Цифровой мир: надёжные смарт-устройства» – девиз Всемирного дня прав потребителей

Всемирный день прав потребителей проводится ежегодно 15 марта, начиная с 1983 года, а с 1994 года широко отмечается и в Российской Федерации.

По сложившейся традиции Международная Федерация потребительских организаций (CI) каждый год определяет тематику Всемирного дня прав потребителей.

Так, 15 марта 2019 года Всемирный день прав потребителей пройдет под девизом **«Trusted Smart Products» - «Цифровой мир: надежные смарт-устройства»**.

К смарт-устройствам традиционно относится так называемая «умная электроника»: смартфоны, носимые фитнес-трекеры, голосовые помощники, «умные» телевизоры, часы, розетки и т.п. Такие смарт-продукты отличаются тем, что имеют функции подключения к Интернету и они непосредственно получают, собирают и отправляют самые различные данные о потребителях и потребительском поведении. В мире в настоящее время насчитывается 23,1 миллиарда смарт-устройств, что превышает число людей в три раза.

По мере того, как все больше людей подключаются к Интернету во всех уголках планеты, смарт-устройства вскоре станут повседневной реальностью для потребителей во всем мире, что ознаменует коренное изменение процесса взаимодействия людей с умной электроникой, носимыми гаджетами и продвинутыми услугами.

Появление «умных» технологий приносит много возможностей для потребителей, однако существуют некоторые серьезные причины для беспокойства: отсутствие безопасности или обнаружение всевозможных сетевых уязвимостей или утечек информации, нарушение конфиденциальности личных данных и не раскрытие информации о рисках, а также отсутствие ясности в отношении того, кто несет ответственность при возникновении возможных убытков.

По мере того, как все больше граждан подключаются к Интернету во всех уголках планеты, смарт-устройства становятся повседневной реальностью для потребителей, что знаменует коренное изменение процесса взаимодействия людей с "умной" электроникой, гаджетами и продвинутыми услугами.

Появление "умных" технологий приносит много возможностей для потребителей, однако существуют некоторые серьезные причины для беспокойства: сетевая уязвимость или утечка информации. Бывает, нарушается конфиденциальность личных данных, люди не знают о возможных рисках и о том, кто несет ответственность при возникновении убытков.

На сегодняшний день в продаже представлено уже достаточно много таких устройств. Ну разве не удобно, находясь в дороге, включить со своего смартфона через мобильный интернет подогрев пола в квартире, заварить себе кофе через соединение с подключенной к сети кофе-машиной как раз к приходу домой или настроить холодильник для заказов в онлайн-магазине доставку молока по определенным дням?

Однако, наряду с очевидными преимуществами, эти функции делают нас более уязвимыми и способны стать причиной проблем, связанных со слежкой и утерей конфиденциальной информации, а также денежных средств.

Как и любой аппарат, наделенный определенным программным функционалом, любое подключенное устройство может быть взломано с помощью вредоносных программ.

Основная угроза в результате такого взлома – это потеря контроля над функционалом устройства. Взломанный прибор, при условии доступа к интернету, может управляться извне. Таким образом, третье лицо может осуществлять действия с устройством, которые не зависят от желание его непосредственного пользователя.

Кроме того, взломанные IoT-устройства могут использоваться для слежки за своим хозяином, отмечая, например, его распорядок дня, вкусовые пристрастия. Также они становятся элементами слежения при условии наличия звукоулавливающих устройств и видеокамер.

Самым опасным вариантом такой несанкционированной деятельности может быть использование программ, которые будут отслеживать и воровать конфиденциальную информацию в домашней сети или сети Wi-Fi. Например, заражение ПК или смартфона банковским троянцем через подключение к зараженному устройству может стать причиной потери денег на карточном счете.

Рассмотрим основные методы защиты современных мобильных устройств.

В данной статье будет рассмотрена актуальная на сегодняшний день тема использования смартфонов, а также защита конфиденциальных данных, хранящихся на них.

На современном этапе развития персональной техники нетрудно заметить, что начинают набирать популярность портативные ПК и КПК. За последние 5–7 лет роль смартфонов в жизни каждого человека, вне зависимости от его статуса и материального положения, приобретает массовый характер.

Уже сегодня многие служащие используют смартфоны, коммуникаторы и PDA для ведения деловых переговоров и хранения важных данных, не нуждаясь при этом в ПК. В дополнение к стандартным телефонным функциям персонал может применять подобные устройства для следующих целей:

- пересылки e-mail;
- пересылки мгновенных сообщений (SMS, MMS, IM-сообщений с помощью ICQ или Windows Messenger);
- применения приложений, в частности ERP-систем, CRM-систем, систем автоматизации продаж;
- просмотра и анализа штрих-кодов;
- сетевых игр;
- разного рода чатов;
- web-серфинга;
- загрузки и совместного использования файлов в Интернете;
- хранения персональной и конфиденциальной информации.

Все это приводит к тому, что данные устройства будут представлять все большую опасность для компаний.

Вместе с тем стоит учитывать, что все больше организаций будет использовать PDA, смартфоны и коммуникаторы для доступа к своим деловым приложениям и данным, что постепенно превратит их в устройства, критические для бизнеса.

Корпорации недооценивают мобильные угрозы

В связи с дальнейшим развитием технологий мобильной связи в будущем возможен бурный всплеск мобильной преступности. Стимулом для этого служит унификация абонентских телефонов.

Наибольшей угрозой для пользователей смартфонов являются действия спамеров, фишеров и вирусописателей. Все действия этих злоумышленников будут направлены прежде всего на хищение конфиденциальной информации, личных данных или на создание проблем в работе устройств. Не стоит недооценивать и еще одну угрозу, о последствиях которой мы все чаще слышим в новостях. Это перехват голосового трафика, то есть незаконное прослушивание телефонов.

Люди доверяют большое количество личной информации средствам связи, в частности смартфонам и планшетам. Потому остро стоит вопрос о защите личных конфиденциальных данных. Существует огромное количество способов защиты этих данных, начиная от ограничения доступа посторонних лиц к защищаемому объекту до обращения к биометрическим системам аутентификации.

Рассмотрим подробнее эти способы защиты, к которым можно отнести: – ограничение доступа к устройству; – использование «шторки»; – PIN-код; – графический ключ; – распознавание лица; – пароль; (adsbygoogle = window.adsbygoogle || []), push({}); – биометрические системы аутентификации.

Самым очевидным способом защиты является минимизация возможности попадания устройства в чужие руки. То есть, нахождение смартфона только в руках владельца не даёт возможности потенциальному злоумышленнику или обычному любопытному пользователю получить какую-либо информацию, хранящуюся на данном устройстве, а также использовать её в личных целях. Следует взять во внимание факт того, что данный метод является одновременно

самым действенным, но в то же время самым ненадёжным. Необходимо пояснить как именно один и тот же способ может, как сохранить ваши данные, так и сыграть против вас. С одной стороны, как было описано выше, вероятность потенциального ущерба, как морального, так и материального, а также возможного хищения информации сводится к минимуму, если физический контакт посторонних лиц с объектом будет ограничен. Рядовому пользователю практически невозможно заполучить личную информацию с вашего устройства без непосредственного взаимодействия с ним, но это не исключает возможности хищения с помощью использования современных беспроводных технологий, таких как Internet, Bluetooth или IrDA. Однако существенным изъяном этого способа защиты является человеческий фактор, такой как банальная невнимательность владельца устройства. Потенциальному злоумышленнику достаточно отвлечь вас чем-либо или дождаться удобного случая и воспользоваться предоставленной возможностью для хищения информации или даже самого устройства. Таким образом, хищение информации с устройства лишь вопрос времени, зависящий от человеческого фактора. И поэтому на современном этапе развития технологий не стоит доверять защиту конфиденциальных данных только лишь этому способу, его стоит комбинировать с одним из других методов, которые будут описаны далее.

Далее будет описан наиболее распространённый способ блокировки смартфона, а именно использование **так называемой «шторки».** Также стоит отметить, что в зависимости от компании-производителя вид «шторки» может быть различным. Например, в последних версиях мобильных операционных систем под этим понятием подразумевается способ разблокировки дисплея «свайпом». Для большей информативности проведём сравнительный анализ этого метода относительно всех других. К его достоинствам, во-первых, можно отнести более быструю разблокировку по сравнению со способами, описанными далее, такими как использование PIN-кода или графического ключа.

Во-вторых, «шторка» представляет собой некую преграду для малолетних детей. То есть, для разблокировки дисплея так или иначе требуется произвести конкретное действие, понять которое маленький ребенок вряд ли сможет. Ну и наконец, основная причина, по которой этот метод является наиболее распространенным, заключается в защите от непреднамеренных действий, которые могут возникнуть в то время, пока телефон находится в кармане или сумке. Основным недостатком использования «шторки» является недостаточный уровень защиты персональных данных от посторонних лиц. Обычный «свайп» не представляет труда для разблокировки рядовому пользователю.

Вторым по популярности в мире способом блокировки смартфона является **использование PIN-кода**. Принцип работы данного метода заключается введении заданной последовательности чисел. Этот способ крайне схож с введением пароля для авторизации на каком-либо сайте. Длина PIN-кода может варьироваться от 4 символов и более, в зависимости от необходимого уровня сложности пароля. Необходимую последовательность цифр вводит сам пользователь смартфона при выборе данного способа защиты. При разблокировке устройства у владельца есть не более трёх попыток для правильного ввода пароля, в противном случае смартфон заблокируется на некоторый промежуток времени, по истечении которого будет предоставлена ещё одна возможность для разблокировки. Стоит отметить, что отрезок времени, на который блокируется смартфон или планшет, увеличивается с каждой неудачной попыткой. (adsbygoogle = window.adsbygoogle || []).push({}); Отметим некоторые достоинства этого метода. Очевидно, что этот способ предоставляет собой более высокий уровень защиты относительно тех, что были описаны ранее. Для обхода такой защиты злоумышленнику необходимо обладать необходимыми навыками работы с цифровыми устройствами, но даже при наличии таковых требуются значительные временные затраты, наличие внешних устройств и специализированного программного обеспечения. Во-вторых, в отличие от похожего метода — графического ключа, при использовании PIN присутствует возможность повторного использования символа, что также повышает уровень защиты. К недостаткам этого метода блокировки можно отнести человеческий фактор. Стоит пояснить, что зачастую люди в качества пароля используют простые, легко запоминающиеся комбинации. Например, дату рождения свою, детей или какое-либо памятное событие. В связи с чем, использование PIN-кода, основанного на подобных комбинациях, существенно уменьшает уровень защиты устройства. Данный PIN может быть легко выявлен в том случае, если человек хорошо знаком с владельцем, а злоумышленнику достаточно немного узнать о владельце. Однако на современном этапе развития редко кто использует такого рода PIN. Зачастую используется та комбинация цифр, которая известна только лишь одному человеку. Из-за широкой популяризации смартфонов увеличивается количество людей, пользующихся ими в общественных местах, в связи,

с чем повышается вероятность того, что данный PIN будет подсмотрен и в случае кражи устройства, ваши персональные данные будут скомпрометированы. При использовании данного способа защиты возможна банальная ситуация, когда пользователь может забыть PIN от устройства. Это может сыграть против владельца, если он окажется в экстренной ситуации, например, если он будет срочно нуждаться в средстве связи. Как было отмечено ранее, после трёх неудачных попыток ввода, следующая будет доступна только по истечении определенного промежутка времени, который с каждым разом будет увеличиваться.

Ещё одним способом, который весьма распространен среди пользователей цифровых мобильных устройств, **является графический ключ**. Стоит отметить, что среди всех методов, описанных раннее, именно этот используется чаще всего владельцами Android-смартфонов. Сам графический ключ по своему принципу схож с PIN-кодом и является его более быстрым аналогом, но представляет собой одну непрерывную линию, форма которой ограничена фантазией владельца аппарата и количеством вершин, предоставленных для ввода ключа. Он также имеет ряд преимуществ по сравнению с остальными видами защиты экрана от разблокировки. К его достоинствам в первую очередь можно отнести скорость. Если сравнить его с PIN, то можно заметить, что он является более быстрым. Обосновано это тем, что в случае ввода числового пароля требуется нажимать на конкретные места экрана. Другими словами, нужно «отрывать» палец от экрана для ввода следующего символа. При использовании графического ключа необходимости в «отрыве» пальца от экрана нет, то есть требуется провести непрерывную линию в заданном направлении. Даже если сами точки представить в виде чисел, а PIN в виде точек, то можно убедиться, что в случае ввода одной и той же комбинации метод с использованием «графического ключа» окажется быстрее. Вторым достоинством метода является дополнительный софт, который может быть установлен с целью увеличения количества точек, предоставленных для ввода ключа. Если у того же PIN используются числа от 0 до 9, то количество точек может быть увеличено до 36. Ясно, что такое количество не используется, однако возможность расширения ключа также можно отнести к достоинствам. Что касается недостатков, то можно отметить, что «графический ключ», так же как и PIN, не лишен возможности блокировки устройства на определенный промежуток времени в случае ввода неправильной комбинации. Число попыток, предоставленных для ввода без угрозы блокировки также равно трем. Далее время, через которое будет доступен последующий ввод, будет расти. Одним из самых значимых недостатков метода является ограниченность последовательности вводимых символов. То есть, например, отсутствует возможность ввода символов, расположенных в противоположных частях диагоналей. Не получится соединить две крайние точки, минуя среднюю. Кроме того, повторное использование точки невозможно. Каждая точка может использоваться только 1 раз. Во всем этом и заключается ограниченность количества допустимых для ввода комбинаций.

Еще один способ блокировки — **это распознавание лица**. Среди всех ранее описанных методов этот является самым нераспространенным. Заключается он в том, что при попытке разблокировки, устройство распознает лицо человека при помощи камеры. (adsbygoogle = window.adsbygoogle || []).push({}); Найти достоинства довольно трудно. Одно из них будет описано далее, но стоит лишь отметить, что без вашего лица доступ к устройству никто не получит. Гораздо больше у него недостатков. Во-первых, как уже было сказано, достаточно вашего лица. То есть камере достаточно будет распознать вас на фотографии. Лицу, которому требуется получить доступ к данным на смартфоне достаточно наличие вашей фотографии, распечатанной или нет. На некоторых устройствах, которые были произведены позднее появления функции распознавания лица, требуется моргнуть. Но это лишь исключает возможность использования вашей фотографии. Во-вторых, большую роль играет аппаратная составляющая устройства. Например, чем лучше камера используется, тем более точным и быстрым окажется распознавание лица, даже в случае его движения. Чем соответственно она хуже, тем более медленно и менее точно работает этот метод. В-третьих, на точность и скорость метода сильно влияет уровень освещённости места, где производится распознавание. Если света недостаточно, то возможен вариант, что даже ваше лицо не будет распознано. Гораздо более простым является использование других методов. В связи со своим неудобством использования, функция распознавания лица была доступна на ограниченном количестве устройств.

Однако, несмотря на все свои недостатки, этот метод привел к развитию несколько иных способов защиты, которые активно используются сейчас. Речь идет **о биометрических технологиях**, к которым **можно отнести сканеры отпечатков пальцев, сканеры сетчатки глаза и сканеры радужки глаза и другие.**

Для минимизации риска заражения своих устройств следует соблюдать несколько несложных правил:

- отключать Bluetooth- и инфракрасный порты в местах массового скопления людей;
- принимать и открывать файлы, присланные только из достоверных источников;
- не отвечать на подозрительные сообщения;
- установить специальные антивирусные программы, которые сегодня существуют практически для всех основных типов мобильных платформ.

Сегодня мобильные устройства не только обеспечивают рост производительности, но и приносят новые угрозы безопасности, нарушение которой может очень дорого стоить предприятию.

Увеличивающееся число мобильных пользователей и взрывной рост Интернета уничтожили понятие периметра организации. Защита сети компании с помощью межсетевого экрана больше не отвечает современным требованиям. Пользователи часто путешествуют вне периметра, где подвергают рискам конфиденциальные и персональные данные и могут подвергнуться нападению. Мобильные устройства могут быть легко атакованы с помощью вредоносного ПО или применяться для его переноса. Другая опасность заключается в мобильности этих устройств — их легко потерять или они могут быть украдены, что поставит под угрозу данные, которые на них хранятся.

Основные риски, связанные с мобильными устройствами:

- потеря конфиденциальных данных из-за хищения или утери мобильных устройств;
- потеря производительности и конфиденциальных данных из-за заражения вредоносным ПО;
- мошенничество; потеря производительности из-за взлома.

Сегодня аппаратные средства стоят во много раз меньше, чем информация, содержащаяся на устройстве. Утраченные данные могут привести к потере репутации, потере конкурентоспособности и потенциальным судебным тяжбам.

Все эти законы предусматривают серьезные штрафы за утрату персональной или корпоративной информации.

Как только ваше устройство похищено (утеряно), ваши данные могут быть утрачены вместе с ним. Для запрета несанкционированного доступа к данным можно использовать две технологии:

- удаленное стирание данных;
- шифрование данных.

Данные могут быть стерты удаленно по специальной команде стирания или автоматически из-за нарушения политики безопасности (превышения количества неудачных входов в систему). Следует учесть, что удаленная команда стирания далеко не всегда эффективна, так как она не может быть передана, если устройство не подключено к Интернету или к беспроводной сети. В таком случае шифрование обеспечит куда более надежную защиту для ваших данных.

Кроме того, не стоит забывать о такой опасности, как несанкционированный доступ к данным во время ремонта (в том числе гарантийного) либо продажи устройств, бывших в употреблении.

Заражение вредоносным ПО

Опасность вредоносного ПО на обычных ПК стала уже привычной. Сегодня для вирусописателей все более привлекательными становятся мобильные устройства. Перспективы распространения вредоносного ПО для мобильных устройств создают серьезные риски для корпоративных пользователей.

Встроенные возможности по управлению почтовыми и текстовыми сообщениями делают данные устройства чрезвычайно привлекательными для злоумышленников. Используя Wi-Fi и Bluetooth, вредоносное ПО потенциально может распространяться внутри образованной ими одноранговой сети.

Не стоит забывать еще об одной проблеме — о спаме! У пользователей, которые отвлекаются на присылаемые SMS, значительно снижается производительность труда.

На рынке мобильной связи наблюдается устойчивая тенденция повышения уровня «интеллекта» средств мобильной связи. Резко увеличивается число смартфонов, что вполне естественно стимулирует рост числа проблем, ранее присущих только ПК. Вирусы, спам, шпионское и рекламное программное обеспечение — увы, распространение подобного ПО — это только вопрос времени. Вместе с тем стоит отметить, что сегодня смартфоны гораздо хуже защищены от вредного воздействия.

Причина вполне естественна — количество вирусов для мобильных устройств так же, как когда-то вирусов для ПК, сегодня исчисляется несколькими десятками.

Большинство известных вирусов для смартфонов относится к классу троянских программ и использует для реализации своей функциональности уязвимости ОС.

Кроме того, существуют мобильные вирусы-черви. Типичный пример —Это был первый сетевой червь, распространявшийся через Bluetooth.

Новые вирусы для мобильных устройств появляются примерно раз в месяц.

Вместе с тем стоит отметить, что небезопасность мобильных устройств обусловлена в первую очередь человеческим фактором, а защищенность операционных систем не внушает доверия. Так, сегодня аппараты под управлением ОС Symbian очень легко вывести из строя. В соответствии с прогнозами экспертов защититься от мобильных вирусов большинству владельцев портативных устройств будет довольно трудно…

Какую опасность современные вирусы представляют для смартфона? Вирусы могут:

- незаметно для пользователя провести массовую рассылку SMS и MMS, за которые абоненту придется платить; несанкционированно звонить на платные номера;
- уничтожить данные пользователя (телефонная книга, файлы и т.д.) или похитить конфиденциальную информацию;
- заблокировать функции телефона (SMS, игры, камеру и т.д.) или аппарат в целом;
- разряжать аккумулятор телефона в несколько раз быстрее обычного;
- рассылать от вашего имени всеми возможными способами (e-mail, Wi-Fi, Bluetooth и т.д.) зараженные файлы;
- при синхронизации смартфона с компьютером переслать на ПК деструктивный код.

Способы проникновения вируса на смартфон:

- через Bluetooth-соединение;
- вместе с MMS-сообщением;
- при загрузке в смартфон ПО из ненадежного источника.

В дополнение к спаму и вредоносному ПО мобильные устройства могут быть подвергнуты обычному взлому с целью прекратить работу устройства. Как только произойдет атака подобного рода, ваш мобильный помощник просто перестанет работать!

Защита мобильных устройств

Как известно, безопасность обеспечивается совместными усилиями людей, процессов и технологий. Для защиты мобильных устройств и корпоративных сетей от потери данных (производительности) руководство организации должно предпринять следующие действия:

- создать в организации понятную политику использования мобильных устройств;
- определить порядок аутентификации пользователей и устройств для доступа к данным;
- зашифровать все данные;
- обеспечить защищенные соединения для доступа к данным;
- создать правила для межсетевого экрана и системы обнаружения вторжения для защиты от взлома;
- установить защиту от вредоносного ПО на мобильных устройствах;
- обеспечить централизованное управление этой защитой;
- обеспечить понимание пользователями необходимости мер безопасности.

Что делать, если возникло подозрение в заражении телефона вирусом

Если появилось подозрение в наличии на телефоне вируса, необходимо предпринять следующие действия:

- узнать, откуда получен вирус:
  - через Bluetooth,
  - через MMS,
  - загружен из Интернета;
- проверить список задач и закрыть все неизвестные;
- проверить, есть ли на экране значок Bluetooth;
- проверить, получают ли от вас другие телефоны, находящиеся рядом, запросы связи по Bluetooth;
- уточнить, есть ли в вашей телефонной книге люди, которые получали от вас MMS-сообщения с приложенными SIS-файлами;
- проверить, работает ли меню телефона;
- проверить, не отображается ли на экране что-то необычное;
- проверить, работает ли менеджер приложений;

- установить «Мобильный антивирус», обновить вирусные базы и произвести полное сканирование системы.

В борьбе с мобильными вирусами существует два подхода: установить антивирус на оборудование оператора связи либо на телефон пользователя.

Дадим несколько советов, что следует делать пользователю:

- установить специализированное антивирусное ПО;
- если вы в данный момент не нуждаетесь во включенном Bluetooth — отключите его;
- если вы все же используете Bluetooth (например, Bluetooth-гарнитуру), включите на вашем телефоне так называемый режим невидимости. Это затруднит работу взломщика, хотя полной гарантии безопасности не даст;
- не принимайте сообщения через Bluetooth, если вы его не ждете, то есть **никогда** не принимайте сообщения с незнакомых номеров;
- не принимайте SMS и MMS, отправленные с незнакомых номеров;
- выключайте Wi-Fi, если вы им не пользуетесь;
- при использовании Wi-Fi не забудьте о необходимости применения межсетевого экрана;
- не загружайте ПО из сомнительных источников;
- не используйте взломанное ПО, ведь стоимость лицензии гораздо ниже, чем стоимость возможного ремонта телефона;
- не забывайте о необходимости шифровать ваши данные;
- будьте внимательнее!

Но если все так грустно, почему не наблюдается вирусных эпидемий? Причина в том, что смартфоны пока еще не слишком широко распространены. Однако это, увы, только вопрос времени.

***

В заключение хотелось бы отметить, что с появлением новых технологий будут возникать и новые угрозы, использующие их уязвимости.

И наша с вами задача — не отстать в этой гонке!

Практика рассмотрения органами по защите прав потребителей поступающих от потребителей вопросов показала, что проводимая разъяснительная работа среди населения о защите прав потребителей позволяет разрешать большинство споров между потребителями и продавцами (исполнителями) в досудебном порядке и поэтому необходимо и в дальнейшем такую работу продолжать.

Просвещение жителей Холмского городского округа в области защиты прав потребителей позволяет потребителю уверенней чувствовать себя на потребительском рынке товаров и услуг, тщательнее и осмотрительнее подходить к приобретению покупок и заказу услуг (работ) и стимулирует граждан к самостоятельному применению положений Закона Российской Федерации «О защите прав потребителей» при возникновении спорных ситуаций, связанных с приобретением товаров, заключением договоров на оказание услуг (работ).