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,

чтобы своевременно обеспечивать надлежащих людей надлежащей информацией [1]. Банковские ИС включают компьютеры, объединенные в сеть, и средства телекоммуникаций. ОО – это совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе эксплуатации ИС [1]. Названные методы и средства описываются в различных инструкциях, положениях, правилах и других организационных документах.

В докладе сравнивается ОО ИС «Банка 1» с аналогичным для другого белорусского банка средней величины (назовём его «Банк 2»). Цель сравнения – проверка того, насколько ОО ИС «Банка 1» является типичным для белорусских средних по величине банков. Особое внимание уделяется защите от потерь за счет отказов составных частей ИС.

Одинаковыми по названию и примерно одинаковыми по содержанию в обоих банках является «Политика информационной безопасности (ИБ) банка».

Практическая реализация основных положений перечисленных документов осуществлена в штатном расписании подразделений банков, ответственных за обслуживание, эксплуатацию и безопасность ИС, и в различных организационных документах.

В отличие от Банка1 штатное расписание Банка 2 включает:

управление безопасности в составе одного отдела (экономической безопасности) и двух секторов (сектора верификации и сектора розничного бизнеса).

департамент информационных технологий в составе двух управлений (управление развития информационных систем, управление эксплуатации информационных систем) и одного отдела (отдел информационной безопасности)

Численность специалистов в низовых подразделениях управлений (отдел и сектор) обоих соответствует пропорции 4:6:3:3:3:3 (в порядке упоминания подразделений).

Организационными документами Банка 2 в части информационной безопасности являются 3 положения («О категорировании информационных ресурсов», «Об оформлении и контроле исполнения прав доступа к программным и информационным ресурсам», «О применимости контролей»), 2 инструкции («Об организации парольной защиты», «По организации антивирусной защиты»), 2 правила («Работы с внешними устройствами», «Работы с мобильными компьютерами») и 1 порядок («Использования информационных ресурсов»). Сравнение показывает, что число вышеперечисленных организационных документов в Банке 2 превышает аналогичное для Банка 1, зато в Банке 1 имеется отсутствующая в Банке 2 «Концепция ИБ банка».

Таким образом, в Банке 2 главным документом в части потерь информации из-за отказов является локальный нормативный правовой акт «Политика Информационной Безопасности», в котором банк устанавливает общие требования по обеспечению информационной безопасности для следующих областей: а) назначение и распределение ролей и доверия к сотрудникам; б) стадии жизненного цикла автоматизированной банковской системы (АБС); в) защита от несанкционированного доступа, управления доступом и регистрацией в АБС; г) антивирусная защита; д) использование ресурсов Интернет; е) использование средств криптографической защиты информации; ж) защита банковских платежных и информационных технологических процессов; з) использование корпоративной электронной почты.

Назначенные приказами и распоряжениями Председателя Правления Банка лица (эксперты) при построении системы управления информационной безопасности должны действовать на основании Политики Информационной Безопасности и своих должностных инструкций, утверждаемых в установленном порядке.

Список использованных источников:

1. Шарлан А. И., Шеремет Д. В. Анализ состава организационного обеспечения информационных систем банка в части защиты информации // Тезисы докл. 48-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению

2. Информационные системы и технологии / под ред. В. Л. Николаенко и Г. В. Сечко, Минск: БГУИР, ИИТ, 7 – 11 мая 2012 года. – Мн.: ИИТ БГУИР, 2012. – 58 с. с ил. – С. 35.

ОПЫТ ПОДДЕРЖАНИЯ РАБОТОСПОСОБНОСТИ ИНТЕГРИРОВАННЫХ СИСТЕМ ОХРАНЫ

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

Матюшонок И. В., Вильчицкий А. Н.

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

В современных системах охраны объектов одной из главных задач является обеспечение и повышение надежности оборудования. В докладе даются предложения по решению этой задачи исходя из опыта работы с системой интегрированной безопасности ИСБ «777»

В настоящий момент каждая организация, независимо от рода деятельности, применяет массу усилий и средств для обеспечения защиты своего имущества и пресечения несанкционированных попыток проникновения в контролируемую зону или несанкционированного выхода из зоны. Для этого необходимо создать все необходимые для защиты объекта: охранная и тревожная сигнализация; система охраны периметра; система контроля и управления доступом; система видеонаблюдения; пожарная сигнализация,