Отдельные аспекты криминогенной обстановки в финансово-кредитной сфере Российской Федерации в 2013 году

VI Уральский форум
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ»
17.02.2014-22.02.2014

О.В. Крылов
Начальник Главного управления безопасности и защиты информации Банка России

Банк России

Виды преступлений в финансово-кредитной сфере Российской Федерации в 2013 году

- Сомнительные банковские операции в целях «обналичивания» денежных средств и легализации доходов, полученных преступным путем
- Мошенничество (незаконная банковская деятельность, незаконное получение кредитов, использование в преступных целях современных банковских технологий в системе дистанционного банковского обслуживания и другие виды «киберпреступлений», финансовые пирамиды)
- Злоупотребление служебным положением со стороны руководителей и служащих кредитных организаций, создающих, тем самым, условия для мошенничества, хищений, выводу денежных средств из легального оборота и за рубеж
- Хищение денежных средств с использованием банкоматов и платежных терминалов, как с использованием поддельных пластиковых карт на основе применения нештатного оборудования (скимминг, кеш-трапинг), так и путем их взлома
- Разбойные нападения на подразделения кредитных организации и лиц, перевозящих ценности и денежные средства
- Изготовление и сбыт поддельных денег и ценных бумаг (фальшивомонетничество)

Факторы , повлиявшие на криминогенную обстановку в финансово-кредитной сфере Российской Федерации (1/2)

- Высокий технологический уровень мошенничеств и квалификация задействованных специалистов;
- Активная деятельность криминальных групп, осуществляющих мошеннические деяния в финансово-кредитной сфере Российской Федерации
- Расширение сферы безналичных расчетов;
- Новизна сферы дистанционного банковского обслуживания и специфичность состава преступлений в этой области
- Увеличение числа банкоматов и терминалов для осуществления банковских услуг и платежных операций с использованием кредитных карт и через Интернет

Факторы , повлиявшие на криминогенную обстановку в финансово-кредитной сфере Российской Федерации (2/2)

- Неверные стратегии кредитных организаций по внедрению современных технических продуктов, обеспечивающих надежное функционирование систем информационной безопасности
- Правовой нигилизм в обществе, финансовая и компьютерная неграмотность и неподготовленность значительной части населения и хозяйствующих субъектов к цивилизованной, законопослушной деятельности в условиях рыночных отношений
- Разобщенность действий правоохранительных, контролирующих органов и подразделений безопасности кредитных организаций, недостаточная активность их работы по выявлению правонарушений в финансово-кредитной сфере Российской Федерации

Использование современных банковских технологий в преступных целях

- По итогам 9 месяцев 2013 года количество уголовных дел по преступлениям, совершаемым с использованием информационных и телекоммуникационных технологий, выросло на 12,6% и составило 5796 (в 2012 году – 4703)
- Динамика покушения на хищения денежных средств клиентов КО приобретает угрожающий характер, особенно в области ДБО
- Рост количества пластиковых карт у населения спровоцировал увеличение фактов правонарушений в этой области. По расчетам компании FICO Российская Федерация находится на пятом месте по объему потерь от «пластикового воровства» (в 2012 году они составили около 91,4 млн. евро). Если в 2006 году на РФ приходилось 2% от общемирового ущерба от «карточных мошенников», то в 2012 - уже 6%
- Все чаще фиксируются факты хищения денежных средств через систему «Банк-Клиент», причем сумма несанкционированного списания может быть как внушительной, так и сравнительно небольшой
- Анализ фактов неправомерного списания денежных средств в 2013 году со счетов клиентов КО системы «Банк-Клиент» показал, что клиенты, как правило, не выполняли базовые требования ИБ при переводе денежных средств

Типичный набор «отмычек»-способов получения неправомерного, несанкционированного доступа к информации пользователей систем ДБО

- Внедрение вредоносного кода (вирусы, троянские программы, сетевые черви, программное обеспечение с недекларированными возможностями и т. д.)
- Сетевые атаки (типа «отказ в обслуживании», перехват передаваемой информации, подмена отправителей или получателей информации и т.д.)
- Атаки на систему авторизации (подбор паролей, компрометация аутентификационных данных, несанкционированное использование средств электронной цифровой подписи и т.д.), перехват управления компьютером клиента, искажение или подмена содержания платежных поручений, фишинг
- Рассылки электронных сообщений, предлагающих ввести определенную информацию в поля экранных форм, либо содержащих во вложениях вредоносное программное обеспечение
- Преступный сговор с инсайдерами, недобросовестными сотрудниками банков, которые располагают нужными полномочиями

Новые способы получения неправомерного, несанкционированного доступа к информации пользователей систем ДБО (1/2)

- Участились случаи выявления сайтов, в наименованиях которых содержатся слова «банк», «bank», и предлагающих банковские услуги от лица организаций, в отношении которых Банком России не принимались решения о государственной регистрации и выдаче лицензии на осуществление банковских операций
- Отмечаются случаи направления мошенниками на мобильные телефоны клиентов кредитных организаций SMS посланий, в которых сообщается о необходимости позвонить по номерам телефонов, которые в действительности не принадлежат этим организациям
- Имеют место звонки клиентам с сообщением автоинформаторов о предоставлении тех или иных продуктов и услуг банка с предложением нажать определенные клавиши на телефоне для подтверждения согласия в их приобретении или использовании. Тем самым клиенты банка провоцируются к вступлению в контакты с мошенниками, целью которых может являться получение конфиденциальной клиентской информации (например, номера банковской карты и/или ПИН-кода)

Новые способы получения неправомерного, несанкционированного доступа к информации пользователей систем ДБО (2/2)

- Держателю пластиковой карты на мобильный телефон приходит SMS сообщение о том, что она заблокирована. Для того, чтобы решить проблему предлагается перезвонить по указанному в SMS номеру телефона. Подписывается такое сообщение: «ЦБ РФ», «Служба безопасности Банка России», Федеральной службы судебных приставов или Арбитражного суда
- Клиент принимает решение звонить якобы в Банк России (иную организацию, от чьего имени прислано SMS), где подтверждается блокировка карты. Для разблокировки карту необходимо вставить в банкомат, набрать определенные символы, которые будут продиктованы мошенниками. Эти символы являются номером телефона или счета. Однако комбинация диктуется так, что человеку это непонятно. В итоге клиент выполняет операцию по переводу денег с банковской карты на счет мобильного телефона злоумышленника. Дальше деньги по цепочке пересылаются со счета на счет и, наконец, «обналичиваются» через пластиковую карту.

Некоторые аспекты, связанные с хищением денежных средств из банкоматов и платежных терминалов

- Установка на банкоматы устройства «кеш-трапинг» (ловушки для денег)
- Многократное использование мошенниками одних и тех же банкоматов в течение короткого промежутка времени (имеются факты, когда мошенники в течение 3-4 дней по нескольку раз в день ставили и снимали на один и тот же банкомат считывающее оборудование)
- Разнообразие и высокое качество используемого мошенниками оборудования, которое практически достигло уровня промышленного производства, как по качеству, так и по сложности выявления
- Широкая география использования скомпрометированных данных: Россия, Европа, Латинская и Северная Америка, страны Азии и Ближнего Востока, ЮАР
- Увеличение количества различных сервисов, доступных в банкоматах
- Расширение сети банкоматов без достаточного внимания их технической защите и укрепленности их мест размещения, при минимизации расходов на систему их безопасности
- Игнорирование рекомендаций Банка России об увеличении количества проверяемых банкоматами защитных признаков купюр. Как следствие возможность «Мошеннического обмена» на настоящие банкноты «резано-склеенных» купюр достоинством 5 000 руб.

Основные тенденции, которые в ближайшее время будут влиять на развитие криминогенной обстановки в финансово-кредитной сфере

- Увеличение кредитными организациями масштабов применения IT-технологий, с одновременным увеличением числа банкоматов и терминалов для обеспечения банковских услуг с использованием кредитных карт, операций через Интернет

- Оптимизация и экономия кредитными организациями средств на обеспечение защитных мероприятий

Меры, которые в ближайшее время могут способствовать улучшению криминогенной обстановки в финансово-кредитной сфере

- Обеспечение технической защищенности банкоматов и терминалов, оборудование их средствами охранной сигнализации, размещение в зоне видеонаблюдения
- Консолидация усилий требуется при взаимодействии с органами внутренних дел для пресечения преступлений, в которых используются продукты высоких технологий
- Установление порядков документирования и расследования преступлений, совершаемых в финансово-кредитной сфере с использованием высоких технологий
- Изменение действующей на сегодняшний момент законодательной и правовой базы, которая в настоящее время не в полной мере позволяет организовывать и проводить эффективные мероприятия по пресечению преступлений в финансово-кредитной сфер

Спасибо за внимание!

Крылов Олег Вячеславович
Начальник Главного управления безопасности
и защиты информации Банка России