

Козырева Е.С.

*Научный руководитель – к.т.н., доцент каф. ФПМ Штыков Р.А.
Муромский институт (филиал) федерального государственного образовательного
учреждения высшего образования «Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
elena.kozireva666@yandex.ru*

Проблемы информационной безопасности в банках

В современном мире хранение банковской информации, ее стоимость и значимость многократно возросли, что, в свою очередь, не могло не привлечь рост преступного интереса к ней.

Необходимость обеспечивать безопасность хранения данных, регулярная смена и проверка паролей и контроль вероятности утечки информации стали неотъемлемой частью работы каждого банка. Объект исследования в данной работе – процесс защиты резервных копий в банке, предмет исследования – средство защиты информации [1].

Целью исследования является обзор и анализ методов защиты информации в банках.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор средств защиты информации.
2. Анализ недостатков средств защиты информации (таблица 1).
3. Результаты исследования.

Рассмотрим проблемы информационной безопасности в банках на защите резервных копий.

Регулярное резервирование всей хранящейся в банке информации — абсолютно необходимая мера. Она позволяет существенно снизить убытки в случае возникновения таких проблем, как порча данных вирусами, выход из строя аппаратного обеспечения и т.п. Но в то же время она усиливает риски, связанные с несанкционированным доступом.

Основная сложность в организации криптографической защиты резервных копий заключается в необходимости разделения обязанностей по управлению архивированием данных. Решить эту проблему можно только путем «встраивания» системы криптографической защиты между системой управления резервным копированием и устройствами, которые осуществляют запись данных (стримеры, DVD-приводы и т.п.).

Таким образом, криптографические продукты для возможности их применения в банках должны также иметь возможность работы с различными устройствами, использующимися для записи резервных копий на носители информации: стримерами, CD- и DVD-приводами, съемными жесткими дисками и т.п.

На сегодня существуют три типа продуктов, призванных минимизировать риски, связанные с несанкционированным доступом к резервным копиям [2]:

1. Специальные устройства. Такие аппаратные решения имеют множество преимуществ, в том числе и надежное шифрование информации, и высокая скорость работы. Однако они обладают тремя существенными недостатками, которые не позволяют использовать их в банках. Первый: очень высокая стоимость (десятки тысяч долларов). Второй: возможные проблемы с ввозом в Россию (нельзя забывать, что мы говорим о криптографических средствах). Третий минус заключается в невозможности подключить к ним внешние сертифицированные криптопровайдеры. Эти платы работают только с реализованными в них на аппаратном уровне алгоритмами шифрования.

2. Модули. Правда, у них есть свои особенности. Самая главная — это работа только со «своим» ПО или накопителем. Между тем информационная система банка постоянно развивается. И возможна ситуация, когда замена или расширение системы резервного копирования может потребовать дополнительных затрат на модификацию системы защиты. Кроме того, в большинстве продуктов этой группы реализованы старые медленные алгоритмы шифрования (например, 3DES), нет средств управления ключами, отсутствует возможность подключения внешних криптопровайдеров.

3. Программные, программно-аппаратные и аппаратные продукты. Они поддерживают широкий спектр устройств записи информации, что позволяет применять их во всем банке, включая и все его филиалы. Это обеспечивает единообразие используемых средств защиты и минимизацию эксплуатационных затрат.

Правда, стоит отметить, что, несмотря на все их преимущества, на рынке представлено совсем немного продуктов из третьей группы. Это объясняется, скорее всего, отсутствием большого спроса на системы криптографической защиты резервных копий. Как только руководство банков и прочих крупных организаций осознает реальность рисков, связанных с архивированием коммерческой информации, число игроков на этом рынке вырастет.

Таблица 1 - Результаты исследования

Тип лицензии	Средняя стоимость	Доступность продукта в России	Высокая скорость работы	Большой выбор продуктов на рынке
Специальные устройства	-	-	+	+
Модули	-	+	-	+
Программные, программно-аппаратные продукты	+	+	+	-

В результате проведенного анализа было выявлено, что наиболее лучшим средством для защиты резервных копий банка, являются программные обеспечения, правда их выбор на рынке, не особо разнообразен.

Литература

1. А. Бабаш, Е. Баранова, Д. Ларин. Информационная безопасность. 2015
2. Информационная безопасность компьютерных систем и сетей.: учеб. пособие/ В. Ф. Шаньгин. - Москва: ФОРУМ, 2011. - 415 с.