

ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ КИБЕРЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ

Игуменцева Н.В., Стеблянка Б.А.

Харьковский национальный университет радиоэлектроники

The number of crimes committed using the Internet is increasing. Criminalization of the Internet facilitates anonymity offender and the ability to remain at a distance of thousands of kilometers away from his victim. One of the dangerous consequences of the possible development of electronic payments is to destroy the system of combating money laundering, the existing banks. In this work we give a brief description assumes some important trends in the use of the Internet for economic crime.

Возрастающие возможности Интернет сегодня активно осваиваются миллионами пользователей. Однако расширение всемирной паутины и возрастание объема и качества доступных ресурсов сопровождается в последние годы стремительным ростом различных злоупотреблений. В условиях широкого распространения интернет-технологий в сфере экономической деятельности киберэкономические преступления сегодня представляют реальную угрозу безопасности потребителей, бизнеса, государства и общества.

Киберэкономические преступления включают в себя:

1. Компьютерную преступность.

Компьютерное преступление как уголовно-правовое понятие - это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства.

Различаются криминологические группы компьютерных преступлений: экономические компьютерные преступления, компьютерные преступления против личных прав и неприкосновенности частной сферы, компьютерные преступления против общественных и государственных интересов. Предметом рассмотрения в данном параграфе являются экономические компьютерные преступления, которые отличаются высокой общественной опасностью и широким распространением.

Компьютерная преступность становится одним из наиболее опасных видов преступных посягательств. Согласно экспертным оценкам, она способна нанести ущерб, сопоставимый с объемом хищений произведений искусства во всем мире.

По данным ООН, уже сегодня ущерб, наносимый компьютерными преступлениями, сопоставим с доходами от незаконного оборота наркотиков и оружия. Только в США ежегодный экономический ущерб от такого рода преступлений составляет около 100 млрд долл. Причем многие потери не обнаруживаются или о них не сообщают.

2. Преступления с использованием банковских карт (кардинг)

Преступления, совершаемые с использованием банковских карт, могут быть объединены в следующие категории:

- злоупотребления с подлинными банковскими картами;
- изготовление поддельных банковских карт;
- сбыт поддельных банковских карт;
- злоупотребления с товарными чеками (слипами);
- использование поддельных банковских карт.

Злоупотребления с подлинными банковскими картами. Данные злоупотребления возможны в случае их попадания в чужие руки, при наличии преступного умысла их законного владельца, а также со стороны руководителей обслуживающих карты лжефирм.

Превышение счета. Данное злоупотребление состоит в получении законным владельцем карты денежных сумм или ценностей, по стоимости значительно превышающих размеры предусмотренного договором лимита.

Фирмы, применяющие в своей работе пластиковые карточки, как правило, имеют ограниченные возможности отслеживания их правомерного использования. В связи с этим в последнее время распространились случаи расчетов чужими карточками в странах, находящихся на значительном удалении от тех, где произошла утеря или похищение.

Ложное заявление о краже или потере банковской карты. Преступление совершает, как правило, законным владельцем карты. Последний подает в банк соответствующее заявление. Как правило, пока процессинговый центр включит номер соответствующей карточки в стоп-лист и известит торговые точки, проходит несколько дней. За это время ее владелец старается провести максимально возможное число операций, а затем выставляет претензии банку.

Временное изъятие карточки у законного владельца для оплаты с ее помощью и присвоения товаров, либо для завышения стоимости фактически оказанных услуг.

Использование карты, которая не была получена законным владельцем, например, по причине перемены им места жительства. В этом случае практикуется

письменное уведомление банка - эмитента с просьбой выслать карточку по новому адресу. Злоумышленникам достаточно узнать о подобном намерении, подделать уведомление о переезде и получить карточку по почте.

Незаконное использование карты в период между открытием счета и доставкой карточки владельцу для совершения операций по ней. Данное злоупотребление является разновидностью предыдущего. Совершаются недобросовестными работниками банков и предприятий, занятых изготовлением карточек.

Похищаемые при пересылке клиенту от эмитента или изготовителя по почте банковские пластиковые карточки представляют для преступников особый интерес по следующим причинам:

- их утрата (кража) замечается с большим опозданием, в результате чего возможность немедленного блокирования карточки отсутствует;
- к моменту кражи они, как правило, не подписаны, поэтому преступник сам может поставить подпись и в дальнейшем использовать их "легально".
- За рубежом уже известны случаи, когда преступники специально устраивались на работу на почту или в частные службы доставки, чтобы изымать отправления с банковскими карточками или перенаправлять их на ложный почтовый адрес.

Мошенничества с банковскими картами в Интернет. С развитием электронной коммерции, появлением виртуальных Интернет-магазинов, где можно сделать заказ на получение товара по почте с персонального компьютера, появляются и новые способы криминальных посягательств с использованием банковских карт (интернет-кардинг). Мошенники пользуются простотой технологии осуществления сделок и несовершенством систем защиты информации в сети.

Так, для оплаты товара в интернет-магазинах достаточно указать реквизиты карточки. При осуществлении любой операции может произойти утечка информации, что чревато для владельца большими потерями. Существует множество различных способов получить у владельца реквизиты карточки.

В настоящее время известно уже около 30 приемов мошеннических действий с помощью Интернета, которые могут практически безнаказанно использоваться мошенниками.

3. Экономическую преступность в Интернет

Возрастающие возможности Интернет сегодня активно осваиваются миллионами пользователей. Однако расширение всемирной паутины и возрастание объема и качества доступных ресурсов сопровождается в последние годы стремительным ростом

различных злоупотреблений. В условиях широкого распространения интернет-технологий в сфере экономической деятельности сетевая преступность сегодня представляет реальную угрозу безопасности потребителей, бизнеса, государства и общества.

Одной из важнейших отличительных особенностей преступлений и злоупотреблений в глобальной сети является специфика способов и приемов их совершения. Эти способы и приемы основаны на использовании возможностей, а также выявлении и эксплуатации уязвимых сторон интернет-технологий.

Рассмотрим классификацию компьютерных преступлений в зависимости от способа использования компьютера при их совершении. Компьютерные преступления, совершаемые в режиме он-лайн, объединяются в три основные категории.

- Компьютер является объектом преступления, когда цель преступника - похитить информацию или нанести вред интересующей его системе.
- Компьютеры используются как средства, способствующие совершению такого преступления как, например, попытка преодоления защиты системы (атака), или более традиционного преступления (например, мошенничества), совершаемого с помощью электронных средств.
- Компьютер используется как запоминающее устройство.

При совершении ряда преступлений могут иметь место все три способа использования компьютера.

Таким образом, число преступлений, совершаемых при помощи информационных технологий, растет, по крайней мере, пропорционально числу пользователей. Криминализации Интернет способствует анонимность преступника и возможность оставаться на расстоянии многих тысяч километров от своей жертвы. Одним из опасных возможных последствий развития электронных расчетов является разрушение системы противодействия отмыванию грязных денег, существующей в банках.