web-портале Банка или через интерфейс мобильного телефона из любой точки мира 24 часа в сутки, 7 дней в неделю [1].

Одновременно с АКБ «Балтика» украинский Приватбанк (филиалы и партнёры в 12 странах) предложил [2] своим клиентам 5 основных (есть и дополнительные) мобильных приложений для платежей со смартфонов. Это 1) Privat24 – приложение для проведения любых финансовых операций с деньгами и картами вне зависимости от дня недели, времени и местонахождения; 2) iPay – позволяет принимать к оплате карточки Visa и MasterCard с мобильного телефона; 3) «Экстренные деньги» – с помощью этого приложения можно снимать деньги в банкоматах ПриватБанка без наличия карты; 4) SMS-банкинг – способ управления своим карт-счётом; владелец банковской пластиковой карты может проводить платежи и получать информацию о проведенных операциях при помощи своего мобильника через SMS; 5) Privat Hot Line – оповещает ПриватБанк о факте мошенничества путём присылки в банк снимка этого факта; если сигнал подтверждается, приславшему выплачивается вознаграждение до 5 000 гривен (5 миллионов рублей).

Перечисленные мобильные приложения подвержены всем угрозам информационной безопасности двух объектов: во-первых, банковских кредитных карт, во-вторых, смартфонов. Для парирования этих угроз в докладе предлагается начать широкую стандартизацию при разработке мобильных приложений, заимствуя при этом передовой зарубежный опыт. Например, в США в 2010 году была организована группа специалистов по работе над безопасностью приёма платежей через мобильные устройства [3]. В том же году с подачи группы разработан стандарт безопасности данных PCI DSS (Payment Card Industry Data Security Standards). В 2012 году Совет по разработке стандартов безопасности PCI (Payment Card Industry Security Standards Council /SSC/) выпустил новый документ «The PCI mobile payment acceptance security guidelines». Согласно документу рекомендуется создавать приложения с поддержкой шифрования данных, защищать приложения паролем. Мобильные приложения, которые осуществляют мобильные платежи, должны обладать функциями обнаружения атак, функциями оповещения об атаках и о введении неправильного пароля или изменении криптографического ключа [3].

Технический директор PCI SSC считает [3], что многочисленные мобильные платформы, различные производители смартфонов и операторы связи чрезвычайно усложняют процесс создания безопасных приложений для приёма платежей через смартфоны. Недостаток практического опыта и необходимой документации позволяет разработчикам мобильного ПО уходить от ответственности за сохранность секретных данных [3].

Анализируя ситуацию с мобильными платежами в Беларуси, несложно заметить, что мобильные платформы в республике, так же как и во всём мире, многочисленны – это и Windows mobile, и Symbian, и Pocket PC, и Android (все перечисленные – различных многочисленных версий), и, в последнее время, Blackberry. Разработкой мобильного ПО в Беларуси занимаются все, кому не лень – от крупных фирм до индивидуальных предпринимателей. В то же время документов, подобных «The PCI mobile payment acceptance security guidelines», в республике нет. В этих условиях широкая стандартизация при разработке мобильных приложений, заимствуя при этом передовой зарубежный опыт, в Беларуси своевременна и актуальна.

Список использованных источников:

1. Мобильные платежи от банка «Балтика» на базе платформы MasterCard Mobile [Электронный ресурс]. – Электронные данные. – Режим доступа www.procontent.ru/news/26942.html. – Дата доступа 23.03.2013.

2. Мобильные приложения ПриватБанка [Электронный ресурс]. – Электронные данные. – Режим доступа privatbank.ua/apps/. – Дата доступа 23.03.2013.

3. Вестервельт Роберт. Новые правила разработки мобильных приложений // Безопасность ИТ-инфраструктуры. – 2012. – № 12 (66). – С. 1-2.

ВРЕДОНОСНОЕ ПО И СМАРТФОНЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Королёв Я. П., Рудский А. В., Масловская А. И.

Шпак И. И. – канд. техн. наук, доцент

Анализируется вредоносное программное обеспечение (компьютерные вирусы, программы шпионы и т.д.) как одна из возможных угроз информационной безопасности смартфонов. Предлагаются мероприятия, которые следует осуществить для парирования данной угрозы

Под смартфо́ном (англ. *Smartphone* — умный телефон) — обычно понимают [1] мобильный телефон, сравнимый с карманным персональным компьютером. В [2] в первом приближении проанализированы основные угрозы информационной безопасности смартфонов. В настоящем докладе анализ угроз информационной безопасности смартфонов продолжен в части защиты их от вредоносного программного обеспечения (ПО). При этом под вредоносным ПО понимаются как компьютерные вирусы, так и программы-шпионы. В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Согласно [3] вирусы принято разделять по следующим критериям классификации а) по поражаемым объектам; б) по поражаемым

операционным системам и платформам; в) по технологиям, используемым вирусом; г) по языку, на котором написан вирус; д) по дополнительной вредоносной функциональности. Рассматривая классификацию по последнему критерию (бэкдоры /backdoor (от англ. *back door*, чёрный ход) — ПО, которое устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе [4]/, кейлоггеры /англ. *keylogger*, правильно читается *«ки-ло́ггер»* — от англ. *key — клавиша* и *logger — регистрирующее устройство*) — ПО или аппаратное устройство, регистрирующее различные действия пользователя — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т.д. [5]/, шпионы /spyware, шпионское ПО, — ПО, осуществляющее деятельность по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя [6]/, и др.) несложно заметить, что в соответствии с [3] программы-шпионы являются также компьютерными вирусами, поэтому сделанное выше определение вредоносного ПО можно понимать и так: вредоносное ПО – это компьютерные вирусы.

Считается [7], что первое мобильное вредоносное ПО – это червь Cabir, который появился ещё в 2004 году (сетевой червь – разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети [8]). Свежим примером мобильного вредоносного ПО является ПО Flame, которое содержит компонент Bluetooth, специально созданный для вытягивания секретов из других мобильных устройств.

В докладе для парирования проникновения в мобильное устройство вредоносного ПО как одной из значимых угроз информационной безопасности смартфонов предлагается ряд мер. Одна из них – разработка специальных антивирусных программных продуктов, возможно, совмещённых с программами Касперского (например, Kaspersky Mobile Security), как это сделано в антивирусном ПО разработки белорусского отделения компании Check Point Software Technologies Ltd. – фирмы ИООО "Чек Поинт Софтвер Текнолоджис Белрус [9]. Как отмечено в [7]: «…Всё дело лишь в программном обеспечении. Мы можем либо собрать все компоненты (ПО) правильно с точки зрения безопасности (и убедиться в том, что они правильно работают) или же мы можем плюнуть на всё и пойти домой.

Список использованных источников:

1. Смартфон [Электронный ресурс]. – Электронные данные. – Режим доступа http:// ru.wikipedia.org/Смартфон. – Дата доступа 23.03.2013.
2.Королёв Я.П., Рудский А.В., Сечко Г.В., Шпак И.И. Анализ угроз информационной безопасности смартфонов // Современные средства связи: материалы XVII Междунар. науч.-техн. конф., 16–18 сент. 2012 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2012. – 332 с. – С. 236.
3. Компьютерный вирус [Электронный ресурс]. – Электронные данные. – Режим доступа http:// ru.wikipedia.org/ Компьютерный_вирус . – Дата доступа 23.03.2013.
4. Бэкдор [Электронный ресурс]. – Электронные данные. – Режим доступа http:// ru.wikipedia.org/Бэкдор. – Дата доступа 23.03.2013.
5. Кейлоггер [Электронный ресурс]. – Электронные данные. – Режим доступа http:// ru.wikipedia.org/ Кейлоггер. – Дата доступа 23.03.2013.
6. Кейлоггер [Электронный ресурс]. – Электронные данные. – Режим доступа http:// ru.wikipedia.org/ Кейлоггер. – Дата доступа 23.03.2013.
7. МакГроу Гэри. Всё упирается в безопасность мобильного ПО // Безопасность ИТ-инфраструктуры. – 2012. – № 9 (63). – С. 14-16.
8. Сетевой червь [Электронный ресурс]. – Электронные данные. – Режим доступа http:// ru.wikipedia.org/Сетевой_червь. – Дата доступа 23.03.2013.
9. Check Point Software Technologies Ltd [Электронный ресурс]. – Электронные данные. – Режим доступа http:// http://companies.dev.by/check-point-software-technologies-ltd. – Дата доступа 23.03.2013.

СРАВНЕНИЕ И АНАЛИЗ СОСТАВА ОРГАНИЗАЦИОННОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ДВУХ БАНКОВ В ЧАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Коурова Ю., Шеремет Д. В.

Сечко Г. В. – канд. техн. наук, доцент

С целью выбора и изучения основных документов в области информационной безопасности для банка средней величины анализируется и сравнивается между собой состав организационного обеспечения информационных систем двух белорусских банков

В [1] с целью изучения и анализа одного из аспектов информационной безопасности в банке описано организационное обеспечение (ОО) информационных систем (ИС) белорусского банка средней величины. Для сохранения коммерческой тайны назовём его «Банк 1». При этом под ИС обычно понимают совокупность технического, программного и организационного обеспечения, а также персонала, предназначенную для того,