МОБИЛЬНЫЕ УСТРОЙСТВА В ИНФОРМАЦИОННЫХ СИСТЕМАХ И УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВЗАИМОСВЯЗИ

***Сидак Алексей Александрович**, кандидат технических наук,*
старший научный сотрудник
Ильин Александр Валентинович
Кубарев Алексей Валентинович

Основной задачей настоящей статьи явилось определение зависимостей между наиболее вероятными специфичными угрозами безопасности информации, содержащейся в информационных системах, при доступе к ним с помощью мобильных устройств и условиями эксплуатации мобильных устройств.

Указанные зависимости определяются впервые.

Для решения поставленной задачи в статье определяются свойства мобильных устройств, влияющие на безопасность информации, условия эксплуатации мобильных устройств, влияющие на безопасность информации, рассматриваются все возможные комбинации указанных условий и для каждой из них определяются наиболее вероятные угрозы безопасности информации.

***Ключевые слова**: мобильные устройства, МУ, безопасность информации, информационные системы, ИС, угрозы безопасности информации, ИСПДн, ГИС, информационные системы персональных данных, государственные информационные системы, модель угроз, свойства мобильных устройств, условия эксплуатации мобильных устройств.*

MOBILE DEVICES IN INFORMATION SYSTEMS AND INFORMATION SECURITY THREATS. INTERCONNECTIONS

***Alexey Sidak**, Ph.D., Associate Professor*
Ilyin Alexander
Kubarev Alexey

The main objective of this article is determination of relations between the most possible specific threats of security of information, containing in information systems, making access to them using mobile devices, and conditions of exploitation of mobile devices.

These relations are determining for the first time.

There are properties of mobile devices, affecting information security, conditions of exploitation of mobile devices, affecting information security, are determining in this article for solving the objective. All possible combinations of specified conditions are considering. There are most possible information security threats are determining for each of combination.

***Keywords**: mobile devices, MD, information security, information systems, IS, information security threats, PDIS, SIS, personal data information systems, state information systems, threat model, mobile devices properties, mobile devices exploitation conditions.*

Введение

К мобильным устройствам принято относить носимые электронные вычислительные машины, обладающие компактными размерами и имеющие каналы коммуникаций с информационными системами или их узлами.

Мобильные устройства в настоящее время являются полноценными вычислительными устройствами, поддерживающими большую часть функционала традиционных электронных вычислительных машин при значительно меньших размерах, что позволяет обрабатывать информацию удаленно и оперативно, сократив затраты времени на перемещение до стационарной рабочей станции, имея мобильную рабочую станцию всегда при себе [6].

Все чаще для доступа к информационным системам используются мобильные устройства, что позволяет операторам информационных систем повысить эффективность использования информационных систем, ликвидировав их простои [7].

Вместе с тем, использование мобильных устройств для доступа к защищаемой информации, содержащейся в информационных системах, порождает дополнительные, специфические угрозы её безопасности [7, 5].

Характерные свойства мобильных устройств

Ввиду того, что мобильные устройства являются электронными вычислительными машинами, им присущи многие свойства традиционных (не носимых, стационарных) электронных вычислительных машин, определяющие их слабые места с точки зрения безопасности информации, в том числе:

1) возможность утечек по техническим каналам;
2) возможность визуального считывания с дисплея устройства;
3) наличие встроенной памяти;
4) возможное наличие уязвимостей в программном и аппаратном обеспечении.

Особенностями мобильных устройств, определяющими специфические для них угрозы безопасности информации, являются [3]:

1) носимость (возможность выноса за пределы контролируемой зоны и возврата в контролируемую зону);
2) компактные размеры;
3) наличие проводных и беспроводных интерфейсов, с помощью которых возможно подключение к различной информационной инфраструктуре за пределами информационной системы;
4) возможность использования в качестве модема для подключения к сетям связи общего пользования;
5) возможность использования в качестве съемного носителя информации.

Специфические угрозы безопасности информации

В силу указанных особенностей мобильных устройств, информационные системы, к которым имеют доступ мобильные устройства, имеют следующие специфические угрозы безопасности информации [2, 4, 8]:

1. Нарушение конфиденциальности, целостности или доступности информации, содержащейся в информационных системах, вследствие кражи или утери мобильных устройств, имеющих доступ к данным информационным системам.

Данная угроза имеет высокую вероятность реализации в том случае, если мобильное устройство, содержащее защищаемую информацию в собственной памяти, используется за пределами территории, на которой действуют организационные меры защиты информации (вне контролируемой зоны).

2. Нарушение конфиденциальности, доступности и целостности информации, содержащейся в информационных системах, вследствие перехвата данных, передаваемых по каналам связи, используемым мобильными устройствами.

Данная угроза имеет высокую вероятность реализации в том случае, если для информационного обмена используется канал связи, который не обеспечивает необходимую степень уверенности в обеспечении конфиденциальности и (или) целостности передаваемых данных (недоверенный канал связи).

3. Нарушение конфиденциальности информации, содержащейся в информационных системах, вследствие прослушивания переговоров, осуществляемых при помощи мобильных устройств.

Данная угроза имеет высокую вероятность реализации в том случае, если мобильное устройство используется для передачи информации, содержащейся в информационной системе, в виде речевого сигнала, не является доверенным, или используется для указанной цели вне контролируемой зоны.

4. Нарушение конфиденциальности информации, содержащейся в информационных системах, вследствие ознакомления с информацией с экранов мобильных устройств при доступе к ней из публичных мест.

Данная угроза имеет высокую вероятность реализации в том случае, если мобильное устройство используется вне контролируемой зоны.

5. Нарушение конфиденциальности информации, содержащейся в информационных системах, вследствие её копирования на незащищенные носители информации мобильных устройств.

Данная угроза имеет высокую вероятность реализации в том случае, если для доступа к защищаемой информации, содержащейся в информационной системе, используется недоверенное мобильное устройство.

6. Нарушение конфиденциальности информации, содержащейся в информационных

системах, вследствие её утечки по техническим каналам.

Данная угроза имеет высокую вероятность реализации в тех случаях, если для обработки защищаемой информации, содержащейся в информационной системе, используется недоверенное мобильное устройство, или если обработка информации осуществляется вне контролируемой зоны.

7. Нарушение конфиденциальности, целостности или доступности информации, содержащейся в информационных системах, вследствие эксплуатации уязвимостей программного и аппаратного обеспечения мобильных устройств, имеющих доступ к данным информационным системам, и используемых ими протоколов передачи данных, внедрения в них вредоносного программного обеспечения.

Данная угроза имеет высокую вероятность реализации в том случае, если для доступа к защищаемой информации, содержащейся в информационной системе, используется недоверенное мобильное устройство.

8. Нарушение конфиденциальности, целостности или доступности информации, содержащейся в информационных системах, вследствие нелегитимного использования мобильных устройств в качестве носителей информации или модемов для подключения к сетям связи общего пользования.

Данная угроза имеет высокую вероятность реализации в тех случаях, если в пределах контролируемой зоны используются недоверенные мобильные устройства.

Условия эксплуатации мобильных устройств, влияющие на безопасность информации

В целях выработки мер по защите информации, содержащейся в информационной системе, при доступе к ней мобильных устройств, осуществляется моделирование угроз безопасности информации информационной системы.

При этом целесообразно учитывать следующие условия использования мобильных устройств: доверенность мобильного устройства, расположение мобильного устройства относительно границ контролируемой зоны, наличие удаленного подключения мобильного устройства к информационной системе и доверенность канала связи в случае наличия удаленного подключения.

Варианты эксплуатации мобильных устройств и наиболее вероятные угрозы безопасности информации

Набор комбинаций указанных условий эксплуатации мобильного устройства, имеющего доступ к информационной системе, составляет следующие случаи использования мобильного устройства для доступа к информационной системе:

1. Доверенное мобильное устройство используется для доступа к информации, содержащейся в информационной системе, из контролируемой зоны по доверенному каналу связи.

Примером такого случая может являться удаленный доступ с корпоративного мобильного устройства из контролируемой зоны удаленного офиса к основной инфраструктуре информационной системы через доверенный канал связи.

В указанном случае высокую вероятность имеет нарушение доступности информации, передаваемой по каналу связи между мобильным устройством и информационной системой.

2. Доверенное мобильное устройство используется для доступа к информации, содержащейся в информационной системе, из контролируемой зоны по недоверенному каналу связи.

Примером такого случая может являться удаленный доступ с корпоративного мобильного устройства из контролируемой зоны удаленного офиса к основной инфраструктуре информационной системы через недоверенный канал связи (интернет без использования необходимых средств защиты информации).

В указанном случае высокую вероятность имеет нарушение доступности, целостности и конфиденциальности информации, передаваемой по каналу связи между мобильным устройством и информационной системой.

3. Доверенное мобильное устройство используется для автономной обработки или хранения защищаемой информации, предварительно загруженной в память мобильного устройства из информационной системы, в пределах контролируемой зоны без подключения к информационной системе.

Примером такого случая может являться автономное использование корпоративного мобильного устройства с содержащейся в его памяти защищаемой информации в пределах офиса.

В указанном случае количество угроз безопасности информации, имеющих высокую вероятность реализации, существенно ограничено.

4. Недоверенное мобильное устройство используется для автономной обработки или хранения защищаемой информации, предварительно загруженной в память мобильного устройства из информационной системы, в пределах контролируемой зоны без подключения к информационной системе.

Примером такого случая может являться автономное использование личного мобильного устройства с содержащейся в его памяти защищаемой информации в пределах офиса.

В указанном случае высокую вероятность имеет нарушение конфиденциальности, целостности и доступности информации, предварительно загруженной в память мобильного устройства из информационной системы, обрабатываемой и хранимой на мобильном устройстве.

5. Мобильное устройство используется для автономной обработки или хранения защищаемой информации, предварительно загруженной в память мобильного устройства из информационной системы, за пределами контролируемой зоны без подключения к информационной системе.

Примером такого случая может являться автономное использование личного или корпоративного мобильного устройства с содержащейся в его памяти защищаемой информации за пределами офиса.

В указанном случае высокую вероятность имеет нарушение конфиденциальности, целостности и доступности информации, предварительно загруженной в память мобильного устройства из информационной системы, обрабатываемой и хранимой на мобильном устройстве.

6. Доверенное мобильное устройство используется для доступа к информации, содержащейся в информационной системе, вне контролируемой зоны по доверенному каналу связи.

Примером такого случая может являться использование корпоративного мобильного устройства для удаленного доступа в инфраструктуру информационной системы при нахождении в местах общего пользования (аэропорт, ресторан и т.п.) с использованием защищенного канала связи (Интернет с использованием средств защиты информации для защиты передаваемой информации).

В указанном случае высокую вероятность имеет нарушение доступности, целостности и конфиденциальности информации, предварительно загруженной в память мобильного устройства из информационной системы, хранимой и обрабатываемой на мобильном устройстве, нарушение доступности информации, передаваемой по каналу связи между мобильным устройством и информационной системой.

7. Доверенное мобильное устройство используется для доступа к информации, содержащейся в информационной системе, вне контролируемой зоны по недоверенному каналу связи.

Примером такого случая может являться использование корпоративного мобильного устройства для удаленного доступа в инфраструктуру информационной системы при нахождении в местах общего пользования (аэропорт, ресторан и т.п.) с использованием незащищенного канала связи (интернет без использования необходимых средств защиты информации).

В указанном случае высокую вероятность имеет нарушение доступности, целостности и конфиденциальности информации, предварительно загруженной в память мобильного устройства из информационной системы, хранимой и обрабатываемой на мобильном устройстве, нарушение доступности, целостности и конфиденциальности информации, передаваемой по каналу связи между мобильным устройством и информационной системой.

8. Недоверенное мобильное устройство используется для доступа к информации, содержащейся в информационной системе, из контролируемой зоны по доверенному каналу связи.

Примером такого случая может являться удаленный доступ с личного мобильного устройства из контролируемой зоны удаленного офиса к основной инфраструктуре информационной системы через доверенный канал связи.

В указанном случае высокую вероятность имеет нарушение доступности, целостности и конфиденциальности информации, хранимой и обрабатываемой в информационной системе, нарушение доступности информации, передаваемой по каналу связи между мобильным устройством и информационной системой, нарушение конфиденциальности, целостности и доступности информации, предварительно загруженной в память мобильного устройства из информационной системы, обрабатываемой и хранимой на мобильном устройстве.

9. Недоверенное мобильное устройство используется для доступа к информации, содержащейся в информационной системе, из контролируемой зоны по недоверенному каналу связи.

Примером такого случая может являться удаленный доступ с личного мобильного устройства из контролируемой зоны удаленного офиса к основной инфраструктуре информационной системы через недоверенный канал связи (интернет без использования необходимых средств защиты информации).

В указанном случае высокую вероятность имеет нарушение доступности, целостности и конфиденциальности информации, хранимой

и обрабатываемой в информационной системе, нарушение доступности, целостности и конфиденциальности информации, передаваемой по каналу связи между мобильным устройством и информационной системой, нарушение конфиденциальности, целостности и доступности информации, предварительно загруженной в память мобильного устройства из информационной системы, обрабатываемой и хранимой на мобильном устройстве.

10. Недоверенное мобильное устройство используется для доступа к информации, содержащейся в информационной системе, вне контролируемой зоны по доверенному каналу связи.

Примером такого случая может являться использование личного мобильного устройства для удаленного доступа в инфраструктуру информационной системы при нахождении в местах общего пользования (аэропорт, ресторан и т.п.) с использованием защищенного канала связи (интернет с использованием средств защиты информации для защиты передаваемой информации).

В указанном случае высокую вероятность имеет нарушение доступности, целостности и конфиденциальности информации, хранимой и обрабатываемой в информационной системе, нарушение доступности информации, передаваемой по каналу связи между мобильным устройством и информационной системой, нарушение конфиденциальности, целостности и доступности информации, предварительно загруженной в память мобильного устройства из информационной системы, обрабатываемой и хранимой на мобильном устройстве.

11. Недоверенное мобильное устройство используется для доступа к информации, содержащейся в информационной системе, вне контролируемой зоны по недоверенному каналу связи.

Примером такого случая может являться использование личного мобильного устройства для удаленного доступа в инфраструктуру информационной системы при нахождении в местах общего пользования (аэропорт, ресторан и т.п.) с использованием незащищенного канала связи (интернет без использования необходимых средств защиты информации).

В указанном случае высокую вероятность нарушение доступности, целостности и конфиденциальности информации, хранимой и обрабатываемой в информационной системе, нарушение доступности, конфиденциальности, целостности информации, передаваемой по каналу связи между мобильным устройством и информационной системой, нарушение конфиденциальности, целостности и доступности информации, предварительно загруженной в память мобильного устройства из информационной системы, обрабатываемой и хранимой на мобильном устройстве.

Выводы

Итак, мобильные устройства обладают основными свойствами традиционных (не носимых, стационарных) электронных вычислительных машин, что обусловило наследование мобильными устройствами основных угроз безопасности информации, присущих традиционным электронным вычислительным машинам.

Вместе с тем, мобильные устройства имеют свои особенности по отношению к другим классам электронных вычислительных машин, что обуславливает наличие специфических для них угроз безопасности информации.

В ходе анализа условий, при которых специфические угрозы безопасности информации, содержащейся в информационных системах, при доступе к ним при помощи мобильных устройств, имеют высокую вероятность реализации, выявлено, что основными условиями эксплуатации мобильных устройств, влияющими на безопасность информации являются: доверенность мобильного устройства, расположение мобильного устройства относительно границ контролируемой зоны, наличие удаленного подключения мобильного устройства к информационной системе и доверенность канала связи в случае наличия удаленного подключения.

Как показывает анализ вариантов эксплуатации мобильных устройств для доступа к информации, содержащейся в информационных системах, мобильные устройства почти во всех случаях создают дополнительные существенные угрозы безопасности информации.

Представленные условия эксплуатации мобильных устройств и соответствующие им угрозы безопасности информации целесообразно учитывать при моделировании угроз безопасности информации, содержащейся в информационных системах, к которым имеют доступ мобильные устройства, а также при выборе организационных и технических мер защиты информации, обрабатываемой в информационных системах.

Литература

1. Безкоровайный Д. Безопасность мобильных устройств//ОТКРЫТЫЕ СИСТЕМЫ. СУБД, М: Издательство «Открытые системы», 2011. – 26 с.
2. Бельтов А.Г., Жуков И.Ю., Новицкий А.В., Михайлов Д.М., Стариковский А.В. Вопросы безопасности мобильных устройств// Безопасность информационных технологий М.: Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации, 2012. - 5-7 с.
3. Ванг Й., Стрефф К., Раман С. Проблемы безопасности смартфонов//ОТКРЫТЫЕ СИСТЕМЫ. СУБД, М: Издательство «Открытые системы», 2013. – 27-31 с.
4. Генералов Д. Н, Шлегель О. А. Идентификация скрытых каналов утечки информации при инсталляции инсайдера в мобильное устройство//Вестник поволжского государственного университета сервиса. Серия: экономика Тольятти: Поволжский государственный университет сервиса, 2009. – 25-31 с.
5. Михайлов Д. М., Жуков И. Ю., Ивашко А. М. Защита мобильных телефонов от атак М.: Фойлис, 2011. -192 с.
6. Орлов А., Подвижные и опасные//Журнал «CIO: руководитель информационной службы» - № 12, 2011. – 13-15 с.
7. Панасенко А. Влияние мобильных устройств на безопасность информации, http://www.anti-malware.ru/node/12301, 2013.
8. Хаккарайнен А., Как защититься от мобильных угроз//Computerworld Россия – № 24, 2007. – 32-34 с.

References

1. Bezkorovajnyj D. Bezopasnost' mobil'nyh ustrojstv (Safety of mobile devices)//OTKRYTYE SISTEMY. SUBD (OPEN SYSTEMS. DBMD), M: Izdatel'stvo «Otkrytye sistemy», 2011. – 26 P.
2. Bel'tov A.G., Zhukov I.Ju., Novickij A.V., Mihajlov D.M., Starikovskij A.V. Voprosy bezopasnosti mobil'nyh ustrojstv (Questions of mobile devices safety)//Bezopasnost' informacionnyh tehnologij (Safety of information technologies) M.: Vserossijskij nauchno-issledovatel'skij institut problem vychislitel'noj tehniki i informatizacii, 2012. - 5-7 P.
3. Vang J., Streff K., Raman S. Problemy bezopasnosti smartfonov (Problems of smartphones safety)//OTKRYTYE SISTEMY. SUBD (OPEN SYSTEMS. DBMD), M: Izdatel'stvo «Otkrytye sistemy», 2013. – 27-31 P.
4. Generalov D. N, Shlegel' O. A. Identifikacija skrytyh kanalov utechki informacii pri installjacii insajdera v mobil'noe ustrojstvo (Identification of hidden information leak channels while insider is installed in mobile device)// Vestnik povolzhskogo gosudarstvennogo universiteta servisa. Serija: jekonomika (Gazette of Volga region state university of service. Series: Economics) Tolyatti: Povolzhskij gosudarstvennyj universitet servisa, 2009. – 25-31 P.
5. Mihajlov D.M., Zhukov I.Ju., Ivashko A.M. Zashhita mobil'nyh telefonov ot atak (Mobile phone protection against attacks) M.: Fojlis, 2011. -192 P.
6. Orlov A., Podvizhnye i opasnye (Mobile and dangerous)// Zhurnal «CIO: rukovoditel' informacionnoy sluzhby» («CIO: Chief Information Officer» Journal) - № 12, 2011. – 13-15 P.
7. Panasenko A. Vlijanie mobil'nyh ustrojstv na bezopasnost' informacii (Mobile devices influence on information security), http://www.anti-malware.ru/node/12301, 2013.
8. Hakkarajnen A., Kak zashhitit'sja ot mobil'nyh ugroz (How to protect yourself against mobile threats)//Computerworld Rossija (Computerworld Russia) – № 24, 2007. – 32-34 с.