INFOWATCH®

МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

AHK Deutsch-Russische Auslandshandelskammer
Российско-Германская внешнеторговая палата

СОВРЕМЕННЫЕ УГРОЗЫ, ИСХОДЯЩИЕ ОТ ИНФОРМАЦИОННЫХ СИСТЕМ

УВАЖАЕМЫЕ КОЛЛЕГИ!

В связи с массовой информатизацией современного общества все большую актуальность приобретает знание способов качественной защиты информационных технологий в повседневной практической деятельности. Наглядными примерами, иллюстрирующими необходимость защиты информации и обеспечения информационной безопасности, являются участившиеся сообщения о компьютерных «взломах» предприятий, росте компьютерного пиратства, распространении компьютерных вирусов.

Число компьютерных преступлений растет, увеличиваются масштабы компьютерных злоупотреблений. Умышленные атаки составляют заметную часть преступлений, но случайных действий пользователей, которые могут быть расценены как злоупотребления или ошибки – еще больше. И основной причиной потерь, как показывает практика, является недостаток информации о современных угрозах утечки конфиденциальных данных. Данная брошюра поможет вам избежать проблем, связанных с утерей критически важной информации предприятия.

Приятного чтения!

Наталья Касперская
Президент ГК InfoWatch, соучредитель
«Лаборатории Касперского»

УВАЖАЕМЫЕ ЧЛЕНЫ РОССИЙСКО-ГЕРМАНСКОЙ ВНЕШНЕТОРГОВОЙ ПАЛАТЫ!

Количество кибератак и утечек конфиденциальной информации растет ежегодно – как в России, так и в Германии.

Так, согласно исследованию аналитического центра компании InfoWatch, многолетнего члена нашей палаты, Россия стала второй страной после США по числу утечек конфиденциальных данных, и число утечек за прошедший год выросло на 80%. При этом по вине внешних злоумышленников в глобальном масштабе случилось 55% утечек, а в каждой третьей утечке были виноваты собственные сотрудники пострадавших организаций.

Кроме того, по данным Google, количество взломанных сайтов по всему миру выросло в 2016 году на 32% по сравнению с 2015 годом. А по данным IBM, количество атак на автоматизированные системы управления технологическими процессами (АСУТП) увеличилось в 2016 году даже на 110%.

Данная брошюра была создана экспертами InfoWatch специально для членов нашей палаты. Она покажет, как вы можете избежать наиболее распространенные риски и защититься как от внутренних, так и от внешних угроз для вашей информационной безопасности.

С наилучшими пожеланиями,

Маттиас Шепп
Председатель правления Российско-Германской
внешнеторговой палаты

Внутренние угрозы предприятия, включая утечки информации

Внешние целевые атаки, включая DDoS-атаки

Атаки на АСУТП

Информационные атаки и войны

ПОЧЕМУ ЭТО ПРОИСХОДИТ?

- Зависимость от ИТ во всех сферах, «цифровой мир»
- Широкое использование Интернета (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

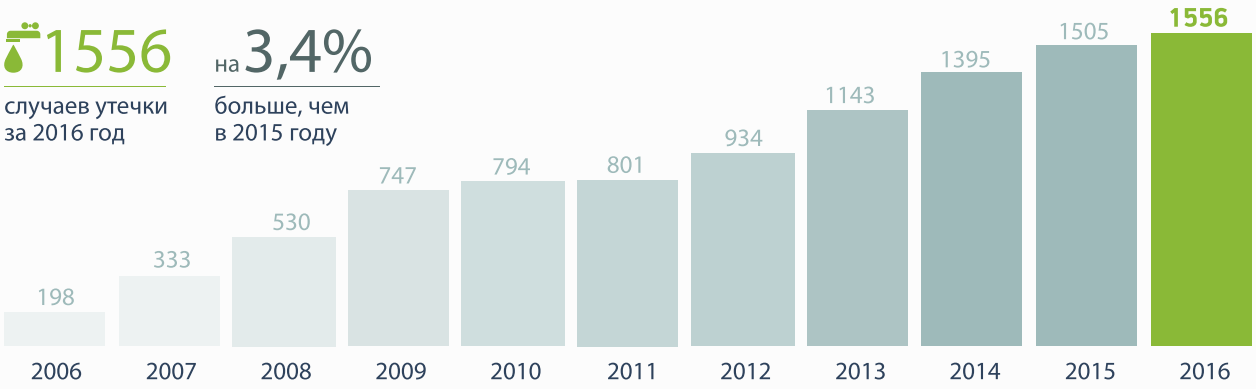
ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ ИТ-УГРОЗ

- Финансовые потери
- Потеря конкурентного преимущества
- Потеря доли рынка
- Штрафные санкции регуляторов
- Угроза стабильности работы инфраструктур
- Потеря клиентов и партнеров
- Ущерб репутации предприятий и их главных лиц

ВНУТРЕННИЕ УГРОЗЫ И УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Внутренние угрозы – это угрозы, которые исходят от сотрудников компании и наносят ей ущерб в результате кражи корпоративной информации или ее утечки по неосторожности, а также коррупции, мошенничества, сговоров, воровства и саботажа.

Ежегодно во всем мире растет количество утечек информации:



По данным аналитического центра InfoWatch, 2017

ПРИМЕР УТЕЧКИ ИНФОРМАЦИИ

«Синдром Клинтон», сентябрь 2016

Хиллари Клинтон было не всегда удобно вести переписку, используя рабочую почту, поэтому она пересылала письма, содержащие конфиденциальную информацию, по внешней почте.

Кроме того, опасаясь хранить важную переписку у себя, она организовала хранение рабочих писем Госдепартамента США на личном сервере.

В итоге эти действия привели к утечке информации, составляющей гостайну.

Скандал, подрыв репутации, выборы проиграны

КАК ЗАЩИЩАТЬСЯ ОТ ВНУТРЕННИХ УГРОЗ И УТЕЧЕК ИНФОРМАЦИИ?

1. Для персонала – соблюдение правил обращения с информацией:

- Не использовать публичные почты для пересылки конфиденциальной информации

- Не оставлять ноутбуки, смартфоны без присмотра

- Не разглашать информацию в соцсетях

- Помнить о шпионских функциях смартфонов

2. Для организации:

- Выявление наиболее вероятных угроз со стороны сотрудников
- Положение о коммерческой тайне и защите персональных данных
- Выбор и назначение ответственных за безопасность
- Разработка процедур по защите информации

Использование технических средств защиты от утечек (DLP)* – например, InfoWatch Traffic Monitor или решения других производителей

* Data Loss Prevention (DLP) – программный комплекс, осуществляющий анализ потоков данных, пересекающих периметр защищаемой локальной сети. При обнаружении в этом потоке данных конфиденциальной информации срабатывает активная компонента системы, которая оповещает ответственного специалиста и, при необходимости, блокирует передачу данных

СЛАБОЕ ЗВЕНО. УТЕЧКИ ЧЕРЕЗ МОБИЛЬНЫЕ УСТРОЙСТВА

Современные смартфоны передают на сторону информацию о пользователе:

- определение местонахождения
- содержание переписки (смс, почта)
- фото- и видеофайлы
- контакты
- связь с браузерами и поисковиками на десктопах
- анализ предпочтений пользователей (политические взгляды, потребительские привычки, личная жизнь)
- все возможности слежки от поисковиков, соцсетей, браузеров, операционной системы

Смартфоны имеют дополнительную встроенную батарею, поэтому даже в выключенном состоянии могут передавать информацию

ВНЕШНИЕ УГРОЗЫ И ЦЕЛЕВЫЕ АТАКИ

Целевые атаки – это заранее спланированные действия по атаке на ИТ-системы конкретной организации. У каждой атаки есть заказчик, исполнитель, объект-жертва и цель.

ОТЛИЧИЕ ЦЕЛЕВЫХ АТАК ОТ ВИРУСОВ:

- Использование нескольких векторов нападения одновременно
- Использование методов социальной инженерии[1]
- Заранее произведена «разведка» – получена информация об инфраструктуре предприятия, используемых методах и средствах защиты
- Как правило, происходит отключение используемой защиты
- Часто целевая атака начинается с DDoS-атаки[2]
- Вредоносный код, как правило, внедряется по частям

1. Социальная инженерия – это метод несанкционированного доступа к информации, основанный на использовании слабостей человеческого фактора и без использования технических средств. Злоумышленник получает информацию, например, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего.
2. DDoS-атака (Distributed Denial of Service) – это атака на веб-ресурс, основной целью которой является выведение его из строя путем подачи большого количества ложных запросов, которые сервер не успевает обрабатывать, и сайт становится недоступным для пользователя.

ПРИМЕР ЦЕЛЕВОЙ АТАКИ

Атака на ЦБ Бангладеш, февраль 2016

Используя социальную инженерию и рассылку писем с вирусом, хакеры проникли в систему ЦБ Бангладеш.

Злоумышленники получили доступ к межбанковской электронной системе передачи информации и совершения платежей SWIFT и попытались направить 35 мошеннических платежных поручений на общую сумму 951 млн долларов.

Хакерам удалось успешно осуществить четыре транзакции и перевести украденные деньги на Филиппины и Шри-Ланку.

Убытки составили $81 млн

ПРИМЕР АТАКИ

Серия DDoS-атак на банки, ноябрь 2016

10 ноября ЦБ РФ заявил, что 5 российских банков подверглись хакерской атаке. Под ударом оказались Сбербанк, Альфа-банк, «Открытие», «ВТБ Банк Москвы» и Росбанк.

По оценке специалистов мощность атак варьировалась от «слабой» до «мощной». Длительность атак составляла от 1 до 12 часов. Некоторые банки подверглись серии от 2 до 4 атак.

Хакеры, организовавшие атаку, использовали ботнет (сеть зараженных устройств), в которую входило 24 000 машин из «Интернета вещей».

Издание Vice сообщило, что за атакой могут стоять «люди, недовольные возможным вмешательством России в выборы президента США». Российские специалисты считают, что атака – это лишь «демонстрация возможностей», а ее причины – сугубо экономические.

! **3 из 5 банков подтвердили атаку**

КАК ЗАЩИЩАТЬСЯ ОТ ЦЕЛЕВЫХ АТАК?

В основном защита осуществляется техническими средствами:

- Антивирусы (Kaspersky, Symantec, G DATA и др.)
- Защитные сетевые экраны (Entensys, Kerio и др.)
- Специализированные средства защиты от DDoS (Attack Killer, Qrator и др.)
- Технологии защиты от уязвимостей (Appercut, Checkmarx, Fortify и др.)
- Специализированные средства по защите от целевых атак (Attack Killer, FireEye и др.)

Правильнее всего выстраивать эшелонированную защиту, используя технологии от различных производителей. Это резко усложняет задачу атакующего. Нет неуязвимых систем. Главное – сделать атаку на вашу систему слишком дорогой и сложной для атакующих.

АТАКИ НА «ИНТЕРНЕТ ВЕЩЕЙ» И АТАКИ С ИСПОЛЬЗОВАНИЕМ «ИНТЕРНЕТА ВЕЩЕЙ»

«Интернет вещей» (Internet of Things, IoT) – компьютерная сеть физических предметов («вещей»), имеющих доступ к сети Интернет. В такую сеть могут быть объединены различные приборы и устройства, например: автомобиль, камера видеонаблюдения, телевизор, сигнализация и т.д.

ОСНОВНЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ IOT:

- Отсутствие каких-либо стандартов безопасности
- Производители не понимают или не заинтересованы в решении проблем с информационной безопасностью, основная цель – быстрый вывод устройства на рынок

Реализовав взлом IoT, хакеры создают ботнет*, использующий компоненты «Интернета вещей» и получают возможность организовывать DDoS-атаки на любую инфораструктуру.

* Ботнет представляет собой сеть устройств, зараженных вредоносным кодом и управляемых злоумышленником централизованно

БОТНЕТ MIRAI

В конце 2016 года произошла мощная DDoS-атака против Dyn DNS, оператора DNS в США. Атака была реализована при помощи ботнета Mirai, первого вируса для «Интернета вещей». Сотни тысяч камер, серверов DVR и других подключенных устройств вплоть до кофеварок с Wi-Fi стали оружием в руках хакеров.

В результате одни из самых посещаемых веб-сайтов в мире часами были недоступны для пользователей, а именно: Twitter, Spotify, Reddit, GitHub, сайты CNN, The New York Times и др.

В 2017 году эксперты компании Imperva сообщили о новом варианте вредоносного ПО Mirai, использовавшемся для осуществления 54-часовой DDoS-атаки. Жертвой атаки стал один из колледжей США, являющийся клиентом Imperva. Атака осуществлялась с помощью ботнета преимущественно из зараженных Mirai камер видеонаблюдения, видеорегистраторов и т.д.

АТАКИ НА АСУТП

Атаки на АСУТП (автоматизированные системы управления технологическими процессами) – хорошо спланированные действия при участии внешних злоумышленников и/или сотрудников компании, цель которых – прерывание или изменение параметров технологических процессов, которое может повлечь за собой серьезные финансовые потери, а также привести к взрывам, пожарам, разливам агрессивных жидкостей и т. п. вплоть до экологических катастроф.

ПРИМЕР АТАКИ НА АСУТП

Сталелитейный завод, 2014*

Хакеры проникли в компьютер, управляющий доменной печью, и установили вредоносную программу, которая заставила печь перегреться и расплавиться.

Системе был нанесен существенный ущерб. Сумма ущерба не разглашается

*по данным источников Bloomberg

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУТП:

1. Индустрия развивается так быстро, что средства обеспечения информационной безопасности не опережают появление новых угроз
2. Большинство датчиков нового поколения не защищены и доступны для взлома
3. Технологи, производители и специалисты по информационной безопасности имеют разные взгляды на бизнес-процессы и на обеспечение безопасности АСУТП
4. Многие производители АСУТП не оперативно реагируют на выявляемые уязвимости
5. Нет готовых («под ключ») средств защиты, все существующие требуют тестирования и доработки под конкретную АСУТП

ТЕМ НЕ МЕНЕЕ, КАК ЗАЩИЩАТЬСЯ ОТ АТАК НА АСУТП?

- Необходимо проведение аудита систем на соответствие требованиям информационной безопасности независимыми компаниями
- Затем – формирование требований к системе защиты АСУТП, проектирование комплексной системы. Оптимально, если система защиты будет проектироваться одновременно с АСУТП (при создании новой, при модернизации)
- Использование в составе системы защиты АСУТП специализированных программно-аппаратных комплексов, например, InfoWatch Automation System Advanced Protector (ASAP) или решений других производителей

ИНФОРМАЦИОННЫЕ АТАКИ И ВОЙНЫ

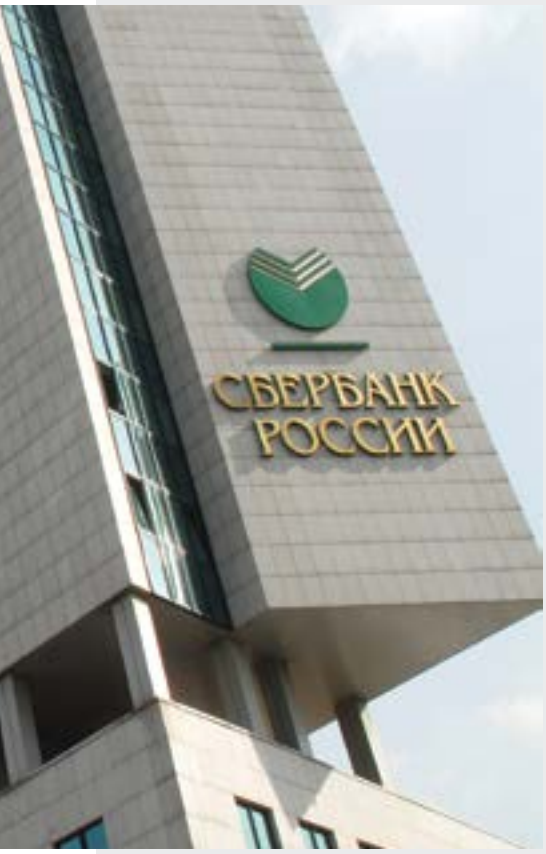
Информационные атаки – это кампании очернения и подрыва репутации предприятия с помощью современных электронных СМИ и соцсетей. Часто такие кампании служат средством конкурентной борьбы.

ВИДЫ ИНФОРМАЦИОННЫХ АТАК:

Атаки на руководство
- «Раскрутка» неудачных высказываний руководителей или учредителей организаций
- Вбросы и раскрутка информации о происшествиях, неудачных решениях, поступках или благосостоянии
- Клевета в отношении руководителей или учредителей организаций

Атаки на предприятие
- Вбросы и раскрутка информации о сбоях и ошибках на предприятии

Длительные кампании очернения
- Серии вбросов
- Подбор негативных тем, вызывающих живой отклик и вирусный рост
- Подогревание темы в течение многих месяцев



ПРИМЕР ИНФОРМАЦИОННОЙ АТАКИ

Атака на Сбербанк, 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 в банкомате, это не технический сбой – денег нет»

Граждане бросились забирать деньги. ЦБ и Правительство предприняли беспрецедентные меры по урегулированию ситуации.

Общий отток денежных средств с депозитов и из банкоматов составил примерно 1,5 трлн руб., которые были довольно быстро восстановлены

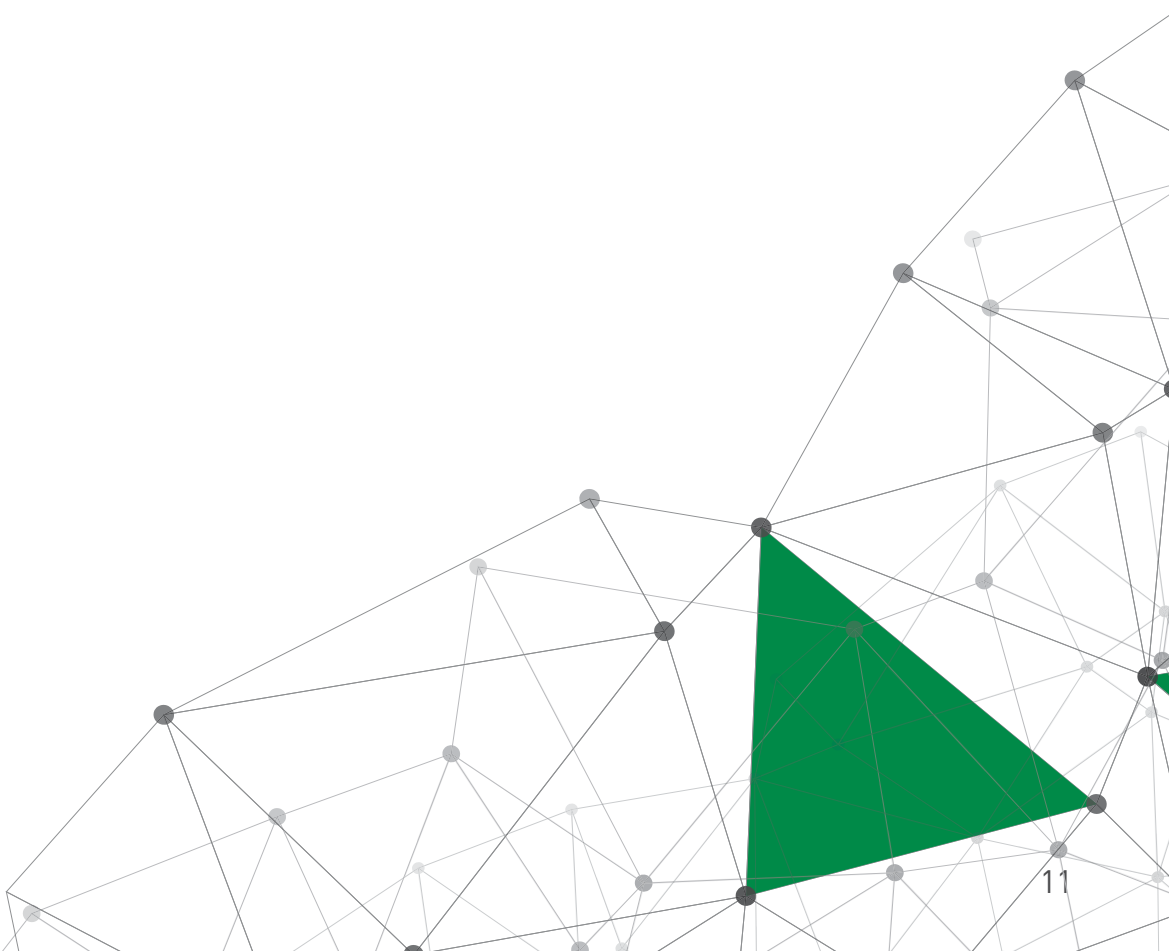
КАК ЗАЩИЩАТЬСЯ ОТ ИНФОРМАЦИОННЫХ АТАК?

1. Использование средств мониторинга социальных сетей, например – InfoWatch Kribrum или решения других производителей

2. Генерация позитивного контента:
   - Сделали, добились
   - Помогли, спасли
   - Любые позитивные примеры

3. Размещение и раскрутка позитивного контента в сетях:
   - Публикации в СМИ
   - Соцсети
   - Интернет-сайты

4. В случае начавшейся атаки публиковать информацию об атаке, разъясняя ее суть



МЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ:

Использование паролей

1. Не используйте один пароль для всех сервисов, которыми вы пользуетесь. Рекомендуется использовать разные пароли для разных сервисов
2. Используйте пароли длиной не менее 8 символов с содержанием строчных и прописных букв, а также цифр и спецсимволов (@, &, % и т.д.). Альтернативной хорошей практикой является использование парольных фраз, состоящих из не менее чем 20 символов, например, «ForestWinterSnowstorm» – их легко запомнить и трудно подобрать
3. Не сохраняйте пароли в веб-браузерах и клиентах электронной почты
4. Не передавайте пароли знакомым и не отправляйте по электронной почте
5. Тщательно храните пароли. Нельзя оставлять записанный пароль на видном месте, клеить его на монитор и т.д.

Защита рабочих станций и собственных устройств

1. Все файлы, скачанные из сети Интернет, перед открытием проверяйте антивирусной программой
2. При получении по электронной почте писем от неизвестных вам лиц, содержащих ссылки и картинки, рекомендуется сразу удалять, не переходя по ссылкам и не открывая приложенные документы
3. Пользуйтесь лицензионным антивирусным ПО, настройте автоматическую проверку загруженных из сети файлов и подключенных носителей информации
4. При возникновении признаков появления вирусов на компьютере проведите полную проверку антивирусным ПО
5. Всегда устанавливайте последние обновления операционных систем
6. Для защиты от вирусов шифровальщиков регулярно создавайте резервные копии ценных для вас данных

Безопасность при осуществлении платежей

1. По возможности, следует использовать дополнительное подтверждение операций, например, с помощью SMS или иным способом (например, по телефону)
2. Не переходите по ссылкам, полученным от недоверенных лиц. При получении писем или сообщений от банков удостоверьтесь, что это именно банк пишет вам
3. Будьте внимательны при осуществлении платежей в сети Интернет. Проверяйте наличие https в адресной строке браузера и точность адреса

Использование сети Интернет и социальных сетей

1. Не пользуйтесь незащищенными Wi-Fi-сетями
2. С осторожностью относитесь к нестандартным сообщениям в сети Интернет (особенно в социальных сетях). Помните, что любые нестандартные просьбы могут быть мошенничеством
3. Не используйте бесплатную почту и чаты для передачи критически важной информации

Защита важной информации

1. Используйте шифрование при передаче критически важной информации
2. С осторожностью относитесь к хранению информации в облаке. Следует шифровать данные для хранения их в облаке либо сделать выбор в пользу хранения информации локально
3. Не берите смартфон на важные переговоры
4. Не используйте мобильное устройство для конфиденциальной переписки

«Интернет вещей»

1. В случае необходимости использования устройств «Интернета вещей» (системы умного дома, управляемые через Интернет электроприборы, замки и т.д.) учитывайте, что на данный момент эти технологии еще не имеют серьезной защиты. И не забудьте поменять стандартный пароль к панели управления ими
2. С осторожностью относитесь к Smart TV, помните, что это устройство двусторонней коммуникации

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

www.infowatch.ru

+7 (495) 22-900-22
+7 (499) 37-251-74
sales@infowatch.ru