Ученые записки Таврического национального университета имени В.И. Вернадского
Серия «Экономика и управление». Том 27 (66). 2014 г. № 4. С. 28-31

УДК 004.056.53

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ

Белименко Б.В.

Таврический национальный университет имени В.И. Вернадского, Симферополь, Республика Крым
E-mail: bolek61@mail.ru

В статье рассматриваются современные проблемы состояния информационной безопасности автоматизированных банковских систем. Проведен анализ функционирования систем выявления мошеннических операций в автоматизированных банковских системах. Предложено использовать специальное программное обеспечение FraudView для решения проблем информационной безопасности автоматизированных банковских систем.
Ключевые слова: информационная безопасность, автоматизированная банковская система, платежная система, программный комплекс, несанкционированный доступ, банковский фрод.

ВВЕДЕНИЕ

Проблемы безопасности информации в автоматизированных банковских системах довольно актуальны, так как 91% банков имеет полностью автоматизированные все процессы, но не все они имеют внедренную систему защиты информации.

По проведенному анализу можно привести данные ущерба от противоправных действий злоумышленников по которым Сбербанк России с начала 2013 года зафиксировал 398 случаев кражи денежных средств со счетов клиентов в области дистанционного обслуживания на сумму более 321 миллиона рублей [1].

Требования безопасности денежных средств клиентов банка изложены в статье 9 Федерального закона № 161-ФЗ «О национальной платежной системе», где банк несет ответственность за несанкционированное списание средств со счетов. Требования информационной безопасности есть, но как можно видеть что довольно часто происходит перехват интернет-соединения клиента с системой дистанционного банковского обслуживания и выполнение финансовых операций от его имени, подбор регистрационного имени и пароля клиента для доступа к системе, что делает данную проблему достаточно актуальной и требует применение специализированного программного обеспечения [2].

Вопросами информационной безопасности в автоматизированных банковских системах, защитой от банковского фрода, рассматриваются в работах таких ученых как В.А. Мерин, О.В. Буркатовский. Однако все они рассматривают полу-комплексное программное обеспечение, которое не имеет возможностей осуществлять защиту от всех возможных угроз автоматизированных банковских систем. Следовательно, данные исследования требуют дальнейших доработок.

Цель исследования состоит в анализе проблематики обеспечения защиты информации от банковского фрода, а также методов и способов, обеспечивающих требуемый уровень защиты банковских систем.

ОСНОВНОЙ МАТЕРИАЛ

Для защиты от банковского фрода можно реализовывать две возможные стратегии защиты – на стороне клиента или на стороне банка. Реализация функций защиты на стороне клиента включает в себя: усиленную аутентификацию пользователя, создание доверенной среды для работы клиент-банка, разработка требований по защите рабочего места, на котором установлена система ДБО и др. К сожалению, в силу сложности задачи, а также не всегда высокого уровня технической квалификации пользователя, полностью решить проблему защиты на уровне клиента не представляется возможным. Именно поэтому банки все чаще в дополнении к существующим средствам защиты реализуют функции безопасности на стороне банка.

Реализация функций защиты на стороне банка предполагает возможность выявления несанкционированных банковских операций, даже если они были выполнены от имени клиентов. Одним из способов решения данной задачи является применение специализированных систем выявления мошеннических операций. Данные системы обеспечивают анализ банковских транзакций с целью выявления и блокирования тех из них, которые связаны с действиями злоумышленников. Необходимость применения специализированных систем для такого анализа обусловлена тем, что большинство банков ежедневно совершают огромное количество транзакций, обработать которые в ручном режиме практически невозможно.

При этом необходимость внедрения подобной системы всегда можно обосновать путем расчета показателя возврата инвестиций. Этот показатель позволяет нам наглядно продемонстрировать руководству банка окупаемость системы за счет возможности предотвращения реальных финансовые потерь со стороны банка посредством блокирования мошеннических транзакций [3].

В общем случае система защиты от банковского фрода должна удовлетворять следующим требованиям методов безопасности:

- обеспечивать минимальное количество ошибок первого рода, связанными с ложными срабатываниями системы (когда система считает транзакцию мошеннической, хотя она таковой не является);
- эффективно выявлять транзакции, связанные с действиями мошенников;
- иметь в составе поставки уже готовый набор правил, учитывающий российскую специфику банковских транзакций;
- обладать свойствами самообучения и простоты эксплуатации;
- обеспечивать прозрачную интеграцию с существующими бизнес-процессами и ИТ-системами банка;
- обеспечивать возможность не только выявления мошеннической транзакции, но и её блокировки;
- работать в реальном масштабе времени, обрабатывая большое количество транзакций.

На сегодняшний день можно выделить следующие возможные способы реализации систем выявления мошеннических операций:

- системы, построенные на базе систем мониторинга событий информационной безопасности;
- системы, которые были разработаны собственными ресурсами банка;
- специализированные системы, предназначенные для выявления банковского фрода;
- системы, которые предлагаются производителями средств дистанционного банковского обслуживания.

Все вышеперечисленные системы выявления банковского фрода имеют свои преимущества и недостатки. В данной статье будет более подробно рассмотрена программа выявления мошеннических действий FraudView компании ArcSight.

Для своевременного выявления фактов мошенничества (банковского фрода) требуется провести глубокий анализ банковских транзакций и выявить те из них, которые представляют реальную угрозу для кредитной организации. При этом с учетом того, что большинство банков ежедневно совершают огромное количество транзакций, обработать их в ручном режиме практически невозможно, поэтому для решения поставленной задачи необходимо использовать специализированные комплексы, позволяющие автоматизировать процесс анализа проводимых банком транзакций.

Программный комплекс FraudView необходим для выявления фактов произошедших противоправных действий в финансово-кредитных организациях. Преимущества данного комплекса в том, что он легко интегрируется со многими банковскими прикладными системами, особенно с системами дистанционного банковского обслуживания «Интернет-банк», «Банк-клиент» автоматизированные банковские системы и др., осуществление обработки и корреляции данных в масштабе реального времени с учетом поступающих данных от средств защиты информации [4].

Вот лишь некоторые яркие примеры действий злоумышленников, которые могут быть выявлены программным комплексом FraudView:

- перехват Интернет-соединения клиента с системой ДБО и выполнение финансовых транзакций от его имени;
- установка на компьютере клиента банка вредоносного программного обеспечения с целью перехвата параметров аутентификации и выполнения транзакций от его имени;
- изготовление дубликата или кража банковской карты клиента и попытка снятия с неё денег через банкомат в другом городе или другой стране;
- компрометация регистрационного имени и пароля клиента для доступа к системе дистанционно-банковского обслуживания (ДБО) с целью выполнения несанкционированных транзакций.

Система включает в себя большое количество уже готовых правил корреляции, позволяющих выявлять различные виды мошенничества. При этом система предусматривает возможность добавления новых правил, что позволяет учесть специфику операционной деятельности российских банков. Помимо использования базы данных экспертных правил, система также позволяет выявлять банковский фрод посредством обнаружения отклонений от штатной работы банковских систем

и их пользователей. Данные отклонения выявляются на основе статистических методов, а также нейросетевых алгоритмов.

Каждой банковской транзакции, которая анализируется системой ArcSight FraudView, присваивается определённый уровень риска, на основе которого устанавливается степень её опасности. Уровень риска определяется на основе результатов анализа следующих основных параметров: тип транзакции, объем платежа, время проведения транзакции, источник платежа, получатель платежа и т.д.

На сегодняшний день ArcSight FraudView уже успешно используется в крупнейших американских и европейских банках. Практический опыт внедрения продукта ArcSight FraudView позволяет существенно повысить защищенность банковских систем посредством своевременного выявления и предотвращения мошеннических транзакций. Перед внедрением данного продукта имеется возможность рассчитать показатель возврата инвестиций, так как использование системы позволяет предотвратить реальные финансовые потери банка [5].

ВЫВОДЫ

Анализ состояния безопасности автоматизированных банковских систем, определяет факт незащищенности их от противоправных действий, а большинство специального программного обеспечения не может решать задачи безопасности, что не определяет комплексность защиты системы.

Одним из возможных путей решения данной проблемы является применение специализированных систем выявления мошеннических операций, примером которых является решение на базе специализированного программного обеспечения FraudView. С принятием специализированного программного обеспечения возможно создание условий для решения проблемы информационной безопасности в автоматизированных банковских системах.

Список литературы

1. Официальный сайт Центрального Банка РФ // [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/statistics/1542
2. Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 22.10.2014) "О национальной платежной системе" // [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_162811/
3. СТАНДАРТ БАНКА РОССИИ, СТО БР ИББС-1.0-2014 // [Электронный ресурс]. – Режим доступа**:** http://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf
4. Гайкович В. Безопасность электронных банковских систем / В. Гайкович, А. Першин // [Электронный ресурс]. – Режим доступа**:** http://www.cplire.ru/koi/casr/os/3_12/1/4.htm
5. Ярочкин В. Средства и методы безопасности банковских систем / В. Ярочкин // [Электронный ресурс]. – Режим доступа: http://www.books.ru/books/bezopasnost-sistem-223945/

Статья поступила в редакцию 10. 11. 2014 г.