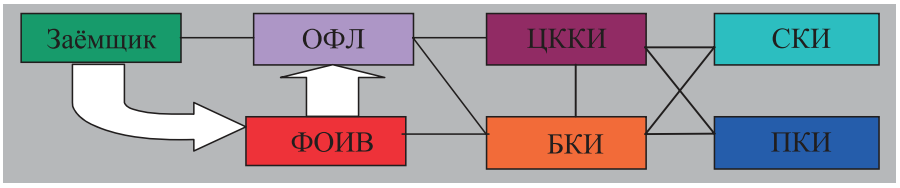
Кредитные истории как объект СТЕГОЗАЩИТЫ

Л. С. Раткин, к. т. н.,
действительный член Международной Академии Информатизации

Завершившийся 2006 год многим остался памятен среди ряда других событий благодаря инциденту с «кредитными историями». Весть о возможном доступе к конфиденциальной информации российских заёмщиков не лучшим образом повлияла на репутацию нового финансового института. Поэтому вопрос защиты данных в информационных системах (ИС), обслуживающих бюро кредитных историй (БКИ), и проектировании соответствующих сетей является достаточно важным. Для того чтобы выбрать оптимальные решения для информационной защиты БКИ, необходимо охарактеризовать БКИ и связанные с ним объекты.

Создание БКИ призвано упорядочить работу кредитных учреждений, минимизировать заёмные риски и отрегулировать различные типы отношений, как то: между заёмщиками и организациями, заключающими с физическими лицами (ОФЛ), в т. ч. с индивидуальными предпринимателями, и/или юридическими лицами договоры займа/кредита, между ОФЛ и БКИ, между ОФЛ и Центральным каталогом кредитных историй (ЦККИ), между ЦККИ и субъектами кредитных историй (СКИ), между ЦККИ и пользователями кредитных историй (ПКИ), между ЦККИ и БКИ, БКИ и ПКИ, БКИ и СКИ, а также между БКИ и федеральным органом исполнительной власти (ФОИВ), уполномоченным контроль и надзор за деятельностью БКИ.

Схема функционирования перечисленных объектов представлена на рисунке. ОФЛ заключает с заёмщиком договор займа (кредита), с передачей данных в ЦККИ и БКИ. ИС ЦККИ и ИС БКИ имеют доступ к ИС СКИ и ИС ПКИ, в которых сведения о заёмщиках, а также кредитные истории (сведения, характеризующие исполнение заёмщиком принятых на себя обязательств по договорам кредита/займа) распределены по соответствующим информационным хранилищам. Поиск необходимых данных



осуществляется по коду СКИ – буквенно-цифровой комбинации, однозначно идентифицирующей любого СКИ в сети ИС. Поскольку кредитная история состоит из основной и дополнительной (закрытой) части, для повышения степени защиты необходимо распределённое хранение и обработка массивов данных с использованием перспективных информационных технологий (ИТ) ограничения доступа (ОД), в частности, компьютерной стеганографии (КС).

Основным отличием КС от других методов защиты данных является невозможность определения факта хранения информации в стегоконтейнере без применения специализированных средств. Например, в криптографии, науке наиболее близкой к КС, факт шифрования данных выявляется на первых же стадиях изучения объекта хранения закрытых данных, в то время как заполненный нешифруемыми скрываемыми данными стегоконтейнер по внешнему виду никак не отличается от пустого, и только применение набора стеганографических процедур (НСП) может дать ответ о его содержимом. Применение КС для БКИ также допустимо потому, что НСП является стандартным, в то время как устойчивость к взлому стегоконтейнера можно повышать [1].

Как видно из схемы, помимо прямого доступа из ИС ЦККИ в ИС БКИ, возможными путями в ИС БКИ являются обходы через ИС СКИ или ИС ПКИ или ИС ОФЛ. Таким образом, ИС ЦККИ и ИС БКИ, имея по 4 точки входа, являются наиболее уязвимыми участками сети (УС), что предполагает для повышения степени защиты данных увеличение количества стегоконтейнеров в несколько раз по сравнению с другими УС. При этом распределение закрытых данных из ИС ЦККИ и ИС БКИ возможно по части подсистем, замаскированных под информационные блоки ИС ОФЛ, ПКИ и СКИ. Подобная декомпозиция соответствует критерию повышенной надёжности (сохранности) наиболее важных компонентов сети. Белыми стрелками на схеме представлены примеры запросов заёмщиков в ФОИВ и осуществления контрольно-надзорных функций (КНФ) государственным органом за БКИ и связанных с ним объёктов. Доступ к ИС ЦККИ осуществим из ИС ОФЛ и ИС БКИ, что упрощает КНФ ФОИВ (т. к. часть информационных блоков ИС ЦККИ хранится в ИС ОФЛ и ИС БКИ). КНФ за эксплуатацией других участков сети выполняются аналогично.

К сожалению, в современных финансовых ИС средства КС применяются нечасто, что может привести к событиям, аналогичным инциденту с БКИ в 2006 году. Между тем, методы КС используются для организации защиты данных в ИС по оборонной продукции [2]. Развитием методов КС, в т. ч., являются стеготранзакция, контроль скрытого доступа к сведениям и стегофрагментация данных.

Литература

Перепелицын Е. Г. Нестандартные методы математической статистики и их приложение к технической диагностике и анализу изображений. // М.: Омега-Л, 2006. – С.194—239.

Раткин Л. С. Проблемы применения стеганографических методов при проектировании КИС по оборонной продукции. // Защита информации. Конфидент, № 2 (56), 2004. – С. 82—84.