The role of monitoring the transactions in the security of plastic cards operations
Efromeeva E.[1], Markov V.[2]

Роль мониторинга транзакций в обеспечении безопасности операций по пластиковым картам
Ефромеева Е. В.[1], Марков В. О.[2]

[1]Ефромеева Елена Валентиновна / Efromeeva Elena - кандидат технических наук, доцент;
[2]Марков Василий Олегович / Markov Vasilij – магистрант,
кафедра информационных технологий и вычислительных систем,
Московский государственный технологический университет «СТАНКИН», г. Москва

Аннотация: *в статье анализируются последствия карточного мошенничества, затрагиваются вопросы безопасности операций по пластиковым картам и создания систем мониторинга транзакций.*
Abstract: *the article analyzes the consequences of card fraud, affected operations security of plastic cards and the creation of transaction monitoring systems.*

Ключевые слова: *мониторинг транзакций, мошенничества с платежными картами, несанкционированные операции в банкоматах.*
Keywords: *monitoring of transactions, payment card fraud, unauthorized transactions at ATMs.*

Данная работа посвящена вопросу создания систем мониторинга транзакций с учетом особенностей современного рынка банковских услуг и специфики страны применения.

По оценкам VISA прямые ежегодные мировые потери от мошенничества с платежными картами составляют порядка 12 миллиардов долларов США. К тому же, 100 долларов прямых потерь в результате мошенничества влекут 200 долларов дополнительных косвенных потерь, связанных с запросами документов, претензионной работой, расходами на сотрудников, программное обеспечение. Россия входит в регион Центральной и Восточной Европы, где потери оцениваются всего около 2 - 3%, однако темпы роста несанкционированных операций по картам существенно превышают рост оборота по картам. Так, например, за первое полугодие 2014 года по сравнению с аналогичным периодом 2012 года объем всех операций в нашей стране вырос на 37% и составил 7,8 триллионов рублей, в то время как общая сумма мошеннических операций удвоилась.

Особенностью мошенничества в России является то, что 40% несанкционированных операций совершаются в банкоматах, в то время как в мире — лишь 5%. Компрометация данных также часто происходит в банкоматах. Злоумышленники устанавливают устройства для считывания данных с магнитной полосы карт и PIN-клавиатуры и внедряют специализированное вредоносное программное обеспечение в среду банкомата. За последнее время количество случаев установки и внедрения такого рода программного обеспечения возросло в несколько раз.

Закон «О национальной платежной системе» в части 15 статьи 9 устанавливает ответственность оператора по переводу денежных средств. Оператор обязан возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло за собой совершение операции без согласия физического лица. Указанная норма актуализирует задачу обеспечения безопасности платежей и неизбежно влияет на управление рисками в банке. Одним из главных факторов снижения операционного риска является организация мониторинга.

Системы мониторинга транзакций относятся к современным технологическим решениям в области снижения мошенничества и риска банка. На рис. 1 представлена общая схема предлагаемого архитектурного решения для мониторинга транзакций.

Авторизационный запрос, попадающий на хост эмитента, сохраняется в базе данных на главном сервере. На slave сервере расположена реплика авторизационной базы данных. Путем настройки асинхронной master-slave репликации достигается отказоустойчивость, масштабируемость и резервирование данных авторизационных запросов. Запросы, входящие в основу балльного метода оценки мошенничества при мониторинге, работают именно с данными авторизационной базы данных на slave сервере. После выполнения всех запросов для оценки и получения итогового результирующего набора мониторинга сотрудниками визуализируется для удобства принятия решения конечный массив информации.

Для более глубокого анализа необходимы «исторические» данные. С этой целью организовано архивное хранение суточного объема авторизационных запросов в DWH. Трансфер, а также валидация, сравнение и приведение сырых данных к необходимому для записи формату осуществляется при помощи ETL.

Данный подход позволяет добиться максимальной гибкости и безопасности системы, а балльный метод оценки повышает точность и однозначность статуса авторизационного запроса.

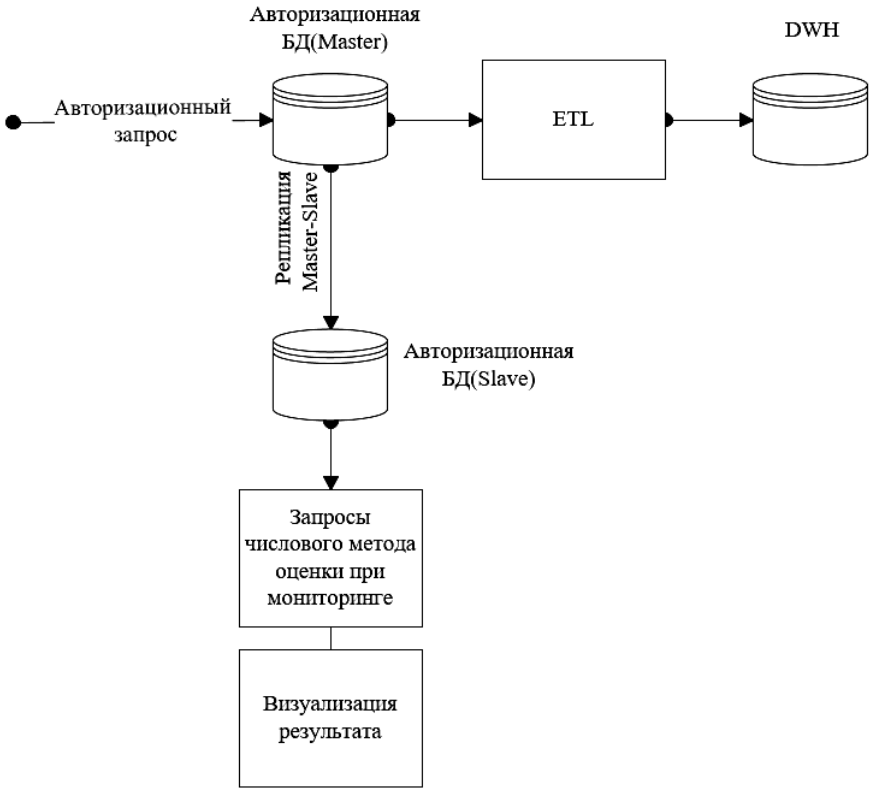

Рис. 1. Архитектура системы мониторинга

Хотя последние 10 лет потери банков от операций по пластиковым картам значительно меньше потерь банков, связанных с клиентским кредитованием, тем не менее, банки и платежные системы уделяют вопросу безопасности операций по пластиковым картам повышенное внимание. Это связано с тем, что в рассматриваемых случаях природа рисков различна. В случае карточного мошенничества страдает клиент. Даже если потери, вызванные мошенничеством, берет на себя эмитент (что случается достаточно редко) моральный ущерб, связанный с возникающими для держателя карты неудобствами, весьма ощутим. Помимо всего прочего это подрывает доверие банковских клиентов к карточной технологии в целом.

К тому же только видимая часть мошенничества составляет около 3 - 4 миллиардов долларов в год. Дело в том, что значительная доля мошенничеств не попадает в отчеты платежных систем, поскольку банки, пытаясь защитить свою репутацию, часто не заявляют о случившихся мошенничествах в платежные системы.

Кроме прямых финансовых потерь банки несут косвенные потери (уход клиентов, уменьшение оборотов, уменьшение притока средств из-за удара по репутации банка — теряется доверие к финансовым продуктам банка). Более 20 тысяч банков эмитируют пластиковые карты. В каждом из них имеется отдел, занимающийся карточной безопасностью. Даже если средний бюджет одного такого отдела составляет 60 тысяч долларов в год, банки ежегодно тратят только на содержание таких отделов более миллиарда долларов. В результате общие годовые потери от последствий карточного мошенничества и затраты на уменьшение этих потерь для банков оказываются значительно больше [1, с. 201].

Вот почему на сегодняшний день так важны современные средства противодействия мошенничеству, организованные на базе систем мониторинга транзакций. Подобные системы позволяют снизить операционный риск банка и обеспечивать проведение операций по пластиковым картам с регламентируемой платежными системами степенью надежности.

Литература

1. Бизнес-энциклопедия «Платежные карты». 2-е изд., перераб. и доп. / И. М. Голдовский, М. Ю. Гончарова, А. Н. Грачев и др.; ред.-сост. А. С. Воронин. М.: КНОРУС, ЦИПСиР, 2014. 560 с.