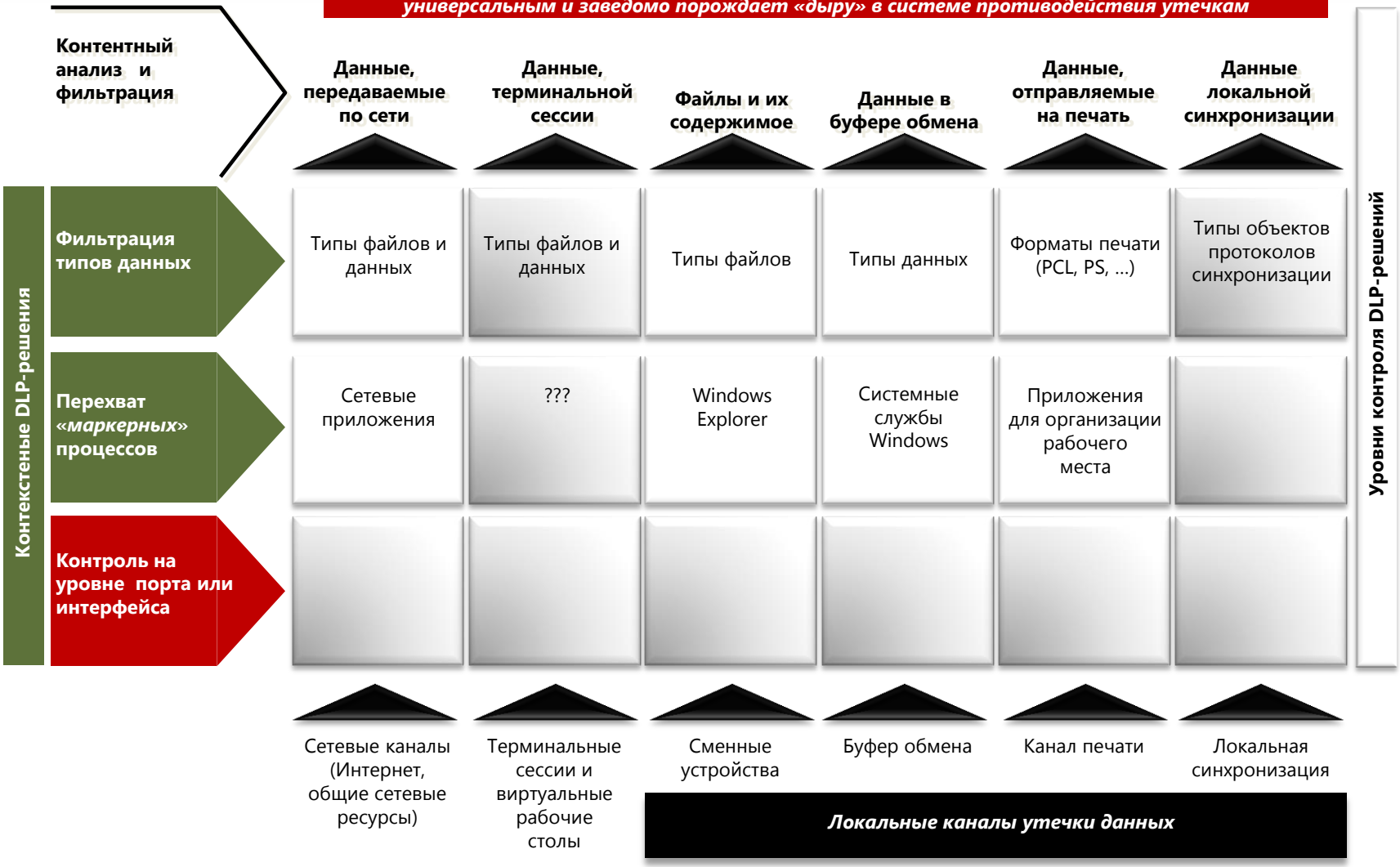


Схема принятия решения при перехвате отдельных процессов

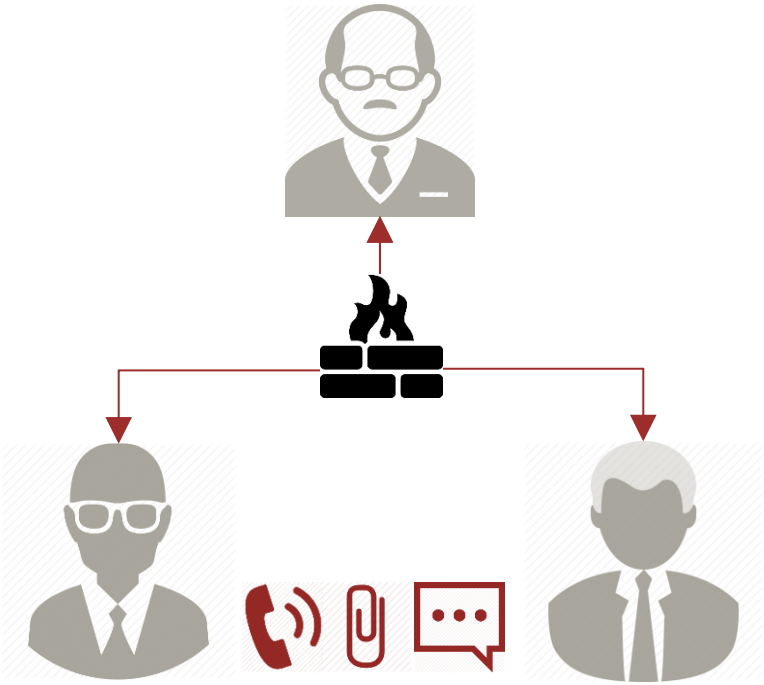
Контроль отдельных процессов (инжектом в приложения) всегда (!) лимитирован, не бывает универсальным и заведомо порождает «дыру» в системе противодействия утечкам



Классический вариант контроля сервиса с многими возможностями

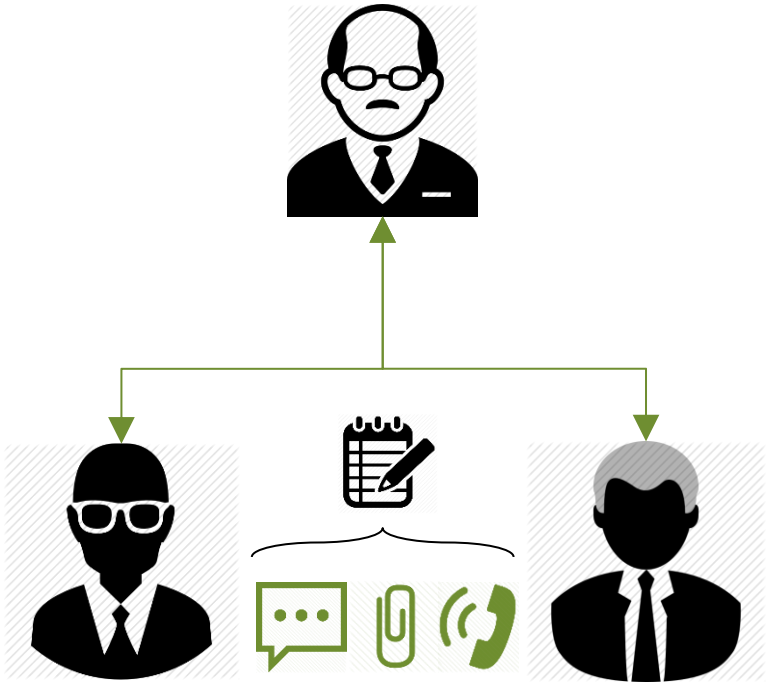
Запрет на уровне файрволла

- Передача всех типов данных запрещена
- Нет протоколирования,
  Нет событийной регистрации
- Не сохраняются теневые копии сообщений и вложений



«Простой» DLP-контроль

- Передача всех типов данных разрешена
- Протоколирование отправки данных в центральном журнале событийной регистрации.
- Сохраняются теневые копии сообщений и вложений.



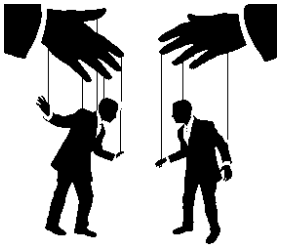
Избирательный контроль сервиса с многими возможностями

Полнофункциональная DLP-система

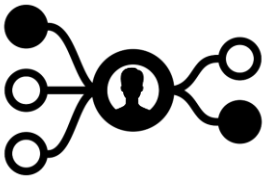
- Передача разрешена только между санкционированными учетными записями
- Событийная регистрация попыток и фактов передачи данных
- Содержимое вложений анализируется и фильтруется
- Сохраняются теневые копии вложений

Следствия ограниченного применения DLP-технологий

Ограниченное применение DLP (контроль устройств и/или сетевых коммуникаций) не может полностью предотвратить риски утечки данных даже при повсеместном внедрении.



Методы социальной инженерии позволяют обойти ограничения доступа



Ряд современных систем DLP существенно ограничен по ширине охвата контролируемых каналов и сервисов

Популярные сетевые сервисы созданы для удобства использования, не для обеспечения ИБ

Важно предотвращение утечек не только передаваемых (data-in-motion) и используемых (data-in-use), но и хранимых данных (data-at-rest)

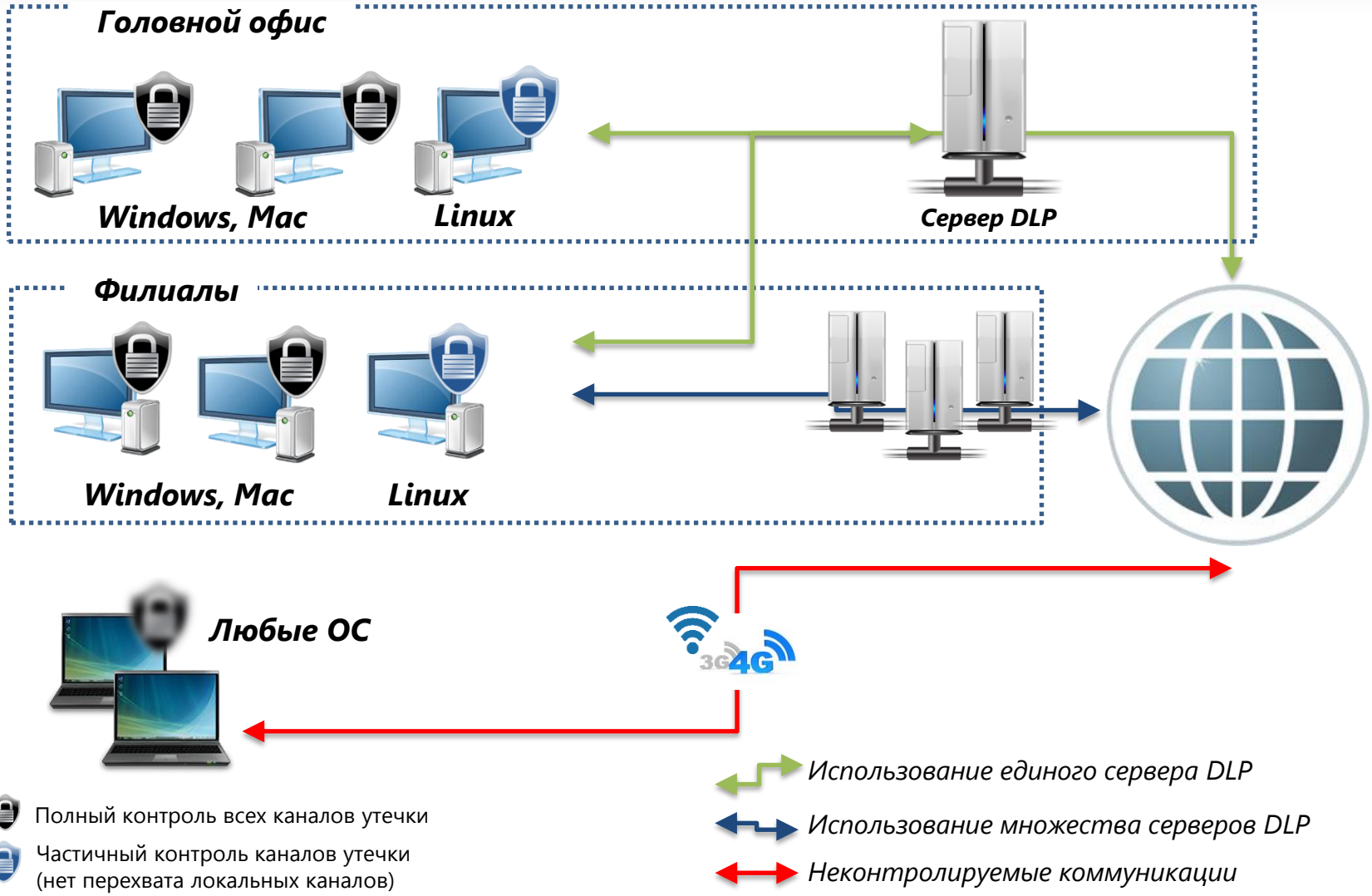
Content Discovery

Поиск и обнаружение в корпоративной ИТ-инфраструктуре конфиденциальных и данных

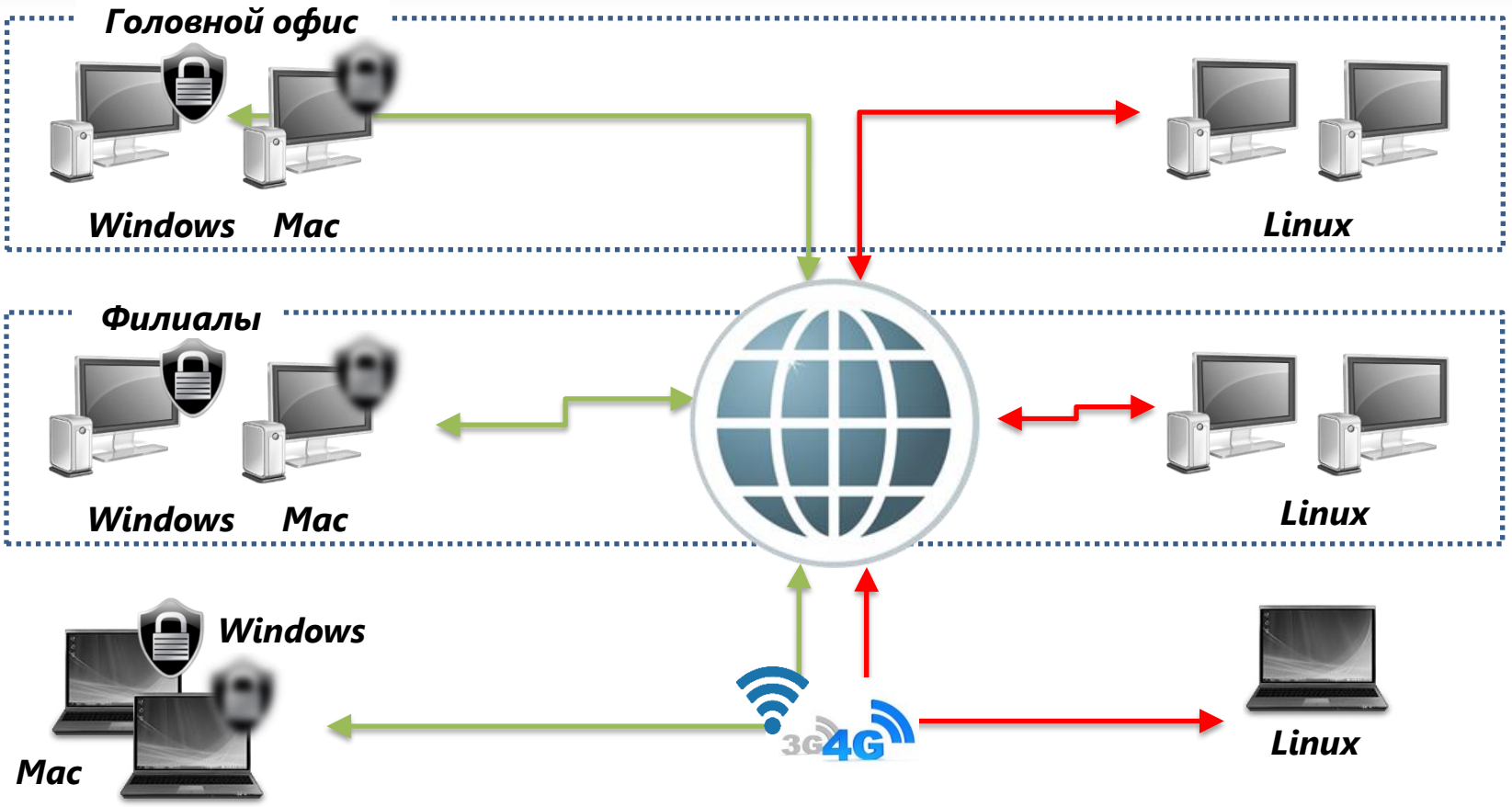
Позволяет выявить факт несанкционированного хранения данных и осуществить превентивную защиту от утечки до момента передачи данных

Устраняет фактор неопределенности канала передачи данных: не важно, какой канал утечки кем и когда может быть задействован

Архитектура сетецентричной DLP-системы на практике



Архитектура хостовой DLP-системы на практике



Полный контроль всех каналов утечки

Частичный контроль каналов утечки (нет перехвата сетевых каналов)

Контролируемые коммуникации

Неконтролируемые коммуникации

«Точки применения» технологий контентного анализа

Когда может выполняться анализ содержимого данных?

Анализ **хранимых** данных (discovery)

Анализ **передаваемых** данных (передача, сохранение, печать)

Анализ **перехваченных** данных (полнотекстовый поиск, фильтрация результатов по контенту)

ПОЛНОФУНКЦИОНАЛЬНЫЕ РЕШЕНИЯ DLP

РЕШЕНИЯ «DLP»

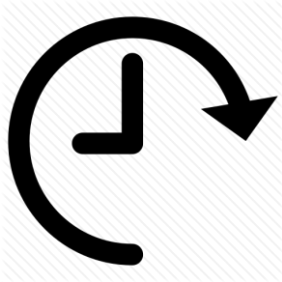
Следствие ограниченного применения контентной фильтрации только для анализа постфактум
- в архиве DLP-системы хранятся ВСЕ перехваченные данные, без разделения на корпоративные и личные.

Контроль личных коммуникаций возможен и реализуем...

...при правильном подходе к использованию технологий контентной фильтрации:

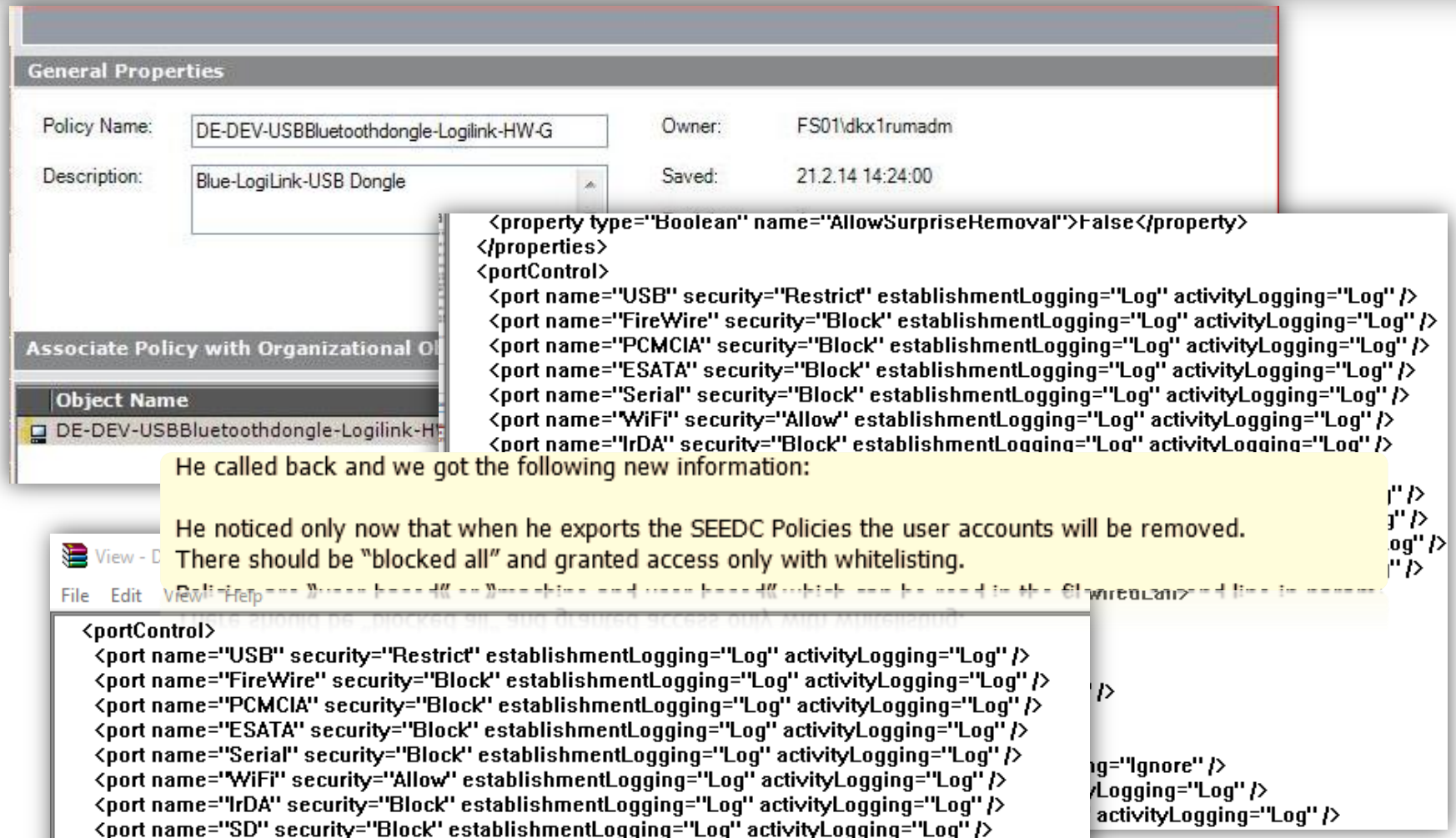
- детектирование на фазе перехвата передаваемых, сохраняемых или печатаемых данных именно тех, которые
  непосредственно являются конфиденциальной корпоративной информацией,
- избирательное сохранение в архиве корпоративных данных
- анализ архива с поиском конфиденциальной информации.

Анализ **передаваемых** данных в целях недопущения утечки и избирательного теневого копирования (наполнения архива).



Анализ **перехваченных** данных в архиве (полнотекстовый поиск, фильтрация результатов по контенту)

Зарубежная практика



DLP система – что это?

Система класса DLP

- ИТ-решение, обеспечивающее детектирование и предотвращение неавторизованного использования, хранения и перемещения данных конфиденциальных, ограниченного доступа и др., используемых в организации
- Использует контекстные методы анализа и контроля
- Использует инспекцию и фильтрацию контента

Функциональные типы DLP

- *Data In Motion (DIM)* – контроль данных, перемещаемых через каналы сетевых коммуникаций

  Email, Webmail, IM, Social Media, Cloud File Sharing, P2P, HTTP(S), FTP(S)
- *Data In Use (DIU)* – контроль доступа и операций перемещения данных через локальные каналы и приложения на рабочих станциях

  Съемные накопители, локальные и перенаправленные хранилища, буфер обмена, канал печати, снимки экранов, общий сетевой доступ
- *Data At Rest (DAR)* – поиск и обнаружение чувствительного содержимого в файлах и данных, хранимых в корпоративной ИТ-инфраструктуре, а также защита обнаруженных данных от неконтролируемого использования и перемещения посредством исполнения заданных автоматизированных действий по устранению выявленных нарушений

  Сетевые файловые ресурсы общего доступа, NAS хранилища, файловые системы рабочих станций, базы данных, системы электронного документооборота и их репозитории

Виды архитектуры DLP решений

- *Сетевые DLP (Network DLP)* – компоненты DLP сетевого размещения (аппаратные или виртуальные шлюзы, MTA или ICAP серверы)
- *Endpoint DLP* – агентные DLP, функционирующие на контролируемых компьютерах (рабочие станции, серверы, мобильные компьютеры)
- *Гибридные DLP* – комбинация Network DLP + Endpoint DLP

Стоимость управления DLP системой – влияющие факторы

- **Доступность развертывания и управления внутренними ресурсами**

  Насколько легко изучить, установить, сконфигурировать и обслуживать систему силами собственного персонала с «обычным» уровнем квалификации (опытные и обученные системные/сетевые администраторы)

- **Легкость использования**

  Наличие инструментария централизованного развертывания, управления и обслуживания

  Отсутствие необходимости вовлечения пользователей и локальных администраторов в процессы управления и обслуживания системы

- **Возможность приобретения только функций, достаточных для решения задач в текущем профиле ИБ с расширением их по необходимости**

  Опциональное лицензирование «по функционалу» с возможностью инкрементального апгрейда

- **Масштабируемость без излишних затрат**

  Высокая масштабируемость – по дизайну и на практике

  Обновления системы без необходимости переустановки и изменений в инфраструктуре

  Накопительные скидки для растущего бизнеса

DLP-технологии на практике – что стоит сделать при внедрении?

Современная корпоративная модель ИБ, чтобы стать реально эффективной, должна быть информационно-центричной, опираться на совокупность контроля непосредственно данных и различных потоков их передачи и распространения.

- Рассмотреть все возможные сценарии утечки данных с оконечных устройств в целях создания избирательной системы контроля передачи данных
- Минимизировать число привилегированных пользователей и внедрить ролевой доступ к системам

Пользователи в действительности не нуждаются в слишком широких привилегиях для выполнения своих бизнес-задач

- Провести классификацию данных и процессов - понять, что именно предстоит защищать и каковы приоритетные направления защиты.

Без расстановки приоритетов все будет защищено одинаково плохо

- Просчитать варианты дальнейшего использования результатов работы DLP-системы в задачах общего анализа состояния информационной безопасности (интеграция с системами SIEM/BI)

Противодействие утечкам – не единственная функция DLP.
DLP-система не должна существовать в вакууме, но должна прозрачно интегрироваться в комплекс средств ИБ предприятия.
DLP – это инструмент работы не только с информацией, но и с сотрудниками, и с бизнес-процессами.

Превентивный контроль: Качество + Эффективность + Надежность

- **Качество – полнота контроля (“дьявол кроется в деталях”)**

  - ***SMTP*** → инспекция контента исходящих сообщений и вложения для **любого SMTP клиента** (не только для MS Outlook, Thunderbird и IBM/Lotus Notes)
  - ***Web-почта*** → инспекция контента исходящих сообщений и вложения для **любого браузера** (не только для IE, Firefox и Chrome)
  - ***Web-доступ (HTTP/HTTPS)*** → инспекция контента в формах и файлах, отправляемых через **любой браузер** или **HTTP агент** (не только для IE, Firefox и Chrome)
  - ***Instant Messengers*** → инспекция контента как для файлов, так и для **исходящих сообщений** (не только для файлов)
  - ***P2P file sharing*** → блокировка файлового обмена для **всех Torrent агентов**
  - ***Детектирование содержимого*** → извлечение и инспекция текстового содержимого **из изображений и графических файлов** (не только из текстовых файлов)
  - ***Печать***→ инспекция контента документов, печатаемых **без сохранения в файл**
  - ***Снимки экрана*** → блокировка снимков экрана, выполняемых **любым приложением** (не только клавишей PrintScreen)
- **Эффективность**
  - Гибкость сочетания контекстных и контентно-зависимых политик для повышения производительности DLP-решения
- **Надежность**
  - Защита от вмешательства пользователя, в особенности с правами **локального системного администратора**

DeviceLock DLP – полноценный контроль на рабочих станциях

ПРЕДОТВРАЩЕНИЕ И КОНТРОЛЬ УТЕЧЕК…

…через локальные порты и устройства

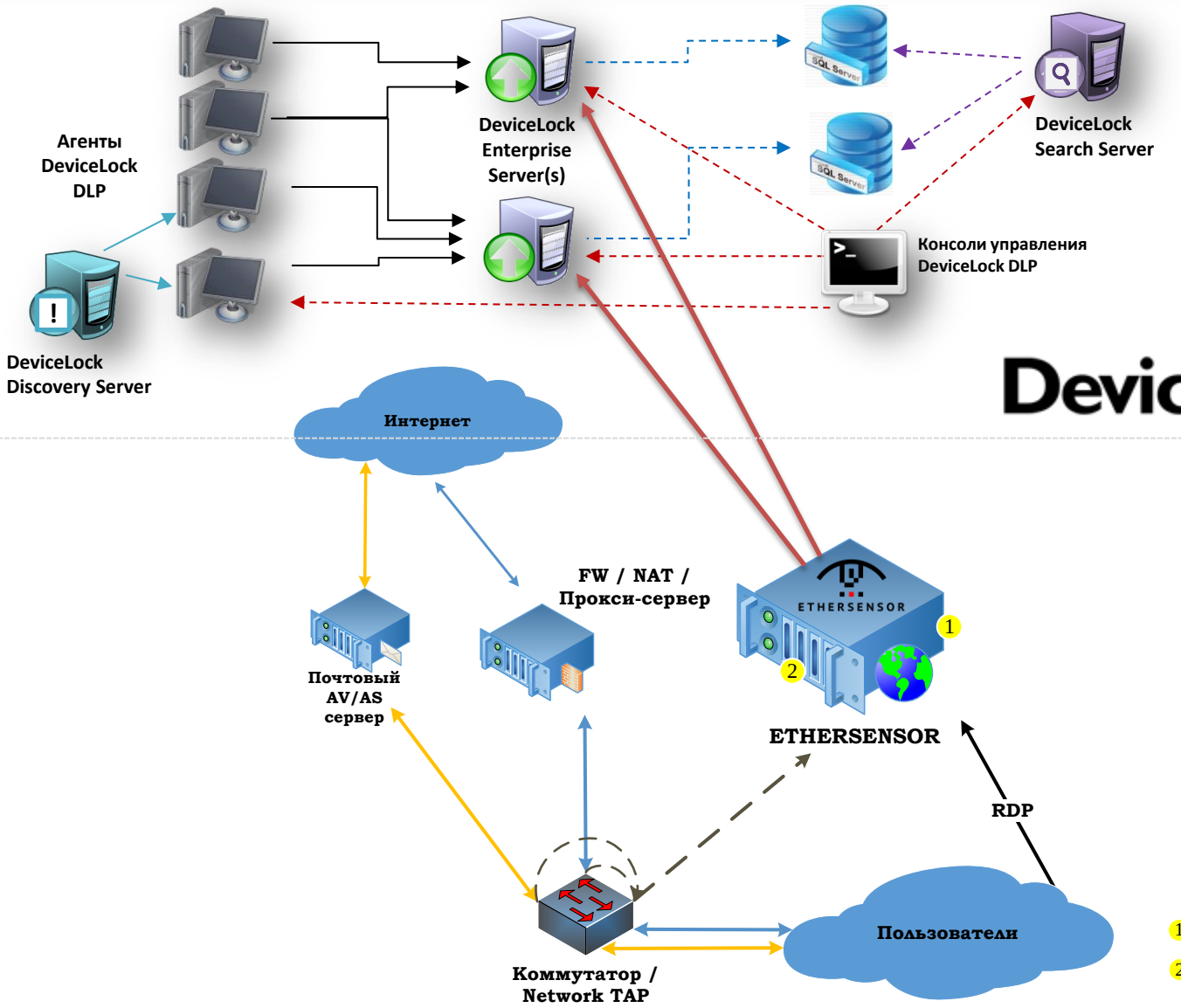
…через различные каналы сетевых коммуникаций

…с применением различных технологий контентной фильтрации

… сканированием хранимых данных.

+ собственный поисковый сервер

Гибридная DLP-система: DeviceLock DLP + MicroOLAP EtherSensor



Уже скоро

DEVICELOCK DLP 8.2

УСИЛЕНИЕ РОЛИ СЕРВЕРА

Граф связей между пользователями внутри организации и с внешними пользователями (по каналам сетевых коммуникаций)

Отправка данных журналов, относящихся к заданным пользователям / группам, на «свои» (заданные) серверы

Распространение политик DLP с сервера

РАЗВИТИЕ КОНТЕНТНОЙ ФИЛЬТРАЦИИ

Использование адресов отправителя и получателя электронных сообщений в правилах анализа и фильтрации содержимого (для ряда каналов сетевых коммуникаций)

Контентный анализ для файлов, передаваемых на перенаправленные в терминальную сессию диски

Теневое копирование как опция контентных правил контроля доступа / обнаружения

ПРОЧЕЕ

Развитие языка и фильтров поисковых запросов сервера полнотекстового поиска Search Server

Поддержка Microsoft SQL Server 2016

Поддержка SYSLOG для интеграции с SIEM системами

Поддержка Skype for Web

АВТОМАТИЧЕСКИЙ ПОЛНОТЕКСТОВЫЙ ПОИСК

- Поисковые задачи по расписанию
- Инкрементальный поиск

СЛЕДУЮЩИЕ ВЕРСИИ

ДАЛЬНЕЙШЕЕ УСИЛЕНИЕ РОЛИ СЕРВЕРА

Автоматическое создание отчетов на основе данных событийного протоколирования и теневого копирования, централизованно хранящихся на сервере

Поддержка цифровых отпечатков данных

РАЗВИТИЕ ФУНКЦИОНАЛА АГЕНТА

Больше контролируемых служб мгновенных сообщений

Снимки экрана - непрерывно и вокруг событий

РАЗВИТИЕ ПОИСКОВОГО СЕРВЕРА

- Полнотекстовый поиск с использованием геоспецифических и промышленных словарей, регулярных выражений

СПАСИБО
ЗА ВНИМАНИЕ!

АО ДИАЛОГНАУКА

Системный интегратор в области ИБ

EMAIL INFO@DIALOGNAUKA.RU
URL WWW.DIALOGNAUKA.RU
TEL +7(495)980-67-76

СЕРГЕЙ ВАХОНИН

Директор по решениям Смарт Лайн Инк

EMAIL SV@DEVICELOCK.COM
FACEBOOK SERGEY.VAKHONIN
MOBILE +79859701707

www.DeviceLock.com