АНАЛИЗ СОСТАВА ОРГАНИЗАЦИОННОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ БАНКА В ЧАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

А. И. Шарлан, Д. В. Шеремет

Г. В. Сечко − к. т. н., доцент

С целью выбора и изучения основных документов в области защиты информации для банка средней величины анализируется состав организационного обеспечения информационных систем банка

Под информационной системой (ИС) обычно понимают совокупность технического, программного и организационного обеспечения, а также персонала, предназначенная для того, чтобы своевременно обеспечивать надлежащих людей надлежащей информацией [1]. Банковские ИС включают компьютеры, объединенные в сеть, и средства телекоммуникаций. Организационное обеспечение (ОО) – это совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе эксплуатации ИС [2]. Названные методы и средства описываются в различных инструкциях, положениях, правилах и других организационных документах.

В докладе анализируется типовое наиболее употребительное ОО минского банка средней величины (Сомбелбанк, Альфабанк, Кредэксбанк и т.д.) в части защиты информации в банковской ИС. Особое внимание уделяется защите от потерь за счет отказов составных частей ИС. Основными из анализируемых документов являются «Концепция информационной безопасности (ИБ) банка» и «Политика ИБ». Практическая реализация основных положений перечисленных документов осуществлена в штатном расписании подразделений банка, ответственных за обслуживание, эксплуатацию и безопасность ИС, и в различных организационных документа. Штатное расписание головного банка включает:

- управление информационных технологий в составе двух отделов (администрирования информационных сетей и телекоммуникаций и внедрения и сопровождения программных продуктов и одного сектора (развития банковских информационных технологий;
- управление безопасности в составе двух отделов (экономической безопасности и внутренней безопасности и одного сектора (развития банковских информационных технологий).

Каждое подразделение (управление, отдел, сектор) возглавляется руководством в составе начальника и его заместителя. Численность специалистов в низовых подразделениях управлений (отдел и сектор) соответствует пропорции 4:6:3:3:3:3 (в порядке упоминания подразделений).

Работа управления безопасности регламентируется следующими организационными документами: 3-мя положениями («Об управлении безопасности», «Об антивирусной защите информации», «Об электронной цифровой подписи»), 2-мя правилами («Обмена информацией в корпоративной информационной сети банка», «Использования ресурсов Интернет») и 4-мя инструкциями («О паролях», «Об ИБ банка», «Об ИБ при использовании электронной почты», «О мероприятиях по обеспечению надежности функционирования ИС банка» / наиболее интересна в части потерь информации за счет отказов».

В последней инструкции рассматриваются как природные (пожар, затопление) и техногенные (отключение электропитания) угрозы ИБ, а также атаки злоумышленников (диверсии, несанкционированное проникновение в ИС банка, вирусное заражение), так и угрозы ИБ в части потерь информации за счет отказов (отдельно оборудования, каналов связи и программного обеспечения (ПО)). Возникновение угрозы именуется в инструкции внештатной ситуацией. Реагирование на такое возникновение возлагается на администраторов или руководство отдела администрирования информационных сетей и телекоммуникаций управления информационных технологий. Отражение атаки и устранение угрозы ИБ в части потерь информации за счет отказов проводится путем переключения оборудования на резервное и путем восстановления работоспособности программного обеспечения специалистами отдела администрирования. После такого восстановления руководитель управления информационных технологий совместно со специалистами управления безопасности должны провести тщательный анализ отказа с целью его недопущения в будущем.

Вывод: основным организационным документом банка средней величины в части потерь информации за счет отказов является инструкция «О мероприятиях по обеспечению надежности функционирования ИС банка», поэтому она должна быть основополагающей при проектировании базы данных [3] по результатам наблюдений за работой банковских ИС.

Список использованных источников

1. Информационные системы [Электронный ресурс] – Электронные данные. – Режим доступа: Alexandr-kisele2011.narod.ru›inform.html. – Дата доступа: 03.04.2012.

2. Организационное обеспечение информационных систем [Электронный ресурс] – Электронные данные. – Режим доступа: itstan.ru›it…is/organizacionnoe-obespechenie… .– Дата доступа : 03.04.2012.

3. Пачинин В.И., Сечко Г.В., Таболич Т.Г., Шеремет Д.В. Взаимосвязь сложности создаваемой базы данных по результатам наблюдений за работой технического объекта с его видом и назначением // Матер. 17-й НТК «Информацион-ные системы и технологии ИСТ-2010», 22 апреля 2011 года, Нижний Новгород. – Нижний Новгород: НГТУ, 2011. – С. 240.