Как защититься от банковского фрода

Текст: **Виктор Сердюк,** генеральный директор ЗАО «ДиалогНаука»

Сегодня организация защиты от мошеннических действий стала одной из наиболее актуальных задач для большинства российских банков. Это связано с ростом финансовых потерь кредитных организаций вследствие действий злоумышленников, направленных на кражу денежных средств со счетов клиентов банка. При этом потенциальные злоумышленники могут действовать как изнутри, так и извне банка.

Для своевременного выявления фактов мошенничества (или так называемого фрода) необходимо провести анализ банковских транзакций и выявить те из них, которые представляют угрозу для кредитной организации. При этом с учетом того, что количество транзакций весьма велико даже не в самых крупных банках, обработать их в ручном режиме практически невозможно. Именно поэтому для решения данной задачи необходимо использовать специализированные комплексы, позволяющие автоматизировать процесс анализа проводимых банком транзакций. Одним из примеров такого комплекса является продукт FraudView, разработанный компанией ArcSight.

ArcSight FraudView представляет собой специализированный программный комплекс, предназначенный для выявления фактов мошенничества со стороны злоумышленников в кредитно-финансовых организациях. FraudView позволяет легко интегрироваться со всеми основными банковскими системами, включая системы дистанционного банковского обслуживания, автоматизированные банковские системы и др. При этом система позволяет в реальном масштабе времени осуществлять обработку и корреляцию данных, поступающих не только от прикладного ПО, но также и от средств защиты информации, общесистемного ПО, коммуникационного оборудования и т.д. Это позволяет обнаруживать сложные информационные атаки, направленные на совершение мошеннических действий.

«Для своевременного выявления фактов мошенничества необходимо использовать специализированные комплексы, позволяющие автоматизировать процесс анализа проводимых банком 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 (см. врез «Примеры фрода»).

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 ряда основных параметров: тип транзакции, объем платежа, время проведения транзакции, источник платежа, получатель платежа идругих.

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. При этом инвестиции в продукт будут оправданы: перед его внедрением банк может рассчитать показатель возврата инвестиций ROI на основании данных о предотвращенных финансовых потерях.

Дополнительная информация о продукте ArcSight FraudView на сайте ЗАО «ДиалогНаука»: www.fraudview.ru, а также по электронному адресу – fraudview@dialognauka.ru

Примеры фрода

Вот лишь некоторые примеры фрода, которые могут быть выявлены при помощи системы **ArcSight FraudView:**

- 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 дистанционного банковского обслуживания с целью выполнения несанкционированных транзакций;
- Установка на компьютере клиента банка вредоносного программного обеспечения с целью перехвата параметров аутентификации и выполнения транзакций от его имени;
- Несанкционированные действия со стороны администраторов банковских систем, связанные с созданием учетной записи получателя платежа и перевода на него денежных сумм.