О Т К Р Ы Т О Е П И С Ь М О

О безопасности мобильных технологий

Уважаемые коллеги!

Межрегиональная общественная организация «Ассоциация руководителей служб информационной безопасности» (АРСИБ) совместно с экспертами по информационной безопасности представила результаты анализа рисков использования мобильных устройств в корпоративной среде.

Мобильные устройства стали неотъемлемой частью бизнес-процессов компаний и государственных организаций, и важным инструментом по повышению эффективности работы сотрудников. Начиная с декабря 2016 г. тема информационных технологий и обеспечения их безопасности постоянно была в центре внимания, принят ряд нормативных документов, направленных на повышение уровня информационной безопасности:

1. Доктрина информационной безопасности Российской Федерации.
2. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы.
3. Программа «Цифровая экономика Российской Федерации».
4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и сопутствующие ему нормативно-правовые акты: Указы Президента РФ, Постановления Правительства РФ, документы ФСБ России и ФСТЭК России.

Также внесены изменения в ранее принятые Федеральные Законы «Об информации, информационных технологиях и о защите информации», «О связи», «О персональных данных».

Такое внимание к вопросам обеспечения информационной безопасности обусловлено усилением противостояния в киберпространстве, о чем свидетельствуют события последнего времени.

Задачи обеспечения информационной безопасности в полной мере относятся и к мобильным технологиям. При этом стремительно развивающиеся мобильные технологии влекут новые вызовы и угрозы, что обусловлено, в том числе, их специфическими особенностями:

– для мобильных технологий понятие «периметр контролируемой зоны» отсутствует;
– существует потенциальная возможность неограниченного во времени и в пространстве несанкционированного доступа к мобильному устройству.

Кроме того, мобильные технологии, как и Интернет, могут использоваться как инструмент для совершения различных противоправных действий.

Притом, что количество киберпреступлений, совершаемых, в том числе, и с использованием мобильных технологий, возросло, повысился и уровень ответственности работников в области информационной безопасности.

Эксперты АРСИБ проанализировав сложившуюся ситуацию, пришли к выводу, что использование мобильных устройств под управлением ОС Google Android для федеральных, муниципальных и иных органов исполнительной и законодательной власти, государственных учреждений и компаний с государственным участием, особенно для тех из

них, в которых мобильные технологии используются в критической информационной инфраструктуре, государственных информационных системах и информационных системах персональных данных небезопасно в силу следующих ключевых факторов**:**

1. Высокая популярность среди пользователей.
2. Низкая вероятность своевременного выхода и установки обновлений ОС для устройств под управлением ОС Google Android.
3. Архитектура и правовая политика Google в отношении операционной системы ОС Google Android не позволяет полноценно управлять передачей пользовательских и технических данных.
4. Лицензионные и санкционные риски: компания-разработчик ОС имеет право в одностороннем порядке изменить функционал и условия использования ОС или ограничить ее использование на определенных территориях или категорией пользователей.
5. Исходный код системы или некоторых ее компонент, в том числе сторонних разработчиков не позволяет провести проверку на отсутствие НДВ. А также верификация источника (магазина) приложений.

Более 90% известного вредоносного кода создано для ОС Google Android. Кроме того, количество уязвимостей для мобильных ОС прямо пропорционально их распространенности.

Риски и угрозы, связанные с использованием мобильных технологий в корпоративном секторе, могут быть минимизированы следующим образом:

1. Применением систем управления мобильными устройствами и приложениями, реализующих какую-либо форму контейнера, и средств криптографической защиты информации на стороне мобильного устройства.
2. Использованием мобильных платформ и систем управления ими, содержащих встроенные средства защиты, включая криптографические.

При этом желательно, чтобы применяемые средства защиты, как на уровне мобильного устройства, так и на уровне системы управления, были сертифицированы соответствующим регулятором. Эксперты АРСИБ не рекомендуют использовать мобильные технологии в бизнес-процессах с использованием мобильных устройств под управлением как ОС Google Android, и ОС Apple iOS, без дополнительных мер защиты.

Рекомендации, как и приведенные выше риски, в полной мере распространяются и на другую мобильную ОС – iOS, устанавливаемую только на мобильные устройства компании Apple, несмотря на декларируемую этой компанией политику защиты пользовательских данных.

Наряду с техническими мерами защиты необходимо применять и организационные (политика безопасности), которые, не заменяя технических, позволяют достаточно эффективно минимизировать риски и противодействовать угрозам, специфичным для мобильных технологий.

Более подробную информацию по теме, а также обзор некоторых российских и зарубежных систем управления и практические рекомендации можно узнать из брошюры «Безопасность мобильных технологий. Общие рекомендации», версия 2.0.

Будьте бдительны и внимательны при использовании мобильных технологий, особенно в тех случаях, когда они реализуют критичные бизнес-процессы!