КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4 октября 2018 г.
г. Красноярск

ВНЕ ПЕРИМЕТРА

#CODEIB

КОТ ИБ

Светлана Марьясова,
Региональный представитель АО «ИнфоВотч»

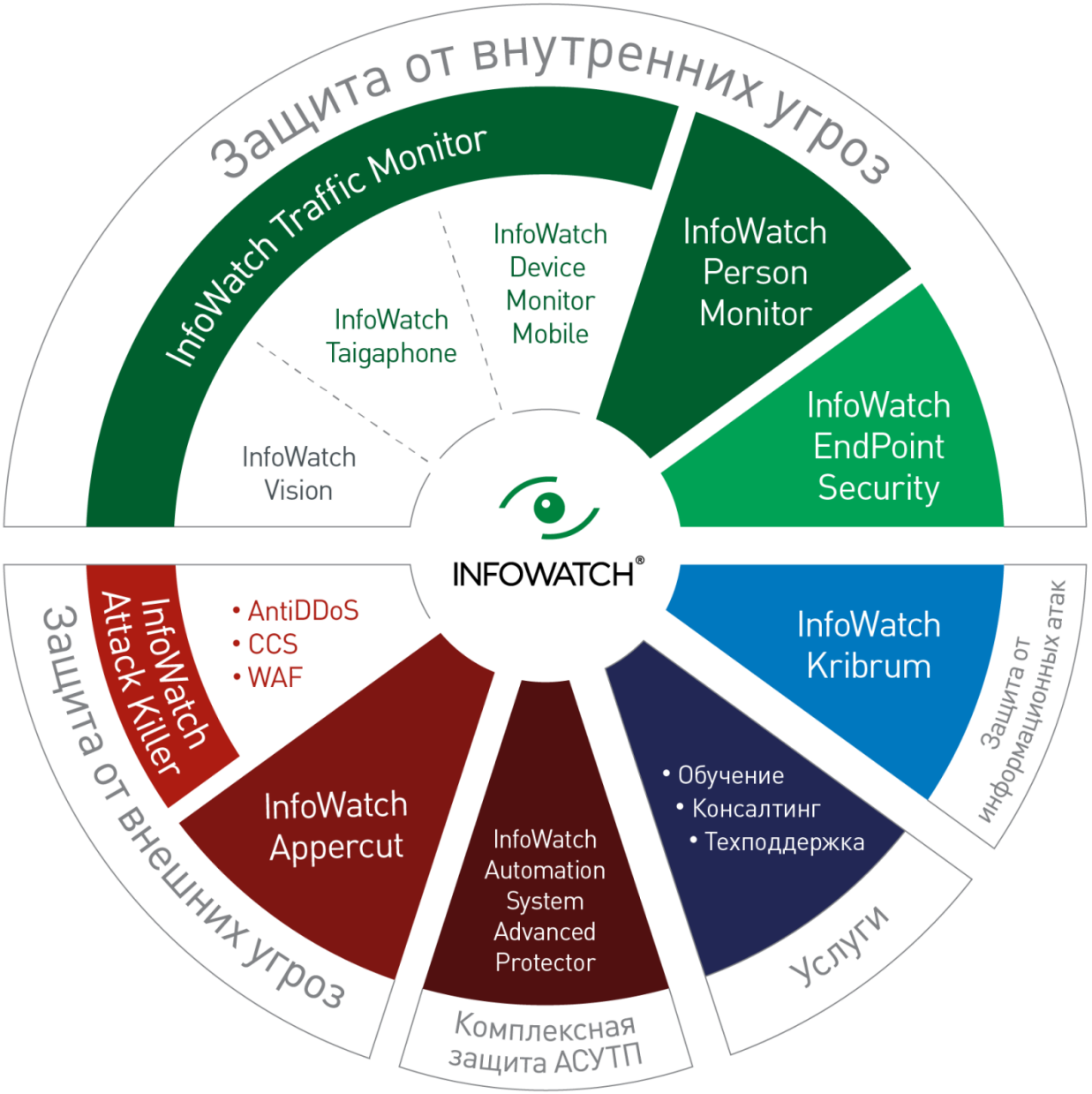
ТЕЛЕФОН: +7 (950) 415-32-00

EMAIL: Svetlana.Maryasova@infowatch.com

КОТ ИБ corporation

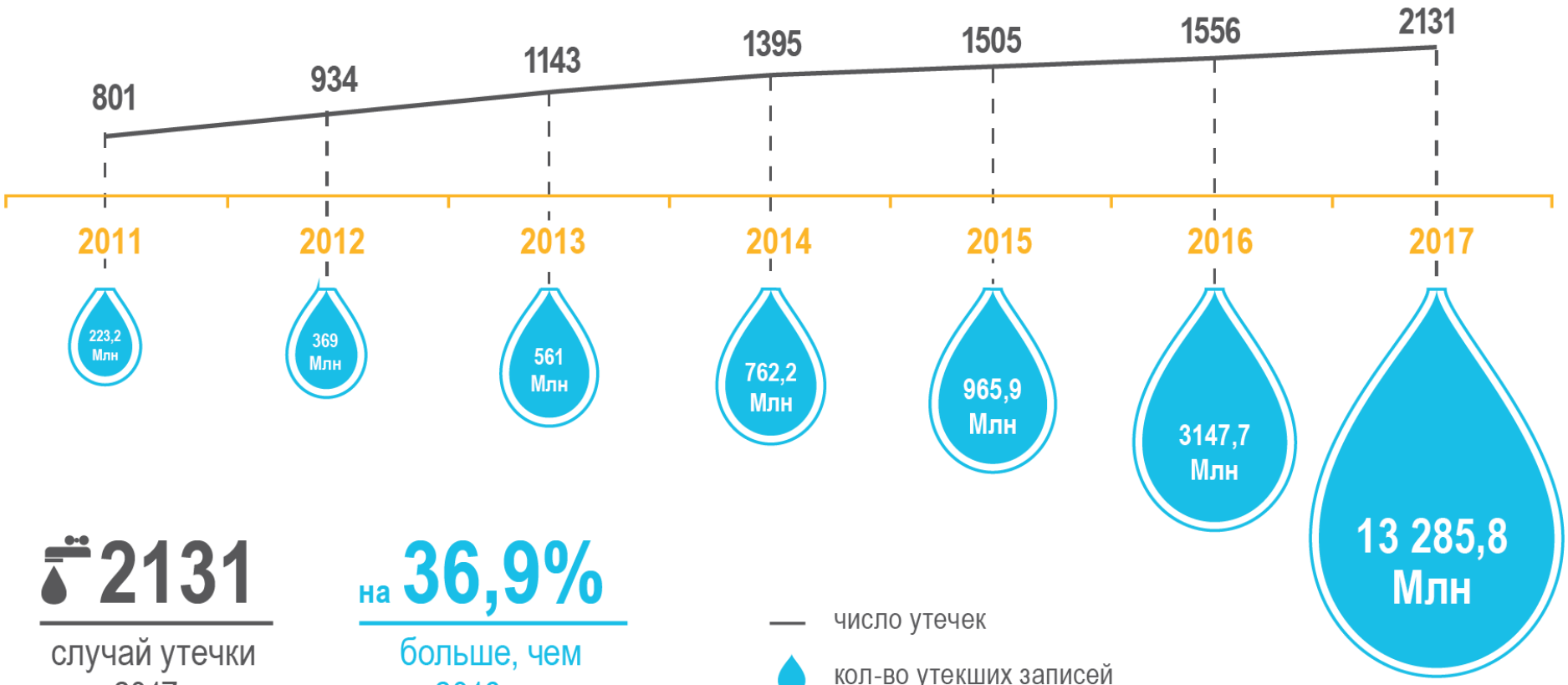
Продуктовый портфель

INFOWATCH®



Исследование информационных утечек

Утечки набирают скорость



2131

случай утечки за 2017 год

на 36,9%

больше, чем в 2016 году

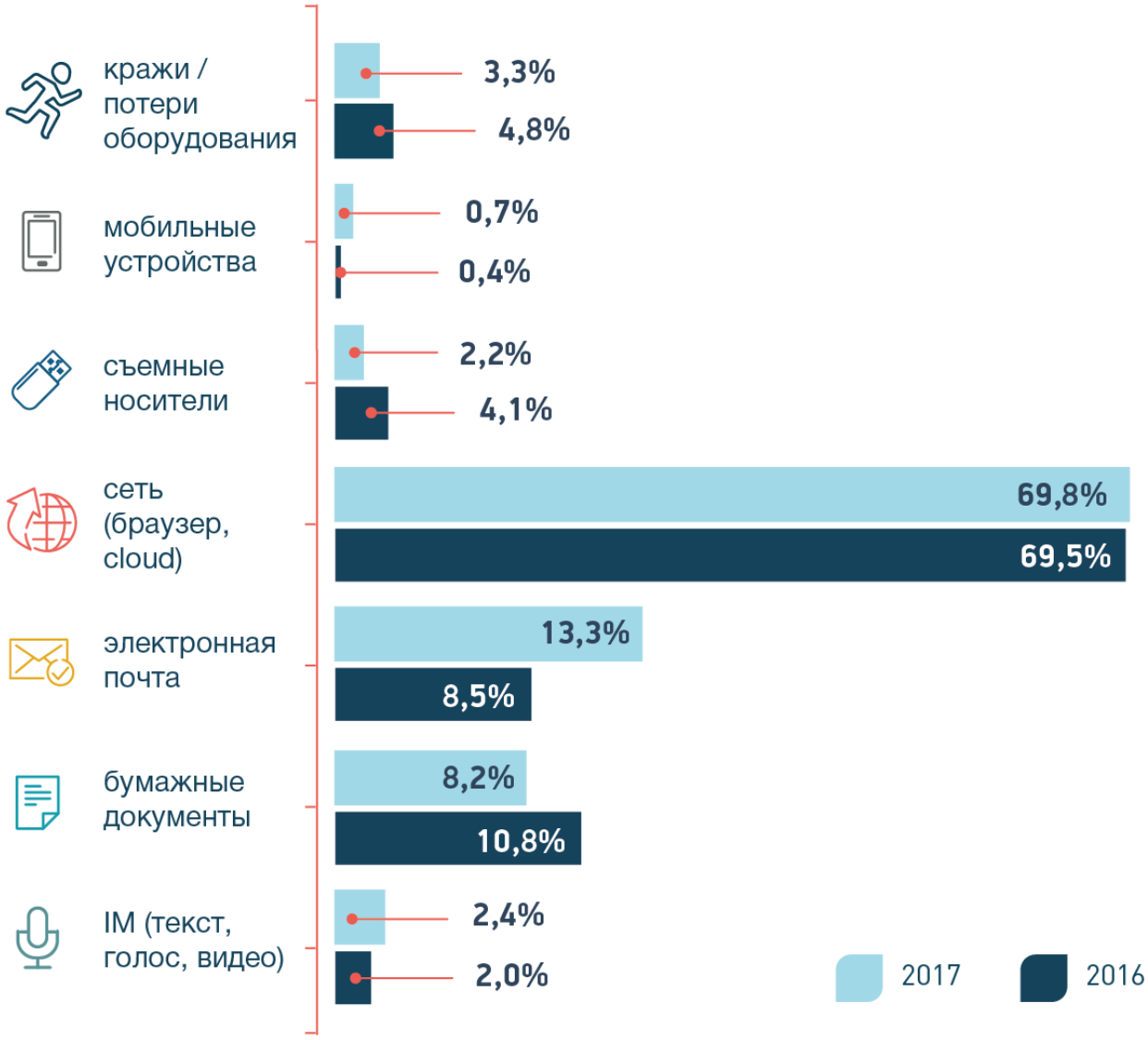
— число утечек

кол-во утекших записей

по данным Аналитического Центра InfoWatch, 2018

Исследование информационных утечек

Каналы утечек



-1,5%
кражи / потери оборудования

0%
мобильные устройства

-1,9%
съемные носители

0%
сеть (браузер, cloud)

+4,8%
электронная почта

-2,2%
бумажные документы

0%
IM (текст, голос, видео)

по данным Аналитического Центра InfoWatch, 2018

Примеры конфиденциальных документов


РОССИЙСКАЯ ФЕДЕРАЦИЯ
ЕДИНЫЙ ГОСУДАРСТВЕННЫЙ РЕЕСТР ПРАВ НА НЕДВИЖИМОЕ ИМУЩЕСТВО И СДЕЛОК С НИМ

СВИДЕТЕЛЬСТВО
О ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРАВА

Московский городской комитет
по государственной регистрации прав
на недвижимое имущество и сделок с ним

Субъект права:
дата рожд.:
паспорт:
выдан:
Вид права: собственность
Описание права: индивидуальная
Объект права: квартира N
по адресу:

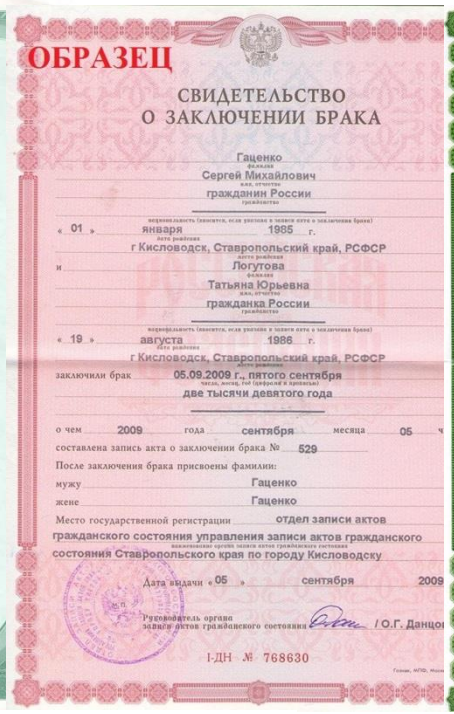
условный номер:
общая площадь
общая площадь без учета лоджий и балконов
жилая площадь кв. м, количество комнат:

о чем в Едином государственном реестре прав на недвижимое имущество и сделок с ним сделана запись регистрации N

Обременение объекта права: не зарегистрировано

Регистратор

77


ОБРАЗЕЦ

СВИДЕТЕЛЬСТВО
О ЗАКЛЮЧЕНИИ БРАКА

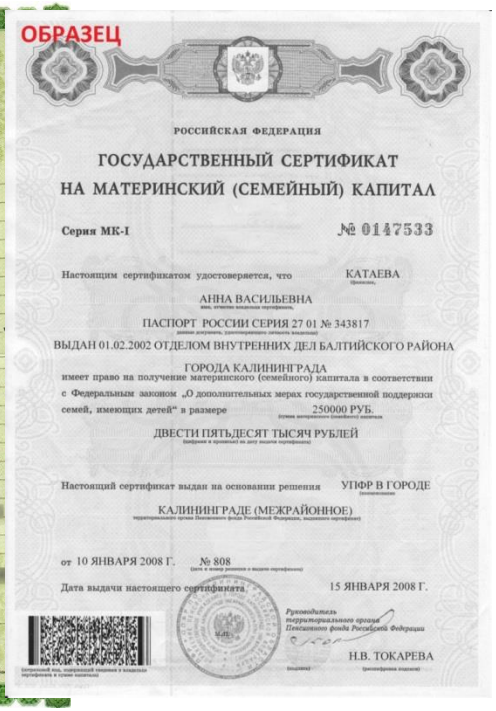
Гаценко
Сергей Михайлович
гражданин России
« 01 » января 1985 г.
г.Кисловодск, Ставропольский край, РСФСР
и
Логутова
Татьяна Юрьевна
гражданка России
« 19 » августа 1986 г.
г.Кисловодск, Ставропольский край, РСФСР
заключили брак 05.09.2009 г., пятого сентября
две тысячи девятого года

о чем 2009 года сентября месяца 05
составлена запись акта о заключении брака № 529
После заключения брака присвоены фамилии:
мужу Гаценко
жене Гаценко
Место государственной регистрации отдел записи актов гражданского состояния управления записи актов гражданского состояния Ставропольского края по городу Кисловодску
Дата выдачи « 05 » сентября 2009
Руководитель органа записи актов гражданского состояния / О.Г. Данцо

I-ДН № 768630


СВИДЕТЕЛЬСТВО
О РОЖДЕНИИ

родился(лась)
место рождения
Российская Федерация
о чем года месяца
составлена запись акта о рождении №
Отец
Мать
Место государственной регистрации
Дата выдачи «
Руководитель органа записи актов гражданского состояния


ОБРАЗЕЦ

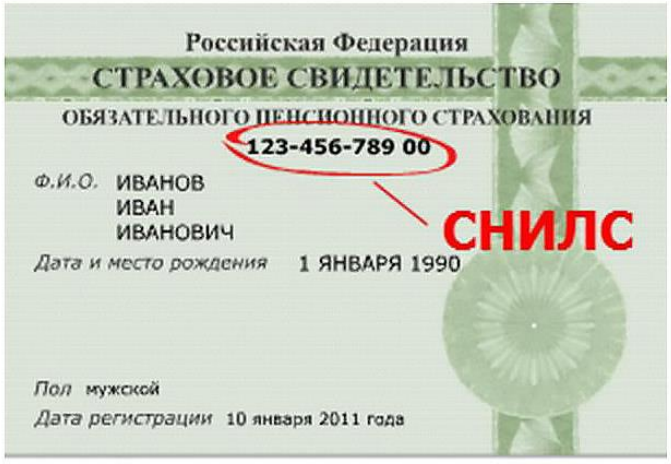
РОССИЙСКАЯ ФЕДЕРАЦИЯ

ГОСУДАРСТВЕННЫЙ СЕРТИФИКАТ
НА МАТЕРИНСКИЙ (СЕМЕЙНЫЙ) КАПИТАЛ

Серия МК-I № 0147533

Настоящим сертификатом удостоверяется, что КАТАЕВА
АННА ВАСИЛЬЕВНА
ПАСПОРТ РОССИИ СЕРИЯ 27 01 № 343817
ВЫДАН 01.02.2002 ОТДЕЛОМ ВНУТРЕННИХ ДЕЛ БАЛТИЙСКОГО РАЙОНА
ГОРОДА КАЛИНИНГРАДА
имеет право на получение материнского (семейного) капитала в соответствии с Федеральным законом „О дополнительных мерах государственной поддержки семей, имеющих детей“ в размере 250000 РУБ.
ДВЕСТИ ПЯТЬДЕСЯТ ТЫСЯЧ РУБЛЕЙ

Настоящий сертификат выдан на основании решения УПФР В ГОРОДЕ
КАЛИНИНГРАДЕ (МЕЖРАЙОННОЕ)
от 10 ЯНВАРЯ 2008 Г. № 808
Дата выдачи настоящего сертификата 15 ЯНВАРЯ 2008 Г.
Руководитель территориального органа Пенсионного фонда Российской Федерации
Н.В. ТОКАРЕВА


Российская Федерация
СТРАХОВОЕ СВИДЕТЕЛЬСТВО
ОБЯЗАТЕЛЬНОГО ПЕНСИОННОГО СТРАХОВАНИЯ
123-456-789 00
СНИЛС
Ф.И.О. ИВАНОВ
ИВАН
ИВАНОВИЧ
Дата и место рождения 1 ЯНВАРЯ 1990
Пол мужской
Дата регистрации 10 января 2011 года


РОССИЙСКАЯ ФЕДЕРАЦИЯ
ПАСПОРТ


RUS
ВОДИТЕЛЬСКОЕ УДОСТОВЕРЕНИЕ
1. СМИРНОВ
SMIRNOV
2. ЮРИЙ СЕРГЕЕВИЧ
YURIY SERGEYEVICH
3. 30.05.1991
КОСТРОМСКАЯ ОБЛ.
KOSTROMSKAYA OBL.
4a) 13.04.2012 4b) 13.04.2022
4c) ГИБДД 37[redacted]
GIBDD 37[redacted]
5. 37[redacted]1
8. ИВАНОВСКАЯ ОБЛ.
IVANOVSKAYA OBL.
9. B C
6.
7.

Как оценить состояние режима работы с конфиденциальной информацией

INFOWATCH®

Пилотный проект InfoWatch Traffic Monitor Enterprise

фрагмент отчета

2. Результаты тестовой эксплуатации

1. Общий объем проанализированного трафика: **52 802** объектов;
2. Общий объем трафика, определенного как запрещенный: **2 999** объектов (**5, 68 %** от общего числа объектов);
3. Статистика по запрещенному трафику – по каналам:
   a. 71,92% - передача информации по почте и в Интернет
   b. 28,08% - действия печати и копировании на съемные носители
   c. 0% - информация, хранящаяся на локальных дисках рабочих станций, разделяемых сетевых ресурсах и файловых хранилищах SharePoint
4. Статистика по запрещенному трафику – по уровню угроз:
   a. 2 846 событий с высоким уровнем угроз (94,9%)
   b. 0 событий – со средним (0%)
   c. 153 события – с низким (5,1%)

Как оценить состояние режима работы с конфиденциальной информацией

INFOWATCH®

фрагмент отчета

Статистика по объектам защиты

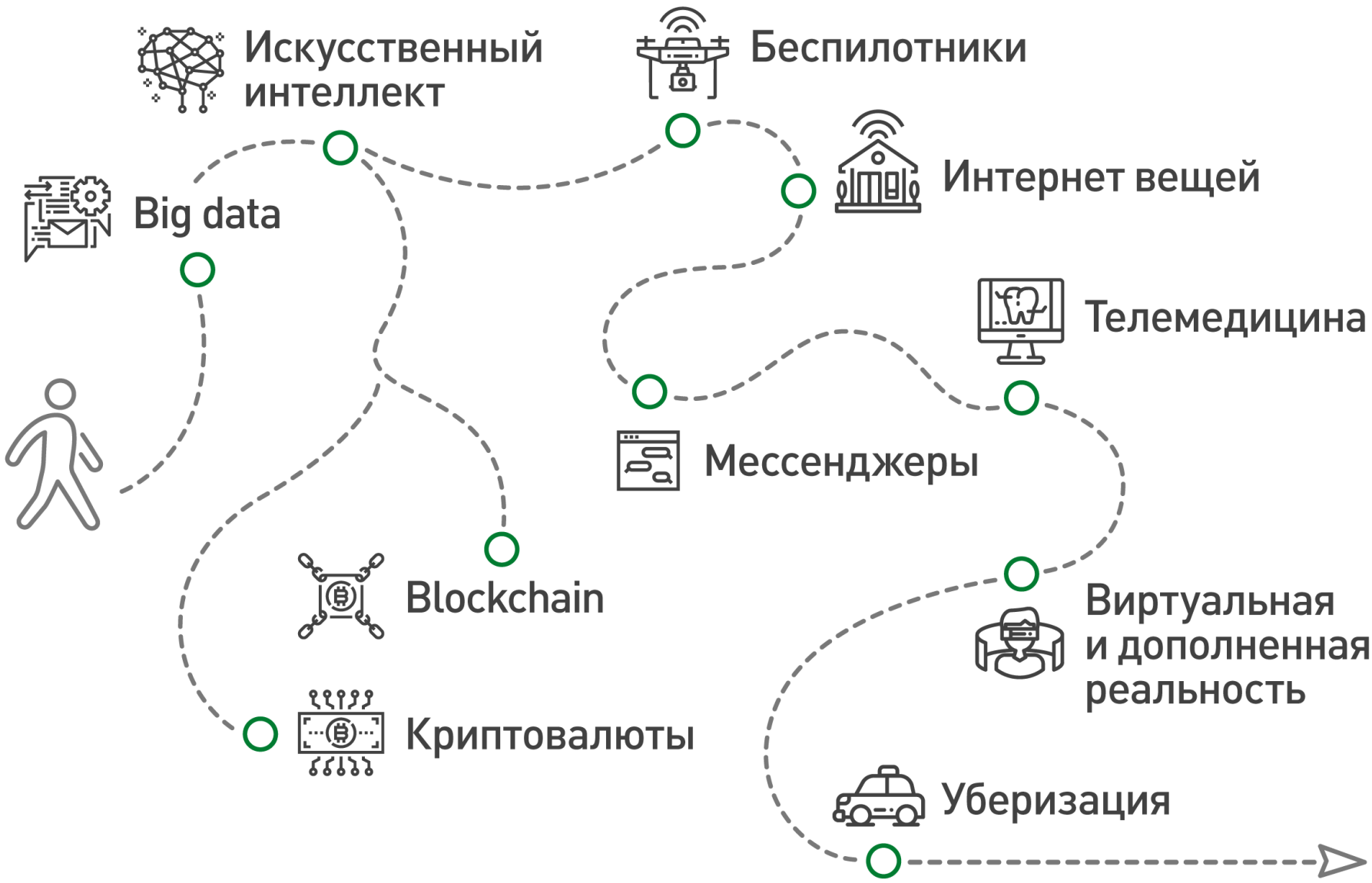
Без учета правил

31.05.2016 - 28.06.2016

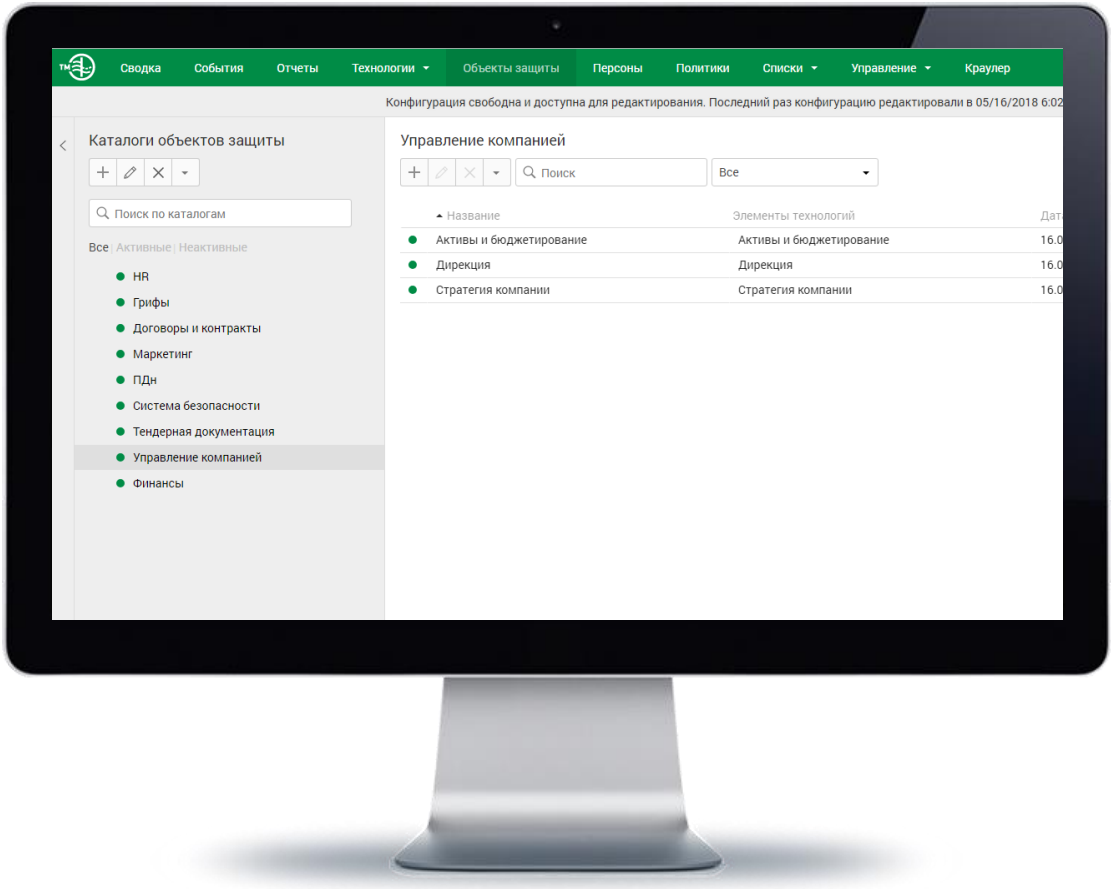
Объекты защиты	Высокий	Средний	Низкий	Отсутствует
Юридическая документация	1132	0	0	158
Информация по кадрам	729	0	0	73
СНИЛС	499	0	0	16
Сведения о государственной регистрации предприятия	491	0	0	190
Внутренние выплаты (сотрудникам)	306	0	0	25
Счета	250	0	0	37
Информация по кредитованию	242	0	0	5
Удостоверения личности	220	0	0	1277
Информация по налогам	50	0	0	14
Бухгалтерская документация	29	0	0	5
Кредитная карта	5	0	0	0
Платежные реквизиты	4	0	0	3
Внешнеэкономическая деятельность	4	0	0	2
Патенты и сертификация	0	0	0	3
Конкурсная деятельность	0	0	0	2

Новые технологии – новые рамки

INFOWATCH®



Интеграция с Microsoft Office 365



Возможности:

- Контроль появления конфиденциальной информации в облаке

Результат:

- Анализ перехваченных данных в InfoWatch Traffic Monitor
- Выявление инцидентов информационной безопасности
- Хранение событий и теневых копий в единой базе данных

Поддержка Astra Linux

INFOWATCH®

ASTRALINUX special edition

Реализована поддержка службы каталогов Astra Linux Directory

Одновременная поддержка сразу двух LDAP (AD и ALD)

Перехват на агенте

Сертификация НДВ-2 Минобороны РФ

Успешные испытания в ряде предприятий ОПК

*Решение **InfoWatch Traffic Monitor** прошло сертификацию совместимости*
РусБИТех / Software Ready for Astra Linux

Контроль голосового трафика (VoIP)

ИНТЕГРАЦИЯ INFOWATCH TRAFFIC MONITOR С РЕШЕНИЕМ SMART LOGGER II

InfoWatch Smart Logger II Adapter – это модуль, который извлекает записи голосовых разговоров в текстовом виде из решения Smart Logger II и передает на анализ в InfoWatch Traffic Monitor. InfoWatch Traffic Monitor применяет весь спектр технологий для анализа текстов разговора и полноценной защиты от внутренних угроз. Интеграция реализована на базе SDK через pushAPI

Источники голосового трафика

- VoIP
- MS Lync
- Интеграция с коммуникационными платформами: Avaya, Cisco, Genesys, Naumen, Siemens (Unify)
- Микрофоны
- Аналоговые и цифровые АТС
- Skype и другие

Какие данные передаются на анализ в InfoWatch Traffic Monitor?

1. Текст разговора
2. Атрибуты разговора (длительность, время звонка)
3. Данные абонентов

ВНЕ ПЕРИМЕТРА БЕЗОПАСНОСТИ

Защита данных на корпоративных мобильных устройствах

INFOWATCH®

InfoWatch
Device Monitor Mobile *–*
модуль DLP-решения InfoWatch Traffic Monitor, защищающий корпоративные данные на мобильных устройствах

Контроль каналов коммуникаций сотрудников на мобильных устройствах

Контроль перемещения информации внутри и вовне периметра безопасности

Автоматическая классификация и анализ данных

Безопасное расширение периметра корпоративной сети

Контролируемые каналы

INFOWATCH®

Электронная почта
- SMTP, IMAP4, POP3
- Теневое копирование всех сообщений и вложенных файлов

Веб-трафик
- HTTP/s трафик
- Веб-ресурсы, социальные сети, облачные хранилища

Камера

Перехват и теневое копирование снятых фотографий

Сообщения
- Перехват и теневое копирование входящих и исходящих сообщений
- Анализ и архивирование SMS-сообщений
- Анализ и архивирование переписки WhatsApp, Viber, Telegram, Skype

Запуск приложений
- «Белые» и «черные» списки
- Запрет использования

Защита данных на личных мобильных устройствах

WorksPad

infotecs®

INFOWATCH®

Совместное решение, разработанное тремя компаниями:

- В решении реализован **принцип «защищенной витрины»** – разграничение корпоративного и личного пространства
- **Поддерживает концепцию BYOD** устанавливается на любое мобильное устройство, независимо от модели, операционной системы и прошивки
- Работоспособность решения **не зависит от обновлений** ОС и приложений
- **Централизованная установка**
- **Мотивация сотрудников** – доступ к корпоративным ресурсам

Решаемые задачи

Безопасное **расширение периметра** корпоративной сети

Контроль **каналов коммуникаций** сотрудников на смартфоне

Доверенное устройство для мобильных сотрудников

Предотвращение утечек конфиденциальных данных с устройства

InfoWatch Taigaphone –

смартфон с доверенной прошивкой на базе Android

Там, где не BYOD не пройдет

В отличие от личного смартфона Taigaphone:

- является **мобильным рабочим местом** с безопасным доступом к корпоративным ресурсам
- **защищен от угрозы** сознательной или случайной утечки конфиденциальной информации
- **администрируется** сотрудниками службы информационной безопасности

Консалтинг

Юридическая значимость DLP и разработка процесса защиты от утечек

Консалтинг: разработка процесса защиты от информационных утечек

Блок 1. Обследование, анализ, разработка процессов категорирования и обращения с информацией

Блок 2. Проведение оценки и ранжирования рисков утечки информации ограниченного доступа

Блок 3. Разработка концепции настройки политик системы мониторинга и контроля

Блок 4. Разработка/актуализация нормативных документов в области информационной безопасности

Блок 5. Разработка, построение модели и регламентирование процесса реагирования и расследования инцидентов, выявляемых системой мониторинга и контроля

Блок 6. Разработка показателей эффективности, создание концепции развития процесса защиты от утечек информации ограниченного доступа и других внутренних угроз

Что вы получаете

- **Перечень** информации **ограниченного доступа**
- **Реестр информационных активов**
- **Описание процесса категоризации и жизненного цикла** информации ограниченного доступа
- **Отчет по оценке рисков утечки** информации ограниченного доступа
- **Карта информационных потоков**
- **Концепция настройки политик** системы мониторинга и контроля
- **Разработка и актуализация правовых и нормативных документов**
- **Регламент реагирования** на события/инциденты
- **Отчет по оценке уровня зрелости процесса** защиты от утечек и других внутренних угроз

Блок 4. Разработка/актуализация нормативных документов в области ИБ

1. обязательство о неразглашении информации ограниченного доступа
2. политика допустимого использования ресурсов
3. положение о защите информации ограниченного доступа
4. положение о порядке обращения с информацией ограниченного доступа
5. регламент мониторинга и контроля
6. согласие на осуществление автоматизированного мониторинга и контроля
7. форма приказа о введении режима защиты информации
8. трудовой договор (внесение изменений)
9. трудовой распорядок (внесение изменений)

Прогнозирование рисков кадровой безопасности

INFOWATCH®

INFOWATCH PREDICTION

Оповещение

— Службы безопасности
— Непосредственного руководителя
— HR-службы

INFOWATCH TRAFFIC MONITOR

— Применение политик «на увольнение»
— Повышенное внимание к действиям сотрудника
— Контроль коммуникаций и списка контактов

Почему InfoWatch

Примеры успешных проектов, о которых заказчики готовы рассказывать

Продукты включены в реестр отечественного ПО

Продукты сертифицированы ФСТЭК

Компания входит в пятерку **крупнейших ИБ-производителей в России**

Собственные запатентованные **технологии**, доказавшие свою эффективность на практике

InfoWatch является одним из лидеров рынка защиты данных **более 14 лет**

Бесплатный пилотный проект и бесплатное обучение для заказчиков


СПАСИБО ЗА ВНИМАНИЕ!
#КОТИБ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4 октября 2018 г.
г. Красноярск

#CODEIB

КОТ ИБ corporation

КОТ ИБ

Светлана Марьясова,
Региональный представитель
АО «ИнфоВотч»

ТЕЛЕФОН: +7 (950) 415-32-00

EMAIL: Svetlana.Maryasova@infowatch.com