Код безопасности

Безопасность мобильных устройств - 2016

Аналитическое исследование
Ноябрь 2016 г.

Содержание

Резюме

Конфиденциальность информации на мобильных устройствах:

- **Каждый третий** пользователь мобильного устройства не применяет пароль для блокировки экрана.
- **46%** пользователей позволяют знакомым пользоваться своим мобильным устройством.
- **3/4 пользователей** заходят в Интернет через публичные точки Wi-Fi.
- Почти **половина** пользователей не делают backup мобильного устройства.
- **48%** менеджеров сохраняют рабочие файлы на мобильном устройстве.
- **30%** сотрудников обсуждают конфиденциальную корпоративную информацию по телефону и в мессенджерах.
- **Топ-менеджеры в 2 раза чаще**, чем **специалисты**, теряют мобильные устройства.

Безопасность мобильных операционных систем:

- Большинство устройств на базе ОС Android в первом полугодии 2016 г. **многократно заражались**.
- Пик активности хакерских атак на мобильные телефоны в первой половине 2016 г. пришелся на **апрель**.
- **Менее 1%** вредоносных мобильных программ освещаются в СМИ.
- Лишь **половина** респондентов обновляют операционную систему мобильного устройства.
- **Каждый четвертый** специалист делает Jailbreak/Rooting мобильного устройства.

Каждая четвертая крупная компания предоставляет сотрудникам мобильное устройство. В SMB так поступают **менее 12%** организаций.

15% крупных российских компаний внедрили MDM-системы, в SMB этот показатель составляет **2-5%**.

Аннотация

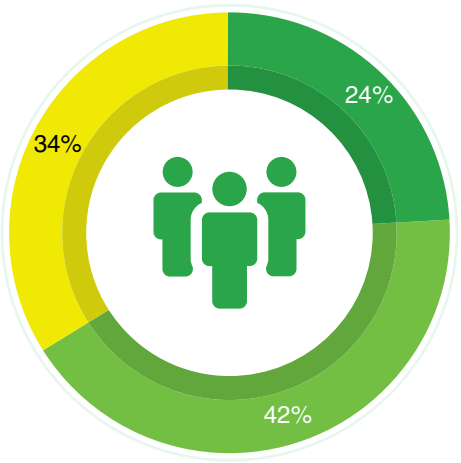
Исследование направлено на определение специфики применения мобильных устройств в российских компаниях. При проведении исследования аналитики «Кода Безопасности» искали ответы на следующие вопросы:

- Каков уровень личной ответственности пользователей при обработке корпоративных данных на мобильном устройстве? Уделяют ли они внимание вопросам информационной безопасности?
- Каковы основные факторы риска при использовании мобильных устройств для передачи корпоративной информации?
- Какие методы используют российские компании при организации защиты мобильных устройств?

Методика сбора данных и анализа

В течение первого полугодия 2016 г. аналитики компании «Код Безопасности» проводили анализ публикаций в открытых источниках СМИ, касающихся мобильных угроз и уязвимостей. В результате он стал базой данного исследования. Сбор данных проводился по России. Также в исследовании использовался количественный метод в форме онлайн-опроса на сайте компании «Код Безопасности» (www.securitycode.ru) и опросов на офлайн-мероприятиях. В исследование вошли ответы 580 респондентов, которые были разделены на 4 основные группы: топ-менеджеры, специалисты по продажам, ИТ-специалисты и другие. При обработке полученных результатов компании были классифицированы по численности сотрудников на малые (до 100 чел.), средние (от 100–1000) и крупные (более 1000 чел.)

Респонденты



- Крупные компании (более 1000 сотрудников)
- Средние компании (от 100 до 1000 сотрудников)
- Малые компании (менее 100 сотрудников)

По должностям:

- Топ-менеджеры
- Менеджеры по продажам
- ИТ-специалисты
- Другие

Общее число респондентов – 580

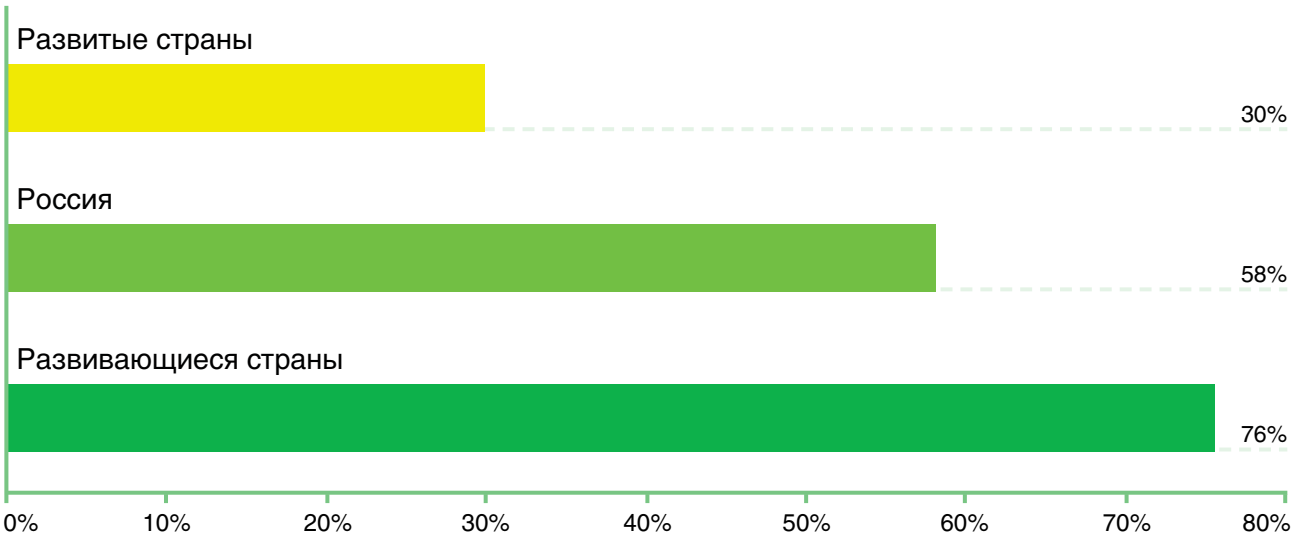
Личные и корпоративные мобильные устройства

По результатам исследования «Кода Безопасности», 65% российских компаний разрешают сотрудникам использовать мобильные устройства в рабочих целях. Этот показатель немного ниже уровня сотрудников, желающих использовать мобильные устройства в работе: по оценке IDC[1] , в России этот показатель составляет 78%. Таким образом, интерес сотрудников к применению мобильных устройств выше, чем готовность компаний его поддержать.

Чтобы минимизировать разрыв бизнес-интересов с вопросами управляемости мобильных устройств, большинство организаций прибегает к одному из следующих решений – приобрести корпоративные мобильные устройства (концепция CYOD) или разрешить сотрудникам применять в работе собственные (концепция BYOD).

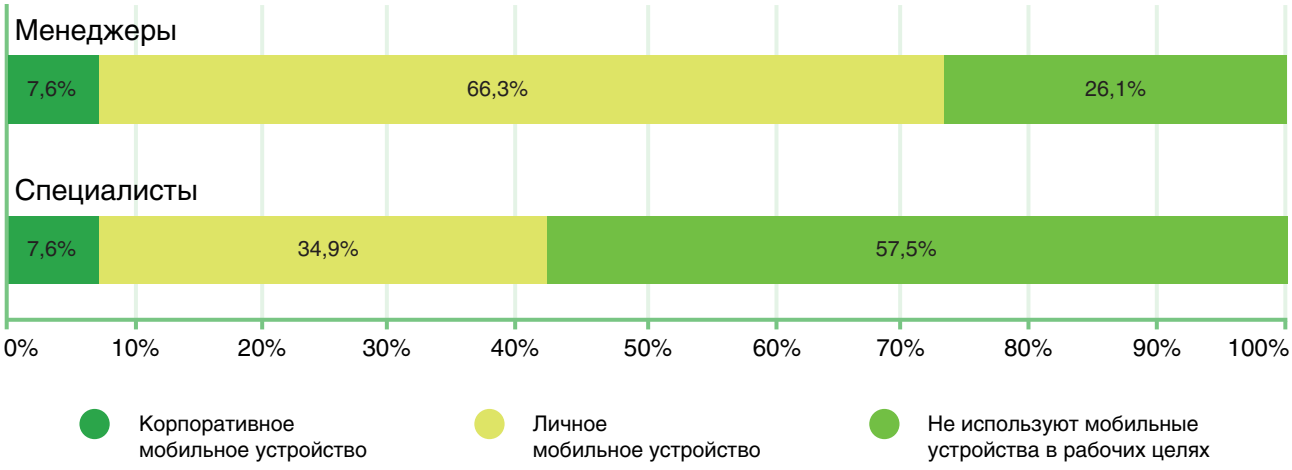
В России более половины сотрудников (58%) для чтения рабочей электронной почты и обработки другой конфиденциальной корпоративной информации используют личные мобильные устройства. Этот показатель находится посередине между данными для стран различных регионов: по данным IDC[2] , в развитых странах 30% сотрудников используют свои устройства в работе, в развивающихся странах – 76% сотрудников.

Использование в работе личных мобильных устройств (BYOD)



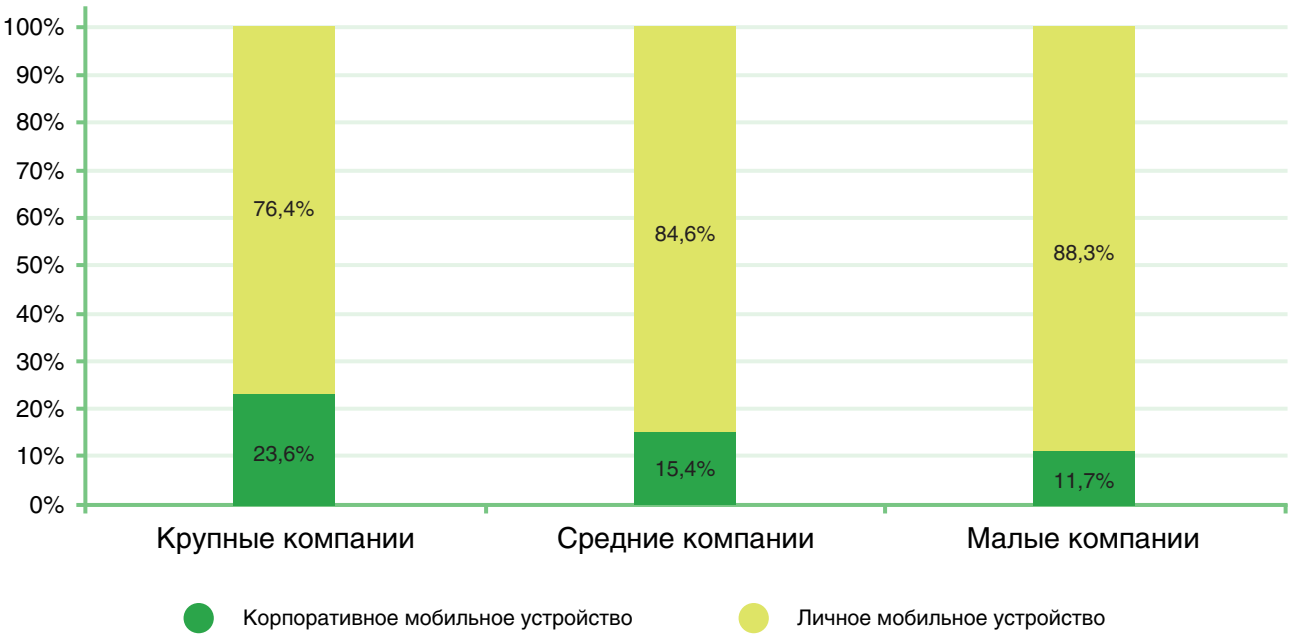
Личные и корпоративные мобильные устройства

Эти показатели сильно разнятся для различных категорий сотрудников: менеджеры в 2 раза чаще, чем специалисты, применяют в работе личные мобильные устройства. При равных показателях использования корпоративных устройств (7,6%) это означает, что специалисты в большинстве случаев предпочитают не решать рабочие вопросы вне офиса (57,5%).



Подход к использованию корпоративных мобильных устройств в компаниях разного масштаба отличается: чем крупнее организация, тем чаще для сотрудников приобретают корпоративные устройства и полностью контролируют безопасность их применения.

В среднем крупные компании в 2 раза чаще предоставляют корпоративные мобильные устройства (23,6%), чем компании SMB-сектора (11,7%).



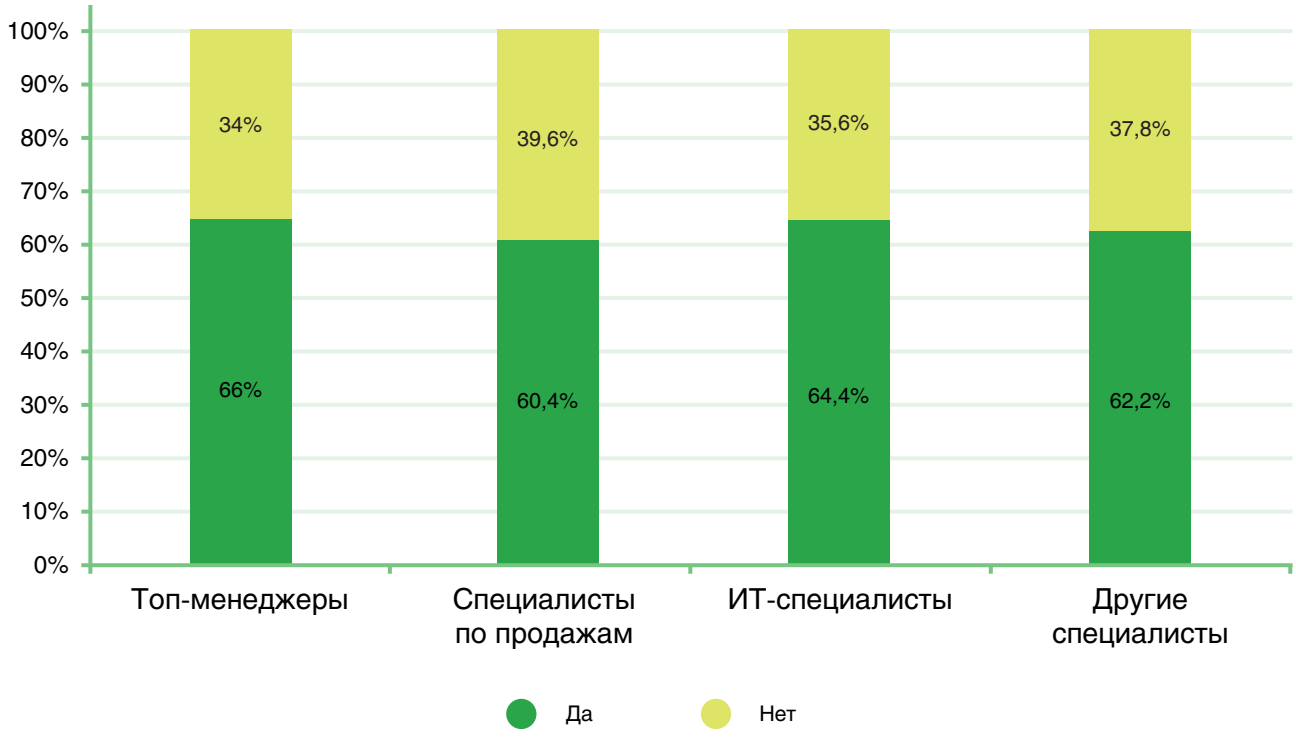
Конфиденциальность информации на мобильных устройствах

Как показали результаты исследования «Кода Безопасности», сотрудники, имеющие доступ к корпоративной информации с мобильного устройства, часто пренебрегают безопасностью устройства, что может стать причиной утечки данных. Рассмотрим несколько ситуаций.

Использование пароля

В случае потери первой линией защиты данных на мобильном устройстве будет блокировка экрана с помощью пароля. Применение парольной политики усложнит работу злоумышленникам и потребует от них большей квалификации для получения доступа к данным.

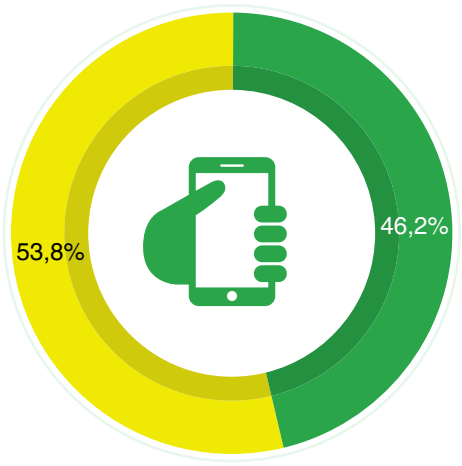
Каждый третий пользователь мобильного устройства не применяет пароль для блокировки экрана. Показатель при этом не зависит от категории пользователей: менеджеры и специалисты одинаково часто забывают применять эту базовую защиту на смартфонах и планшетах.



Конфиденциальность информации на мобильных устройствах

Передача устройства третьим лицам

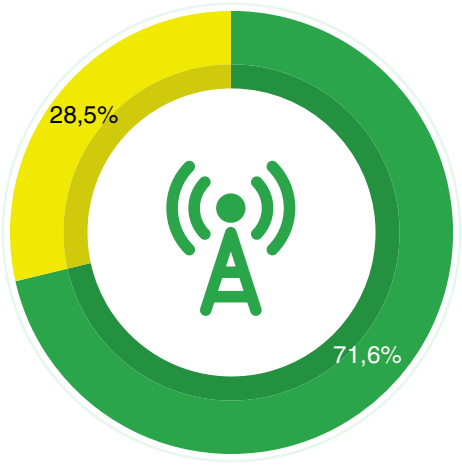
Несмотря на то что на телефоне могут храниться конфиденциальные данные, принадлежащие компании, почти половина респондентов передают телефон знакомым.



- Передают мобильные устройства третьим лицам
- Не передают мобильные устройства третьим лицам

Подключение к публичному Wi-Fi

Три четверти пользователей заходят в Интернет через публичные точки Wi-Fi.
Чем это опасно? Как выяснила компания Crowd Research Partners[3], около 20% пользователей подвергались взлому системы безопасности из-за использования мобильных устройств в первую очередь при подключении к вредоносным точкам доступа Wi-Fi. При этом подобные взломы могут не только коснуться личной информации конкретного пользователя, но и поставить под угрозу безопасность всей компании, в случае если сотрудник пользуется корпоративным устройством. Кроме того, после увольнения работников лишь 34% работодателей, участвовавших в опросе, удаляли важные данные. Это значит, что опасность потери конфиденциальной информации только увеличивается .



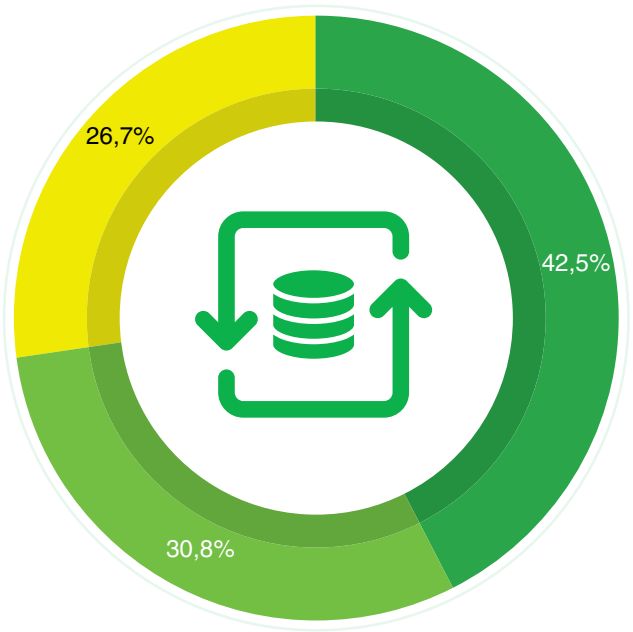
- Подключаются к публичному Wi-Fi
- Не подключаются к публичному Wi-Fi

Конфиденциальность информации на мобильных устройствах

Резервное копирование мобильных устройств

Потеря данных с мобильного устройства может привести не только к утечке конфиденциальной информации, но и к невозможности ее восстановления для продолжения работы. Регулярный backup устройства позволяет сотруднику при поломке или потере мобильного устройства максимально быстро вернуться к работе.

При этом лишь ¼ пользователей регулярно делают backup мобильных устройств. 42,5% респондентов не делают резервные копии своих устройств. В случае потери устройства им будет очень тяжело восстановить сохраненные на телефоне данные, контакты и настройки для доступа к корпоративным системам.



Не делают резервные копии мобильных устройств

Редко делают резервные копии мобильных устройств

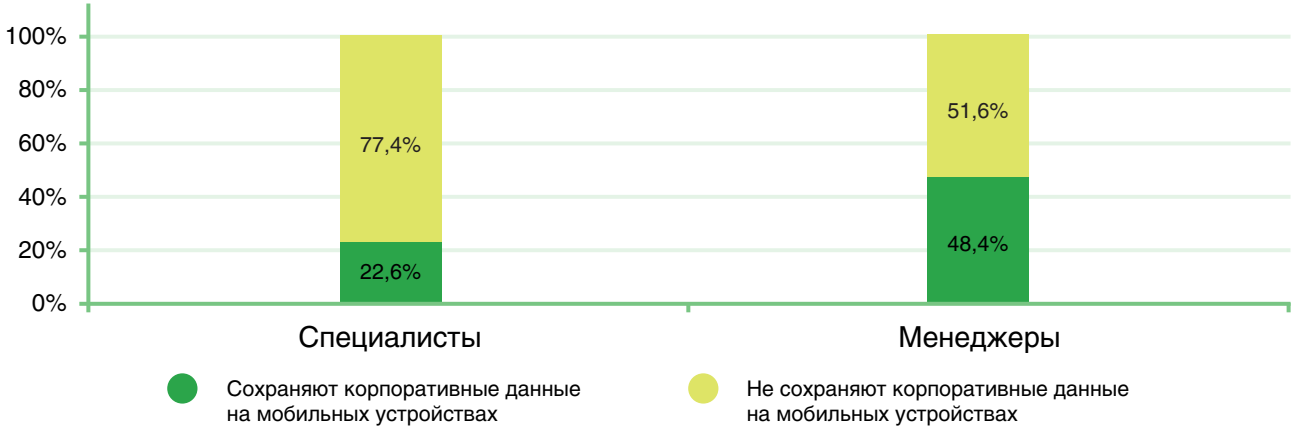
Делают регулярные резервные копии мобильных устройств

Конфиденциальность информации на мобильных устройствах

Сохранение корпоративных данных на мобильном устройстве

Сохранение данных на мобильном устройстве обеспечивает их доступность в случае отсутствия подключения к Интернету, но при этом создает дополнительные риски при потере или компрометации устройства.

Как показали результаты исследования, почти половина топ-менеджеров и менеджеров по продажам сохраняет данные локально на мобильный телефон. Эта цифра в 2 раза выше, чем у специалистов.

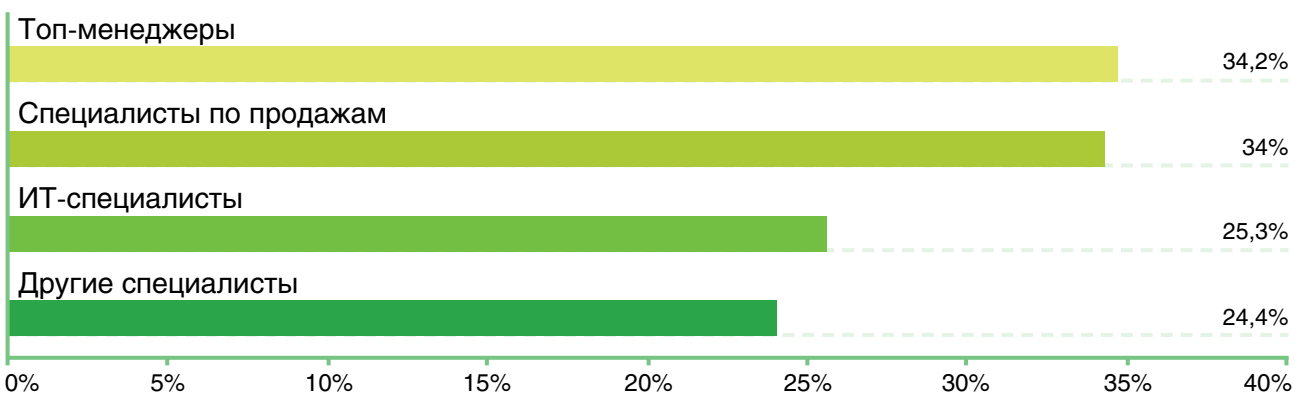


Обсуждение конфиденциальной информации

Потеря мобильного телефона или целенаправленная атака на него создаст серьезную угрозу конфиденциальности данных в случае, если переписка или устное обсуждение ведутся посредством незащищенных мобильных устройств и мессенджеров.

По результатам опроса, многие сотрудники компаний обсуждают конфиденциальную корпоративную информацию по телефону и в мобильных чатах. Наибольший процент приходится на топ-менеджеров (34,2%) и специалистов по продажам (34%).

Обсуждение конфиденциальной информации по телефону и в мессенджерах

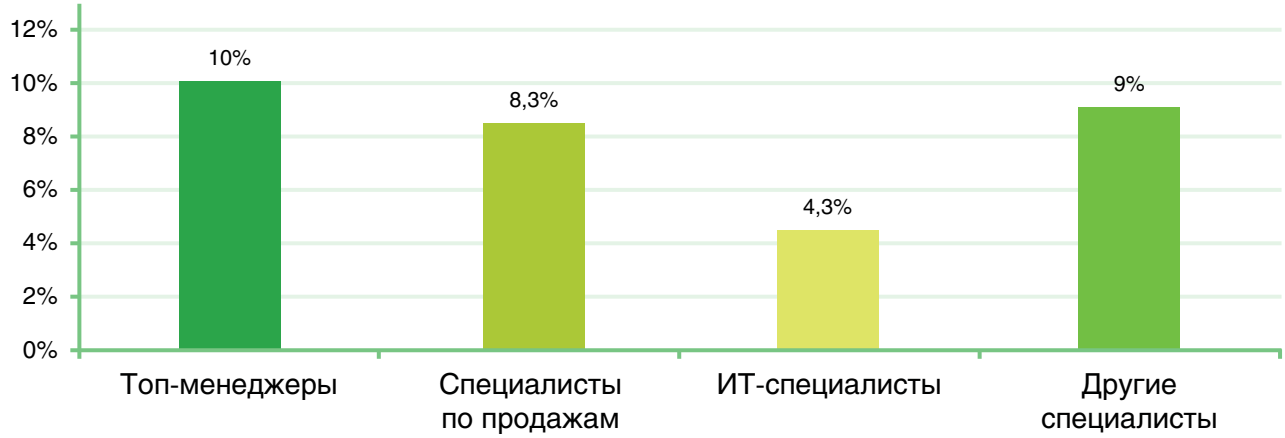


Конфиденциальность информации на мобильных устройствах

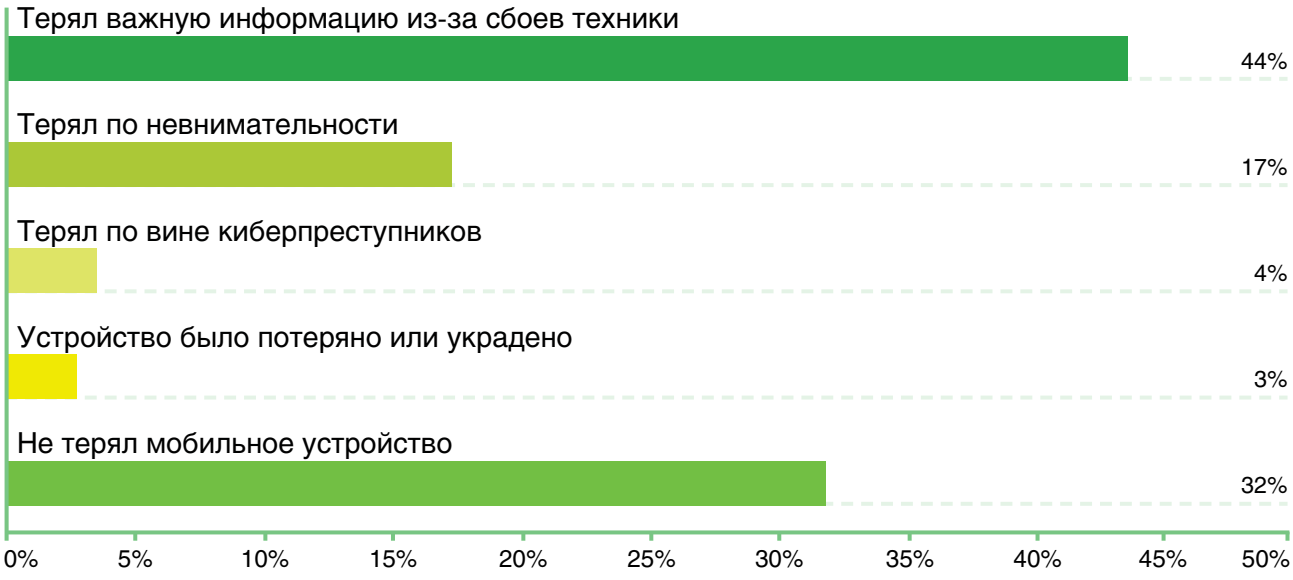
Потеря мобильных устройств

Один из основных рисков использования мобильного устройства – это его потеря. Пользователю необходимо время на то, чтобы купить или получить замену, восстановить данные из резервной копии (если она есть). Если на телефоне сохранились корпоративные данные или сохранились данные для доступа к корпоративным системам, это создает серьезные риски для организации.

На телефонах топ-менеджеров хранится большое количество конфиденциальной корпоративной информации, поэтому их устройства наиболее интересны злоумышленникам. Данные подтверждают и результаты опроса: 10% руководителей высшего звена хотя бы раз теряли свои мобильные устройства. Это в 2 раза чаще, чем потери устройств специалистами.



Приведем пример опроса, проведенного в марте 2016 г. Hi-Tech Mail.Ru. 4093 участникам был задан вопрос: «А вы когда-нибудь теряли важную информацию?» Как выяснилось, 2/3 респондентов хотя бы раз теряли мобильные устройства по различным причинам:



Безопасность мобильных операционных систем

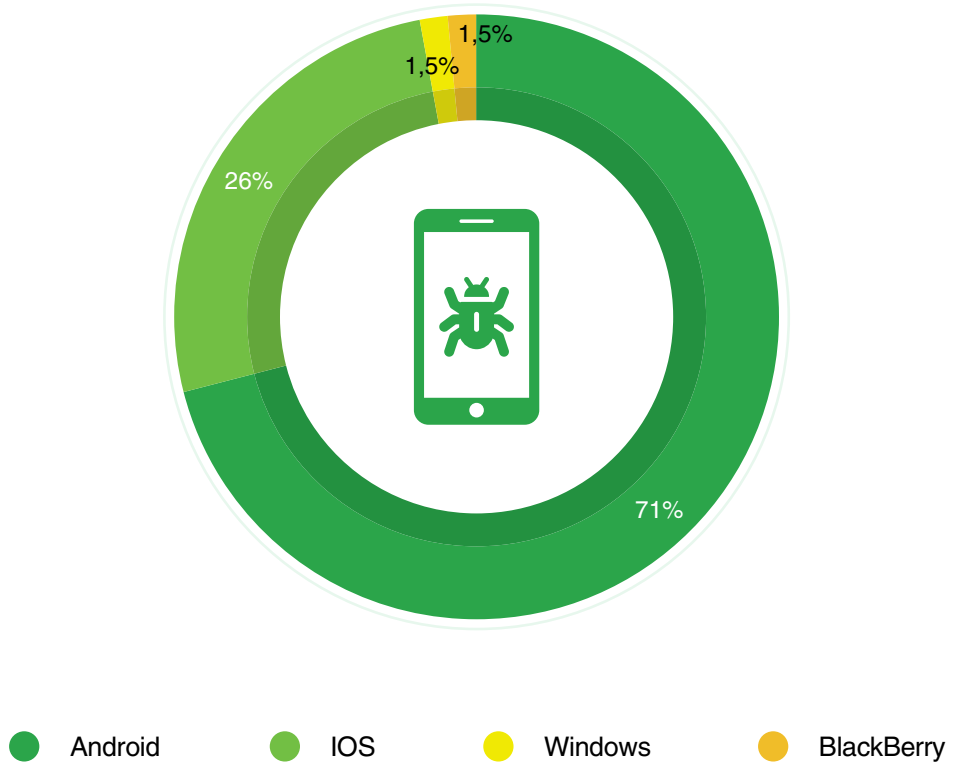
Уязвимости и вредоносные программы

По данным аналитиков «Кода Безопасности», за первое полугодие 2016 г. в российских СМИ были опубликованы 117 различных новостных статей о вредоносных программах для мобильных устройств и об обнаружении уязвимостей в мобильных ОС. «Лаборатория Касперского[4]» за тот же период обнаружила 7 834 597 вредоносных мобильных программ. Это означает, что СМИ осветили менее 1% информации о вредоносах.

Таким образом, люди, даже если они внимательно следят за новостями о мобильных вирусах, не могут самостоятельно защитить от них мобильные устройства по причине слабой осведомленности. Это также означает, что реальную безопасность обеспечивают только средства автоматизированного контроля уровня защищенности.

Большая часть упоминаний о вредоносных программах касается операционной системы Android – 71% всех публикаций. На втором месте по упоминаемости iOS от компании Apple.

Уязвимости мобильных операционных систем

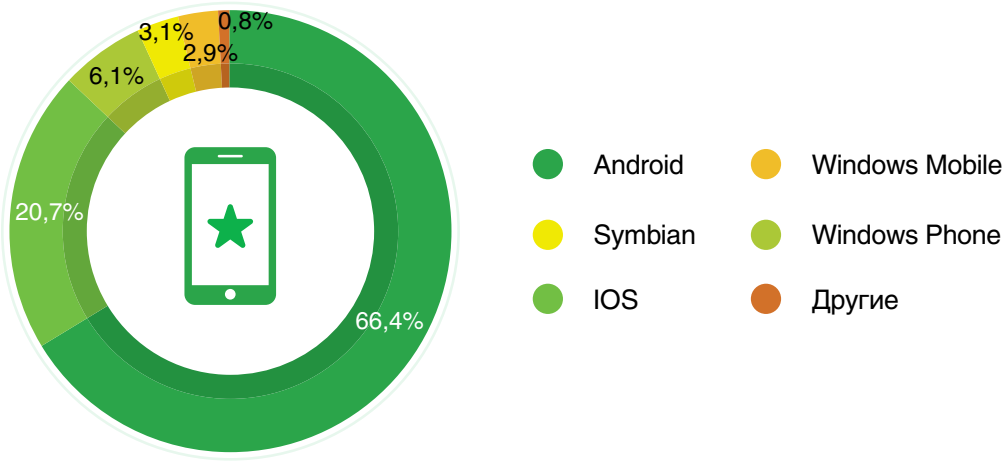


Безопасность мобильных операционных систем

Наиболее уязвимая операционная система Android одновременно является еще и наиболее популярной. 2/3 респондентов отметили, что для обработки корпоративной информации они используют мобильные устройства на базе ОС Android.

За первое полугодие 2016 г. в СМИ были опубликованы данные о заражении 1 105 084 848 устройств с данной операционной системой. Учитывая соотношение количества публикаций и реально существующих вирусов, можно сделать вывод: **устройства в течение полугода заражаются многократно.**

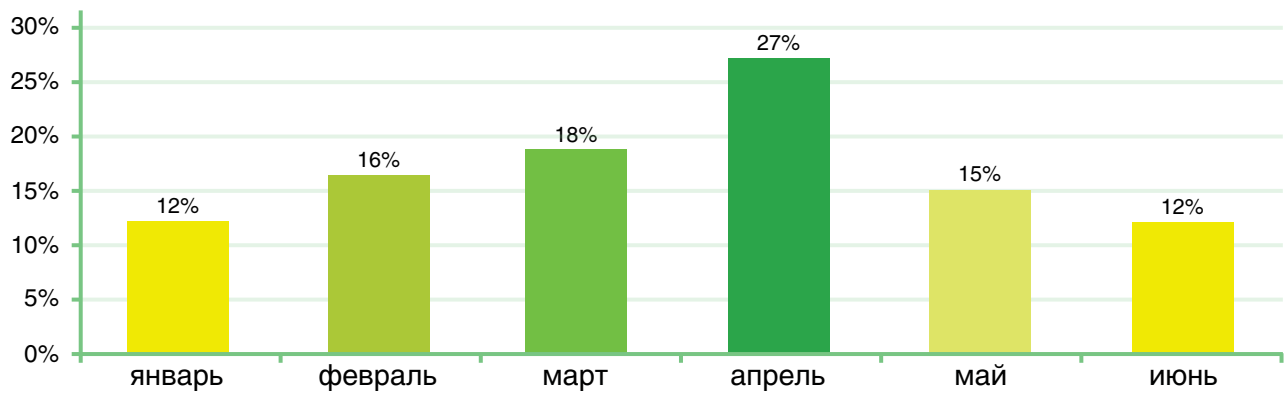
Популярность мобильных операционных систем



Аналитики «Кода Безопасности» подтверждают, что больше всего упоминаний уязвимостей Android было в апреле 2016 г.

Пик упоминаемости о появлении новых вредоносных программ для мобильных ОС в первом полугодии пришелся на апрель. В апреле также наблюдается пик бизнес-активности пользователей, что может свидетельствовать об усилении попыток злоумышленников получить конфиденциальную информацию.

Публикации об уязвимостях и вредоносных программах для мобильных ОС за 1 полугодие 2016 г.

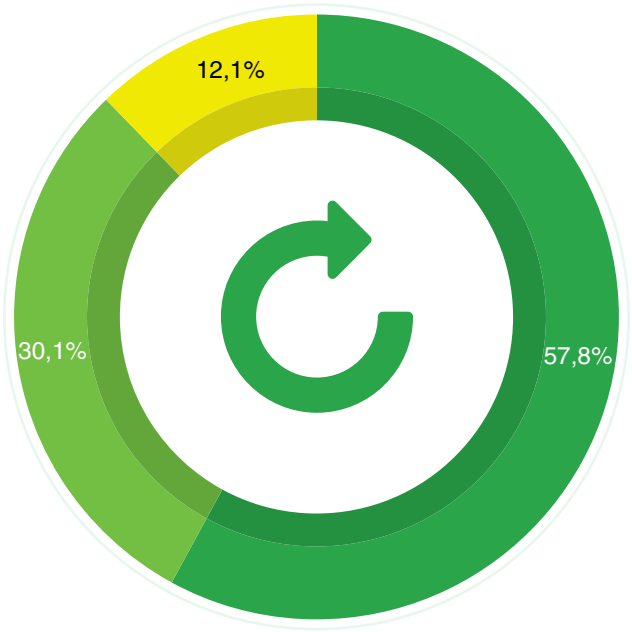


Безопасность мобильных операционных систем

Обновление мобильной операционной системы

Как показал анализ защищенности мобильных ОС, любые из них имеют 0day-уязвимости. Здесь производители устройств делятся на две категории: часть из них (например, Apple) постоянно работают над устранением уязвимостей и обновлениями ОС, другие же (работающие с ОС Android) довольно быстро прекращают поддержку и обновление версий системы для старых моделей мобильных устройств. В первом случае ответственность за обновление лежит на пользователе, во втором – на производителе, но результат применения устаревших версий операционных всегда один: злоумышленник может воспользоваться одним из множества выложенных в Интернет инструментов для взлома устройства.

По результатам исследования, почти половина пользователей (42%) по тем или иным причинам совсем не обновляет мобильную ОС, либо делает это редко. При этом более ответственной категорией пользователей являются топ-менеджеры: они на 25% чаще, чем специалисты, обновляют мобильную операционную систему.



Обновляют мобильную ОС сразу после выхода патча

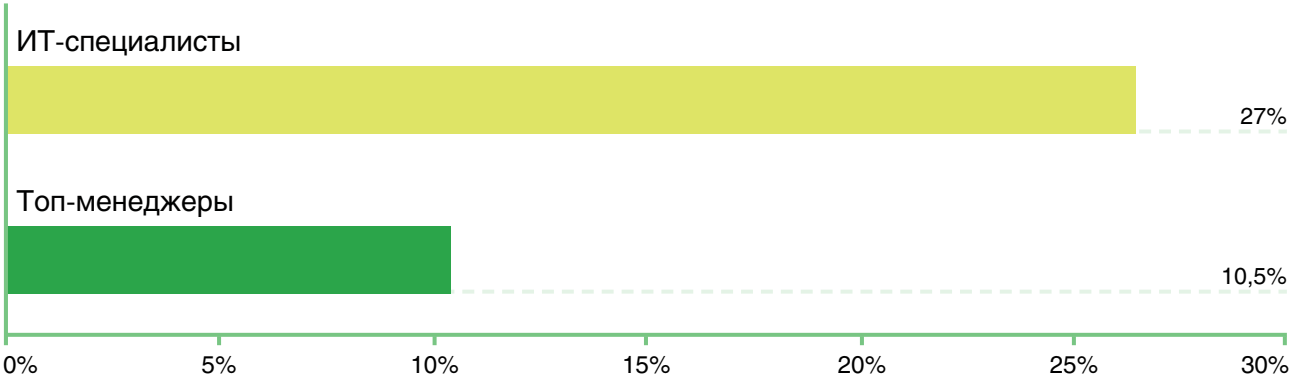
Редко обновляют мобильную ОС

Не обновляют мобильную ОС

Безопасность мобильных операционных систем

Jailbreak/Rooting мобильных устройств

Расширение стандартных прав пользователя мобильного устройства (Jailbreak для iOS или получение прав пользователя Root для Android) снижает уровень безопасности мобильного устройства. При этом многие предпочитают пренебречь безопасностью, особенно ИТ-специалисты: они в 3 раза чаще, чем топ-менеджеры, расширяют свои пользовательские права.



Корпоративная безопасность мобильных устройств

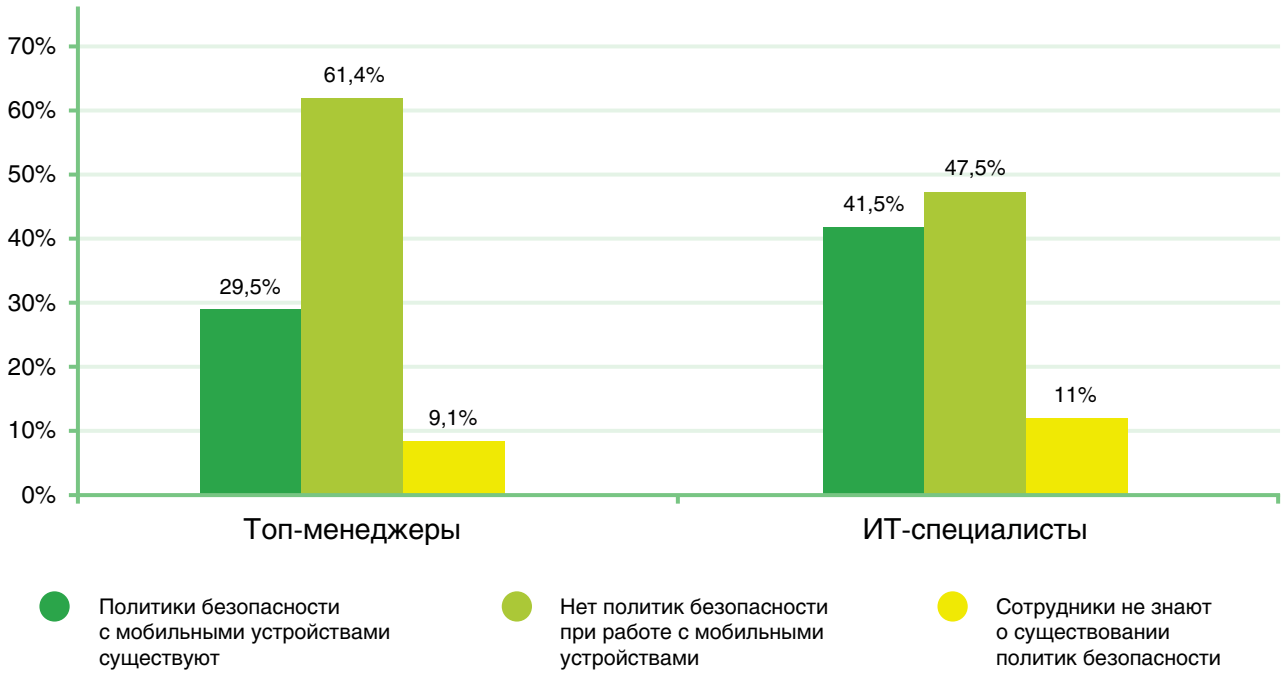
Обеспечение безопасности использования мобильных устройств в организации – зона ответственности ИБ-служб. Как показали результаты исследования, сами пользователи редко заботятся о конфиденциальности корпоративных данных. Рассмотрим, как обеспечивается защита на уровне организаций.

Политики безопасности

Наименее затратным способом снижения рисков являются организационные меры. Организация создает политику безопасности, в которой фиксирует требования к безопасности мобильных устройств своих сотрудников.

Но во многих ли компаниях разработаны политики безопасности при работе с мобильными устройствами? И соблюдают ли эти политики сотрудники? Респонденты сообщили, что в большинстве случаев политик просто не существует, а около 10% сотрудников не знают о существовании политик либо их игнорируют.

Данные по результатам опроса различаются для топ-менеджеров и ИТ-специалистов: первые в 70% случаев заявили об отсутствии политик (или об их незнании), вторые ответили аналогичным образом лишь в 58% случаев.

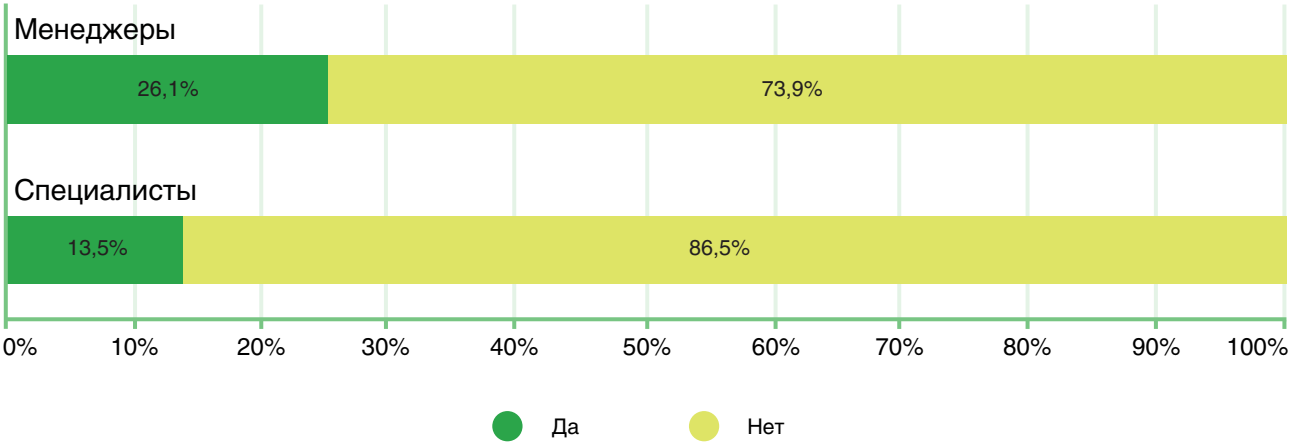


Полученные данные схожи с результатами опроса компании VMware[5], где только 41% сотрудников сообщили, что им известны все установленные их компанией мобильные политики. Остальные даже не знают, нарушают ли они эти правила или нет. Немаловажен тот факт, что более трети (35%) ИТ-директоров заявляют о том, что топ-менеджеры запрашивают доступ к корпоративным данным с личных мобильных устройств, даже если это идет вразрез с политикой безопасности.

Корпоративная безопасность мобильных устройств

Защищенные корпоративные приложения

Некоторые компании для доступа к конфиденциальным данным предоставляют сотрудникам специальные мобильные приложения: для хранения файлов, совместного просмотра документов, доступа к CRM, обеспечения видео-конференц-связи, обмена текстовыми сообщениями и др. Использование таких приложений в большинстве случаев обеспечивает соблюдение политик безопасности при работе с конфиденциальной информацией.
Как показали результаты исследования, менеджеры в 2 раза чаще используют специальные корпоративные приложения для хранения и обмена конфиденциальной информацией, чем специалисты. При этом уровень использования корпоративных сервисов в целом остается очень низким.

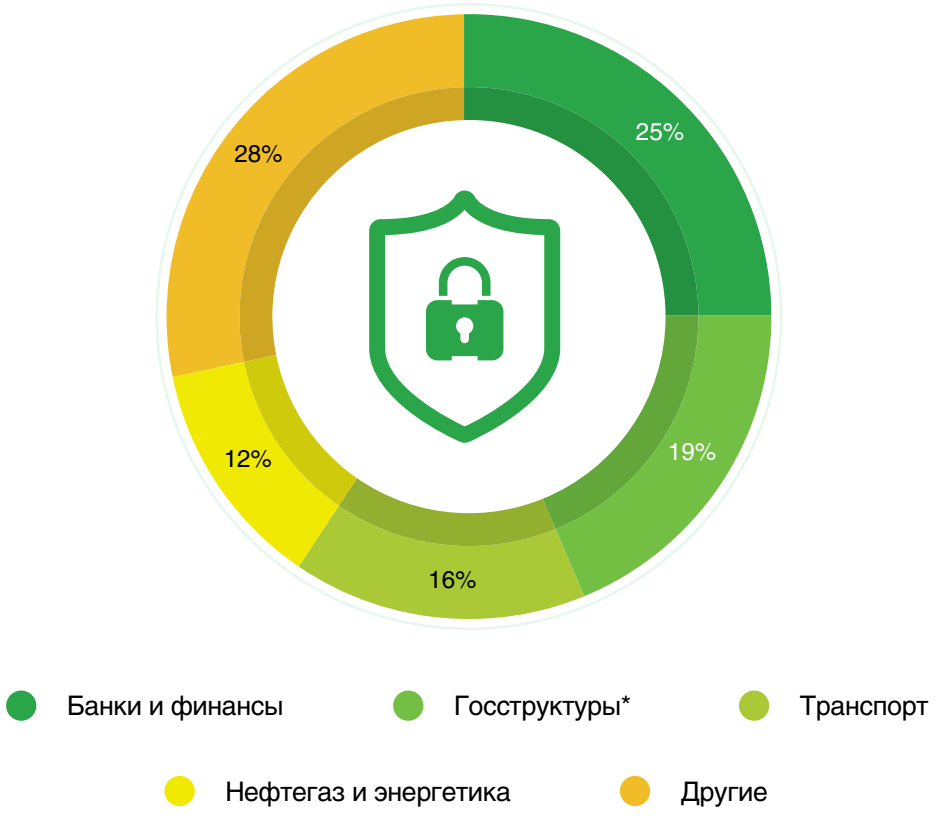


Корпоративная безопасность мобильных устройств

Использование системы управления и защиты мобильных устройств (MDM)

Для управления мобильными устройствами и защиты корпоративных данных в рамках организации одним из наиболее эффективных методов является использование специальных систем класса MDM (Mobile Device Management) или, как говорится в последних отчетах аналитиков Gartner, – EMM (Enterprise Mobility Management).
MDM-система, в первую очередь, позволяет централизованно управлять политиками безопасности на мобильных устройствах, что минимизирует участие пользователя в контроле состояния безопасности. Кроме того, MDM осуществляет централизованную установку корпоративных приложений, применение которых минимизирует риск утечки конфиденциальной информации.
Аналитики «Кода Безопасности» проанализировали внедрение MDM-систем в России и пришли к неутешительным выводам: на текущий момент лишь небольшое число компаний внедрили такие решения. В период с 2011 по 2016 -г. внедрения прошли в крупных банках, крупнейших телеком-операторах, госорганизациях, транспортных и ряде других компаний.

Распределение проектов внедрения MDM по отраслям

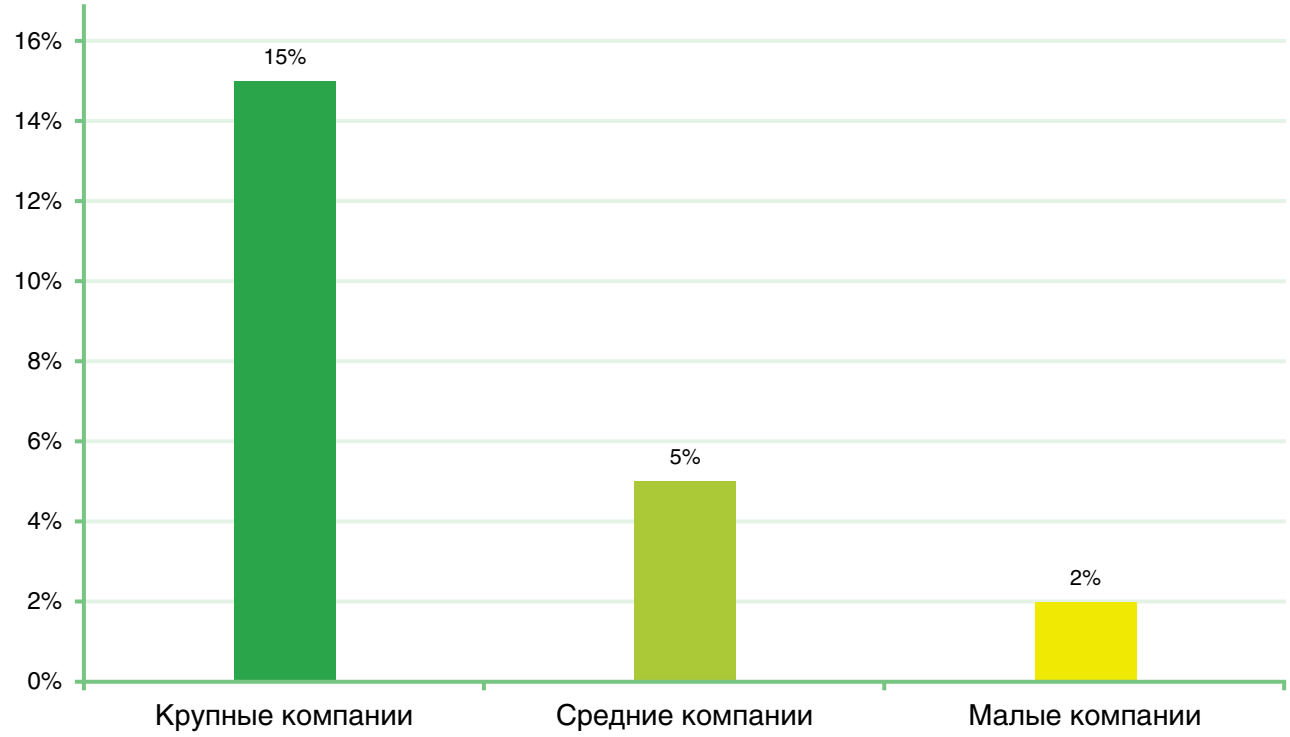


* Госструктуры – организации с полным или частичным гос. участием.

Корпоративная безопасность мобильных устройств

Анализ также показал, что большинство внедрений приходится на крупные компании развитых секторов экономики, где безопасности, в том числе и мобильной, уделяется больше внимания. Так, в компаниях с численностью сотрудников более 1000 система MDM внедрена у 15%. На средние и малые компании приходится 5% и 2% соответственно.

Внедрение MDM



Заключение

Применение мобильных устройств в работе помимо несомненной пользы в виде повышения продуктивности сотрудников может привести и к негативным последствиям – утечке конфиденциальной информации.

Утечка может происходить по нескольким причинам:

- невнимательное отношение пользователей к вопросам защиты данных (отсутствие пароля, передача смартфона третьим лицам и др.);
- отсутствие на мобильных устройствах базовых средств защиты и отказ от установки обновлений операционной системы;
- возможность перехвата мобильных сообщений, звонков и передаваемых файлов по незащищенным каналам связи (подключение к публичным точкам Wi-Fi, использование незащищенных приложений для звонков, сообщений и хранения файлов и др.);
- отсутствие или игнорирование сотрудниками корпоративных политик безопасности при работе с мобильными устройствами.

Единственным вариантом решения вопросов защиты корпоративных данных на мобильных устройствах является применение технического решения, которое обеспечит реализацию базовых политик безопасности, управляемость и защиту данных при потере устройства.

Стоит отметить, что поведение крупных компаний в части организации защиты мобильных устройств сильно отличается от SMB-сектора. Если первые хотя бы в четверти случаев предоставляют управляемые корпоративные устройства и разворачивают MDM-системы (15%), то вторые в большинстве случаев разрешают использовать личные мобильные устройства и не контролируют распространение конфиденциальной информации через них.

Однако есть и положительная тенденция: все больше компаний приходит к пониманию необходимости использования средств защиты и управления мобильными устройствами. На рынке появляется все больше MDM-решений, способных удовлетворить потребности одновременно крупного, среднего и малого бизнеса, прибегая к гибким политикам лицензирования продуктов.

[1] Результаты опроса руководителей IT-отделов и бизнес-подразделений, проведенного аналитиками IDC в 2015 г.

[2] Результаты опроса руководителей IT-отделов и бизнес-подразделений, проведенного аналитиками IDC в 2015 г.

[3] Результаты онлайн-опроса Crowd Research Partners (март 2016 г.).

[4] Исследование «Развитие информационных угроз» за 1 и 2 кварталы 2016 г. «Лаборатории Касперского».

[5] Результаты опроса VMware (июль 2016 г.).

Код Безопасности

«Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, облачных сред, мобильных устройств, а также коммерческой и государственной тайны. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

Тел.: +7 (495) 982 30 20

buy@securitycode.ru

www.securitycode.ru