2014

Проект типологического
исследования на тему

Киберпреступность и отмывание денег

Евразийская группа по противодействию легализации
преступных доходов и финансированию терроризма

СОДЕРЖАНИЕ

ВСТУПЛЕНИЕ

Современное общество информационных технологий основано на повседневном использовании компьютерной техники, сетей связи, мобильных средств коммуникации и других технических средств. Ежедневное функционирование государственных структур, банковской, энергетической, транспортной и многих других систем невозможно без надежной работы компьютерной техники и средств коммуникаций. Информационные технологии стали постоянным спутником современного человека не только на рабочем месте, они вошли почти во все сферы человеческой жизни.

Распространение новых информационных технологий, в основе которых лежит широкое использование компьютерной техники и средств коммуникаций, оптимизации и автоматизации процессов во всех без исключения сферах жизнедеятельности, привело вместе с этим к нивелированию границ и переплетению национальных экономик и национальных инфраструктур стран мира.

Более того, указанные тенденции привели к формированию единого мирового информационного пространства, где каждый может получить доступ к любой информации в любой точке планеты, осуществлять дистанционно управление собственными активами и активами компании, заключать хозяйственные договора с иностранными субъектами хозяйствования без необходимости личного контакта и т.д.

Вместе с этим, информационное пространство стало местом и, в то же время, непосредственно инструментом преступления. Отныне преступление не требует предварительной «обработки клиента» и личного контакта с потенциальной жертвой. Главным инструментом преступника становится лишь компьютер и доступ к информационно-коммуникационным системам, где он с помощью компьютерных вирусов и других противозаконных технических средств получает доступ к базам данных, банковским счетам, автоматизированным системам управления.

Так, кражи данных платежных карт (банковских счетов) или данных доступа к системе Интернет-банкинга с целью завладения средствами клиентов банка, кража персональных данных и коммерческой информации из частных компьютеров или серверов, умышленное повреждение информационных систем или средств коммуникаций с целью создания убытков компаниям – это далеко не полный перечень подобных угроз, связанных с бурным развитием современных информационных технологий. Все это приводит к появлению такого понятия как киберпреступность.

При этом киберпреступность приобретает мировой масштаб, новейшие технологии превращают реальных преступников в анонимных, а возможность быстрого обогащения привлекает все больше людей к этой преступной деятельности.

В частности, по разным оценкам Интернетом пользуется до 40% населения планеты (то есть около 2,5 млрд. человек) и при этом, количество Интернет-пользователей постоянно растет. Прогнозируется, что еще около 1,5 млрд. человек получат доступ к Интернету в ближайшие четыре года.

Популярность сети Интернет вполне закономерна, поскольку пользователь имеет возможность: круглосуточного доступа к значительному объему информации; быстрого обмена информацией с другими пользователями; проведение банковских, торговых, биржевых операций с любого места в удобное время и многое другое.

Банковская система является одной из сфер, где наиболее широко и активно используются современные возможности информационных технологий и сети Интернет. А учитывая, что указанные технологии используются для денежных переводов, указанная сфера привлекает все большее внимание преступников.

Наиболее распространенными преступлениями в сфере информационных и компьютерных технологий являются – несанкционированное списание денег с банковских счетов, мошенничество с платежными картами, вмешательство в работу Интернет-банкинга, распространение компьютерных вирусов, DDoS атаки на Интернет-ресурсы, мошенничество в информационных сетях. По оценкам некоторых экспертов ежегодные убытки от деятельности киберпреступников в мировом масштабе превышают 100 млрд. долл. США.

Подготовка и совершение киберпреступлений может осуществлятся не отходя от «рабочего места», то есть такие преступления являются доступными, поскольку компьютерная техника постоянно дешевеет, преступления можно совершать из любой точки планеты, в любом населенном пункте, а объекты преступных посягательств могут находиться за тысячи километров от преступника.

Кроме того, достаточно сложно обнаружить, зафиксировать и изъять криминалистически значимую информацию при выполнении следственных действий для использования ее в качестве вещественного доказательства.

Вышеуказанные особенности данного вида преступлений наряду с их значительной доходностью стали, безусловно, существенными преимуществами по сравнению с другими преступлениями.

Таким образом, проведение типологического исследования относительно основных схем и способов отмывания доходов, полученных в сфере киберпреступности, на сегодня является актуальным и необходимым.

Учитывая актуальность данной тематики на 19-ом пленарном заседании стран – членов ЕАГ, проходившем в ноябре 2013 года, принято решение о проведении в 2014 году типологического исследования на тему «Киберпреступность и отмывание денег». Возглавляет данное исследование

Государственная служба финансового мониторинга Украины (далее Госфинмониторинг).

В рамках исследования Госфинмониторингом был подготовлен вопросник, который разослан странам – участницам типологического исследования.

Исследование проводилось с использованием информации, поступившей в рамках ответов на указанный вопросник от следующих стран:

- Республика Беларусь (член ЕАГ);
- Республика Казахстан (член ЕАГ);
- Республика Таджикистан (член ЕАГ);
- Республика Узбекистан (член ЕАГ);
- Российская Федерация (член ЕАГ);
- Армения (наблюдатель ЕАГ);
- Турция (наблюдатель ЕАГ);
- Украина (наблюдатель ЕАГ);
- Вьетнам;
- Макао;
- Словакия;
- Словения;
- Швеция;
- Эстония.

Основными вопросами, которые рассмотрены в рамках данного типологического исследования являются:

• определение сущности киберпреступности и выявления наиболее распространенных способов совершения киберпреступлений;

• рассмотрение типичных механизмов, методов и инструментов отмывания доходов, полученных в сфере киберпреступности;

• систематизация критериев и признаков для своевременного выявления финансовых операций, которые могут быть связаны с отмыванием доходов, полученных в сфере киберпреступности;

• ознакомление со способами и методами противодействия киберпреступности и отмыванию средств, полученных в сфере киберпреступности.

1. КИБЕРПРЕСТУПНОСТЬ: СУТЬ, ВИДЫ, УГРОЗЫ И РИСКИ

1.1. Международный и национальный аспекты борьбы с киберпреступностью

Вопросы поиска путей предупреждения и противодействия преступлениям с использованием информационно-коммуникационных систем уже долгое время находятся в сфере внимания, как государственных органов, так и международного сообщества.

Принимая во внимание, что развитие технологий идет быстрее, чем принимаются нормативно-правовые акты, которыми они регулируются, а объемы незаконно полученных киберпреступниками средств растут, необходимо на постоянной основе находить пути решения новых задач, связанных с такими сферами, как защита данных, трансграничный доступ правоохранительных органов к данным и обмен информацией между государственными и частными структурами.

Международное сообщество, учитывая негативные последствия этого явления, находится в постоянном поиске мер, которые позволяют минимизировать угрозы влияния киберпреступности на общество. В последние годы наблюдается значительная активность в принятии международных и региональных документов, направленных на противодействие киберпреступности, которые включают как обязательные, так и необязательные к исполнению требования.

Так, в исследовании, проведенном Управлением Организации Объединенных Наций по наркотикам и преступности на тему «Всестороннее исследование проблемы киберпреступности и ответных мер со стороны стран-участниц, международного сообщества и частного сектора», выделено 5 групп документов, в которые входят акты, разработанные в контексте или под эгидой:

I) Совета Европы или Европейского Союза;

II) Содружества независимых государств и Шанхайской организации сотрудничества;

III) Межправительственных африканских организаций;

IV) Лиги арабских государств;

V) Организации Объединенных Наций (далее - ООН).

Все эти документы в значительной степени дополняют друг друга, в том числе в части, которая касается концепций и подходов, описанных в Конвенции Совета Европы о преступности в киберпространстве, принятой 23 ноября 2001 года в Будапеште, Венгрия (далее – Будапештская конвенция). В настоящее время Будапештская конвенция является фундаментом для разработки законодательства по борьбе с

киберпреступлениями как для каждой страны в отдельности, так и для общемирового законодательства.

Будапештская Конвенция требует от государств:

– криминализировать атаки на компьютерные данные и системы (то есть незаконный доступ, нелегальный перехват, вмешательство в данные, вмешательство в систему, злоупотребление устройствами), а также правонарушения с использованием компьютеров (подделка и мошенничество), правонарушения, связанные с содержанием (детская порнография) и правонарушения в сфере авторских и смежных прав;

– совершенствовать законодательство для того, чтобы компетентные органы смогли эффективно проводить расследования киберпреступлений и хранить электронные доказательства, включая срочное сохранение компьютерных данных, срочное сохранение и частичное раскрытие данных о движении информации, обыск и арест компьютерных данных, сбор данных о движении информации в режиме реального времени, перехват данных о содержании информации;

– расширять международное сотрудничество с другими странами-участницами Конвенции через общие (выдача, взаимная помощь, добровольное предоставление информации и т.п.) и специальные мероприятия (срочное сохранение и раскрытие сохраненных данных о движении информации, взаимная помощь по доступу к компьютерным данным, трансграничный доступ к компьютерным данным, создание круглосуточных сетей и т.п.).

Комитет Конвенции против киберпреступности (T-CY) был создан для того, чтобы помочь странам-участницам обмениваться информацией и рассматривать необходимость внесения дополнений или протоколов к Конвенции.

Кроме того, в 2006 году Совет Европы инициировал Международный проект по борьбе с киберпреступностью, который направлен на:

- содействие странам в вопросах совершенствования законодательства;
- обучение сотрудников правоохранительных органов, органов прокуратуры и судейского корпуса;
- укрепление сотрудничества между государственным и частным сектором;
- выработку мер для защиты персональных данных, а также защиты детей от сексуальной эксплуатации и насилия.

Собственная стратегия по решению проблем противодействия киберпреступности разработана также Европейским полицейским ведомством (Европол). В настоящее время Европол оказывает членам ЕС следственную и аналитическую поддержку через свою систему онлайн-расследований и базу данных преступлений.

С января 2013 года под эгидой Европола начал деятельность новый Европейский центр борьбы с киберпреступностью (далее – ЕЦБК). Среди приоритетов ЕЦБК – расследование мошенничества через онлайн-сети, в том числе в системе электронного банкинга и других видах финансовой деятельности, противодействие сексуальной эксплуатации детей через Интернет, а также расследование других преступлений, которые посягают на безопасность важной инфраструктуры и информационных систем ЕС.

За первый год своего существования Европейский центр борьбы с киберпреступностью провел девятнадцать крупных операций против мошенничества в интернете, взлома финансовых сайтов и распространения детской порнографии.

В настоящее время ЕЦБК поддерживает девять проводимых в рамках ЕС крупных полицейских операций против сексуальной эксплуатации детей в интернете. Расследуются факты распространения детской порнографии и ее использования в целях шантажа.

ЕЦБК оказывает оперативную и аналитическую поддержку в 16 расследованиях мошенничества в платежных сетях. В 2013 году раскрыты три международных организации мошенников с кредитными картами.

В результате одной из них арестованы 29 подозреваемых, которые украли 9 миллионов евро у 30 тысяч держателей карт.

В ходе ликвидации другой сети арестованы 59 человек, раскрыты два подпольных цеха считывающих устройств и программного обеспечения, изъяты фальшивые карты и наличные деньги. Члены группы ограбили 36 тысяч держателей банковских карт в 16 европейских странах.

Третья операция была направлена против азиатской преступной сети, которая перехватывала данные кредитных карт при покупке авиабилетов. Данные 15 тысяч карт найдены в изъятых у преступников компьютерах. ЕЦБК координировал операцию в 38 аэропортах 16 европейских стран. Арестовано 117 человек, выявлена их связь с другими преступлениями: наркотрафиком, торговлей людьми, подделкой документов.

Значительную роль в преодолении проблем международного сотрудничества в сфере борьбы с киберпреступностью играет ООН, которая уделяет достаточное внимание вопросам распространения преступлений, связанных с использованием информационных и компьютерных систем, и борьбы с таким преступлениями. ООН неоднократно подчеркивала транснациональный характер киберпреступлений и необходимость координации в мировом масштабе мер по предотвращению таких преступлений и их расследования.

В мае 2011 года Управлением ООН по наркотикам и преступности и Международным союзом электросвязи было подписано соглашение о борьбе с киберпреступностью, направленное на разработку правовых рамок и юридических механизмов противодействия угрозам.

С целью ограничения угроз и незащищенности в информационном пространстве Международным союзом электросвязи, как специализированным учреждением ООН, разработаны: Глобальная программа кибербезопасности; Указания по защите детей в онлайновой среде; Указания для родителей, опекунов и учителей по защите ребенка в онлайновой среде; Указания для отрасли по защите ребенка в онлайновой среде; Указания для директивных органов по защите ребенка в онлайновой среде; Элементы для создания глобальной культуры кибербезопасности.

Экспертами Управления ООН по наркотикам и преступности также отмечается, что формы международного сотрудничества включают выдачу преступников, оказание взаимной правовой помощи, взаимное признание иностранных судебных решений и неофициальное сотрудничество между правоохранительными органами разных стран. Кроме того, неустойчивый характер электронных доказательств в рамках международного сотрудничества в уголовных вопросах в сфере киберпреступности требует своевременного предоставления ответов и наличия возможностей обращаться с просьбой о проведении специализированных следственных действий, таких как сохранение компьютерных данных.

Важным этапом в построении эффективной системы борьбы с правонарушениями в информационном обществе, является разработка Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности.

Основными направлениями взаимодействия и сотрудничества в рамках данного Соглашения являются:

- сближение нормативных правовых актов и нормативно-методических документов государств – участников настоящего Соглашения, регламентирующих отношения в сфере обеспечения информационной безопасности;
- разработка нормативных правовых актов для проведения совместных скоординированных мероприятий в информационном пространстве, направленных на обеспечение информационной безопасности в государствах – участниках настоящего Соглашения;
- разработка и доведение до пользователей нормативных документов, регулирующих вопросы обеспечения информационной безопасности; нормативное правовое обеспечение развития производства программно-технических средств и средств защиты информации;
- разработка межгосударственных стандартов в области информационной безопасности, совместимых с иными международными стандартами в этой области;
- создание защищенных информационных систем различного прикладного назначения;

- организация трансграничной передачи информации;
- совершенствование технологии защиты информационных систем и ресурсов от потенциальных и реальных угроз;
- анализ и оценка угроз информационной безопасности информационных систем;
- совершенствование деятельности в области выявления и нейтрализации устройств и программ, представляющих опасность для функционирования информационных систем;
- реализация согласованных мероприятий, направленных на недопущение несанкционированного доступа к информации, размещенной в информационных системах, и ее утечки по техническим каналам;
- обеспечение защиты информации ограниченного доступа и информационных технологий при взаимодействии информационных систем различных классов защищенности;
- модернизация принадлежащих государствам – участникам настоящего Соглашения сегментов межгосударственных информационных систем и их программного обеспечения;
- установление согласованного порядка сертификации и взаимного признания результатов сертификации средств защиты информации;
- разработка перспективных информационных технологий в области информационной безопасности;
- экспертиза научно-исследовательских и опытно-конструкторских работ, научно-технической продукции в области информационной безопасности;
- профессиональная переподготовка и повышение квалификации кадров в области обеспечения информационной безопасности;
- обобщение, распространение и внедрение передового опыта;
- организация и проведение научных конференций, симпозиумов и совещаний.

В сентябре 2014 года в Сингапуре состоялась презентация здания Международного центра Интерпола по инновациям. Задача Центра – консолидация усилий правоохранительных органов разных стран в борьбе с киберпреступностью. Функционировать Международный центр начнет в 2015 году, после завершения его оснащения суперсовременным оборудованием.

Работа в новом Центре будет сконцентрирована на четырех основных направлениях: оперативная поддержка и содействие расследованиям, инновации, исследования и компьютерная безопасность, подготовка полицейских кадров, международное партнерство и развитие.

На национальном уровне предупреждения преступности состоит из стратегий и мероприятий, направленных на снижение риска совершения преступлений и нейтрализацию потенциально вредных последствий для частных лиц и общества. К числу оптимальных мер в области предупреждения киберпреступности принадлежат принятие законов, стратегий противодействия киберпреступности, эффективное руководство, развитие потенциала органов уголовного правосудия и правоохранительных органов, информационно - просветительская деятельность, создание прочной базы знаний и сотрудничество между органами государственного управления, общинами, частным сектором.

1.2. Суть и виды киберпреступлений

В законодательстве подавляющего большинства стран – участниц типологического исследования отсутствует определение понятия «киберпреступность». Лишь законодательство Республики Казахстан содержит определение информационной преступности (киберпреступности) – вид уголовной преступности, подразумевающий уголовно наказуемые деяния, совершаемые с использованием информационных технологий.

В целом, большинство участников аналогично описывают киберпреступность как незаконные (уголовно наказуемые) действия в сфере информационных (компьютерных) технологий или с их использованием.

Экспертами Управления ООН по наркотикам и преступности отмечается, что определение «киберпреступности» главным образом зависит от того, в каких целях этот термин будет использоваться.

Основу киберпреступности составляют ограниченное число деяний, направленных против конфиденциальности, целостности и доступности компьютерных данных или систем. Однако, если этим не ограничиваться, то в отношении деяний, предусматривающих использование компьютера в целях получения личной или финансовой прибыли или причинения личного или финансового ущерба, включая формы преступлений, связанных с использованием персональных данных, и деяния, связанные с информацией, хранящейся в компьютере (все они входят в более широкое понятие «киберпреступность»), достаточно проблематично найти всеобъемлющее юридическое определение.

В глобальном плане наблюдается широкий диапазон киберпреступлений, которые включают преступления, совершаемые в целях получения финансовой выгоды, преступления, связанные с использованием информации, которая содержится в компьютере, а также преступления, направленные против конфиденциальности, целостности и доступности компьютерных систем.

Будапештская Конвенция, как основополагающий документ в сфере борьбы с киберпреступностью, предоставляет следующую классификацию киберпреступлений:

1) правонарушения против конфиденциальности, целостности и доступности компьютерных данных и систем, в частности:

- незаконный доступ, например, путем взлома, обмана и другими средствами;
- нелегальный перехват компьютерных данных;
- вмешательства в данные, включая умышленно повреждение, уничтожение, ухудшение, изменение или сокрытие компьютерной информации без права на это;
- вмешательства в систему, включая умышленное создание серьезных помех функционированию компьютерной системы, например, путем распределенных атак на ключевую информационную инфраструктуру;
- злоупотребления устройствами, то есть изготовление, продажа, приобретение для использования, распространения устройств, компьютерных программ, компьютерных паролей или кодов доступа с целью осуществления киберпреступлений;

2) правонарушения, связанные с компьютерами, включая подделку и мошенничество, совершенные с использованием компьютеров;

3) правонарушения, связанные с содержанием информации, в частности, детская порнография, расизм и ксенофобия;

4) правонарушения, связанные с нарушением авторских и смежных прав, например незаконное воспроизведение и использование компьютерных программ, аудио/видео и других видов цифровой продукции, а также баз данных и книг.

В то же время, с учетом мотивации преступников, киберпреступления представляется возможным условно разделить на следующие категории:

- кибермошенничество с целью завладения средствами;
- кибермошенничество с целью завладения информацией (для собственного пользования или для последующей продажи);
- вмешательства в работу информационных систем с целью получения доступа к автоматизированным системам управления (для умышленного повреждения за вознаграждение или для нанесения ущерба конкурентам);
- другие преступления.

Первая категория преступлений – присвоение денежных средств, при котором мошенники используют различные способы, иногда вынуждая пользователей самостоятельно раскрывать конфиденциальные данные.

Наиболее распространенные преступления, которые относятся ко второй и третьей категории – это взлом баз данных и вывод из строя компьютерных

систем компаний и государственных организаций, а также кража инноваций или технологий.

В рамках данного исследования наиболее подробно рассмотрены киберпреступления, в результате которых возникает финансовая или иная материальная выгода в виде незаконно полученных доходов. В первую очередь, речь идет об использовании информационно-коммуникационных систем и компьютерных технологий для доступа к частной собственности юридических и физических лиц и дальнейших действий по управлению или распоряжению этой собственностью. В частности, наиболее популярным на сегодня среди киберпреступлений является получение доступа к средствам клиентов банковских учреждений.

В этой категории наиболее распространенными являются следующие виды преступлений:

1) мошенничество в сети Интернет, в частности:

- создание «финансовых пирамид» в сети Интернет;
- мошенничество при продаже товаров (услуг) через Интернет или на Интернет-аукционах;
- деятельность по созданию программных средств с целью хищения финансовой, коммерческой или персональной информации (создание фиктивных WEB-сайтов, распространение компьютерных вирусов и троянских программ, перехват трафика и т.п.);

2) мошенничество в системах дистанционного банковского обслуживания (далее – ДБО), в частности:

- создание компьютерных вирусов и троянских программ для скрытого перехвата управления компьютером клиента с установленным программным обеспечением ДБО;
- открытие счетов, проведение несанкционированных операций и получения наличных средств в результате несанкционированных операций в системах ДБО;
- получение платежей от иностранных отправителей через международную систему SWIFT вследствие вмешательства в работу компьютеров и систем ДБО клиентов иностранных банковских учреждений.

3) подделка платежных карт и банкоматное мошенничество, в частности:

- использование утраченных/похищенных/поддельных платежных карт;
- похищение реквизитов платежных карт, в том числе с применением технических средств их «клонирования»;

- скимминг – изготовление, сбыт и установка на банкоматы устройств считывания/копирования информации с магнитной полосы платежной карты и получение ПИН-кода к ней;
- использования «белого пластика» для «клонирования» (подделки) платежной карты и снятия наличных в банкоматах;
- Transaction Reversal Fraud – вмешательство в работу банкомата при осуществлении операций выдачи наличных, которое оставляет неизменным баланс карточного счета при фактическом получении наличных злоумышленником;
- Cash Trapping – заклеивание диспенсера для присвоения злоумышленником наличности, которая была списана с карточного счета законного держателя карты.

Следует отметить, что стремительное развитие сферы информационных технологий постоянно генерирует новые виды услуг, в том числе в финансовой сфере. Это, в свою очередь, заставляет преступников совершенствовать свои способности и придумывать новые способы незаконного заработка в киберсреде.

1.3. Угрозы и риски, связанные с киберпреступностью

В типологическом исследовании MONEYVAL «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками» рассмотрены следующие риски киберпреступности и отмывания преступных доходов:

- технические риски;
- операционные риски;
- юридические риски;
- географические или юрисдикционные риски.

В то же время, такая классификация является несколько обобщенной и требует более детального рассмотрения с учетом сути угроз и уязвимостей обществу и государству от киберпреступности, последствий их реализации и возможностей им противостоять или уменьшать их влияние.

Исходя из сущности и классификации киберпреступлений выделяют следующие угрозы обществу и государству:

- открытость общества и государства.

Созданная на основе компьютерных сетей и информационных технологий удобная инфраструктура для международных поставок товаров, оказания услуг, перевода средств между физическими и юридическими лицами, хранения информации в сети Интернет и подключение к ней каждого компьютера, предоставляет одновременно широкие возможности,

как собственно для киберпреступлений, так и для отмывания денег от этих или других преступлений с помощью компьютерных технологий;

- скорость и невысокая стоимость преступления.

Вышеуказанная инфраструктура также предоставляет преступникам возможность быстрого доступа к любой информации, документам и наконец, частной собственности, и одновременно к дешевым, оперативным и практически анонимным платежным системам, что позволяет быстро, без дополнительных затрат и эффективно скрыть следы преступления и дальнейшего движения незаконно полученных доходов;

- высокая технологичность.

Чрезвычайно быстрое развитие информационных технологий и сложность этой сферы, наряду с относительно длительным и бюрократическим подходом к развитию нормативно-правовых баз, приводит к значительному отставанию мероприятий по предупреждению и борьбе с киберпреступностью;

- сложный характер преступления.

Кроме того, что киберпреступники получают финансовые или другие материальные выгоды от совершения преступления, они используют компьютерные технологии, информационно-коммуникационные сети из социально-психологических соображений. В частности для дискредитации правительств и государств, создания сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния (что является своего рода дополнением к традиционному виду терроризма);

- анонимность преступления.

Преступников привлекает отсутствие физического контакта с жертвой, относительная мягкость наказания в некоторых странах и, безусловно, сложность обнаружения, фиксации и изъятия криминалистически-значимой информации в виртуальном пространстве;

- транснациональный и популярный характер преступления.

Особенностью данного вида преступности является то, что подготовка и совершение преступления, при наличии доступа к сети Интернет, может осуществляться практически с любого места. А учитывая, что компьютерная техника и Интернет-услуги становятся доступными для все более широкого круга лиц, киберпреступность становится все более популярной.

Транснациональное функционирование предоставляет преступникам очень привлекательные возможности, то есть они могут осуществлять свою деятельность с территорий тех юрисдикций, в которых недостаточно развит режим противодействия киберпреступлениям, а также отмыванию доходов и финансированию терроризма и соответствующий надзор, а также, где они не

станут субъектами расследования, проводимого иностранными правоохранительными органами.

Некоторые страны используются как транзитные узлы, то есть денежные потоки идут в эти страны, но в то же время денежные потоки из этих стран растекаются по другим направлениям;

- организованный характер и смешанный состав участников преступления.

В современных условиях масштабные успешные киберпреступления возможно совершать только при условии соответствующей организации и подготовки, которая носит фактически организованный преступный характер. Действия киберпреступников нацелены главным образом на получение сверхприбылей, что соответственно приводит к увеличению количества компьютерных преступлений именно в финансовой сфере, что требует понимания сферы финансовых отношений и банковской деятельности. При этом киберпреступники активно сотрудничают с представителями традиционной преступности, которые помогают первым трансформировать похищенные средства в наличность.

Все вышеуказанные угрозы приводят к появлению и развитию уязвимостей системы противодействия киберпреступлений, которые в первую очередь связаны с:

- своевременностью выявления киберпреступлений;

- продолжительностью и сложностью расследования и использования доказательств (в том числе в электронной форме) в судебном производстве.

Определенные характеристики электронных платежных систем (относительная легкость создания наряду с низкими затратами на развитие) могут быть факторами риска отмывания преступных доходов. Скорость, с которой проводятся операции, включая трансграничные переводы, только способствуют реализации схем отмывания преступных доходов. Низкая стоимость таких операций означает и низкую стоимость услуг по отмыванию и стимулирует преступников на поиск незаконных источников получения прибыли. Легкая конвертация в реальные деньги и наличные может предоставлять возможность для отмывания денег во многих юрисдикциях.

Следствием значительного количества киберпреступлений в указанной сфере является снижение доверия граждан в целом к надежности финансовой системы, института банковской тайны, надежности защиты персональных данных, а также финансовых операций, проводимых с использованием новейших технологий. При этом недоверие населения к рынкам финансовых услуг не дает возможности активно использовать свободные средства граждан как инвестиционные ресурсы, направляемые на развитие экономики.

В целом такие последствия можно разделить на следующие группы:

- финансовые – потеря средств банковскими учреждениями и их клиентами (юридическими и физическими лицами), недополученная выгода правообладателей, замедление темпов развития банковской сферы;
- имиджевые (репутационные) – раскрытие конфиденциальной информации, в том числе банковской тайны и персональных данных; недоверие клиентов к банковской системе в целом, и системам ДБО в частности, что влечет за собой уменьшение объема безналичных операций;
- юридические – иски клиентов;
- технологические – с целью обеспечения надежной работы информационных, компьютерных и телекоммуникационных систем банковские учреждения, предприятия и организации вынуждены создавать (или приобретать) сложные, дорогие и менее удобные в использовании средства защиты.

1.4. Риски, связанные с дистанционным обслуживанием

На сегодняшний день банковская система большинства стран предоставляет достаточно широкие возможности дистанционного управления финансовыми ресурсами. Наибольшее распространение получили такие системы дистанционного обслуживания как «клиент-банк», «клиент-Интернет-банк», «телефонный банкинг».

Как правило, прежде чем получить доступ к электронным банковским услугам, от клиентов требуется открыть счета, лично явившись в банк, а также пройти надлежащую проверку. Если личная встреча невозможна, то применяются усиленные меры надлежащей проверки клиентов для снижения повышенного риска. Такие меры могут включать предоставление информации, которая может быть проверена по данным из независимого источника, дополнительная проверка предоставляемых документов, подтверждение организации, которая рекомендует клиента и провела в отношении него такую же надлежащую проверку. Однако банкам не рекомендуется открывать счета для оказания электронных банковских услуг без личного контакта с клиентами.

Дистанционная идентификация делает возможным более широкое использование подставных компаний и физических лиц, которым нет необходимости приходить в банк лично, что затрудняет выявление личностей организаторов и исполнителей киберпреступлений.

В дальнейшем при проведении клиентом операции с использованием удаленного доступа, его идентификация может осуществляться с помощью:

- идентификатора (логина) пользователя, пароля, условной фразы, кода, вопросов и ответов (заранее согласованные или задаваемые в определённом порядке вопросы и ответы);

- применения пользователями ключей, смарт-карт, брелоков и т.д.;

- направление одноразового пароля по СМС;

- электронной цифровой подписи.

Подключение финансовой системы к сети Интернет для осуществления дистанционного обслуживания клиентов предоставляет киберпреступникам широкие возможности несанкционированного вмешательства в работу банковских и других платежных систем.

Наиболее значимыми угрозами для систем ДБО со стороны киберпреступников являются:

- кража или изменение (уничтожение) банковской или персональной информации;

- заражение вредоносным программным обеспечением банковских систем;

- блокирование работы систем ДБО с помощью отправки огромного количества массовых запросов через сеть зараженных компьютеров (бот-сеть).

Имеется множество уязвимых мест, связанных с киберпреступностью, в том числе, использование вредоносного программного обеспечения для хищения клиентской информации кредитных учреждений, хищения интеллектуальной собственности, хищения технологий и т.д.

С целью неправомерного получения персональной информации клиентам кредитных организаций по электронной почте могут направляться сообщения, в которых под какими-либо предлогами (техническое перевооружение организации, обновление или сверка баз данных) предлагается ввести с клавиатуры компьютера указанные коды в поля экранных форм в ходе имитируемых сеансов информационного взаимодействия с кредитной организацией (к примеру, через созданный дубликат ее веб-сайта). Одновременно на компьютер клиента с веб-сайта могут передаваться вредоносные программы, являющиеся компьютерными вирусами или «закладками», выполняющими в фоновом режиме работы скрытые функции, связанные с неправомерным получением персональной информации пользователей систем ДБО.

Уязвимости финансовой системы по отношению к киберпреступности в значительной мере обусловлены недостаточно надежным режимом защиты банковской информации.

Зачастую, вместо попыток атаковать банковские системы, имеющие более надёжную защиту, киберпреступники предпочитают использовать

порталы электронной торговли и платежных систем, на которых хранится и обрабатывается большое количество персональных данных и данных кредитных карт. В дальнейшем, похищенные персональные данные и информация о банковских картах используется для проведения незаконных операций через банковскую систему.

Также, уязвимость финансовой системы по отношению к киберпреступности в значительной мере обусловлена низкой осведомленностью клиентов банковских учреждений и несоблюдением основных правил безопасности работы в системах ДБО.

Так, клиенты банков нередко используют нелицензионное программное обеспечение (в частности антивирусную защиту), ненадлежащим образом используют и хранят личные пароли доступа, посещают различные Интернет-ресурсы с компьютеров, на которых установлены системы ДБО. Такие действия, приводят к заражению компьютеров вредоносными программами и облегчают доступ к банковской и личной информации для киберпреступников.

Следует отметить, что в последнее время данная сфера не ограничивается классическим Интернет-банкингом, а также включает в себя электронную торговлю и банковские услуги с использованием мобильных телефонов и карманных устройств.

Киберпреступники активно используют уязвимые места мобильных устройств, и масштабы этой угрозы растут быстрее, нежели в случае персональных компьютеров. В отличие от персональных компьютеров, в которых антивирусные программы обычно устанавливаются производителями при сборке, смартфоны и планшеты, как правило, не оборудованы никаким защитным программным обеспечением или устройствами. Кроме того, владельцы мобильных устройств часто подключают их к бесплатным беспроводным сетям, особенно при выезде за рубеж. Сегодня такие мобильные устройства представляют значительные риски для совершения киберпреступлений.

Киберпреступникам могут осуществлять подмену номера во входящем СМС-сообщении и обманным путём заставляют владельцев мобильных устройств просматривать поддельный URL-адрес. Целью атаки является хищение реквизитов банковского счёта в тот момент, когда клиент заходит на поддельный веб-сайт.

Кроме того, дистанционные операции могут осуществляться третьими лицами, чья личность не установлена банками или платежными компаниями. Подлинная личность людей, проводящих дистанционные операции, остаётся скрытой, и поэтому система может использоваться для осуществления незаконной деятельности или для отмывания денег.

2. ДОХОДЫ В СФЕРЕ КИБЕРПРЕСТУПНОСТИ

2.1. Мошенничество с финансовыми ресурсами с использованием компьютерных технологий и информационно-коммуникационных систем

В рамках данного исследования, под кибермошенничеством понимается мошенничество, совершенное с использованием компьютеров, компьютерных сетей, информационно-коммуникационных систем и сети Интернет.

Следует отметить, что в современных условиях значительная часть традиционного бизнеса переходит в виртуальную среду, что объясняется стремительным развитием сети Интернет. Это, прежде всего, касается размещения в сети Интернет рекламы товаров и услуг и Интернет-торговли, которая является достаточно распространенной в мире и, в определенных сферах, составляет значительную конкуренцию традиционной торговле.

Мошенники так же используют современные возможности сети Интернет для своих махинаций. Достаточно распространенными являются:

- мошенничество при продаже товаров (услуг) через Интернет или на Интернет-аукционах (создание сайтов-двойников известных Интернет-магазинов, продажа несуществующих или поддельных товаров и услуг и т.д.);
- создание «финансовых пирамид» в сети Интернет;
- проведения запрещенных азартных игр онлайн;
- размещения мошеннических объявлений по сбору средств (благотворительные пожертвования) и др.

Пример (Украина)

Гражданин П под видом осуществления законной деятельности филиала Инвестиционной фондовой биржи «К», привлекал лиц для внесения денежных средств с целью проведения рыночной трейдерской деятельности на веб-сайте сети общего доступа Интернет.

Лицам, которые стали членами Инвестиционной фондовой биржи «К» предлагалось получение возможности получить финансовую выгоду не только от личного вклада, но и за счет привлечения к финансовой пирамиде денежных средств других лиц.

Для вступления на биржу в качестве рыночного трейдера, участникам необходимо было осуществить взнос в размере 20,0 тыс. грн. (эквивалент 2,5 тыс. долл. США).

При большем взносе за указанную сумму, трейдерам предлагались более выгодные условия для осуществления деятельности.

После составления фиктивного инвестиционного договора с участниками, на их аккаунты зачислялись средства в электронном виде, однако они имели лишь формальный характер. Самостоятельно перевести заработанные денежные средства в денежную наличность вкладчики не имели возможности. При обращении трейдеров к гражданину П с требованием выплаты заработанных средств или возвращения вложенных денежных средств, последний избегал осуществления выплат.

Инвестиционная фондовая биржа «К» и ее филиалы на территории Украины не зарегистрированы.

Более 50 потерпевшим лицам от незаконной деятельности нанесены убытки на сумму свыше 1,0 млн. грн. (эквивалент 125 тыс. долл. США).

Пример (Украина)

Правоохранительным органом выявлена группа мошенников, которые завладевали средствами граждан под видом реализации товаров на Интернет аукционах.

При прохождении регистрации в качестве продавца товара на Интернет-сайте злоумышленники отмечали данные (ПІБ, идентификационные коды, место жительства, номера банковских карт, другое) посторонних лиц.

Указанные данные они заранее получали из мест лишения свободы.

Кроме того, для регистрации каждого нового аккаунта арендовали в разных городах Украины квартиры с обязательным наличием в них подключения к сети Интернет.

Также, для утаивания своей личности, во время аренды каждой следующей квартиры предоставляли владельцам помещения подделанные документы, которые идентифицируют лицо, а при каждой регистрации на Интернет аукционе использовали новую компьютерную технику и пользовались услугами свыше 10 Интернет провайдеров разных регионов Украины.

Установленное количество пострадавших из всех регионов Украины составляет 140 лиц.

Пример (Украина)

В результате мониторинга сети Интернет правоохранительным органом была получена информация о преступной деятельности ряда лиц, связанной с мошенническим привлечением денежных средств граждан.

Группа лиц в сети Интернет разработала, организовала и администрировала On-line ресурс «А» в котором под видом агентства по

привлечению инвестиций организована деятельность «финансовой пирамиды».

Схема указанной преступной деятельности предусматривала привлечение денег граждан под видом финансовых инвестиций с возможностью получения прибылей в виде дивидендов и подарков, а именно квартир, автомобилей и разных бытовых товаров. В меру увеличения количества инвесторов при наличии достаточного объема инвестиции осуществлены единичные выплаты «дивидендов» отдельным участникам. При достижении момента, когда количество необходимых выплат превышало количество привлеченных средств, деятельность финансовой пирамиды была прекращена.

Около 150 жителей СНГ приняли участие в инвестиционном проекте «А» и вложили средства в сумме свыше 0,5 млн. грн. (эквивалент 62,5 тыс. долл. США).

В результате проведенных в офисе и по месту проживания организаторов пирамиды обысков была изъята компьютерная техника, на которой размещена база участников пирамиды (общая численность превышает 8 тыс. лиц), а также документация о финансовой деятельности инвестиционного проекта.

По факту мошеннических действий было зарегистрировано криминальное производство, по признакам преступления, предусмотренного ч. 3 ст. 190 «Мошенничество» УК Украины.

Пример (Украина)

Граждане Украины, Кипра, Италии, Израиля и неустановленные лица, которые, распределили между собой роли, организовали во всемирной сети Интернет казино, в котором в режиме реального времени ведется игра в такие азартные игры как покер, блекджек, рулетка.

Гражданин Италии и другие неустановленные лица осуществляли финансирование данного проекта. Гражданин Израиля обеспечивал роботу программных комплексов, гражданин Кипра контролировал работу игрового зала, а гражданин Украины содержал и организовывал работу зала, а также осуществлял набор девушек для работы крупье.

Во время игры использовались программные комплексы, которые автоматически считывают игральные карты и место нахождения шарика на рулеточном столе. Ставки принимались от граждан всего мира, включая Украину. Программное обеспечение автоматически определяло выигрыш или проигрыш ставок, а крупье перед вебкамерами осуществляли раздачу игральных карт и руководили рулеткой.

Установлено, что главный сервер, который расположен в Великобритании, является базовой платформой для ресурсов, которые

предоставляют услуги владельцам игральных Интернет ресурсов или залов, как в городе Киеве, так и за границей.

Относительно лиц, которые входили в организованную группу, возбуждено уголовное дело по признакам состава преступления, предусмотренного ст. 203-2 «Занятие игорным бизнесом» УК Украины.

В ходе проведения обыска в помещении игрового зала во время проведения игры задержан гражданин Кипра.

Вместе с ним задержаны 24 крупье и 3 системных администратора, которые осуществляли обеспечение работы компьютеров. Изъято 19 игральных столов, оборудованных сканерами штрих кодов, видеокамерами и мониторами, на которых видно ники игроков и ставки, 22 персональных компьютера, серверное оборудование и документы, которые подтверждают причастность указанных лиц к совершению данного преступления.

2.2. Мошенничество в системах дистанционного банковского обслуживания

В современных условиях системы ДБО (Клиент-Банк, Интернет-Клиент-Банк, Интернет-банкинг и т.п.) стали неотъемлемой частью финансовой системы во всем мире.

Дистанционное банковское обслуживание (ДБО) – общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленно (без визита в банк).

Система ДБО – это многофункциональный программно-технический комплекс, позволяющий клиентам банка готовить и направлять в банк на исполнение платежные и другие документы, контролировать состояние своих счетов, а также получать широкий спектр актуальной финансовой информации без непосредственного обращения в банк.

Использование системы ДБО, бесспорно, имеет свои преимущества. Прежде всего следует выделить следующие:

- оперативность и экономичность. Использование системы ДБО позволяет из офиса осуществлять управление финансовыми потоками предприятия и существенно сокращает затраты рабочего времени персонала, связанные с посещением банка;
- простота и удобство. Автоматизация процесса подготовки платежных и других документов, а также наличие программного контроля по заполнению обязательных реквизитов в документах значительно упрощает пользование подсистемами и позволяет минимизировать операционные ошибки;

- безопасность и эффективность. Система ДБО, при условии правильного использования, позволяет увеличить безопасность и конфиденциальность документооборота с банком; в любой момент получить выписку, которая содержит информацию обо всех входящих и исходящих документах в расширенном формате, без посещения банка.

В то же время, системы ДБО, как инструмент доступа к денежным переводам, сегодня все чаще становятся мишенью для киберпреступников.

Вмешательство в работу систем ДБО обычно происходит путем заражения компьютера вирусным программным обеспечением через вредоносную спам-рассылку, посещение зараженных сайтов или использование зараженными носителями информации.

Загрузки вируса на компьютер жертвы происходит практически незаметно. Основная задача вируса на начальном этапе – это наблюдение, сбор информации и передача его на компьютер мошенников. Вирус может похищать пароли доступа к системам ДБО, ключи электронной цифровой подписи, считывать реквизиты платежей. Это также могут быть программы, которые отслеживают появление на экране окна подключение к ДБО с целью дальнейшего перехвата секретной информации, которая вводится в это окно, или копируют содержимое буфера обмена в момент подключения к системам электронных платежей.

Цель мошенников исказить информацию, сформировать с помощью ДБО и провести платеж, который по содержанию не будет выделяться в потоке обычной деятельности жертвы, но переведет деньги на счета подставного лица или фиктивной фирмы, используя обычное для данного клиента назначение платежа. В дальнейшем чаще всего украденные средства со счета переводятся в наличные. Снятие наличных производится в основном через банкоматы с целью избежания общения с работниками банка.

Пример (Украина)

На счет гражданина Украины Г от компании-нерезидента, зарегистрированной на территории США, зачислены денежные средства в сумме 0,4 млн. долл. США (3,1 млн. грн.) как оплата труда по контракту.

Вместе с тем, получатель средств – гражданин Г – является молодым человеком (18 лет). Информация относительно официальных доходов отсутствует, хозяйственной деятельностью не занимается.

По информации правоохранительных органов США средства были перечислены в результате вмешательства неизвестного лица в компьютерную сеть компании-нерезидента с использованием вредоносного программного обеспечения – трояна Zeus.

С учетом информации правоохранительных органов США ПФР Украины принято решения относительно остановки финансовых операций по счету гражданина Украины.

Возбуждено уголовное дело по ч. 1 ст. 190 «Мошенничество» УК Украины. Следствие продолжается.

Пример (Украина)

Гражданин М познакомился с неустановленным следствием лицом, которое предложило ему принять участие в завладении средствами ООО «А».

В дальнейшем гражданин М, используя заведомо подделанный паспорт, выданный другому лицу, обратился в офис ООО «Б» с целью регистрации ООО «К» как директор и единый учредитель.

Для осуществления незаконной деятельности, связанной с завладением средствами ООО «А», уполномочил работников ООО «Б» быть его представителями во всех учреждениях и организациях независимо от форм собственности по вопросам проведения государственной регистрации.

В дальнейшем было зарегистрировано ООО «К» и открыто текущий счет в банке «Ф».

Также с помощью системы «Клиент-Банк» созданы поддельные платежные документы на перевод средств в сумме 3,7 млн. грн. (эквивалент 0,5 млн. долл. США) со счета ООО «А» на счет ООО «К».

В этот же день гражданин М, как директор ООО «К», обратился в банк «Ф» и по поддельным денежным чеками получил в кассе указанного банка средства в сумме 3,7 млн. грн. (эквивалент 0,5 млн. долл. США)

Приговором суда гражданин М признан виновным в совершении преступлений, предусмотренных ч. 4 ст. 190 «Мошенничество», ч. 2 ст. 200 «Незаконные действия с документами на перевод, платежными картами и другими средствами доступа к банковским счетам, электронными деньгами, оборудованием для их изготовления», ч. 1 ст. 205 «Фиктивное предпринимательство» УК Украины и назначено наказание в виде 8 лет лишения свободы с конфискацией всего имущества.

В дальнейшем постановлением апелляционного суда назначено наказание гражданину М по ч. 4 ст. 190 «Мошенничество» УК Украины в виде 6 лет лишения свободы с конфискацией всего имущества.

Пример (Украина)

Правоохранительным органом выявлен факт несанкционированного вмешательства в систему «Клиент-Банк» Госпредприятия «Ц» и незаконного перечисления с расчетного счета указанного предприятия

средств в сумме 2,0 млн. грн. (эквивалент 250 тыс. долл. США) на счета четырех предприятий, открытых в разных банках.

По данному факту начато криминальное расследование по признакам преступления, предусмотренного ч. 2 ст. 361 «Несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи» УК Украины.

В ходе досудебного следствия установлено, что компьютер Госпредприятия «Ц», на котором установлена система «Клиент-Банк», был заражен вредным программным обеспечением, и через удаленный доступ злоумышленники, используя электронные ключи с цифровыми подписями должностных лиц, сформировали и отправили соответствующие платежные доверенности от лица этого предприятия. Компьютер изъят и направлен на исследование.

Работниками правоохранительного органа срочно предоставлена информация ПФР Украины, которым остановлены расходные операции по счетам указанных субъектов предпринимательской деятельности.

Следствие продолжается.

Пример (Беларусь)

Четверо граждан Республики Беларусь действуя в составе организованной преступной группы с иными неустановленными лицами, в период с января по апрель 2010 года, находясь на территории Республики Беларусь в г. Минске, в г. Киеве Украины, под предлогом продажи антивирусного программного обеспечения получали сведения о личных данных пользователей сети интернет и реквизитах их банковских пластиковых карточек, которые впоследствии использовали путем введения в компьютерные системы процессинговых центров платежных систем и банковских учреждений США и иных государств заведомо ложной информации о якобы покупке антивирусного программного обеспечения, в результате чего совершили хищения денежных средств на общую сумму 5 млд. 160 миллионов рублей (189 227 эпизодов).

Пример (Таджикистан)

Неизвестными лицами путем взлома системы защиты пункта денежных переводов филиала одного из банков в г. Y, нанесено ущерб на сумму 130 200 долларов США, путем перевода их на счета нескольких граждан другой страны. Ведется уголовное расследование по статьям 298 ч.1 «Неправомерный доступ к компьютерной информации» и 244 ч.4 «Кража» УК Республики Таджикистан.

2.3. Подделка платежных карт и банкоматное мошенничество

Платежные карты в современных условиях являются не только средством для получения заработной платы, пенсии или иных зачислений, но и эффективным и удобным инструментом для полноценного банковского обслуживания.

Использование платежных карт позволяет:

- уменьшить объемы использования наличных;
- дополнительно защитить денежные средства (при утере карты денежные средства блокируются и остаются на счете держателя карты);
- проводить операции не только в национальной, но в иностранной валюте (мультивалютные карты);
- проводить расчеты круглосуточно и в разных странах мира.

Значительные объемы финансовых операций с использованием платежных карт является основным фактором, который привлекает к этой сфере особое внимание преступников. С целью завладения денежными средствами держателей платежных карт преступники придумывают самые разнообразные способы. Это в частности могут быть:

- технические устройства, которые устанавливаются на банкомат с целью завладения платежной картой или деньгами;
- электронные устройства, которые позволяют считывать необходимую информацию с платежной карты или с клавиатуры банкомата;
- заражения компьютеров специализированными вирусами с целью получения информации о платежных картах (путем подделки или взлома сайтов, использование бот-сетей для рассылки вредоносного спама);
- подделка платежных карт с использованием похищенной информации;
- телефонное мошенничество (когда преступники выдают себя за сотрудников банка и пытаются получить необходимую информацию).

Существует множество видов мошенничества с платежными картами и банкоматами (фишинг, фарминг, трешинг, скимминг, траппинг, фантом, шаттер, шимминг и т.д.), но все они направлены на похищение непосредственно денежных средств, платежной карты или ее реквизитов, таких как:

- номер карты;
- дата выпуска/окончания действия карты;
- код CVV2 (трехзначное число на обратной стороне платежной карты, служит кодом подтверждения операций, совершаемых в сети Интернет или с помощью телефона);

- написания фамилии и имени клиента на латыни;
- ПИН-код.

При этом похищенная информация может быть использована преступниками не только для подделки платежной карты или списания средств, но и выставлена на продажу на специализированных сайтах или форумах.

Пример (Украина)

Гражданин М с целью завладения чужим имуществом посредством обмана, используя электронно-вычислительную технику через сеть Интернет заказал на имя гражданина Б телевизор марки «Самсунг», за который осуществил перечисление средств на счет ФЛП «К» с использованием реквизитов банковской карты, которая принадлежит неустановленному следствием лицу, и соответственно которая не принадлежала гражданину М.

В этот же день телевизор марки «Самсунг» стоимостью 16,6 тыс. грн. (эквивалент 2,1 тыс. долл. США) получил гражданин Б, который уплатил гражданину М средства в сумме 7,0 тыс. грн. (эквивалент 0,9 тыс. долл. США), поскольку последний сообщил гражданину Б неправдивую информацию о том, что он договорился с продавцом относительно продажи товара по заниженной цене. Таким образом, гражданин М распорядился данным имуществом на собственное усмотрение.

Кроме того, гражданин М с целью завладения чужим имуществом посредством обмана, используя электронно-вычислительную технику через сеть Интернет повторно заказал телевизор марки «Самсунг» и ноутбук, за который осуществил перечисление средств на счет ФЛП «К» с использованием реквизитов банковской карты, которая принадлежит неустановленному следствием лицу, и соответственно которая не принадлежала гражданину М.

В этот же день по месту проживания гражданина М была доставлена заказанная продукция на сумму 14,4 тыс. грн. (эквивалент 1,8 тыс. дол. США), которой гражданин М распорядился по собственному усмотрению.

В дальнейшем банковским учреждением, через которое проходили несанкционированные операции, подтверждена незаконность перечисления средств, в результате чего ФЛП «К» причинен имущественный вред на вышеуказанные суммы.

Приговором суда гражданин М признан виновным в преступлении, предусмотренном ч. 3 ст. 190 «Мошенничество» УК Украины и назначено ему наказание в виде 4 лет лишения свободы, но в силу ст. 75 «Освобождение от отбытия наказания с испытанием» УК Украины освобожден от отбытия наказания с испытанием (установлен испытательный срок 3 года).

Пример (Украина)

В правоохранительные органы обратился директор банковского учреждения относительно несанкционированной установки считываемых устройств на банкоматы указанного банка и дальнейшего снятия денежных средств с карточных счетов клиентов.

В результате оперативных мероприятий был задержан на месте преступления гражданин Республики Болгария, который с целью похищения денег с банковских счетов путем использованием подделанных платежных карт устанавливал самодельные устройства для считывания информации из банкоматов указанного банковского учреждения.

В ходе проведения досудебного следствия установлено, что злоумышленник входил в преступную группу в количестве 5 граждан Болгарии, которые совершали аналогичные преступления на территории Украины и государств СНГ.

Также разоблачено и задержано на месте совершения преступления другого члена указанной преступной группы – гражданина Республики Болгария, который с целью незаконного снятия денежных средств с банковских счетов путем использования подделанных платежных карт несанкционированно установил самодельные устройства для считывания информации из банкоматов другого банковского учреждения.

По месту его временного проживания в номере отеля были изъяты самодельные устройства для считывания информации с платежных карт.

Криминальные производства открыты за совершение преступлений, предусмотренных ч. 3 ст. 190 «Мошенничество» и ч. 1 ст. 200 «Незаконные действия с документами на перевод, платежными картами и другими средствами доступа к банковским счетам, электронными деньгами, оборудованием для их изготовления» УК Украины.

Пример (Украина)

Правоохранительным органом в ходе досудебного следствия установлено, что группой граждан Румынии на входной двери банковского учреждения установлено скимминговое устройство, предназначенное для считывания магнитной полосы банковской платежной карты, и видеокамеру для снятия информации о пин-кодах карт. В дальнейшем указанные граждане изготовили дубликаты банковских платежных карт, эмитированных украинскими банками, и сняли в банкоматах со счетов клиентов банковского учреждения денежные средства в сумме 14,7 тыс. грн. (эквивалент 1,8 тыс. долл. США).

Во время попытки снятия установленного скимминговое устройства двое граждан Румынии были задержаны.

Приговором суда вышеупомянутые граждане осуждены по ч. 2 ст. 185 «Кража», ч. 3 ст. 190 «Мошенничество», ч. 2 ст. 200 «Незаконные действия с документами на перевод, платежными картами и другими средствами доступа к банковским счетам, электронными деньгами, оборудованием для их изготовления», ст. 231 «Незаконный сбор с целью использования или использование сведений, которые представляют коммерческую или банковскую тайну» и вынесен приговор в виде 3 лет лишения свободы и штрафа в размере 85,0 тыс. грн. каждому (эквивалент 10,6 тыс. долл. США).

Пример (Беларусь)

Четверо граждан Республики Беларусь действуя по предварительному сговору, с целью совершения хищения денежных средств, установили в банкоматах одного из белорусских банков, специальные устройства, предназначенные для считывания информации с магнитных полос банковских карточек, и осуществили несанкционированное копирования информации, держателями которых они не являются. После чего похитили принадлежащие клиентам банковских учреждений Республики Беларусь денежные средства в общей сумме 98 миллионов рублей (260 эпизодов). В ходе обыска по месту жительства указанных лиц была обнаружена подпольная лаборатория по производству специальных устройств, предназначенных для считывания информации с магнитных полос банковских карточек. Изъято 3 готовых устройства и 69 заготовок.

Пример (Казахстан)

Менеджером по развитию кредитной политики одного из белорусских банков гражданкой Г установлена недоработка банковской программы STL, отвечающей за формирование заявки на выдачу кредитов, о чем был поставлен в известность судимый за убийство гражданин Ч.

Создав преступную группу из 4-х человек, гражданин Ч изготовил 24 кредитные карты (на данные карты было начислено более 1,4 млрд. тенге), при оформлении которых использовались сведения реальных людей. В результате преступных действий было похищено 395 млн. тенге, остальные средства заблокированы.

За совершение преступлений гражданин Ч осужден к 10 годам лишения свободы, его соучастник гражданин П (сотрудник службы безопасности банка) к 8 годам лишения свободы. Уголовное дело в отношении трех других лиц прекращено за примирением сторон.

Пример (Казахстан)

В апреле 2013 года в г. Алматы задержан граждан Молдавии, который приехал в Казахстан для совершения хищений денежных средств с пластиковых счетов граждан путем установления на банкоматы скимминговых устройств. По результатам расследования ему доказана вина в совершении 4 краж, последний осужден к 3,5 годам лишения свободы. Также в апреле 2013 года в г. Алматы за аналогичное преступление задержан гражданин Болгарии, который осужден к 5 годам лишения свободы.

2.4. Киберпреступность нефинансового характера

В рамках данного исследования, к киберпреступлениям нефинансового характера, отнесены преступления в киберпространстве, которые непосредственно не касаются сферы финансовых услуг и перевода денежных средств. Однако получение незаконных доходов является основной целью совершения этих преступлений.

К таким преступлениям следует отнести:

- выведение из строя компьютеров и компьютерных сетей (DDoS-атаки на сайты, блокирование работы конкурентов и т.д.);
- похищение деловой или личной информации;
- кибер-вымогательство, запугивание, клевета и распространение ложной информации в сети Интернет;
- нарушением авторских и смежных прав путем незаконного воспроизводства и использования компьютерных программ, размещения в сети Интернет аудио/видео и других видов цифровой продукции;
- преступления, связанные с содержанием данных, в частности, детская порнография, детская эксплуатация и сексуальное насилие, расизм, ксенофобия.

Пример (Украина)

Группой лиц организованы компьютерные атаки и похищена бизнес-информация из рабочих компьютеров граждан Турции, США и Германии.

В дальнейшем, за возвращение похищенной информации требовались денежные средства, которые были присланы в Украину через Western Union в пользу организатора схемы и сняты наличными с карточного счета доверенным лицом.

Общая сумма полученных физическими лицами средств составляет 20,0 тыс. долл. США.

Правоохранительным органом по материалам ПФР Украины ведется досудебное расследование по ч. 3 ст. 209 «Легализация (отмывание) доходов, полученных преступным путем» УК Украины.

Пример (Украина)

Гражданин М осуществлял компьютерные атаки (DDoS) на информационные ресурсы украинских и зарубежных коммерческих структур. С помощью специально модифицированного вредоносного программного кода он создавал бот-сети (большое количество инфицированных компьютеров).

В частности, для совершения атак использовалось программное обеспечение «DirtJumperV5», которое позволяло удаленно управлять сетью из более чем пяти тысяч «зомбированных» (зараженных) компьютеров, расположенных в разных странах мира. Гражданин М с использованием бот-сетей осуществил более 50 DDoS-атак.

Атаки проводились по заказу конкурирующих бизнес-структур.

Гражданин М принимал оплату с помощью виртуальных платежных систем (Интернет-кошельки были зарегистрированы на подставных лиц). Для соединения с системой Интернет на условиях предоплаты использовал радиомодемы.

Приговором суда за совершение преступления, предусмотренного ч. 1 ст. 361 «Несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи» УК Украины задержанный осужден к уплате штрафа в размере 700 необлагаемых минимумов доходов граждан 11,9 тыс. грн. (эквивалент 1,5 тыс. долл. США), с конфискацией программных и технических средств, с помощью которых было совершено несанкционированное вмешательство.

Пример (Беларусь)

16 октября 2012 года в результате проведения комплекса оперативно-розыскных мероприятий по месту жительства задержан официально неработающий, выпускник одного их белорусских университетов, имеющий ученую степень магистра технических наук, который в период с июня по июль 2012 года с использованием вредоносного программного обеспечения осуществил умышленное блокирование персональных компьютеров на территории Республики Беларусь.

Так, в вышеуказанный период от граждан Республики Беларусь в УРПСВТ МВД поступали многочисленные сообщения о том, что принадлежащие им компьютеры после работы в сети Интернет по неустановленной причине не функционируют, т.е. при загрузке операционной

системы деятельность всех устройств ввода-вывода (клавиатура, «мышь») прекращалась, а на экране появлялось сообщение о том, что компьютер заблокирован Министерством внутренних дел Республики Беларусь за просмотр и распространение порнографических материалов. Согласно тексту сообщения, для разблокировки ЭВМ, пользователю необходимо осуществить перечисление денежной суммы в размере 100 000 белорусских рублей на счет электронного кошелька системы «EasyPay», либо пополнить баланс мобильного телефона оператора «Life».

Вышеуказанные обстоятельства дискредитировали Министерство внутренних дел Республики Беларусь и негативно повлияли на имидж правоохранительных органов.

Пример (Беларусь)

Гражданин Республики Беларусь в период с марта 2012 года по декабрь 2012 года путем использования персонального компьютера и самостоятельно разработанного программного обеспечения осуществил несанкционированный доступ к компьютерной информации, хранящейся в компьютерной системе одного их белорусских предприятий.

Также он осуществил несанкционированное копирование информации, хранящейся на машинных носителях персональных компьютеров жителей г. Минска, в том числе информации о реквизитах доступа к системе «Интернет-банкинг», электронных почтовых ящиках, личных страницах в социальной сети.

Кроме этого он с целью несанкционированного копирования информации, хранящейся в компьютерной сети БГУ, самостоятельно разрабатывал и использовал вредоносное программное обеспечение.

По данным фактам возбуждены уголовные дела по ст.349 «Несанкционированный доступ к компьютерной информации», ст.352 – 3 «Неправомерное завладение компьютерной информацией», ст.354 «Разработка, использование либо распространение вредоносных программ» УК Республики Беларусь.

Пример (Узбекистан)

Органами внутренних дел расследовалось уголовное дело, возбужденное в отношении иностранного гражданина А по п.«а» ч.2 ст.278-3 «Изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе» УК Республики Узбекистан.

В ходе расследования уголовного дела установлено, что гражданин А по предварительному сговору с неустановленными следствием лицами Б и В, в период с ноября 2011 года по 31 января 2012 года с целью незаконного

доступа к защищенной компьютерной системе, обеспечивающей международную телефонную связь, нарушив установленные законодательством требования, установил и подключил специальное техническое оборудование к Интернету, посредством которого вышеуказанные лица незаконно осуществляли звонки из-за рубежа на территорию Республики Узбекистан, минуя технические средства телекоммуникационной компании».

Общая продолжительность разговоров по указанным звонкам составила 5.002.843 минут, чем телекоммуникационной компании был нанесен ущерб в размере 280.159,21 долларов США.

По данному факту гражданин А привлечен к уголовной ответственности в качестве обвиняемого в совершении преступления, предусмотренного п. «а» ч. 2 ст. 278-3 «Изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе» УК Республики Узбекистан. Уголовное дело в отношении «А» 29.11.2012 года направлено в прокуратуру с обвинительным заключением в порядке ст. 381 «Направление уголовного дела прокурору» УПК Республики Узбекистан.

3. КИБЕРПРЕСТУПНОСТЬ И ОТМЫВАНИЕ ПРЕСТУПНЫХ ДОХОДОВ

В отличие от «традиционного» отмывание денег, для осуществления которого используется банковская система, кибер-отмывание основано на использовании различных видов операций и поставщиков финансовых услуг, начиная с банковских переводов, внесения/снятия наличных, использования электронных денег и заканчивая «денежными мулами» и услугами по переводу денег.

Обычно цепочка прерывается на операции с наличными средствами, проводимой как правило «денежными мулами», за которой следует использование традиционной платежной системы. Если в соответствующий платежный сервис интегрированы услуги онлайновых платежей, то деньги могут быть переведены в электронные и без промедления, практически анонимно, переведены в другое государство.

Таким образом, выявление и преследование преступных денежных потоков является достаточно сложной задачей для правоохранительных органов.

Такие запутанные схемы являются вызовом мощному, но традиционному программному обеспечению для сбора данных в сфере противодействия отмыванию доходов и финансированию терроризма, основанном на поведении клиента, если часть «отмывочной» цепочки реализуется в совершенно иной финансовой ситуации.

Методы осуществления платежей в Интернете предоставляют возможность удаленно осуществлять финансовые транзакции практически из любой страны. Это является еще одним препятствием для правоохранительных органов в части выявления и преследования преступных доходов.

3.1. Основные механизмы отмывания преступных доходов, полученных от киберпреступности

Полученные преступным путем доходы требуют от преступников быстрого и эффективного проведения их легализации. Причем, учитывая специфику киберпреступности, организаторы и исполнители схем преимущественно являются образованными и технически грамотными людьми, соответственно и методы, которыми они пользуются при легализации полученных средств, могут также быть довольно сложными и нестандартными.

Инструменты и механизмы, которыми пользуются преступники во время осуществления отмывания доходов, полученных в сфере киберпреступности, являются достаточно разнообразными. В частности при

отмывании доходов от киберпреступлений характерным является использование следующих механизмов:

- использование счетов, открытых по утраченным документам или на подставных лиц;
- использование фиктивных (транзитных) предприятий;
- проведения цепи финансовых операций через несколько банковских счетов с помощью удаленного доступа;
- использования наличных на последнем этапе цепи финансовых операций;
- использования альтернативных платежных систем (электронные платежи), как национальных, так и международных;
- покупка электронных денег и использования систем платежей через электронные кошельки;
- конвертация незаконных доходов в товары путем приобретения последних через сеть Интернет.

Перевод похищенных средств в наличность является распространенным, поскольку дальнейшее перемещение наличности вне банковской системы почти невозможно отследить. Широко практикуется снятие наличных через банкоматы с целью избегания общения участников схемы с работниками банковских учреждений. В дальнейшем наличные средства через курьеров (денежных мулов) могут быть беспрепятственно переданы анонимном организатору киберпреступления.

Полученные преступным путем средства используются для покупки высоколиквидных товаров или предоплаченных карт для дальнейшей их перепродажи и получения наличных. Также средства могут быть использованы для приобретения через Интернет билетов, проездных документов, предметов быта и других товаров для дальнейшего их использования, перепродажи и получения наличных денежных средств.

Часть преступных доходов используется на приобретение нового оборудования и разработку более эффективного вредоносного программного обеспечения с тем, чтобы обойти системы безопасности.

Следует отметить также, что основаниями для платежей, связанных с несанкционированным списанием денежных средств, могут быть разнообразные назначения, которые не дают возможности отделять их от других финансовых операций.

В то же время, иногда преступники указывают достаточно специфические основания для зачислений денежных средств из-за рубежа, в частности выигрыш в казино, продажа прав интеллектуальной собственности, продажа веб-сайтов или Интернет-магазинов, виртуальных казино и т.д.

Пример (Украина)

Выявлен факт несанкционированного списания средств в сумме 0,9 млн. грн. (эквивалент 112,5 тыс. долл. США) с использованием похищенного электронного ключа в системе «Клиент-Банк» с текущего счета ООО «С» в пользу ООО «Г».

Счет, на который поступили похищенные средства, открыт за 10 дней до проведения вышеупомянутых операций.

В течение одного дня похищенные средства были перечислены транзитом через счета ряда предприятий.

В результате своевременно принятых мер средства в полном объеме вернулись на счет ООО «Г» и были заблокированы по решению ПФР Украины.

Кроме того, ООО «Г» предпринята попытка перечисления незаконно полученных средств на счет ООО «Л», однако банковским учреждением было отказано в проведении указанной финансовой операции.

Директор и учредитель ООО «Г» – гражданин Н – является фигурантом уголовного дела по ч. 1 ст. 191 «Присвоение, растрата имущества или завладение им путем злоупотребления служебным положением» УК Украины.

Пример (Украина)

Выявлены несанкционированные переводы от значительного количества предприятий на счета частного предпринимателя «Ш», которые открыты в банках «А» и «Б».

Списание со счетов четырех предприятий на счет частного предпринимателя «Ш» в банке «А» происходило в течение одного дня. В дальнейшем часть средств частным предпринимателем «Ш» была снята со счета наличными.

Мошеннические переводы были осуществлены путем вмешательства в работу системы «Клиент-Банк» и изменения реквизитов получателя.

По имеющейся информации частный предприниматель ФЛП «Ш» является подставным лицом и ведет антисоциальный образ жизни.

Также, на счет частного предпринимателя «Ш» в банке «Б» был осуществлен несанкционированный перевод со счета предприятия «С» в сумме 280,0 тыс. грн. (эквивалент 35 тыс. долл. США). В тот же день средства были возвращены отправителю.

В этот же день со счета предприятия «С» были осуществлены несанкционированные переводы на карточные счета семи граждан Украины.

ПФР Украины приостановлены финансовые операции по счетам указанных граждан Украины. По указанным фактам начато уголовное производство по ч. 4 ст. 190 «Мошенничество» УК Украины.

Пример (Украина)

Группой граждан организована сеть специализированных игровых залов закрытого типа по предоставлению услуг игорного бизнеса населению, а именно доступ к азартным играм на компьютерных носителях через Интернет (в Украине запрещен игорный бизнес).

В результате деятельности такого Интернет-бизнеса одним из организаторов получен доход в сумме более 1,0 млн. грн. (эквивалент 125 тыс. долл. США).

С целью легализации незаконного дохода указанным лицом средства направлены на приобретение изделий из драгоценных металлов, которые в последующем размещены для хранения, в соответствии с договорами на пользование индивидуальными сейфами в хранилищах коммерческих банков.

По материалам правоохранительных органов открыто уголовное производство по ч. 1 ст. 203-2 «Занятие игорным бизнесом» УК Украины по факту обнаружения подпольных игорных заведений.

В результате проведения обысков в помещениях игорных заведений, офиса и по месту жительства фигурантов изъято 317,0 тыс. грн. (эквивалент 39,6 тыс. долл. США), 19,8 тыс. долл. США, 7,1 тыс. евро, 56 единиц игровых автоматов, 526 единиц компьютерной техники (системные блоки, мониторы, ноутбуки, модемы), 57 мобильных телефонов, 2 электронные рулетки, пистолет с признаками переделки системы «Наган» с глушителем и патроны к нему калибром 9 мм в количестве 15 шт.

В ходе расследования открыто уголовное производство по ч. 2 ст. 209 «Легализация (отмывание) доходов, полученных преступным путем» УК Украины в отношении одного из организаторов незаконной деятельности.

Пример (Украина)

Гражданка Л, занимая должность ведущего эксперта Банка, путем обмана и злоупотребления доверием, используя электронно-вычислительную технику, а именно установленный на ее рабочем месте и присоединенный к сети системы «Клиент-Банк» компьютер, завладела средствами, которые находились на счете гражданина Ш.

Будучи осведомленной о незаконном происхождении средств с целью маскировки незаконного их происхождения, гражданка Л перечислила средства на расчетный счет своего мужа.

Средства, полученные преступным путем, гражданка Л использовала с целью увеличения общего семейного бюджета, получения и оплаты общих бытовых благ, приобретение товаров и услуг, а также предоставление возможности использования данных средств ее мужем в его предпринимательской деятельности.

Гражданка Л осуществила легализацию средств, полученных преступным путем, на общую сумму 307,1 тыс. грн. (эквивалент 38,4 тыс. долл. США).

С целью обеспечения возмещения нанесенного ущерба правоохранительным органом наложен арест на имущество на общую сумму 200,0 тыс. грн. (эквивалент 25 тыс. долл. США). В результате проведенных мероприятий возмещен ущерб на сумму 123,6 тыс. грн. (эквивалент 15,5 тыс. долл. США).

Согласно приговору суда гражданка Л признана виновной в совершении преступлений, предусмотренных ч. 3 ст. 190 «Мошенничество», ч. 1, ч. 2 ст. 209 «Легализация (отмывание) доходов, полученных преступным путем» УК Украины. Ей назначено наказание в виде лишения свободы на 5 лет с лишением права занимать должности, связанные с обслуживанием денежных средств в кредитно-финансовых учреждениях, на 3 года с конфискацией средств полученных преступным путем в сумме 307,1 тыс. грн. (эквивалент 38,4 тыс. долл. США).

Пример (Таджикистан)

Гражданин Б завладел информацией о наличии у нерезидента-предпринимателя Н 106 000 долларов США, предназначенных для перевода в государство З. Гражданин Б, используя свой компьютер, зашел на электронный адрес Н и изменив адрес банка-получателя направил эту сумму в другой банк государства З. Затем гражданин Б, вылетев в государство З, получил и присвоил указанные средства. Уголовное расследование проводилось по статьям 244 ч.3 «Кража», 298 ч.1 «Неправомерный доступ к компьютерной информации» и 299 ч.1 «Модификация компьютерной информации» УК Республики Таджикистан.

Пример (Словения)

Ряд словенских банков и их клиенты стали жертвами серии атак на информационные системы, приведших к хищению денежных средств в крупных размерах. Было совершено порядка 50 таких атак, в результате которых со счетов клиентов было похищено более 1 500 000 евро. Следствие выявило одного человека, который совершил все эти атаки, а также установило группу лиц, участвовавших в отмывании денег и получении доходов. В настоящее время решается вопрос о привлечении к уголовной ответственности за совершение преступлений в составе организованной преступной группировки (ОПГ).

Атаки совершались изощрёнными способами с использованием компьютерных вирусов и других хакерских программ для хищения банковских данных (паролей, цифровых удостоверений) у клиентов. В целях отмывания денег использовались банковские счета физических (подставных) лиц, завуалированные под счета юридических лиц. Некоторые из этих подставных лиц являлись членами ОПГ, некоторые были «невинными жертвами», нанятыми для выполнения этой работы через Интернет, а некоторые согласились на это, поскольку находились в тяжёлом материальном положении. Разработанная схема предусматривала перевод преступных доходов на банковские счета подставных лиц, с которых эти лица снимали наличные деньги и передавали их организаторам этой преступной схемы.

После получения первых СПО, касающихся указанной схемы, ПФР провело анализ информации для выявления схемы и поиска путей её пресечения. Было установлено, что все атаки на информационные системы проводились между 00:00 и 6:00 часами утра. Мошеннические операции скрывались за тысячами законных операций (связанных с начислением и получением заработных плат, процентов, прямых списаний и т.д.), проводимых в тот же период времени. Самым слабым звеном этой схемы являлось снятие наличных денег, которое, как правило, осуществлялось в тот же день сразу же после открытия банков, обычно между 8:00 и 12:00 часами. В ряде случаем между временем совершения предикатных преступлений и временем снятия наличных доходов проходило всего 3-4 часа. ПФР проинформировало банки об установленных фактах, и Ассоциация банков Словении выпустила указание, направленное на недопущение и выявление таких случаев. Банкам было предписано выявлять случаи осуществления большого количества операций за короткий промежуток времени, операции по переводу крупных сумм на неактивные «спящие» счета, а также переводы крупных сумм денег на недавно открытые счета. Поскольку фактор времени имел ключевое значение, банки, ПФР и полиция согласились использовать неофициальные способы и каналы обмена информацией. Например, ПФР согласилось начинать расследование и приостанавливать операции на основании телефонного звонка, а банки могли направлять официальные СПО позднее. В свою очередь банки согласились передавать информацию и документы в ПФР на основании телефонного запроса или запроса по электронной почте. Всё это делалось для того ускорить процесс расследования, пресечь эти операции и задержать подставных лиц. После осуществления ещё нескольких атак ПФР удалось приостановить несколько наиболее крупных операций, однако операции на мелкие суммы оставались не выявленными.

В ответ ОПГ незамедлительно стала использовать большее количество банковских счетов и осуществлять операции на меньшие суммы. Один раз преступники попытались сокрыть 50 000 евро, «распылив» их путём осуществления более 10 операций между 6 банковскими счетами двух

физических и двух юридических лиц, прежде чем снять наличные деньги. Стало очевидно, что после успеха, достигнутого правоохранительными органами, изменился сам характер атак на информационные системы.

В общей сложности ПФР отдало свыше 20 распоряжений о приостановке операций, связанных с этой преступной деятельностью, на сумму порядка 800 000 евро. Однако это составило лишь половину того, что похитили преступники. Лидеру ОПГ предъявлено обвинение в хищении в крупных размерах по 32 пунктам, а также в отмывании денег по 17 пунктам. Ему грозит наказание в виде лишения свободы на 22 года (также подготавливается обвинение в совершении некоторых других уголовных преступлений). Кроме того, заведено более 30 уголовных дел в отношении других лиц, обвиняемых только в отмывании денег. Например, один из преступников, участвовавший в указанной схеме и снявший около 200 000 евро наличными, был приговорён к лишению свободы на 4 года за отмывание денег.

3.2. Использование альтернативных платежных систем и электронных денег для отмывания доходов

С целью удобного и быстрого перевода денежных средств, полученных в сфере киберпреступности, преступниками широко используются возможности платежных систем, электронных денег и систем перевода средств.

Для перемещения преступных доходов могут использоваться как внутригосударственные (обеспечивающие перевод средств исключительно в пределах одной страны), так и международные платежные системы.

Электронные платежные системы, имеют ряд неоспоримых преимуществ, которые и обуславливают их быстрое развитие, а именно:

- доступность – открытие собственного электронного счета является бесплатным для любого пользователя;
- простота использования – открытие и использование электронного счета является интуитивно понятным и не требует специальных знаний;
- мобильность – пользователь через сеть Интернет может осуществлять управление своим счетом из любого места;
- оперативность – транзакции по счету происходят в течение нескольких секунд;
- безопасность – передача информации ведется с использованием криптографической защиты.

Чтобы стать участником и пользоваться услугами платежной системы нужно пройти процесс регистрации и открыть в ней электронный счет в виде

электронного кошелька. Электронный кошелек хранит информацию о сумме средств на счету пользователя в платежной системе.

Для проведения финансовых операций, необходимо ввести деньги в платежную систему, то есть пополнить электронный счет. Разные платежные системы предлагают разные способы пополнения электронных кошельков. Это может быть банковский перевод, почтовый перевод, приобретения предоплаченной карты, пополнение через платежный терминал и др.

Электронные платежные системы функционируют с использованием электронных денег – инструмента, позволяющего осуществлять обмен прав требования на ценности между пользователями с использованием виртуальных счетов, электронных учетных записей (электронная почта и т.п.), а также позволяющего конвертировать данное право требования в денежные средства и другие высоколиквидные инструменты.

Электронные деньги дают возможность осуществлять следующие платежи:

- платежи внутри системы на счета физических и юридических лиц;
- оплата товаров в Интернет-магазинах;
- оплата услуг операторов мобильной связи;
- оплата коммунальных услуг;
- оплата Интернет-услуг;
- оплата государственных сборов, пошлин и штрафов;
- покупка ж/д и авиабилетов;
- покупка топлива;
- бронирование отелей и др.

Для преступников несомненным преимуществом использования электронных денег является возможность анонимного открытия и пополнения электронных кошельков, а также круглосуточная доступность и скорость проведения транзакций (в течение нескольких секунд). Электронный кошелек физического лица чаще всего имеет привязку к электронной почте или номеру мобильного телефона.

Кроме того, для перемещения наличных средств между участниками схемы могут использоваться срочные переводы через международные системы перевода средств.

Механизм таких переводов является достаточно простым и удобным. Для этого в отделение системы или ее партнера обращается лицо (необходимо иметь документ, удостоверяющий личность), которая вносит необходимые средства и заполняет бланк с указанием фамилии и имени получателя и страну отправления перевода. В дальнейшем от оператора получается номер перевода, который необходимо сообщить получателю.

Получатель средств (с документом, удостоверяющим личность) обращается в отделение системы или ее партнера и заполняет бланк на выдачу наличных с указанием номера перевода, фамилию и имя отправителя, страну отправления перевода, суммы и валюты перевода.

Осуществление перевода и получения денег занимает лишь несколько минут.

Пример (Украина)

С карточного счета гражданки Украины осуществлено несанкционированное списание средств. В результате дальнейших несанкционированных переводов средства зачислены на карточные счета двух граждан Российской Федерации.

Переводы осуществлены с помощью электронной платежной системы LIQPAY с использованием сети Интернет и доступа через мобильные телефоны.

Правоохранительным органом начато уголовное производство по ч. 1, 2 ст. 361 «Несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи» и ч. 3 ст. 190 «Мошенничество» УК Украины.

Пример (Украина)

Организованная преступная группа, путем телефонных угроз и запугивания, шантажируя здоровьем и безопасностью родственников, склоняла физических лиц к пополнению электронных кошельков, которые им не известны.

На электронные кошельки, открытые в платежной системе, запуганными физическими лицами внесены средства в общей сумме 30,0 тыс. грн. (около 4 тыс. долл. США).

В дальнейшем, с целью легализации вышеуказанных средств, с указанных электронных кошельков осуществлены переводы на другие платежные системы.

Электронные средства были предназначены для обмена на безналичные средства и дальнейшего перевода для пополнения электронных кошельков международной платежной системы.

Правоохранительным органом по материалам ПФР Украины ведется расследование.

Пример (Украина)

Тремя физическими лицами организованы и совершены мошеннические действия по несанкционированному списанию денежных средств со счетов юридических лиц через удаленное управление ими с использованием новейших информационных технологий.

Несанкционированно списанные денежные средства со счетов 3 юридических лиц, зарегистрированных в разных регионах Украины, перечисленные транзитом через счета физических лиц и зачислены на карточные счета третьих физических лиц. В дальнейшем, часть средств переведена в «электронные деньги» и снята наличными.

Правоохранительным органом по материалам ПФР Украины ведется досудебное расследование по ч. 3 ст. 209 УК Украины «Легализация (отмывание) доходов, полученных преступным путем».

4. СПОСОБЫ И МЕТОДЫ ПРЕДУПРЕЖДЕНИЯ И ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ ДОХОДОВ, ПОЛУЧЕННЫХ В СФЕРЕ КИБЕРПРЕСТУПНОСТИ

4.1. Выявление подозрительных финансовых операций, которые могут быть связаны с отмыванием доходов, полученных в сфере киберпреступности

Несмотря на изобретательность киберпреступников и использование широкого инструментария для схем легализации незаконных доходов, представляется возможным разделить финансовые операции по уровню риска.

Более того, возможно также определить сферы и услуги, которые имеют повышенный риск и, соответственно, требуют повышенного внимания.

Следует отметить, что клиентам, которые устанавливают деловые отношения с банком или пользуются банковскими услугами с использованием новейших технологий без непосредственного контакта с банком часто устанавливается более высокий уровень риска отмывания преступных доходов.

Индикаторами подозрительности финансовых операций указанной направленности для банковских учреждений косвенно могут быть следующие факторы:

- попытка входа с запрещенного/нового IP-адреса;
- попытка использования просроченных первичных/рабочих или старых ключей после сертификации новых;
- использование для банковских операций IP-адресов или имен пользователей, относительно которых предварительный мониторинг выявил причастность к мошенническим операциям;
- трансакции в нестандартное время или подключения к системе в вечернее время;
- необычные условия или сложность операции: высокая частота переводов в течение небольшого периода времени, большое количество разнообразных источников происхождения средств и платежных методов (инструментов);
- лицо не осведомлено о характере деятельности юридического лица, которое оно представляет;
- лицо не может объяснить необходимость предоставления той или иной банковской услуги;
- привлечения к проведению операций лиц молодого возраста и/или вновь созданных предприятий;

- проведения операций с использованием утерянных документов;
- открытие счета, на который зачисляются средства в результате несанкционированного списания, незадолго до проведения таких операций;
- попытки снять средства в день их зачисления;
- попытки клиента получить две или более банковских карт, что не соответствует сути его деятельности или обороту;
- зачисления средств на карточные счета физических лиц с последующим снятием через банкоматы (в т.ч. других банков);
- операции не соответствуют предыдущим операциям клиента;
- отсутствие информации о хозяйственной деятельности клиента или использование онлайновых платежных систем вместо традиционных;
- нетипичные международные переводы, которые не соответствуют деятельности клиента.

ПФР для выявления подозрительных финансовых операций, связанных с киберпреступностью, могут использоваться некоторые из индикаторов, указанных выше, а также другие:

- отсутствие очевидной связи между отправителем денег из-за рубежа и получающим их частным лицом;
- частные переводы, направляемые частному лицу, указывают на возможное осуществление коммерческой деятельности (например, провайдеры услуг по обмену биткоинов, веб-мани и т.д.);
- перевод клиентом денег, с помощью дистанционного доступа, на банковский счет для другого лица;
- использование трансграничных операций, проводимых путем денежных переводов или с помощью услуг Интернет-банкинга;
- перевод денег в/из отдаленных мест, не имеющих прямой и очевидной связи с деятельностью или счётом клиента;
- участие большого количества зарубежных третьих лиц, как физических, так и юридических;
- использование компаний-пустышек;
- разведывательная информация от зарубежных ПФР или правоохранительных органов.

4.2. Общие направления противодействия киберпреступности

Чрезвычайно быстрое развитие информационных и компьютерных технологий в последнее время приводит к стремительному развитию киберпреступности, поэтому особую актуальность приобретают вопросы предупреждения и противодействия преступлениям в киберпространстве.

Предупреждения киберпреступности базируется на мероприятиях, направленных на снижение риска совершения таких преступлений и нейтрализацию вредных последствий для общества и частного сектора.

Эффективное противодействие киберпреступлениям должно сочетать комплекс правовых (законодательных), технических, организационных и информационных мероприятий.

Крайне необходима, выработка корректного понятийного аппарата, как первого шага на пути к уголовно-правовой борьбе с киберпреступностью. К определению киберпреступности и киберпреступления нужно подходить тщательно не только потому, что в результате неправильной законодательной формулировки можно получить «мертвую» или плохо применимую на практике норму. В силу специфической природы этого вида преступлений, законодательство о борьбе с ними должно приниматься в соответствии со специальными международными документами (такими, например, как Конвенция Совета Европы о киберпреступности), поскольку эффективное противодействие киберпреступности в границах одной страны, без международного сотрудничества, в настоящее время не представляется возможным.

Важно включить учреждения, выпускающие предоплаченные карты и электронные деньги в список учреждений, на которые распространяются требования законодательства о ПОД/ФТ, и установить для них виды подозрительных операций.

Необходимо усилить ответственность провайдеров услуг для гарантии того, что они анализируют то, как используются их услуги, а также для обеспечения их мотивации по снижению рисков незаконного использования их услуг в целях совершения преступлений.

Совершенствование нормативно-правового обеспечения в сфере предупреждения и противодействия легализации доходов, связанных с преступлениями в сфере киберпреступности, возможно также по следующим направлениям:

- усиление ответственности за преступления в сфере компьютерных и информационных технологий;
- введение обязательной идентификации при личном контакте клиентов, пользующихся услугами дистанционного обслуживания или электронных платежных систем;
- признание электронных документов и других электронных данных в качестве доказательной базы при расследовании киберпреступлений;
- регулирование вопросов, касающихся юрисдикции, при оказании услуг через Интернет;
- снижение количества анонимных платежей и переводов денежных средств;

- введение сертификации электронных платежных средств;
- четкая регламентация механизмов взаимодействия между клиентом и банком, между банком отправителя денег и банком получателя средств в случае несанкционированного списания средств клиента.

С целью предупреждения киберпреступлений банковскими учреждениями могут внедряться следующие технические и организационные мероприятия:

- периодический осмотр банкоматов для выявления незаконно установленных устройств;
- внедрение для клиентов банка карт с микропроцессором (чипом), как более защищенных от подделки;
- ведение «черного» списка счетов (идентификационных кодов, IP-адресов) мошенников для своевременного блокирования операций;
- требования двухфакторной/двухканальной аутентификации;
- использование токенов для хранения электронных цифровых подписей;
- обязательное информирование клиентов о каждой проведенной операции;
- подтверждения платежа в телефонном режиме;
- генерация клиентского ключа самим клиентом, что делает невозможным совершение неправомерных действий со стороны работников банка;
- привязка ключа клиента к серийному номеру жесткого диска/флэш накопителя/дискеты, делает невозможным копирование ключей Клиент-Банка и доступ к странице клиента с помощью других компьютеров;
- использование ряда логических правил для типовых/нетиповых/подозрительных платежей в системе Клиент-Банк;
- использование клиентом отдельного компьютера, который предназначен только для системы Клиент-Банк (Интернет-банкинг), с настроенными сетевыми фильтрами;
- статистический анализ трафика (Netflow) для выявления аномалий;
- введение лимитов на проведение операций в сети Интернет;
- введение лимитов на проведение операций в определенных рисковых странах;
- введение лимитов на проведение операций по их периодичности.

Следует отметить, что значительная часть киберпреступлений, становится возможной благодаря неосведомленности населения и клиентов

финансовых организаций, а также несоблюдения ними основных правил безопасности. Такими факторами в частности являются:

- ограниченное количество данных и информации о киберпреступлениях;
- низкий уровень осведомленности относительно рисков, вызванных внедрением новых платежных систем и сервисов, а также относительно связанного с ним отмывания средств;
- установка и использование нелицензионного программного обеспечения (операционные системы, антивирусы и т.д.);
- ненадежное хранение электронной цифровой подписи и кодов доступа (паролей) клиентами банковских учреждений;
- пренебрежение элементарными правилами безопасности при пользовании Интернет-банкингом и специальными платежными средствами в сети Интернет;
- невыполнение политики кодовой (парольной) и информационной безопасности.

В связи с этим, значительную пользу в предупреждении киберпреступности, имеют информационно-просветительские мероприятия в отношении новых рисков и угроз в информационных и компьютерных системах.

Важным фактором является также надлежащее отношение к соответствующей компьютерной информации, которая представляет собой экономический интерес для другого субъекта, ограничение доступа к ней, использование лицензированных компьютерных программ и антивирусных софтов для защиты компьютера от незаконного взлома.

Важным является так же усовершенствование нормативно-регулятивной базы для обеспечения информационной безопасности, как на государственном, так и на частном уровне. В частности, необходимо наличие и усовершенствование соответствующей системы информационной безопасности в каждом государственном и частном учреждении. Учреждения должны иметь внутренние правовые акты, регламентирующие вопросы информационной безопасности и предусматривающие ответственность сотрудников за несоблюдение правил компьютерной безопасности. Допуск к информации, содержащей государственную, банковскую и иную тайну должны иметь только те сотрудники, функции которых связаны с регламентированным использованием вышеуказанной информации и которые наделены полномочиями владения такой информацией. Важно так же осуществление надлежащего контроля и надзора за соблюдением правил информационной безопасности.

ВЫВОДЫ

Несмотря на отсутствие на сегодня общепринятого определения киберпреступления наблюдается достаточно широкое и исчерпывающее понимание его сути и способов его совершения, а также угроз и рисков, что дает возможность разрабатывать и внедрять меры противодействия данному виду преступления.

Отсутствие физического контакта с жертвой или представителями финансового учреждения, а также анонимность, скорость осуществления и невысокая стоимость преступления стали ключевыми предпосылками повышения заинтересованности преступников киберпространством.

Киберпространство стало не только местом совершения преступления и получения незаконного дохода, но и местом легализации такого дохода. При этом многообразие видов киберпреступлений в совокупности с многообразием способов отмывания доходов, полученных от совершения данных видов преступлений, приводят к сложности их выявления и расследования.

Выявленные схемы и механизмы отмывания доходов, полученных от киберпреступности, позволяют утверждать, что перемещение средств осуществляется как традиционными способами перевода, так и с использованием современных систем срочных переводов, электронных платежных систем и электронных денег.

При этом средства используются в одних случаях для приобретения предоплаченных карт, товаров или услуг в сети Интернет, а в других переводятся в игровые фишки казино или электронные деньги, перечисляются между электронными кошельками с последующей конвертацией и обналичиванием.

В свою очередь, использование наличности остается одним из наиболее распространенных способов сокрытия дальнейшего движения незаконного дохода и направлений его вложения, а также источников происхождения таких средств во время ввода денег в банковскую систему. Это позволяет преступникам поддерживать анонимность, приобретенную на этапе получения незаконного дохода, и во время отмывания доходов.

Противодействие киберпреступности сочетает в себе комплекс правовых, технических, организационных и информационных мероприятий. При этом роль каждого из этих мероприятий не может быть определена приоритетной или второстепенной.

Поэтому эффективное противодействие отмыванию преступных доходов и снижение уровня преступности в этой сфере возможны благодаря своевременному выявлению финансовых операций, которые могут быть связаны с отмыванием доходов, полученных в сфере киберпреступности, и эффективному международному сотрудничеству, а также сотрудничеству между государственным и частным сектором.