

# Безопасность мобильных устройств в аспекте угроз компрометации персональных и коммерческих данных

Е.А. Пшехотская, О.О. Михальский

Московский политехнический институт

pshehotskaya@gmail.com, oleg@mikhalsky.ru

## Аннотация

Статья посвящена вопросам безопасности мобильных устройств от угроз компрометации персональных и коммерческих данных. В работе рассматриваются различные классификации мобильных устройств, их программного обеспечения и интернет-сервисов, а также типы поведения пользователей и сопутствующие этому поведению угрозы неавторизованного доступа к данным, хранимым локально и удалённо. Приводится также категоризация потенциальных рисков, возникающих при компрометации различных классов данных.

**Ключевые слова:** безопасность мобильных устройств, проникновения в информационные системы, персональные данные, оценка рисков

## 1. Введение

Непрерывное развитие компьютерных технологий уже де-факто привело к почти полной зависимости цивилизации от огромных объемов хранимых данных и средств их обработки. Постоянно совершенствующиеся возможности программного и аппаратного обеспечения позволили преодолеть два препятствия на пути к информационному обществу, а именно: барьеры технологической/финансовой доступности и простоты/надёжности использования.

Первое препятствие заключалось в недостаточной распространенности или полном отсутствии инфраструктуры для обработки данных, что приводило к запретительно высокой стоимости приобретения как вычислительных устройств, так и сопутствующего программного обеспечения. Эти обстоятельства изначально обеспечивали относительную сохранность данных, поскольку пользователей было немного и большинство из них принадлежало узким профессиональным группам с высоким уровнем технического

образования. Рост производства доступного по цене аппаратного обеспечения и увеличение количества каналов связи привели к появлению электронных досок объявлений [1] с более крупными пользовательскими сообществами, что сделало невозможным персональное отслеживание действий каждого пользователя и оперативную реакцию на них. В свою очередь, это привело к первым масштабным эпидемиям быстро распространяющегося вредоносного программного обеспечения в виде примитивных вирусов и червей [2].

На том этапе развития угроза была ограничена вторым препятствием, выразившимся в виде высокой сложности компьютерных приложений, требующих от пользователей соответствующей квалификации для эффективной работы с ними, поскольку неправильное применение могло повлечь порчу данных. Тем не менее, количество пользователей продолжало расти с постепенным улучшением программных интерфейсов и механизмов обеспечения сохранности данных, предотвращавших неумышленную порчу данных.

Распространение персональных компьютеров и расширение доступа в Интернет привело к росту количества различных кибер-преступлений. Эти кибер-преступления изначально были окупаемы только при атаках на крупные организации, в основном финансовые и правительственные в силу исключительности возможностей по эффективной обработке крупных массивов пользовательских данных по сравнению с частными организациями меньшего масштаба. Первой вредоносной активностью, умышленно направленной против рядовых пользователей, были спам рассылки электронных писем, в особенности такого их жанра как мошеннические «Нигерийские письма» и аналогичные им формы обмана методами социальной инженерии. С развитием интернет-банкинга и интернет-торговли распространение получили более опасные преступления, такие как кража личности. Это повлекло ответ в виде государственной кибер-полиции и частных охранных компаний по кибер-безопасности, выросших из ранних поставщиков антивирусного программного обеспечения.

На текущий момент, объемы данных и количество производимых устройств испытывают практически неограниченный рост [3]. Производимые устройства с доступом в глобальную сеть превышают по количеству совокупное земное население. Подобный феномен наличия огромного количества стандартизованных узлов связи, обычно называемый Интернетом вещей, считается третьим препятствием на пути к следующему поколению информационного общества. Основная проблема в третьем препятствии заключается в уязвимости большинства устройств, не оборудованных в силу простоты и дешевизны изготовления каких-либо значимых средств аутентификации входящих соединений. Типы устройств варьируются от цифровых модулей с сетевым протоколом MQTT для вещания показаний примитивных датчиков (например, бытовых Wi-Fi термометров) до встраиваемых компьютеров на единичной плате (например, Raspberry Pi) для более сложной потребительской электроники как холодильники, стиральные машины или телевизоры. В силу стандартизации как машинной архитектуры, так и протоколов связи каждый узел может оказаться точкой проникновения вредоносной кибер-активности. Например, известным фактом является то, что

умные телевизоры уже способны выполнять неавторизованную аудиозапись даже без уведомления пользователей [4]. Такая же активность была обнаружена и в поведении смартфонов, обнаруживающего акустический паттерн включения телевизора и выполняющего сбор статистики по просматриваемым телеканалам. Подобный тип технологии известен как перекрестное межприборное слежение через акустические маяки [5]. Этот механизм активно разрабатывается лидером соответствующей индустрии SilverPush [6] и его конкурентами как Drawbridge, Flurry и Adobe.

Так, современные технологии порождают широкий диапазон различных угроз пользовательским данным со множеством векторов атаки. Следовательно, желательно обеспечить средство для оценки рисков пользовательских данных на основе характеристик устройств, сервисов и поведения пользователя. Целью работы является обсуждение возможности построения подобной методологии оценки угроз.

## 2. Угрозы пользовательским данным

Имеется несколько способов потенциального доступа к пользовательским данным со стороны неавторизованных участников информационного обмена. Эти способы варьируются по масштабу и сложности реализации, а также по сопутствующим расходам и частоте встречаемости. Наиболее частыми векторами неавторизованного доступа являются следующие события:

- кража физического устройства с пользовательскими данными;
- копирование пользовательских данных с помощью вредоносных приложений, установленных на устройстве локально;
- копирование пользовательских данных путём перехвата передачи по каналам связи;
- копирование реплик пользовательских данных через проникновение в удалённые хранилища данных.

Кража является наиболее распространённым и обнаруживаемым преступлением, затрагивающим электронные устройства. Исследования Consumer Reports показывают, что только в США за 2013 год порядка 3.1 миллиона пользователей стали жертвами кражи смартфонов [7], что почти вдвое превысило эти же показатели за 2012 год. В 2014 году количество зарегистрированных краж снизилось до 2.1 миллиона [8]. Снижение было вызвано такими мерами противодействия кражам как механизмы локального запирания устройства и его удалённая блокировка, внесёнными в программно-аппаратную архитектуру смартфонов многими производителями. Несмотря на изменение тренда в сторону понижения показателей, общее количество краж мобильных устройств по всему миру остаётся высоким и грубо оценивается в десятки миллионов краж в год. Согласно докладу Lookout Mobile Security [9], 44 процента всех утраченных мобильных устройств были оставлены в общественных местах, тогда как 14 процентов были украдены из дома или машины, а 11 процентов украдены из кармана. Более того, основной риск и ущерб краж мобильных устройств сместились от потери данных к компрометации данных, поскольку восстановление пользователем утраченных данных из резервной копии является несравнимо более простым действием, чем

надёжное уничтожение данных с украденного накопителя до того момента, пока данные не подверглись неавторизованному копированию.

Результаты исследований, ежегодно представляемые российским Аналитическим центром ГК Infowatch, свидетельствуют, что в распределении утечек конфиденциальной информации по регионам Российская Федерация занимает вторую позицию, отставая от США с большим отрывом по числу случаев компрометации данных. Так, в отчёте Infowatch [10] указано, что за 2016 год в России было зарегистрировано 213 инцидентов, почти вдвое превысивших по сравнению с 2015 годом, но вчетверо уступающих аналогичным происшествиям в США (838 утечек). Также, согласно данным этого отчёта, совокупный канал утечек, суммирующий статистику по кражам/потерям оборудования, утечкам со съёмных носителей и утечкам с мобильных устройств, составил 9,3 процента, лишь немного уступив доле утечек с бумажных носителей. Вместе с этим, преобладающим каналом является сетевой канал компрометации данных обобщающий утечки через локальный браузер, вредоносные приложения или облачные службы.

Менее очевидным способом компрометации пользовательских данных является активность вредоносных приложений, установленных на устройстве. Эти приложения функционируют либо в автоматическом режиме, сканируя накопители по поисковым шаблонам, либо обеспечивают тайное удаленное управление устройством. Обычно, подобные вредоносные приложения распространяются через различные полу-пиратские сайты-репозитории программного обеспечения и скрываются под видом известных коммерческих приложений с отключённой лицензионной защитой. Кроме того, нередко случаи заражения с официальных сайтов-магазинов, когда вредоносные приложения по недосмотру проходят проверку на безопасность. Согласно актуальному докладу Mobile threat report [11] от подразделения Intel Security, за три месяца сканирования официальных сайтов мобильных приложений App-Stores было выявлено более 9 миллионов вредоносных программ и дополнительно 9 миллионов подозрительных приложений из всего 150 миллионов проверенных приложений. Всего за шесть месяцев на различных сайтах с мобильными приложениями было обнаружено 37 миллионов вредоносных программ.

В исключительных случаях подозрительная активность как отмечено в материалах [12,13] может быть даже частью фабрично-установленной операционной системы, предназначенной для сканирования носителей данных и отправки данных на сторонние серверы. Имеются также модельные подтверждения концепции того, что приложения, использующие функциональные возможности смартфона в максимальном объеме, могут преодолевать изоляционный беспроводной барьер по воздуху с помощью акустической передачи данных другим ожидающим устройствам [14,15]. Известно, что современное высокотехнологичное вредоносное программное обеспечение построено по сложной архитектуре наподобие Stuxnet [16], Flame [17], Duqu [18], Downandup, а также EquationDrug и GrayFish [19]. Анализ этих архитектур и их функциональных возможностей показывает, что будущее вредоносное программное обеспечение будет использовать компрометирующее излучение, включая радио и электрические сигналы, звуки и вибрации, и

потенциально обладать возможностью преодолеть защитные протоколы TEMPEST. С одной стороны, подобное высокотехнологичное кибероружие государственной разработки служит для достижения специальных целей и с низкой долей вероятности представляет угрозу обычным пользователям. С другой стороны, само оружие, само являясь цифровыми данными, может быть утеряно или украдено, а далее подвергнуто реверсивному проектированию и свободно распространено (как Stuxnet), тем самым скомпрометировав средства контроля над его использованием.

Другой тип неочевидных атак нацелен на перехват конфиденциальных данных, передаваемых по каналам связи между устройствами. Эти атаки обычно осуществляются посредством взломанных или злонамеренно организованных точек доступа Wi-Fi с открытым доступом без пароля и скомпрометированным HTTPS-протоколом [20]. Практически каждый пользователь, устанавливающий подобное соединение, компрометирует свой трафик. Единственным исключением являются технически-грамотные пользователи, применяющие VPN-туннелирование до безопасных серверов. В редких случаях, благодаря природе радиосигнала Wi-Fi, трафик пассивно перехватывается системами специального назначения [21]. Тем не менее, подобные профессиональные разведывательные устройства являются дорогостоящими и ограниченными к продаже, а, следовательно, редко встречающимися в гражданском обращении.

Наиболее опасной угрозой пользовательским данным считается проникновение в хранилище данных, поскольку одновременно компрометируется большой объем данных по пользовательским учётным записям. Согласно отчёту Breach Index [22] от компании Gemalto, опубликованное количество скомпрометированных пользовательских учётных записей с 2003 года по настоящее время приближается к шести миллиардам [23]. В этих статистических данных только 4 процента скомпрометированных записей были защищенными, т.е. украденные данные были зашифрованными и, таким образом, бесполезными для воров. Поскольку все кражи данных происходят на стороне сервера, пользователь не имеет возможности предотвратить компрометацию своих данных даже при идеальном соблюдении защиты со стороны своего устройства. Это обстоятельство служит еще одним примером взаимоисключающих требований целостности и безопасности, поскольку соблюдение целостности данных требует размещения легко доступных реплик данных на сервисах удалённого хранения данных, тогда как соблюдение безопасности требует минимизации количества сильно зашифрованных копий данных. Статистика Gemalto подтверждает тезис о том, что большинство провайдеров услуг задают значительный приоритет сохранности данных перед безопасностью данных.

### **3. Оценка рисков пользовательским данным**

#### **3.1. Классификация устройств**

На текущем этапе развития средств глобальной мировой связи пользовательские данные практически всегда подвержены рискам различной

степени опасности, зависящим от типа устройства пользователя, пользовательских приложений и сервисов, а также типа самих пользовательских данных. В этой части статьи рассматриваются следующие категории, характеризующие персональные электронные устройства:

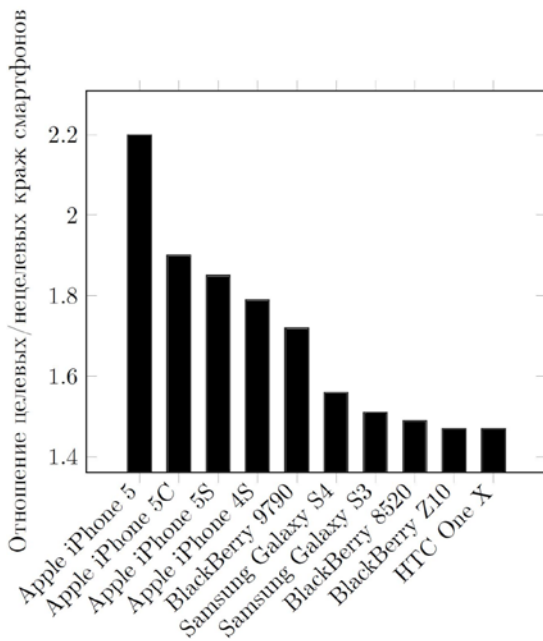
- цена;
- мобильность;
- вариативность;
- контролируемость;
- аппаратная безопасность.

Цена устройства является одной из наиболее важных характеристик, определяющих риск кражи. Очевидно, что наиболее дорогие флагманские устройства из верхней части ценовой линейки привлекают больше внимания воров, нежели устаревшие аналоги в нижней и средней части ценового диапазона. Например, исследование по кражам смартфонов, проведенное Behavioural Insights Team of Home Office [24], показывает, что смартфоны различных моделей и брендов производителей значительно отличаются по вероятности быть украденными. Величины привлекательности модели для краж представлены на рис.1–2. Значения на этих графиках являются отношением всех краж моделей как целенаправленных, в случае кражи из кармана, так и не целенаправленных, в случае ограбления жилища, к доле не целенаправленных краж. Статистика варьируется со временем и в идеале должна обновляться через регулярные интервалы времени порядка годового квартала или даже ежемесячно, если это технически осуществимо. Статистика также показывает статус выбранных моделей смартфонов, поскольку, например, iPhones подвергаются кражам более целенаправленно, чем другие бренды, несмотря на то, что Apple занимает меньшую долю рынка, чем бренд Samsung.

Мобильность означает такие характеристики устройства, как габариты, вес и время работы от аккумулятора. Очевидно, что небольшие устройства как смартфоны, планшеты или переносные накопители данных больше подвержены риску потери и кражи, чем большие ноутбуки, настольные ПК и серверные стойки. Тем не менее, большие устройства обычно имеют модульное строение и могут быть разобраны на месте с целью извлечения компонент, хранящих конфиденциальные данные, например, жёсткие диски, твердотельные накопители или даже модули оперативной памяти в случае атаки типа Cold Boot.

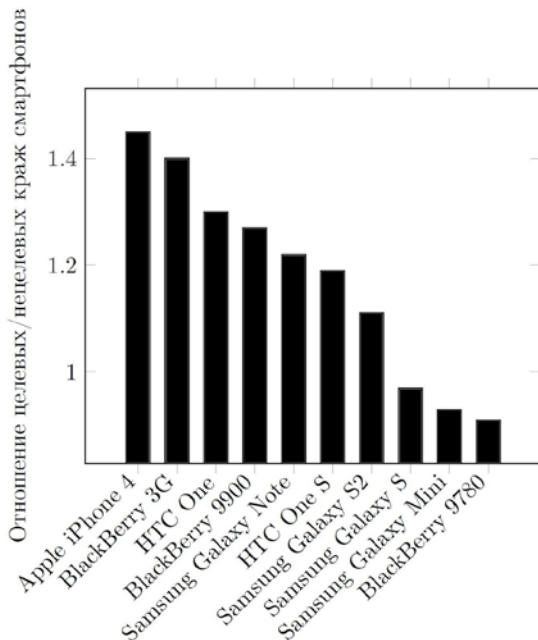
Вариативность показывает, насколько разнообразна продуктовая линейка производителя. Другими словами, характеристика свидетельствует о разнообразии архитектуры в части применяемого аппаратного и программного обеспечения. Если продуктовая линейка очень мала, тогда устройства более подвержены специализированным целевым атакам на их аппаратную и программную части. Продукты с одинаковой архитектурой могут быть изначально более устойчивы к взлому, но будучи единожды скомпрометированными, могут подвергнуть риску всех пользователей целой продуктовой линейки. Продукты с варьирующимися элементами архитектуры могут быть менее устойчивы к атакам, но взломанная модель компрометирует лишь соответствующую часть пользователей. Более того, в последнем случае пользователи могут перейти на другой продукт линейки без каких-либо

изменений своих привычек. Тем не менее, некоторые архитектурные недостатки могут быть общими для обширного диапазона моделей устройств, не зависящего от конкретных производителей. Например, недавно обнаруженный набор уязвимостей «Quadrooter» в микросхемах Qualcomm [25] затрагивает более 900 миллионов смартфонов и планшетов с операционной системой Android, раскрывая злоумышленникам доступ корневого уровня.



**Рис. 1.** Привлекательность моделей смартфонов для краж

Контролируемость показывает, насколько полно пользователь может распоряжаться устройством. Например, позволяет ли операционная система пользователю по умолчанию работать с файловой системой или требует специализированного взлома и обхода ограничений, прекращающих действие гарантии на устройство. Характеристики аппаратной безопасности, как правило, показывают наличие сенсоров отпечатков пальцев и защиты электронных цепей устройства от физического воздействия. Тем не менее, решения, реализующие авторизацию по отпечаткам пальцев подвержены ложноположительным срабатываниям по искусственно-сгенерированным входным данным.



**Рис. 2.** Привлекательность моделей смартфонов для краж, продолжение

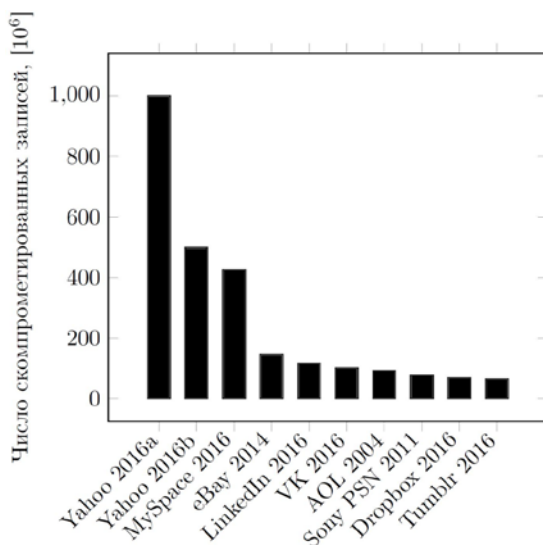
### 3.2. Типы поведения пользователей

В работе также рассматривается поведение пользователей, особенно интернет-активность, поскольку она также составляет один из рисков безопасности данных. Согласно отчёту Consumer Reports за 2014 год, только 36 процентов пользователей приложений установили четырехзначный экранный PIN-замок, 14 процентов установили антивирусное приложение, 11 процентов применили многозначный PIN-замок или графический замок, 8 процентов установили программное обеспечение по удалению данных, а 7 процентов использовали шифрование. Напротив, 34 процента пользователей не воспользовались ни одним из этих средств безопасности. Тем не менее, правильное безопасное обращение со смартфоном является только частью политик сокращения рисков, поскольку снижает лишь две угрозы, а именно: кражу устройства и кражу данных вредоносными приложениями. Два оставшихся риска существенно зависят от интернет-активности пользователя. Таким образом, пользовательское поведение может быть разделено на следующие категории:

- локальное обращение с устройством;
- сетевое обращение;
- обращение с удаленными сервисами.

Категория сетевого обращения показывает, насколько строгими являются предпочтения пользователя при выборе неизвестных узлов связи. В настоящее время наиболее распространены Wi-Fi и Bluetooth узлы. Актуальный отчёт Лаборатории Касперского [26] показывает, что среди 31 миллиона проанализированных точек доступа Wi-Fi почти 22 процента не имеют никакой

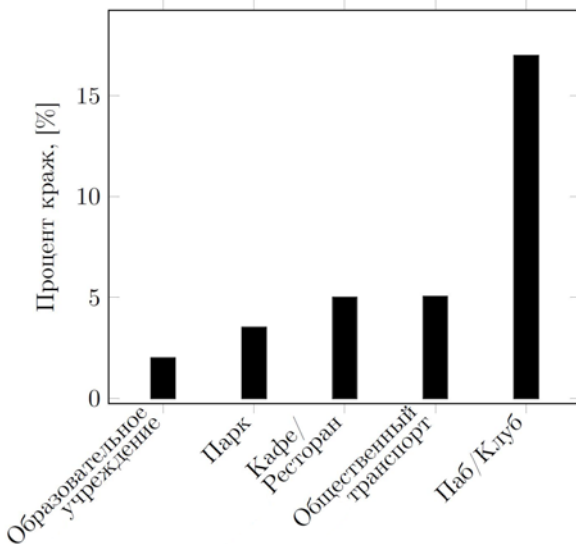
защиты, а еще 2.7 процента имеют устаревший легко взламываемый WEP-протокол защиты. Другое исследование, проведенное корпорацией Symantec [27], выявило, что 61 процент из 9135 респондентов полностью пренебрегают рисками общественных Wi-Fi сетей, считая свою информацию в безопасности. Это исследование также показывает, что преувеличенное доверие к точкам доступа связано с возрастом пользователей, поскольку больше доверяет общественным сетям молодёжь (68 процентов), чем пользователи старшего возраста. Несмотря на это, недавний опрос [28] 1516 респондентов, проведенный ISPreview.co.uk, свидетельствует, что пользователи отдают предпочтение сотовому Интернету 3G/4G (72 процента), нежели общественным точкам доступа Wi-Fi (21 процент). Тем не менее, даже сотовые линии связи могут быть скомпрометированы посредством подложных базовых станций, осуществляющих атаки типа «человек посередине» [29].



**Рис. 3.** Количество скомпрометированных записей в крупномасштабных взломах, начиная с 2013 года

Удаленные онлайн сервисы предоставляют пользователю множество приложений для различных целей, варьирующихся от развлечения и редактирования документов до научных исследований и онлайн-банкинга. Отличительной особенностью всех онлайн сервисов является огромный массив хранимых пользовательских данных. Подобные объемы конфиденциальных данных делают эти сервисы привлекательными для взлома. Несмотря на меры безопасности корпоративного уровня, количество крупномасштабных проникновений повышается с каждым годом. Отчёты Gemalto показывают 1541 зарегистрированный взлом за 2014 год [22] и 1673 случая за 2015 год [30], а также 974 проникновения за первую половину 2016 года [31]. Взломанные организации относятся как к коммерческому, так и к государственному секторам. В список атакованных организаций входят: медицинская база данных U.S. Healthcare Insurers database, офис управления персоналом U.S. Office of

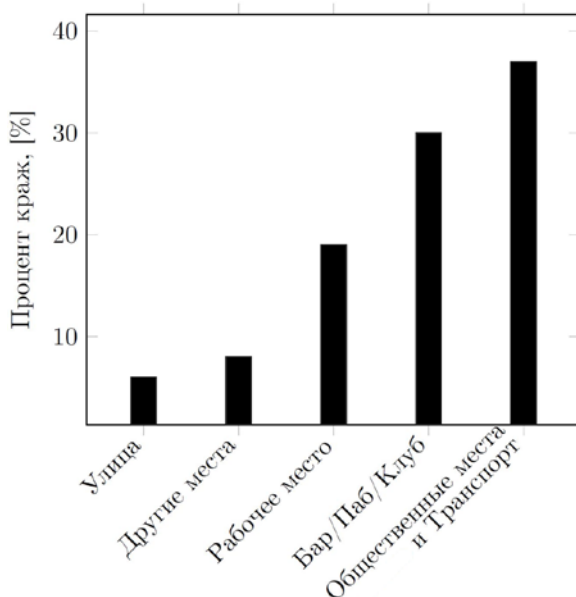
Personnel Management (OPM), филиппинская комиссия по выборам Philippines Commission on Elections, служба голосования Мексики Mexican Voters, генеральный директорат Турции по делам населения и гражданства Turkish General Directorate of Population and Citizenship Affairs, а также JP Morgan Chase, AliExpress и Sony Pictures Entertainment. Актуальный отчёт Statista [32] показывает, что наиболее крупные из всех взломов датируются, начиная с 2013 года, и выражаются в миллиардах скомпрометированных учётных записей пользователей Yahoo, без учёта более позднего отдельного взлома 500 миллионов записей этой корпорации. Общий график по количеству скомпрометированных учётных записей приведен на рис. 3. Меньшие по масштабу сервисы могут подвергаться взлому и даже не публиковать информацию об этом. Таким образом, пользователям рекомендуется тщательно выбирать объем и содержание своего присутствия в глобальной сети. Разумно предположить, что чем большим количеством учётных записей обладает пользователь, тем выше риски соответствующим конфиденциальным данным. Тем не менее, пользователь не может полностью исключить своё присутствие в сети, поскольку некоторая информация собирается государственными учреждениями и хранится в обязательном порядке. Более того. Технологии перекрёстной авторизации в социальных сетях, когда данные из учётной записи одной сети позволяют осуществлять доступ к учётной записи другой сети, существенно снижают общий уровень безопасности в случае компрометации главной учётной записи пользователя.



**Рис. 4.** Процент краж смартфонов в Лондоне по месту кражи

Имеется также множество привычек пользователей, которые косвенно влияют на риски, которым подвергаются пользовательские данные. Правительственный отчёт The Great Britain Home Office по кражам смартфонов [24] показывает зависимость между частотой и местом краж (см. рис. 4–5). Так, наибольшее количество краж в Лондоне происходит в пабах и клубах (17

процентов), тогда как наименьшее количество регистрируется в образовательных учреждениях (2 процента). Отчёт Lookout [33] несколько расходится с такими оценками, помещая рестораны в верхнюю позицию мест с наиболее частыми кражами (16 процентов), как показано на рис.6. Таким образом, привычка посещать определенные места неявно влияет на общие риски безопасности данных. Даже место переноски устройства влияет на вероятность кражи. Например, кража из кармана менее вероятна, чем кража из сумки [24] (см. рис.7).

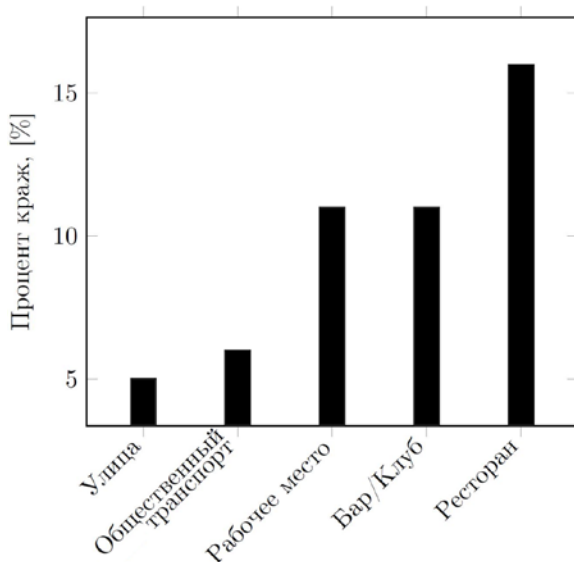


**Рис. 5.** Процент краж смартфонов в Англии и Уэльсе по месту кражи

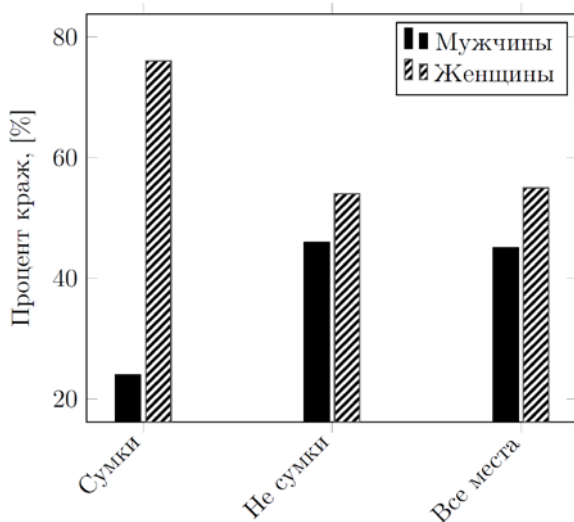
### 3.2. Типы пользовательских данных

Риски безопасности пользовательских данных зависят не только от инфраструктуры хранения и передачи данных, но и от типа самих данных. Согласно опросу Norton [27], пользователи больше всего озабочены следующими угрозами:

- кража пользовательской информации (83 процента);
- неавторизованный доступ к финансовой информации (85 процентов);
- заражение вредоносным программным обеспечением (84 процента);
- неавторизованным доступом к личным фотографиям/видеозаписям (72 процента).



**Рис. 6.** Процент краж смартфонов в США по месту кражи



**Рис. 7.** Пропорции краж смартфонов в Лондоне по категориям пола и места переноски устройства

Эти индикаторы хорошо согласуются с данными Gemalto [30], в которых перечисляются типы компрометируемых данных и их доля в годовом объеме взломов:

- данные, составляющие идентичность пользователя (53 процента);
- данные для доступа к финансовой информации (22 процентов);

- данные для доступа к учётным записям (11 процента);
- бытовые данные (11 процентов);
- несущественные данные (4 процента).

Более детально типы данных рассмотрены в исследовании Lookout [34]. Опубликованные результаты представлены на рис. 8 и подтверждают опросы Gemalto и Norton. Такие данные как SSN, номер водительских прав, номер паспорта, а также номер медицинской страховки представляют собой цифровую личность пользователя. Номер банковского счёта, номера кредитных карт, информация налогоплательщика относятся к финансовым данным. Данные по логинам и паролям соответствуют доступу к учётным записям, а бытовые данные представлены адресом электронной почты и телефонным номером.

Указанные выше типы данных позволяют оценить риски пользователя, однако степени рисков варьируются в зависимости от степени информатизации стран и государств. Так, по данным справки Аналитического центра ГК Infowatch [35], несмотря на то, что в России стремительно возрастает вовлеченность граждан в процессы электронного взаимодействия, отсутствует статистика, какие из электронных идентификаторов личности подвержены наибольшему риску компрометации. Недостаточность накопленной статистики можно объяснить тем, что по данным Минкомсвязи России из общего числа пользователей Единого портала госуслуг (40 миллионов человек), более 18 миллионов зарегистрировались на портале в 2016 году.

### 3.3. Классификация рисков и потерь

Каждый тип вышеуказанных данных соответствует множеству рисков с различным уровнем потерь пользователя при компрометации данных. Логично провести классификацию рисков по масштабу потенциального вреда:

- кража личности;
- финансовые потери;
- кража учётной записи;
- бытовые потери.

Кража личности является наиболее сложным и тяжелым риском, который можно испытать. Этот риск включает в себя меньшие риски от финансовых до бытовых потерь и требует значительных усилий для устранения последствий, поскольку выражается в полной имперсонации пользователя. Скомпрометированные данные включают в себя номера документов и персональных идентификаторов, логины и пароли, а также геолокационные данные, социальные связи и массив поведенческих примеров и истории личной активности. Так, атакованный пользователь должен подтвердить свою личность, вернуть свои данные в соответствующее реальности состояние и минимизировать ответственность за действия, совершенные злоумышленниками от его лица. Обычно невозможно полностью аннулировать последствия и сопутствующие потери, например, финансовые и репутационные. В худшем случае пользователю может грозить уголовное преследование при невозможности доказать свою непричастность к действиям, совершенным с помощью его цифровой личности.

Частичная кража личности может привести к финансовым потерям, поскольку соответствующие учреждения на законных основаниях избегают компенсации кому-либо де-факто авторизованных расходов. Тем не менее, стандарт проведения финансовых транзакций требует осуществления двухфакторной авторизации, которая является достаточно надёжной защитой от атак среднего уровня без привлечения большой инфраструктуры.

Кража учётных записей представляет собой перехват контроля над нефинансовыми учётными записями пользователей, когда основной ущерб наносится в виде репутационных потерь из-за утечки частной информации, такой как фотографии или письменные документы. Более того, кража учётной записи может служить промежуточным этапом для атак более высокого уровня посредством глубокого поиска данных в собранных объемах пользовательской информации.

Бытовые потери обычно недооцениваются, поскольку имеют ограниченное влияние на финансовое благополучие и репутацию. Например, заблокированная учётная запись является бытовым неудобством, поскольку пользователю необходимо потратить время на смену одного или нескольких паролей для этой учётной записи и других, связанных с ней. Бытовые потери включают компрометацию истории геолокации, адресов электронной почты и телефонных номеров, что подвергает пользователя дополнительным потокам спам-рассылок. Вместе с этим не рекомендуется пренебрегать бытовыми потерями, поскольку они могут накапливаться до критического уровня и порождать риски более высокого порядка.

## Заключение

В настоящей работе была проведена классификация различных угроз и потерь, а также сопутствующих им зависимостей типов устройств, программного обеспечения, онлайн-сервисов и поведения пользователей. По мнению исследователей, предложенная классификация может быть успешно использована для оценки уровня угроз по шаблонам поведения пользователей.

## Литература

- [1] Gilbertson, S. Feb. 16, 1978: Bulletin Board Goes Electronic // Wired, 02.16.10 URL: <https://www.wired.com/2010/02/0216cbbs-first-bbs-bulletin-board/> (дата обращения: 01.05.2016).
- [2] A Short History of Computer Viruses // Comodo Antivirus, 04.09.2014. URL: <https://antivirus.comodo.com/blog/computer-safety/short-history-computer-viruses/> (дата обращения: 01.05.2016).
- [3] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) // Statista. URL: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/> (дата обращения: 01.05.2016).
- [4] Harris, S. Your Samsung SmartTV Is Spying on You, Basically // The Daily Beast, 06.02.15.

- URL: <http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html> (дата обращения: 01.05.2016).
- [5] На, А. SilverPush Says It's Using «Audio Beacons» For An Unusual Approach To Cross-Device Ad Targeting // Tech Crunch, 24.06.2014. URL: <https://techcrunch.com/2014/07/24/silverpush-audio-beacons> (дата обращения: 01.05.2016).
- [6] Goodwin, D. Law & Disorder Beware of ads that use inaudible sound to link your phone, TV, tablet, and PC // ArsTechnica, 13.11.2015. URL: <https://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc> (дата обращения: 01.05.2016).
- [7] Tapellini, D. Smart phone thefts rose to 3.1 million in 2013. Industry solution falls short, while legislative efforts to curb theft continue // Consumer Reports, 28.05.2014. URL: <http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm> (дата обращения: 01.05.2016).
- [8] Deitrick, C. Smartphone thefts drop as kill switch usage grows but Android users are still waiting for the technology // Consumer Reports, 11.06.2015. URL: <http://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm> (дата обращения: 01.05.2016).
- [9] Eadicicco, L. People Are Willing To Go To Extreme Lengths To Retrieve Their Stolen Smartphones // Business Insider, 07.05.2014. URL: <http://www.businessinsider.com/smartphone-theft-statistics-2014-5> (дата обращения: 01.05.2016).
- [10] Исследование утечек конфиденциальной информации в 2016 году // Аналитический центр InfoWatch, 23.03.2017. URL: <https://www.infowatch.ru/report2016> (дата обращения: 01.05.2016)
- [11] Snell, B. Mobile Threat Report. What's on the Horizon for 2016 // Intel Security, 01.03.2016. URL: <https://www.mcafee.com/us/resources/reports/gr-mobile-threat-report-2016.pdf> (дата обращения: 01.05.2016).
- [12] Ещё немного про телефоны Xiaomi и борьбу с ними. Updated // HabraHabr, 27.01.2017. URL: <https://habrahabr.ru/post/320612> (дата обращения: 01.05.2016).
- [13] На Android-смартфонах Xiaomi обнаружен таинственный бэкдор // Security Lab, 16.09.2016. URL: <http://www.securitylab.ru/news/483861.php> (дата обращения: 01.05.2016).
- [14] Goodwin, D. Scientist-developed malware prototype covertly jumps air gaps using inaudible sound. Malware communicates at a distance of 65 feet using built-in mics and speakers // Ars Technica, 02.12.2013. URL: <https://arstechnica.com/security/2013/12/scientist-developed-malware-covertly-jumps-air-gaps-using-inaudible-sound> (дата обращения: 01.05.2016).
- [15] Wisneski, C. Ultrasonic Local Area Communication // MIT. URL: <http://alumni.media.mit.edu/wiz/ultracom.html> (дата обращения: 01.05.2016).
- [16] Zetter, K. Law & Disorder How digital detectives deciphered Stuxnet, the most menacing malware in history // Ars Technica, 11.07.2011. URL: <https://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history> (дата обращения: 01.05.2016).

- [17] Goodwin, D. Spy malware infecting Iranian networks is engineering marvel to behold // Ars Technica, 29.05.2012. URL: <https://arstechnica.com/security/2012/05/spy-malware-infecting-iranian-networks-is-engineering-marvel-to-behold> (дата обращения: 01.05.2016).
- [18] Brodtkin, J. Spotted in Iran, trojan Duqu may not be «Son of Stuxnet» after all // Ars Technica, 27.10.2011. URL: <https://arstechnica.com/business/2011/10/spotted-in-iran-trojan-duqu-may-not-be-son-of-stuxnet-after-all> (дата обращения: 01.05.2016).
- [19] Zetter, K. How the NSA`s Firmware Hacking Works and Why It`s So Unsettling // Wired, 22.02.15. URL: <https://www.wired.com/2015/02/nsa-firmware-hacking> Mobile Device Security, Management of Personal Privacy and Business Data (дата обращения: 01.05.2016).
- [20] Geier, E. Here`s what an eavesdropper sees when you use an unsecured Wi-Fi hotspot // PCWorld, 28.06.2013. URL: <http://www.pcworld.com/article/2043095/heres-what-an-eavesdropper-sees-when-you-use-an-unsecured-wi-fi-hotspot.html> (дата обращения: 01.05.2016).
- [21] Wi-Fi Interception System (SCL-2052) // Shoghi. URL: <http://www.shoghicom.com/wifi-interception.php> (дата обращения: 01.05.2016).
- [22] 2014 Year of Mega Breaches & Identity Theft // Gemalto. URL: <http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf> (дата обращения: 01.05.2016).
- [23] Breachlevelindex.com. URL: <http://breachlevelindex.com> (дата обращения: 01.05.2016).
- [24] The Behavioural Insights Team. Reducing Mobile Phone Theft and Improving Security // Home Office, 2014. URL: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/390901/HO\\_Mobile\\_theft\\_paper\\_Dec\\_14\\_WEB.PDF](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/390901/HO_Mobile_theft_paper_Dec_14_WEB.PDF) (дата обращения: 01.05.2016).
- [25] Khandelwal, S. Warning! Over 900 Million Android Phones Vulnerable to New `QuadRooter` Attack // The Hacker News, 07.08.2016. URL: <http://thehackernews.com/2016/08/hack-android-phone.html> (дата обращения: 01.05.2016).
- [26] Jackson, M. Kaspersky Lab Reports 25% of WiFi Internet Hotspots are Unsecured // ISP News, 28.11.2016. URL: <http://www.ispreview.co.uk/index.php/2016/11/kaspersky-lab-reports-25-wifi-internet-hotspots-unsecured.html> (дата обращения: 01.05.2016).
- [27] Jackson, M. Norton — Only 42% of People Can Tell if a Wi-Fi Network is Secure or Not // ISP News, 29.06.2016. URL: <http://www.ispreview.co.uk/index.php/2016/06/norton-42-people-can-tell-wi-fi-network-secure-not.html> (дата обращения: 01.05.2016).
- [28] Jackson, M. Study — Mobile Broadband Still More Popular than Risky Public Wi-Fi // ISP News, 25.10.2016. URL: <http://www.ispreview.co.uk/index.php/2016/10/study-mobile-broadband-still-popular-risky-public-wi-fi.html> (дата обращения: 01.05.2016).
- [29] Bargaonkar, R., Shaik, A. et al. LTE and IMSI catcher myths // BlackHat. URL: <https://www.blackhat.com/docs/eu-15/materials/eu-15-Bargaonkar-LTE-And-IMSI-Catcher-Myths-wp.pdf> (дата обращения: 01.05.2016).

- [30] 2015. The Year Data Breaches Got Personal // Gemalto. URL: <http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach-Level-Index-Annual-Report-2015.pdf> (дата обращения: 01.05.2016).
- [31] 2016. It's All About Identity Theft // Gemalto. URL: <http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf> (дата обращения: 01.05.2016).
- [32] Richter, F. Latest Yahoo Hack Is the Largest Data Breach To Date // Statista, 15.12.2016. URL: <https://www.statista.com/chart/5983/data-breaches> (дата обращения: 01.05.2016).
- [33] Phone Theft in America. Breaking down the phone theft epidemic // Lookout, 2014. URL: <https://transition.fcc.gov/cgb/events/Lookout-phone-theft-in-america.pdf> (дата обращения: 01.05.2016).
- [34] Identity Theft in America. Shedding light on an evolving epidemic // Lookout, 2016. URL: <https://info.lookout.com/rs/051-ESQ-475/images/lookout-breach-identity-protection.pdf> (дата обращения: 01.05.2016).
- [35] Справка Аналитического центра ГК InfoWatch о «краже личности» // Аналитический центр InfoWatch, 22.03.2017. URL: [https://www.infowatch.ru/analytics/leaks\\_monitoring/17489](https://www.infowatch.ru/analytics/leaks_monitoring/17489) (дата обращения: 01.05.2016).

### **Mobile device security, threats to personal and business data**

Е.А. Pshehotskaya , О.О. Mikhalsky  
Moscow polytechnic university

This paper is concerned with arising problems on security and privacy of personal data on mobile devices. We consider various classifications of mobile devices and their software services as well as types of user behavior regarding the involved security risks of unauthorized access to the data stored both locally and remotely. We also categorize potential threats that originate from compromised data of different classes. Based on provided categorization we discuss the means to generalize user patterns and evaluate the corresponding vulnerability level.

**Keywords:** mobile device security, personal privacy, data breaches, risks estimation