Проблема защиты от банковского фрода и возможные пути ее решения

Виктор Сердюк, генеральный директор ЗАО «ДиалогНаука»

Сегодня проблема защиты от мошеннических действий злоумышленников является одной из наиболее актуальных задач для большинства российских банков. Это связано с ростом финансовых потерь кредитных организаций вследствие несанкционированных действий злоумышленников, направленных на кражу денежных средств со счетов клиентов банка. При этом в качестве клиентов могут выступать как физические, так и юридические лица.

Вот лишь некоторые примеры действий злоумышленников, которые могут нанести ущерб банку и его клиентам:

- 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;
- установка на компьютере клиента банка вредоносного программного обеспечения с целью перехвата параметров аутентификации и выполнения транзакций от его имени;
- перехват Интернет-соединения клиента с системой ДБО и выполнение финансовых транзакций от его имени.

В качестве примера возможного ущерба от действий злоумышленников можно привести данные, согласно которым Сбербанк России с начала 2012 года зафиксировал в общей сложности 467 случаев хищения денежных средств со счетов своих клиентов в рамках дистанционно-банковского обслуживания на сумму более 362 миллиона рублей.

Актуальность данной проблемы подтверждается и требованиями статьи 9 Федерального закона № 161-ФЗ «О национальной платежной системе», которая перекладывает на банк ответственность за несанкционированное списание средств со счета клиента. То есть, если клиент сообщил, что средства были списаны со счета без его согласия не позднее чем через день после получения уведомления о транзакции, банк обязан в течение суток возместить ему утраченные средства. Несмотря на то, что вступление данной статьи отложено на один год, в интересах банков уже сейчас начать предпринять меры по повышению уровня защиты от возможных действий злоумышленников.

Возможные пути защиты от банковского фрода

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 ROI (Return of Investments). Данный показатель позволяет наглядно продемонстрировать руководству банка окупаемость системы за счет возможности предотвращения реальных финансовые потерь со стороны банка посредством блокирования мошеннических транзакций.

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

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

Схема размещения системы выявления мошеннических операций и её взаимодействие с компонентами системы ДБО показана на рисунке ниже.

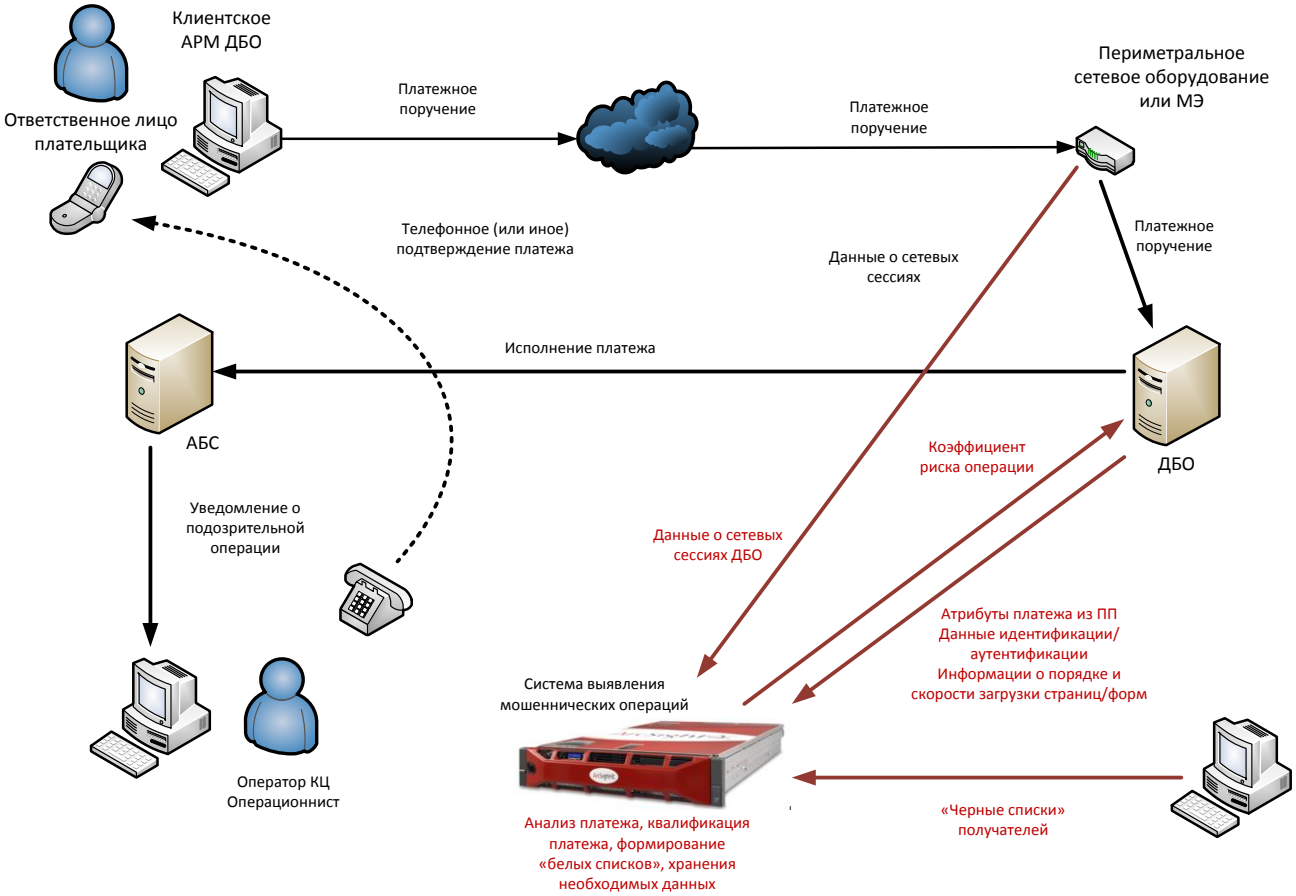

Рис. 1. Схема размещения системы выявления мошеннических действий

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

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

Каждый из вышеперечисленных классов систем выявления банковского фрода имеет свои преимущества и недостатки. В данной статье будет более подробно рассмотрен последний вариант реализации системы выявления фрода на базе решения ArcSight компании Hewlett Packard.

Применение системы защиты от банковского фрода на базе решения HP ArcSight

Система ArcSight представляет собой специализированное решение, предназначенное для автоматизации процесса сбора и анализа информации о событиях безопасности, поступающих из различных источников. В качестве таких источников могут выступать средства защиты информации, общесистемное и прикладное ПО, телекоммуникационное обеспечение и др. На сегодняшний день ArcSight является одной из ведущих систем мирового уровня, получившая наибольшее распространение в России.

Построение системы выявления банковского фрода на базе решения ArcSight предполагает установку и настройку пакета дополнительных правил и отчетов, которые позволяют средствами ArcSight выявлять мошеннические транзакции. ArcSight позволяет легко интегрироваться со всеми основными банковскими прикладными системами, включая системы дистанционного банковского обслуживания «Банк-Клиент», «Интернет-Банк», автоматизированные банковские системы и др. При этом система в реальном масштабе времени осуществляет обработку и корреляцию данных, поступающих не только от прикладного ПО, но от других источников, что позволяет выявлять сложные информационные атаки, направленные на совершение мошеннических действий.

Еще одним преимуществом системы ArcSight является тот факт, что она уже успешно применяется в большом количестве российских банков для мониторинга событий информационной безопасности. Система обладает возможностью обработки до 10 тысяч транзакций в секунду, что позволяет применять её в банке любого уровня.

Принцип работы системы выявления мошеннических действий заключается в следующем. Система в режиме реального времени выполняет анализ атрибутов каждого платежного поручения на основании данных, получаемых из системы ДБО и других систем Банка. На основании результатов такого анализа и в соответствии с определенными правилами, система ArcSight осуществляет расчет коэффициента, характеризующего величину риска платежной операции. Система, осуществляющая обработку платежных операций (ДБО, АБС, иная процессинговая система), должна проводить транзакцию или отклонять ее с учетом величины риска конкретной транзакции. Иными словами, функционал АБС или ДБО должен иметь возможность отклонения транзакции при превышении коэффициента риска транзакции определенного порога.

В таблице ниже приведены основные атрибуты платежного поручения, которые анализируются системой ArcSight на предмет выявления мошеннических транзакций.

Таблица 1

Параметры анализа платежного поручения

№	Наименование	Алгоритм анализа

	параметра	
1	Наличие получателя платежа в «белом списке»	«Белый список» содержит реквизиты организации, платежи которым рассматриваются как легальные. При этом система позволяет автоматически вести «белый список» таких получателей следующим образом – если операция перевода денежных средств определенному получателю прошла ранее и не была опротестована, то он автоматически попадает в такой список
2	Наличие получателя платежа в «черном списке»	«Черный список» содержит реквизиты организации, платежи которым рассматриваются как несанкционированные
3	Тип платежа	В системе существует собственная классификация платежей: платежи в федеральный бюджет, внутрибанковский платежи и др. На основе такой классификации система позволяет выявить те платежи, которые являются легальными и не представляют опасность для банка и клиента
4	Сумма платежа	Анализ суммы позволяет выявлять нетипичные платежи для конкретного клиента
5	Атрибуты отправителя платежа	Анализ изменения IP-адресов отправителя позволяет выявлять действия злоумышленников, которые выполняют транзакции от имени клиента банка
6	Время проведения финансовой транзакции	Анализ данного параметра позволяет выявлять транзакции, которые выполняются в нетипичное для клиента время

Помимо параметров, приведенных в таблице выше, система ArcSight может анализировать большое количество других атрибутов, которые позволяют выявлять мошеннические действия злоумышленника. Так, например, система может выявлять множественные транзакции на разных получателей с одинаковым назначением платежа и др.

Необходимо отметить, что ArcSight 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.

В процессе своей работы система позволяет однозначно квалифицировать подавляющее большинство транзакций как надежные или рискованные. Для некоторых транзакций, по которым нельзя принять однозначного решения, требуется дополнительная проверка со стороны оператора. Таким образом, решение на базе ArcSight, позволяет в значительной степени автоматизировать и упростить процесс анализа параметров платежных поручений с целью выявления фактов мошенничества.

Основные этапы внедрения системы защиты от фрода

Процесс внедрения системы выявления мошеннических транзакций включает в себя следующие основные этапы:

- сбор информации об используемых в банке системах ДБО, АБС. По результатам обследования формируются требования к архитектуре и функциональным возможностям системы.
- разработка технического решения, в котором описывается конфигурация оборудования и программного обеспечения, порядок внедрения, схема информационных потоков, требования к внешнему окружению системы и т.д.;
- установка системы защиты от фрода, интеграция системы с средствами ДБО, БС и другими банковскими приложениями;

- настройка параметров функционирования системы. Как правило, настройка осуществляется путем загрузки в систему архива транзакций за последние несколько месяцев;
- опытная эксплуатация системы, в процессе которого система работает в пассивном режиме, не блокируя мошеннические транзакции. На данном этапе осуществляется отладка процессов эксплуатации комплекса;
- перевод системы защиты от фрода в промышленную эксплуатацию;
- разработка документации, необходимой для дальнейшей эксплуатации системы;
- обучение сотрудников, которые будут отвечать за эксплуатацию системы выявления мошеннических транзакций;
- техническое сопровождение системы.

Заключение

На сегодняшний день практически любой российский банк сталкивается проблемой фрода. Одним из возможных путей решения данной проблемы является применение специализированных систем выявления мошеннических операций, примером которой является решение на базе продукта HP ArcSight. Данное решение уже успешно используется в российских банках и практический опыт его эксплуатации доказал его эффективность за счет предотвращения реального ущерба, который мог бы быть нанесен банку действиями мошенников.