Отдельные аспекты криминогенной обстановки в финансово-кредитной сфере Российской Федерации

Крылов Олег Вячеславович

Главное управление безопасности и защиты информации Банка России

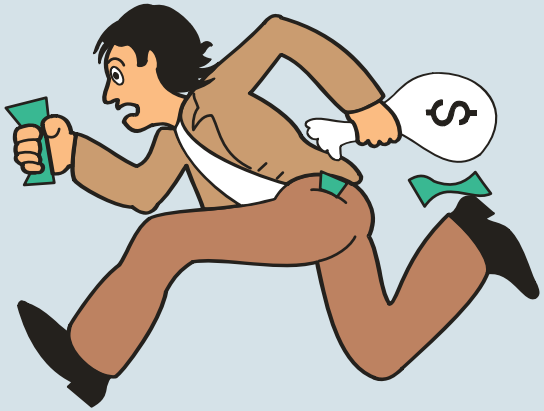
Москва, 20 ноября 2013 года

Преступления в финансово-кредитной сфере

сомнительные банковские операции по «обналичиванию» денежных средств и легализации доходов, полученных преступным путем;

совершение преступлений сотрудниками кредитных организаций;

использование современных банковских технологий в преступных целях;



хищение денежных средств из банкоматов и терминалов;

фальшивомонетничество;

разбойные нападения на структурные подразделения кредитных организаций и лиц, перевозящих ценности и денежные средства.

Сомнительные операции по «обналичиванию» денежных средств

Присвоение активов, легализация (отмывание) денежных средств или иного имущества, приобретенного преступным путем, «обналичивание» наносят серьезный ущерб финансово-кредитной сфере.

Отмечается заметная активизация использования современных технических приемов для хищения денежных средств физических и юридических лиц, как в крупных, так и в особо крупных размерах, все активнее используются технологии безналичных переводов, снятия наличных денежных средств, внедряемых не только через широкую сеть банкоматов и платежные терминалы, но и через Интернет.

Совершение преступлений в финансово-кредитной сфере сотрудниками кредитных организаций

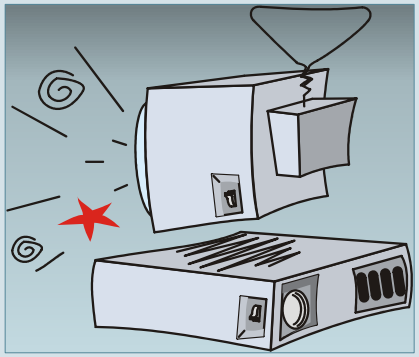
Доступ к банковской информации и возможность ее корректировки, позволяют злоумышленникам, работающим в банковских структурах, действовать в корыстных целях.

Все чаще возникают ситуации, связанные с попытками подкупа заинтересованными лицами сотрудников и руководителей кредитных организаций.

Отмечается активизация преступной деятельности, связанной с упрощенной схемой получения кредитов.

Использование современных банковских технологий в преступных целях

Динамика покушения на хищения денежных средств клиентов кредитных организаций приобретает угрожающий характер, особенно в области ДБО. Выявленные факты покушений, как правило, связаны с неправомерным доступом к компьютерной информации клиентов банков, пользующихся услугами ДБО, что обусловлено малым количеством примеров неотвратимости наказания за совершенные преступления.



Основная доля мошеннических транзакций происходит через удаленные терминалы, банкоматы и интернет.

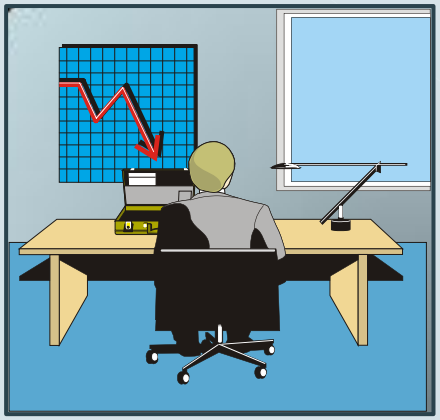
Мошеннические операции с использованием высокотехнологичных методов сегодня не ограничиваются пределами России – данный вид противоправной деятельности транснационален и динамично развивается.

Тенденции характерные для компрометации банкоматов

- рост количества случаев скимминга;
- компрометация пассивных антискиммингоных накладок;
- многократное использование мошенниками одних и тех же банкоматов в течение короткого промежутка времени;

- разнообразие и высокое качество, используемого мошенниками оборудования;
- широкая география использования скомпрометированных данных: Россия, Европа, Латинская и Северная Америка, страны Азии и Ближнего Востока, ЮАР;
- увеличение количества различных сервисов, доступных в банкоматах.

Типичные способы получения неправомерного, несанкционированного доступа к информации пользователей систем ДБО



внедрение вредоносного кода;

сетевые атаки;

атаки на систему авторизации;

перехват управления компьютером клиента;

скимминг;

рассылки электронных сообщений, предлагающих ввести определенную информацию в поля экранных форм, либо содержащих во вложениях вредоносное программное обеспечение;

искажение или подмена содержания платежных поручений;

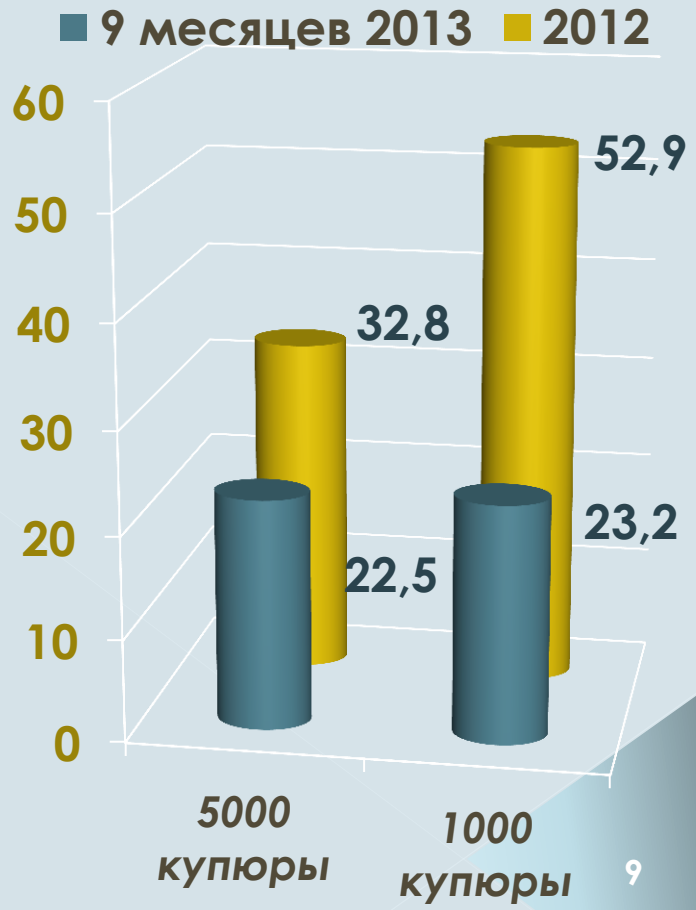
преступный сговор с инсайдерами, недобросовестными сотрудниками банков, которые располагают нужными полномочиями.

Хищения из банкоматов и терминалов

Количество банкоматов, устанавливаемых в сети розничной торговли, растет, вместе с тем не все их владельцы в достаточной степени уделяют внимание технической защите и укреплен-ности непосредственных мест их установки.

Одной из проблем, требующей разрешения в работе по обеспечению защиты банковских объектов, является стремление руководителей кредитных организаций минимизировать расходы на систему своей безопасности, снижая количество используемых услуг, предоставляемых охранными организациями, и недостаточно контролируя их качество. Среди физических атак наиболее актуальными являются взломы банкоматов. Подобные действия могут сопровождаться нападением на охрану, т.к. часто осуществляются в отношении банкоматов, установленных в помещениях, принадлежащих различным организациям.

Количество поддельных денежных знаков выявленных за 9 месяцев 2013 года



Данные выявляемого оборота фальшивых денежных знаков свидетельствует о следующем:

- улучшилось качество подделок, что является следствием профессионального роста преступников;

- большая часть фальшивых денежных знаков изготовлена на специальном высокотехнологическом оборудовании;

- отличить «фальшивки» от подлинных денег без применения специальных приборов и методик стало практически невозможно;

- расширяется география распространения поддельных денег, преступники продумывают пути сбыта «фальшивок» логистически.

Разбойные нападения на структурные подразделения кредитных организаций и лиц, перевозящих ценности и денежные средства

Мишенью грабителей чаще всего становятся небольшие коммерческие банки или их филиалы, которые в основной своей массе пренебрегают необходимыми мерами безопасности – экономят на охранных системах, а порой арендуют для своих офисов такие помещения, попасть в которые не составляет труда.

Отмечается создание устойчивых преступных группировок, специализирующихся на вооруженных нападениях на автомобильный транспорт, обеспечивающий перевозку денежных средств коммерческих банков и других организаций, которым разрешено совершать операции с ценностями, в том числе на инкассаторов РОСИНКАС Банка России.

Спасибо за внимание