



СБЕРБАНК

Всегда рядом

Правоприменительная практика в противодействии киберпреступности

Бондарев С.Н., заместитель Директора
Департамента безопасности ОАО «Сбербанк России»

Несанкционированный доступ

Уголовный кодекс России в целом позволяет успешно противодействовать киберпреступности. Возбуждаются и расследуются уголовные дела, выносятся обвинительные приговоры.

- ❖ В ноябре 2013 г. районным судом г.Новосибирска вынесен приговор в отношении бывшего администратора АБС Банка, обвиняемого по ст. **Ст. 159.6** ч.1 УК РФ, **Ст. 159.6** ч.4 (Мошенничество в сфере компьютерной информации), **Ст. 174.1** ч.1 (. Легализация (отмывание)) в совершении хищения из средств со счетов умерших клиентов в размере 11,7 млн. рублей. Приговором суда обвиняемому было назначено наказание в виде **лишения свободы в исправительной колонии общего режима на срок 3 года 2 месяца, наложен штраф в размере 100 тыс. рублей.** Кроме того, суд удовлетворил иск Банка в части возмещения причиненного мошенником финансового ущерба.
- ❖ Районным судом г. Москвы вынесен приговор членам хакерской группы., обвиняемым в совершении преступлений, предусмотренных ч.1 ст. **273** (Создание, использование и распространение вредоносных программ для ЭВМ), ч.2 ст. **272** (Неправомерный доступ к компьютерной информации), ч.4 ст. **159.6** (Мошенничество в сфере компьютерной информации) и ч.3 ст. **30** (Приготовление к преступлению и покушение на преступление) УК РФ. Приговором суда двум обвиняемым было назначено **условное наказание с испытательным сроком на 5 лет,** третьему – **сроком на 4 года, а также наказание в виде штрафа.**

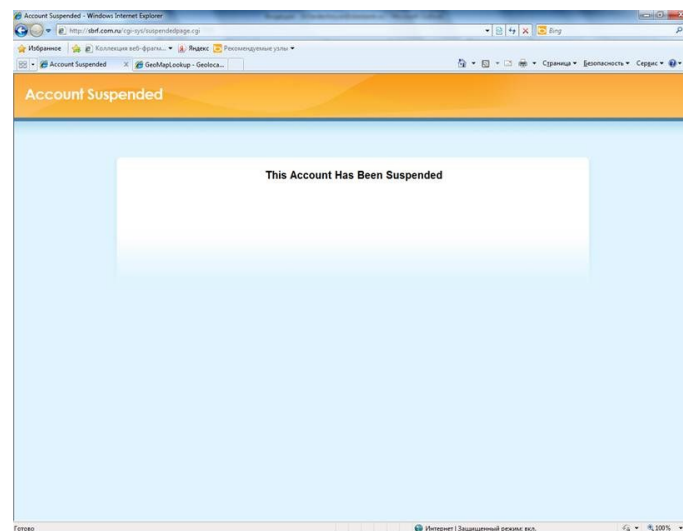
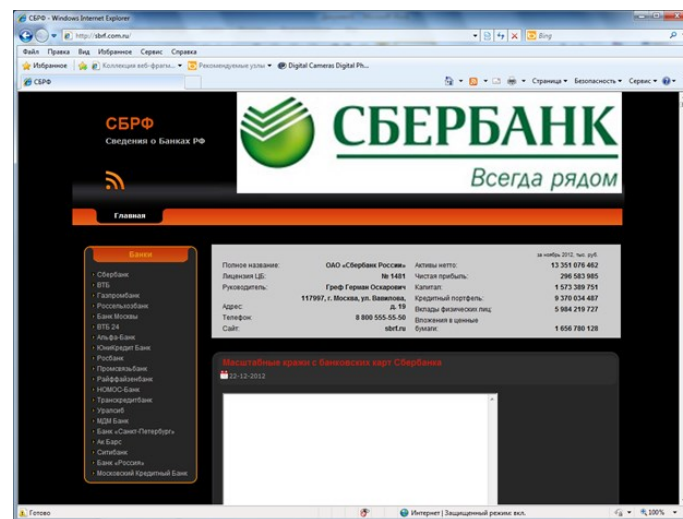
С января 2012 г. на электронные адреса Руководителей банка приходили письма с предложениями продажи доменного имени, схожего по написанию с доменами Банка.

Автор писем угрожал продать домен мошенникам, которые организуют фишинговые атаки на клиентов систем ДБО банка, а также разместить компромат.

Обращение Банка в ГУВД по месту жительства киберсквоттера о проведении проверки по данному факту привело лишь к его переходу на полную анонимность с использованием технологии TOR и началу размещения видеоматериалов негативного характера о банке.

Однако после заявления Банка о возбуждении уголовного дела по статье 179 УК РФ «Принуждение к совершению сделки или к отказу от ее совершения» злоумышленник полностью удалил контент со своего сайта, а затем закрыл его.

В возбуждении уголовного дела было отказано ввиду отсутствия состава преступления по статье 163 (Вымогательство)!!!



Скимминг уже давно стал наиболее быстрорастущим видом высокотехнологичных преступлений против граждан России как по количеству фактов, так и по размеру наносимого ущерба. Производство скиммингового оборудования в основном осуществляется за рубежом на подпольных заводах, обеспечивающих высокий уровень качества изготовления и промышленный дизайн, маскирующий оборудование под штатные элементы банкоматов и терминалов.

Негласно полученные данные держателей передаются через Интернет за границу и в различные регионы страны, где другими лицами происходит изготовление поддельных карт и снятие наличных в банкоматах.

За 2013 год выявлено более 2500 фактов установки скиммингового оборудования на УС Банка. Однако возбуждено только 60 уголовных дел и осуждено 7 человек.

- ❖ В Егорьевске три жителя Молдовы , осуждены по ч.3 ст. **183** (Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну), ч.4 ст. **158 УК РФ** (снятие денежных средств со счетов с использованием поддельных банковских карт и кодов доступа) к **2 годам и 6 месяцам лишения свободы с отбыванием наказания в исправительной колонии общего режима.**
- ❖ В Твери задержанный с поличным скиммингист осужден по ст. **272** УК РФ (несанкционированный доступ к компьютерной информации) с **наказанием в виде штрафа 110 000 руб.**, ст. **138.1** (Незаконный оборот СТС негласного сбора информации) выделена в отдельное производство и направлена по месту приобретения СТС.

Основная проблема:

Для привлечения скиммингистов к ответственности за хищение средств или неправомерный доступ к компьютерной информации необходимо наступление *вредных последствий (нанесение ущерба)*, которые, как правило, существенно разнесены по времени и географически от установки скиммингового оборудования.

В условиях жестких временных процессуальных рамок это крайне тяжело, особенно в регионах, что создает условия для ухода от ответственности пойманных мошенников.

Статья 138.1 *Формально по техническим признакам и характеристикам скимминговое оборудование подходит под классификацию специальных технических средств негласного получения информации:*

- ✓ Скрытая миниатюрная видеокамера;
- ✓ Закладка для подключения к информационному каналу;
- ✓ Маскировка под дизайн мест установки.

Однако статья 138.1:

- ✓ Относится к разделу УК РФ «Преступления против конституционных прав и свобод гражданина»;
- ✓ Подразумевает наличие легального оборота СТС
- ✓ Относится к оперативно розыскной деятельности

Дополнить Уголовный кодекс Российской Федерации новой статьей 187.1, поместив ее рядом со статьей 187 «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов», поскольку предлагаемое для криминализации деяние имеет сходный со статьей 187 родовой объект - использование платежных карт и иных электронных средств платежа в сфере предпринимательской деятельности.

Статья 187.1 Использование технических устройств получения данных владельца платежной карты, необходимых для доступа к его счетам.

1. Неправомерная установка на оборудование кредитной организации, банковского платежного агента (субагента) технических устройств, специально приспособленных для негласного фиксирования и сохранения визуальной и (или) компьютерной информации, необходимой для идентификации владельца платежной карты и доступа к его счетам, а равно изготовление, приобретение, транспортировка, хранение или сбыт таких технических устройств, наказываются принудительными работами на срок до пяти лет либо лишением свободы на срок до шести лет со штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет.

2. Те же деяния, совершенные организованной группой, - наказываются принудительными работами на срок до пяти лет либо лишением свободы на срок до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет или без такового.

Привлечение к уголовной ответственности по действующей статье 187 УК РФ возможно только в случае наличия доказательства самого факта **изготовления с целью сбыта** поддельных карт и других платежных инструментов. Поскольку под **сбытом** понимается **любая форма отчуждения**, а у мошенников, изготавливающих подделки в целях непосредственного хищения средств, **они не отчуждаются, а остаются в руках**, то данное преступное по сути деяние исключаются из-под действия статьи, хотя как раз именно оно наносит гражданам, предприятиям и организациям страны основной материальный и моральный ущерб.

В то же время в отношении преступной деятельности, связанной с подделкой наличных денежных знаков законодатель более последователен и предусмотрел уголовную ответственность не только за изготовление и сбыт фальшивых банкнот, но и за их транспортировку и хранение (статья 186 УК РФ).

Статья 187. Неправомерное изготовление, транспортировка, хранение, сбыт и использование средств платежей, платежных документов.

1. Изготовление и(или) транспортировка, и(или) хранение, и(или) сбыт, и(или) использование поддельных кредитных либо расчетных карт, платежных документов, не являющихся ценными бумагами, а также электронных средств и носителей информации, иных технических устройств, компьютерных программ, предназначенных для неправомерного получения наличных денежных средств или осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов;

Предлагаемые решения Форума



МВД России были отклонены все предложения, поступившие от банка в ходе общественного обсуждения подготовленного министерством проекта Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации», в части статьи 187 УК РФ.

В отличие от статьи 186 УК РФ практическая польза от статьи 187 как в действующей, так и в предложенная МВД России редакции отсутствует.

В связи с этим, предложения ОАО «Сбербанк России» по внесению изменений в статьи УК РФ были направлены в Комитет Государственной Думы по финансовому рынку для внесения в качестве законодательной инициативы.

Призываем банковское сообщество поддержать предложения ОАО «Сбербанк России» и отразить это в решениях Форума.

Введение прямой уголовной ответственности за скимминг сыграет прежде всего огромную профилактическую роль в борьбе с этим видом постоянно растущего мошенничества.

Спасибо за внимание!