www.coe.int/moneyval
www.coe.int/cybercrime

МАНИВЭЛ (2012) 6

9 марта 2012 г.

Типологическое исследование

Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками[1]

[1] Принято на 38 Пленарном заседании МАНИВЭЛ (5-9 марта 2012 г.)
Перевод осуществлен Международным учебно-методическим центром по финансовому мониторингу

Содержание

1. **Введение** 8

1.1 Задачи исследования 8
1.2 Методология 10

2. **Обзор инициатив и вопросы для обсуждения** 14

2.1 Общие положения 14
2.1.1 Меры борьбы с киберпреступностью 14
2.1.2 Меры борьбы с отмывание денег и финансированием терроризма, а также меры, направленные на розыск, арест и конфискацию доходов от преступлений 16
2.1.3 Основные международные стандарты 17
2.2 Киберпреступность: угрозы, тенденции, инструменты и инфраструктура 18
2.2.1 Виды киберпреступности 18
2.2.2 Киберпреступность: инструменты и инфраструктура 21
2.2.3 Новые платформы для киберпреступности 27
2.2.4 Предпосылки для киберпреступности 28
2.3 Преступления в Интернете, приносящие доход 31
2.3.1 Мошенничество 33
2.3.2 Иные категории преступлений в Интернете, приносящие доход 48
2.4 Составление картины рисков и «слабых» мест, связанных с киберпреступностью 53
2.4.1 Технические риски 54
2.4.2 Анонимность 55
2.4.3 Ограничения в части лицензирования и надзора 57
2.4.4 Географические или юрисдикционные риски 58
2.4.5 Сложность схем отмывания 59
2.4.6 Иные факторы риска 60

3. **Типологии и избранные примеры** 61
61

3.1 Потоки криминальных денег в Интернете и их отмывание: методы, приемы, механизмы и инструменты 62
3.1.1 Услуги по переводу денежных средств 67
3.1.2 Электронные денежные переводы/присвоение или открытие банковского счета 70
3.1.3 Снятие наличных со счета 73
3.1.4 Системы Интернет-платежей 77

3.1.5 «Денежные мулы» 83
3.1.6 Международные переводы 85
3.1.7 Электронные деньги 88
3.1.8 Покупки в Интернете 89
3.1.9 Компании — оболочки 91
3.1.10 Предоплаченные карты 94
3.1.11 Платформы для он-лайн игр и он-лайн торговли 95
3.2 Индикаторы деятельности, связанной с возможным отмыванием денег: показатели риска отмывания денег 99
4. **Контрмеры** 107
108
4.1 Сообщение об Е-преступлениях 109
4.1.1 Центр приема сообщений об Интернет-преступлениях (IC3) 109
4.1.2 MELANI 110
4.1.3 Национальный центр по сообщениям о мошенничестве
4.1.4 Он-лайн система приема сообщений об Интернет-преступлениях (I-CROS) 111
111
4.1.5 Signal spam
4.1.6 Сообщения о Е-преступности: использование обычного формата данных 112
113
4.2 Предотвращение и осведомленность общества 113
4.3 Меры регулирования и надзора 115
4.3.1 Меры по управлению рисками и надлежащей проверке 116
4.3.2 Надлежащая проверка для регистраторов и реестродержателей
4.4 Единая правовая система, основанная на международных стандартах 117
4.4.1 Реализация положений Будапештской Конвенции о киберпреступности 118
4.4.2 Реализация положений Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма 121
121
4.5 Создание специализированный подразделений для борьбы с преступлениями в области высоких технологий 123
4.6 Межведомственное сотрудничество 123
4.6.1 Германия: проектная группа «Электронные платежные системы» 123
4.6.2 Албания: меморандумы о сотрудничестве
4.7 Сотрудничество между государственным и частным сектором и обмен информацией 125
126
4.7.1 Форум по борьбе с преступлениями в области высоких технологий Федерации ирландских банкиров 126
4.7.2 Венгрия: Рабочая группа по управлению инцидентами

4.7.3 Американский национальный альянс по компьютерной криминалистике и подготовке NCFTA 127
4.7.4 Центры анализа и обмена информацией (ISAC) для финансовых служб 128
4.7.5 Европейская финансовая коалиция против коммерческой сексуальной эксплуатации детей в Сети 129
4.7.6 Специальные группы по борьбе Е-преступностью (Секретная служба США) 129 130
4.7.7 Европейская группа по борьбе с Е-преступностью (EECTF)
4.7.8 Инициатива против киберпреступности для частного сектора и правоохранительных органов (CICILE) 131 131
4.7.9 Руководства по сотрудничеству между правоохранительными органами и ISP для борьбы с киберпреступностью 132
4.8 Обучение
4.8.1 Европейская группа по образованию и обучению для борьбы с киберпреступностью (ECTEG) 133
4.8.2 Центр Университетского колледжа Дублина по расследованию киберпреступлений (UCD CCI) 133
4.8.3 Юго-восточная Европа — стратегии обучения для правоохранительных органов 135
4.8.4 Концепция Совета Европы по обучению судей и прокуроров 135 136

5. **Результаты** 139

5.1 Киберпреступность и криминальные денежные потоки 144
5.2 Отмывание денег и вопросы киберпреступности
5.3 Выводы и направления развития 144 147

6. **Приложение**

6.1 Концепция исследования
6.2 Ссылки

КРАТКИЙ ОБЗОР

1. Данное типологическое исследование является успешным результатом совместных усилий МАНИВЭЛ[2], Международного проекта Совета Европы по борьбе с киберпреступностью[3], а также Проекта Совета Европы по противодействию отмыванию преступных доходов и финансированию терроризма в Российской Федерации (MOLI-RU2). Основой для данного исследования послужило желание практиков проанализировать взаимосвязь между киберпреступностью и отмыванием денег, наиболее часто используемые методы и средства для отмывания преступных доходов от киберпреступлений и через Интернет, а также риски и незащищенность, возникающие от этой разновидности отмывания денег.

2. Это типологическое исследование несколько отличается от тех, которые ранее проводил МАНИВЭЛ с учетом того, что оно было подготовлено с использованием большого количества данных, собранных в результате обзоров, проведенных МАНИВЭЛ, ФАТФ и ЕАГ с привлечением государственных экспертов своих государств-членов, а также представителей финансовых учреждений, специализирующихся на киберпреступности. В результате впервые удалось объединить достаточные ресурсы и опыт подразделений финансовой разведки, служб, проводящих финансовые расследования и расследования преступлений в сфере высоких технологий, а также опыт основных представителей частного сектора, которые привнесли свои знания в этот проект.

3. Исследование говорит о том, что киберпреступность широко распространена и с ее помощью генерируются огромные суммы преступных доходов, а данные об отмывании денег и успешных действиях правоохранительных органах — незначительны. При этом внося свой вклад в повышении осведомленности о текущих инициативах, направленных на предотвращение и борьбу с киберпреступностью и отмыванием денег, а также преступлениями в Интернете, направленными на извлечение прибыли. В исследовании рассматриваются риски, уязвимые места, выявленные в результате анализа предоставленных примеров, методов, техник и средств отмывания денег от киберпреступлений. Были получены типологические схемы, а также определенные показатели возможного отмывания денег.

4. В отличие от традиционных схем отмывания денег с использованием банковской системы для кибер-отмывания используются сложные схемы, разные виды операций, финансовых услуг (от банковских переводов, внесения/снятия наличных, использования электронных денег до «денежных мулов» и поставщиков услуг по переводу денежных средств). В

2 Для дополнительной информации см. www.coe.int/moneyval
3 Для дополнительной информации см. www.coe.int/cybercrime

то же время осведомленность о рисках, которые несут новые платежные системы и сервисы, а также о связанных с ними отмывании денег — низкая. Таким образом, выявление и пресечение потоков преступных денег является очень сложной задачей для правоохранительных органов. Более того, существует явный риск того, что в большинстве стран киберпреступления не выявляются или уровень сообщений о них очень низок, что в свою очередь ведет к отсутствию финансовых расследований и расследований дел, связанных с отмыванием денег.

5. В заключительной части исследования содержатся некоторые выводы о киберпреступности, отмывании денег и имеющихся в наличии контрмерах, а также полезный опыт некоторых стран, который может вдохновить политиков и регуляторов или стать частью более системных подходов или стратегий, направленных на борьбу с отмыванием денег и финансированием терроризма, а также на выявление, изъятие и конфискацию преступных доходов, полученных через Интернет. Были выявлены ряд направлений, которые дают возможность активизировать совместные действия и внести свой вклад в те усилия, которые направлены на предотвращение отмывания денег.

СПИСОК АББРЕВИАТУР

АКП	АВТОМАТИЗИРОВАННАЯ КЛИРИНГОВАЯ ПАЛАТА
ПОД/ФТ	противодействие отмыванию денег и финансирование терроризма
АРГ	Антифишинговая рабочая группа
АТМ	Банкомат
ВКА	Федеральная уголовная полиция Германии
МПМ	Мониторинг протоколов маршрутизации
Группа CERT	Группа реагирования на нарушения компьютерной защиты в сети Интернет
НПК	Надлежащая проверка клиента
CNP	Карта физически отсутствует
CSIRT	Группа реагирования на инциденты, связанные с компьютерной безопасностью
DDOS	Распределенная атака типа отказ в обслуживании
ECCP	Европейская платформа по борьбе с киберпреступностью
ECE	Европейская серия договоров (с 1.01.2004, СДСЕ — Серия договоров Совета Европы)
ЕС	Европейский Союз
ФАТФ	Группа разработки финансовых мер борьбы с отмыванием денег
ПФР	Подразделение финансовой разведки
РГТФ	Региональные группы по типу ФАТФ
ФТ	Финансирование терроризма
ПКК	Правительственный консультативный комитет _____
IC3	Центр приема сообщений об Интернет-преступлениях
ICANN	Организация по присвоению имени и адресов в Интернете
ИКТ	Информационно-коммуникационные технологии
I-CROS	Он-лайн система приема сообщений об Интернет-преступлениях
ИД	Идентификационные данные
ПСИ	Платежные сервисы Интернета
ISP	Поставщик Интернет-услуг
ЗСК	Знай своего клиента
ОД	Отмывание денег
МАНИВЭЛ	Комитет экспертов Совета Европы по оценке мер противодействия отмыванию денег и финансированию терроризма
ПИН	Персональный идентификационный номер
СПО	Сообщения о подозрительных операциях
СВИФТ	Международная межбанковская электронная система платежей
T-CY	Комитет Конвенции Совета Европы о киберпреступности
VOIP	Протокол передачи голоса через Интернет
США	Соединенные Штаты Америки

1. ВВЕДЕНИЕ

1.1 Задачи исследования

1. Информационно-коммуникационные технологии (ИКТ) и, в частности, Интернет связывают между собой компьютеры во всем мире, предлагая сообществам уникальную возможность. Интернет позволяет все большему количеству людей[4] и организаций общаться, обмениваться информацией, предлагать и использовать услуги и пользоваться своими правами. Но с другой стороны использование ИТК и Интернета делают сообщества более уязвимыми для такой угрозы как киберпреступность.

2. Для целей настоящего исследования киберпреступность означает[5]:

– преступление против компьютерных данных и систем: данная категория включает в себя так называемые «c.i.a.-преступления» против конфиденциальности, целостности и доступности компьютерных систем и данных;
– преступления, совершенные с использованием компьютерных данных и систем: данная категория включает в себя, например, мошенничество, детскую порнографию или преступления, связанные с нарушением прав на интеллектуальную собственность, если совершаются в коммерческом масштабе и с помощью компьютерной системы

3. Тот факт, что для совершения экономических или тяжких преступлений могут быть использованы компьютерные системы делает киберпреступность очень доступным и дешевым инструментом. При этом необходимо учитывать, что киберпреступность уже сама по себе интернациональна. Она все больше и больше переориентируется на извлечение прибыли в результате совершения различных видов мошенничества, экономических преступлений и деятельности организованной преступности. В то время как появились новые виды преступлений, «традиционные» преступления начали более эффективно совершаться через Интернет. Кроме того, сформировалась электронная теневая экономика, объемы которой продолжают расти, и в функционирование которой вовлечены организованная преступность,

4 Для ознакомления со статистикой пользования Интернетом см. http://www.internetworldstats.com/stats.htm. По оценкам на март 2011 более 2 миллиардов людей являются пользователями Интернета (представляя расширение темпов охвата на 30 % от всего населения и рост на 480.4% в период с 2000 г. по 2011 г.)

5 Данное «определение» основано на том, которое дано в Будапештской Конвенции о киберпреступности (www.coe.int/cybercrime)

эксперты в сфере ИКТ, хакеры, мулы и иные лица, которых легко нанять и обладающие всеми необходимыми навыками для предоставления соответствующего инструментария или услуг для совершения киберпреступлений или для распоряжения преступными доходами. Организованным преступным группам необязательно обладать каким-либо собственным опытом деятельности в Интернете, поскольку лиц, обладающими соответствующими навыками или предоставляющими необходимые услуги, можно нанять, создавая, таким образом, что-то наподобие деловой сети, объединяющей как мелких преступников, так и организованные преступные группы, которые могут находиться в разных частях света. Все это приводит к появлению «грязных» денег в Интернете.

4. Когда отмывание денег криминализовано на основании подхода «охватываются все преступления», то и любые киберпреступления, приносящие преступный доход, будут считаться предикатными по отношению к отмыванию денег, а имущество, отмытое, благодаря введению или выведению его в/из системы на любой стадии, считается отмыванием денег. Борьба с киберпреступностью имеет большое значение для усилий, предпринимаемых в сфере ПОД/ФТ.

5. Для борьбы с такими преступлениями задействован широкий круг участников как из государственного, так и из частного сектора. Несмотря на примеры совместных действий, все же прилагаемые усилия носят точечный характер. Инициативы, направленные на борьбу с мошенничеством в Интернете, не всегда увязаны с той деятельностью, которую осуществляют подразделения финансовой разведки или правоохранительные органы, ответственные за проведение финансовых расследований.

6. Одним словом, с одной стороны, был достигнут значительный прогресс с конца 1980-х в части создания системы предотвращения отмывания денег, а чуть позже финансирования терроризма, и контроля за ней; с середины 1990-х — в части разработки методик проведения финансовых расследований, направленных на конфискацию доходов, что является частью расследования по уголовному делу. Также с 2001 г. Очевиден значительный прогресс в результате введения в действие законодательства о борьбе с киберпреступностью, создания специализированных подразделений по борьбе с преступлениями в сфере высоких технологий, и условий для расследования, преследования, вынесения приговоров по

киберпреступлениям, а также международного сотрудничества и недавнего усиления сотрудничества между государственным и частным сектором. С другой стороны, сферы противодействия киберпреступности, финансированию терроризма, отмыванию денег и проведения финансовых расследований слабо взаимосвязаны между собой.

7. Совершенствование знаний относительно методов, используемых в Интернете для отмывания преступных доходов, включая мошенничество и финансирование терроризма, путем обмена информацией между представителями государственного и частного секторов будет только способствовать более эффективному проведению финансовых расследований, аресту и конфискации преступных доходов и предотвращению совершения преступлений через Интернет.

8. Задачи исследования:

- рассмотреть отдельные риски отмывания денег и финансирования терроризма, методы, тенденции и типологии;
- разработать критерии для выявления потоков преступных денег и отмывания денег в Интернете;
- определить возможные пути решения в части превентивных мер, совместных действий, ареста и конфискации преступных доходов, проведения расследований отмывания денег и финансирования терроризма через Интернет, а где возможно разработать документы, содержащие полезный опыт.

1.2 Методология

9. Данное типологическое исследование является успешным результатом совместных усилий МАНИВЭЛ[6], Международного проекта Совета Европы по борьбе с киберпреступностью[7], а также Проекта Совета Европы по противодействию отмыванию преступных доходов и финансированию терроризма в Российской Федерации (MOLI-RU2) вслед за принятием на Пленарном заседании МАНИВЭЛ в сентябре 2008 г. решения о проведении проекта.

6 Для дополнительной информации см. www.coe.int/moneyval
7 Для дополнительной информации см. www.coe.int/cybercrime

10. Исследование было подготовлено группой, состоящей из представителей Росфинмониторинга (Подразделение финансовой разведки Российской Федерации, сопредседатель проекта), Министерства внутренних дел Российской Федерации, ПФР (NOCPML) Румынии, Государственного комитета по финансовому мониторингу (ПФР) Украины, Федерального бюро Германии по финансовому надзору (BAFIN), Всемирного банка, проекта МОЛИ-РУ2, Секретариата МАНИВЭЛ (сопредседатель проекта) и Международного проекта по борьбе с киберпреступностью (сопредседатель проекта). На разных этапах реализации проекта свой вклад внесли "McAfee Labs", "PayPal", "Team Cymru" и "UK Payments". Два консультанта Адриана Хольтслаг-Альварез (Голландия) и Дэйв О'Райлли (Ирландия) оказали содействие в подготовке списка литературы, вопросника и плана исследования, а также внесли свой вклад в его содержательную часть.

11. При подготовке данного исследования проектная группа использовала данные и информацию из вопросника, который 20 января 2010 г. был направлен членам МАНИВЭЛ и ФАТФ, а также представителям правоохранительных органов и частного сектора, занимающихся вопросами противодействия киберпреступности. Учитывая проведение совместного заседания МАНИВЭЛ и Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ) по типологиям было принято решение привлечь государства-члены ЕАГ[8] к данному исследованию. Их ответы на вопросник были получены в июне 2010 г. Было получено 22 ответа[9], что дало возможность обобщить ценную информацию.

8 Членами Евразийской группы являются: Беларусь, Китай, Казахстан, Кыргызстан, Россия, Таджикистан, Туркменистан и Узбекистан

9 Ответы на вопросник были также получены от Албании (Государственная полиция Албании, Подразделение по преступным активам и Подразделение по борьбе с киберпреступностью), Андорры (Управление полиции, Министерство внутренних дел), Белоруссии (Департамент по финансовому мониторингу), Болгарии (Управление финансовой разведки Государственного агентства по национальной безопасности) Китая (Национальный банк Китая), Эстонии (ПФР), Германии (ПФР), Венгрии (Управление Венгрии по финансовому надзору), Италии (Прокуратура при суде общей юрисдикции, Милан), Кыргызстана (Государственная служба финансовой разведки), Польши (Министерство финансов), Румынии (Прокуратура при Высшем кассационном суде/Департамент по расследованию дел, связанных с организованной преступностью и терроризмом), Российской Федерации (проектная группа включала в себя представителей Росфинмониторинга, Министерства внутренних дел, ФСКН России, Международного учебного центра Росфинмониторинга), Словении (ПФР), Таджикистана (Национальный банк Таджикистана), Бывшей югославской Республики Македония (Бюро по борьбе с отмыванием денег и финансированием терроризма), Украины (ПФР), США (Министерство финансов); частного сектора "McAfee Labs", Франция, Рабочей группы по борьбе со злоупотреблениями в системах передачи сообщений (MAAWG), Франция, "PayPal", Центра Университетского колледжа Дублина по расследованию киберпреступлений

12. Члены проектной группы провели несколько рабочих встреч в ходе реализации проекта. Представители Росфинмониторинга и Международного проекта по борьбе с киберпреступностью провели предварительную встречу в Москве в 2009 г. Учитывая подобранную литературу и первые полученные ответы, удалось подготовить первый проект исследования, который обсуждался проектной группой на заседании Совета Европы в марте 2010 г., в результате чего выкристаллизовались те вопросы, которые необходимо охватить в данном исследовании. Приблизительно в тот же промежуток времени произошел обмен мнениями с рядом представителей частного сектора. В июне 2010 г. участники распределили подготовку отдельных частей исследования между собой с тем, чтобы к октябрю был подготовлен новый проект, который они могли бы обсудить в октябре 2010 г.

13. В ходе совместного заседания экспертов МАНИВЭЛ и ЕАГ по типологиям противодействия отмыванию денег и финансированию терроризма (Москва, 9-10 ноября 2010 г.) был проведен отдельный семинар, посвященный таким вопросам как потоки криминальных денег в Интернете (на основе типологического исследования МАНИВЭЛ) и риски ненадлежащего использования электронных денег для отмывания денег и финансирования терроризма (на основании типологического исследования ЕАГ). Участие членов ЕАГ и МАНИВЭЛ, а также доклады представителей государственного и частного секторов подпитали дополнительной информацией данное исследование и помогли обосновать некоторые промежуточные аспекты.

14. Кроме того, было использовано большое количество источников, находящихся в широком доступе. В данном исследовании также учтены результаты типологических исследований ФАТФ, посвященных вопросу использования он-лайновых платежных систем для отмывания денег и финансирования терроризма (июнь 2008 г.[10] и октябрь 2010 г.[11]). Если исследования ФАТФ в большей степени затрагивают вопросы использования новых платежных методов то данное исследование предоставляет более полную картину относительно взаимосвязей, рисков,

10 Группа разработки финансовых мер борьбы с отмыванием денег: «Уязвимость коммерческих сайтов и он-лайн платежных систем для отмывания денег и финансирования терроризма» (июнь 2008 г.) http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

11 Группа разработки финансовых мер борьбы с отмыванием денег: «Отмывание денег, финансирования терроризма и новые платежные методы» (октябрь 2010 г.) http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf

контрмер, принимаемых для борьбы с киберпреступностью, преступными денежными потоками и отмыванием денег в Интернете.

15. Члены проектной группы провели ряд консультаций в период с декабря 2010 г. по декабрь 2011 г., что привело к завершению работы над данным исследованием.

2. Обзор инициатив и вопросы для обсуждения

2.1 Общие положения

2.1.1 Меры борьбы с киберпреступностью

16. Конвенция против киберпреступности была открыта для подписания в Будапеште в ноябре 2011 г. К январю 2012 г. она была ратифицирована 32 государствами (31 европейское государство и США). Кроме того, она была подписана еще 15 странами (11 европейскими, а также Канадой, Японией и ЮАР). Настоящая Конвенция в соответствии со ст. 37 открыта для присоединения Государств - членов Совета Европы и не являющихся его членами, а также Государств, которые не участвовали в ее разработке. Таким образом, Аргентина, Австралия, Чили, Коста-Рика, Доминиканская Республика, Мексика, Филиппины и Сенегал получили приглашение присоединиться к Конвенции. Кроме того, большое количество государств используют положения Будапештской Конвенции для того, чтобы изменить свое законодательство. Конвенция служит основой для борьбы с киберпреступностью, учебным пособием, модельным законодательством и технической помощью. Будапештская Конвенция, таким образом, является всеобъемлющей основой для законодательства о борьбе с киберпреступностью.

17. Будапештская Конвенция обязывает государства:

- криминализовать атаки на компьютерные данные и системы (то есть незаконный доступ, неправомерный перехват, воздействие на данные и функционирование системы, противозаконное использование устройств[12]), а также преступления, совершенные с использованием компьютерных технологий (включая подлог и мошенничество[13], детскую порнографию[14] и нарушение авторских и смежных прав[15]);
- предпринять процессуальные законодательные меры для того, чтобы компетентные органы смогли проводить расследование киберпреступлений и сохранить легко изменяемые электронные доказательства наиболее

12 См. ст.2-6 Будапештской Конвенции против киберпреступности (СДСЕ 185)
13 Статьи 7 и 8 Будапештской Конвенции
14 Ст.9 Будапештской Конвенции. Понятие «детская порнография» в контексте борьбы с киберпреступностью очень ограничено. Преступления, указанные в Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия (СДСЕ 201), предусматривают более широкое определение.
15 См.ст.10 Будапештской Конвенции

эффективно, включая оперативное обеспечение сохранности данных, обыск и выемку хранимых компьютерных данных, перехват данных и т.д.)[16];

– сотрудничать эффективно с другими странами-участницами Конвенции через общие (выдача, взаимная правовая помощь и другие) и специальные процессуальные меры (оперативное обеспечение данных, доступ к хранящимся данным, перехват телекоммуникационных сообщений, создание контактных центров, работающих 24 часа в сутки семь дней в неделю и другие) для международного сотрудничества.

18. Конвенция была дополнена Протоколом СДСЕ 189 (2003 г.) о ксенофобии и расизме, совершенных при помощи компьютерных систем.

19. В соответствии со ст.46 был создан Комитет Конвенции против киберпреступности (T-CY) для того, чтобы помочь странам-участницам обмениваться информацией и рассматривать необходимость внесения дополнений или протоколов к Конвенции. T-CY не наделена функцией мониторинга или оценки, но в ноябре 2011 г. было принято решение начать оценку выполнения государствами положений Будапештской Конвенции.

20. Для того, чтобы помочь странам реализовать положения Будапештской Конвенции в 2006 г. Совет Европы запустил Международный проект по борьбе с киберпреступностью, который направлен на то, чтобы оказать содействие странам по совершенствованию законодательства, обучению сотрудников правоохранительных органов, органов прокуратуры и судейского корпуса, укреплению сотрудничества между государственным и частным сектором, выработки мер для защиты персональных данных, а также защиты детей от сексуальной эксплуатации и насилия. Третья фаза проекта началась в январе 2012 г.[17] Эта фаза также включает в себя деятельность, связанную с отслеживанием потоков преступных денег в Интернете. Международный проект дополняется проведением национальных и региональных проектов.

16 Процессуальные полномочия применяются не только к преступлениям, предусмотренным ст.2-10 Конвенции. В ст. 14 (2) Будапештской Конвенции предусматривается, что процессуальное законодательство применяется к всем уголовным преступлениям, совершенным при помощи компьютерной системы и сбора доказательств в электронной форме уголовного преступления

17 Международный проект по борьбе с киберпреступностью финансируется и государственным, и частным сектором. Что касается фазы 1 и фазы 2, т. е. между сентябрем 2006 г. и декабрем 2011 г., то правительства Эстонии, Японии, Монако и Румынии, а также представители частного сектор — компании “McAfee”, «Виза Европа» и в частности «Майкрософт» - сделали добровольный взнос, обеспечив дополнительное финансирование проекта наряду со средствами, поступающими из Совета Европы.

2.1.2 Меры борьбы с отмывание денег и финансированием терроризма, а также меры, направленные на розыск, арест и конфискацию доходов от преступлений

21. Что касается международных стандартов, то Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма 2005 г. (далее - «Варшавская Конвенция» СДСЕ 198) дополняет и уточняет положения Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности 1990 г. (далее — Страсбургская Конвенция,СДСЕ 141). К обеим Конвенциям могут присоединиться страны, не входящие в Совет Европы. СДСЕ 141 была ратифицирована 47 государствами-членами Совета Европы и Австралией. В настоящее время обе Конвенции действуют одновременно.

22. Варшавская Конвенция была открыта для подписания 16 мая 2005 г. и вступила в силу 1 мая 2008 г. На январь 2012 г. 22 государства ратифицировали ее и еще 12, включая Европейский Союз — подписали ее. Ожидается, что все 47 государств-членов станут участницами СДСЕ 198, как это случилось со Страсбургской Конвенцией, которая была ратифицирована самым широким кругом участников. Конвенция, помимо всего прочего, содержит положения о конфискационных мерах (статья 3), следственных и предварительных мерах (статья 4), замораживании, изъятии и конфискации (статья 5), управлении замороженным и изъятым имуществом (статья 6), о следственных полномочиях и приемах (статья 7), криминализации преступлений, связанных с отмыванием денег (статья 9), создании подразделений финансовой разведки (ПФР) (статья 12), предупредительных мерах (статья 13), приостановлении подозрительных операций внутри государства, международных запросах о предоставлении информации по банковским счетам (статья 17), запросах информации по банковским операциям (статья 18), запросах о мониторинге банковских операций (статья 19), о применении предварительных мер (статьи 21 и 22), конфискации (статьи 23 и 24) и сотрудничестве между ПФР (статья 46). Конвенция предусматривает механизм обзора посредством проведения Конференции стран — участниц с тем, чтобы обеспечить эффективное выполнение ее положений.

23. Комитет экспертов Совета Европы по оценке мер противодействия

отмыванию денег и финансированию терроризма (МАНИВЭЛ) — является независимым органом обзора, который Комитет министров Совета Европы наделил полномочиями по проведению оценок соответствия основным принципам противодействия отмыванию денег и финансированию терроризма (ПОД/ФТ) и эффективности их реализации. МАНИВЭЛ не только отслеживает соответствие стандартам СЕ, но и ФАТФ, Европейского Союза через систему взаимных экспертных оценок. 28 государств-членов Совета Европы, Израиль и Святой Престол (включая город-государство Ватикан) проходят такую оценку.

24. Выработка стандартов (в частности Страсбургская и Варшавская Конвенции) и оценочная деятельность, осуществляемая МАНИВЭЛ, дополненные проектами по оказанию технического содействия, помогают странам последовательно и настойчиво реализовывать стандарты ФАТФ и МАНИВЭЛ. Большинство из них — это совместные проекты Совета Европы и Европейского союза, в том числе и проекты МОЛИ-РУ2 по противодействию легализации преступных доходов и финансированию терроризма в Российской Федерации18.

2.1.3 Основные международные стандарты

Основные международные стандарты по борьбе с киберпреступностью

Совет Европы

- Конвенция против киберпреступности (СДСЕ 185 - 2001 г.) - Будапештская Конвенция
- Дополнительный протокол к Дополнительному протоколу к Конвенции о киберпреступности о криминализации действий расистского и ксенофобного характера, совершенных с помощью компьютерных систем (СДСЕ 189)

Международные стандарты о противодействии отмыванию денег финансированию терроризма

Совет Европы

18 Первая фаза проекта началась в феврале 2003 г. Вторая фаза проекта МОЛИ-Ру2 была завершена в декабре 2010 г. Аналогичные проекты были реализованы в Молдове, Сербии, Бывшей югославской республике Македония и Украине

- Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности (СДСЕ 141, 1990 г.)
-Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансированиеи трроризма (СДСЕ 198, 2005 г.)

Европейский Союз

-Директива Европейского Парламента и Европейского Совета 2005/60/ЕС от 26 октября 2005 г. о предотвращении использования финансовой системы для отмывания денежных средств и финансирования терроризма и мерах по ее реализации
-Постановление (ЕС) № 1781/2006 об обязательном включении информации о плательшике при осуществлении перевода
- Постановление (ЕС) № 1889/2005 по контролю за наличными денежными средствами ввозимыми в или вывозимыми из Сообщества
-Директива Европейского парламента и Совета 2007/64/ЕС о платежных услугах на внутреннем рынке.

Группа разработки финансовых мер борьбы с отмыванием денег

- Сорок Рекомендаций (по состоянию на февраль 2012 г.)

Организация Объединенных Наций

- Международная Конвенция ООН о борьбе с финансированием терроризма (1999 г.) (Нью-Йоркская Конвенция)
-Конвенция ООН против транснациональной организованной преступности (КТОП)

2.2 Киберпреступность: угрозы, тенденции, инструменты и инфраструктура

2.2.1 Виды киберпреступности

25. Киберпреступность можно разделить на следующие категории:

– преступления против конфиденциальности, целостности и доступности компьютерных систем и данных (так называемые «CIA-преступления»), включая:

– неправомерный доступ, например, путем взлома, обмана и иными средствами;

– неправомерный перехват компьютерных данных;

– воздействие на данные, включая повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных;

– воздействие на функционирование системы, включая создание серьезных помех функционированию компьютерной системы, например, путем распределенных атак на ключевую информационную инфраструктуру типа отказ в обслуживании;

– противозаконное использование устройств, то есть, например, производство, продажа или иные действия, направленные на обеспечение доступности программ, устройств и иных средств, предназначенных для совершения «CIA-преступлений»

– преступления, совершенные при помощи компьютерных систем, включая[19]:

– подлог и мошенничество, совершенные с использованием компьютерных технологий;

– преступления, связанные с содержанием данных, в частности детская порнография, детская эксплуатация и сексуальное насилие, расизм, ксенофобия, а также консультирование, подстрекательство, содействие путем указаний и предложение совершить преступление, начиная с убийства и кончая изнасилованием, пытками, диверсией и терроризмом. Под эту же категорию подпадают кибер-вымогательство, запугивание, клевета, распространение ложной информации в Интернете, азартные игры он-лайн.

– преступления, связанные с нарушением авторских и смежных прав, например незаконное воспроизводство и использованием компьютерных программ, аудио/видео и иных видов цифровой формы, а также баз данных и книг.

26. Данная классификация представляется полезной для улучшения

19 Эта категория не ограничивается данным перечнем. В нее могут быть включены преступления, совершаемые с использованием тем или иным способом компьютерных систем

судебного реагирования[20], а также для аналитических задач. Однако в действительности преступление представляет собой совокупность различных видов преступного поведения как описано в примере ниже, включая незаконный доступ, неправомерный перехват, воздействие на данные и систему, а также подлог и мошенничество.

Пример: Киберпреступность нацелилась на клиентов Интернет-банкинга[21]

Между июлем и августом 2010 г. около 675,000 фунтов стерлингов было похищено из банка, находящегося на территории Соединенного Королевства. Кроме того, около 3000 счетов были взломаны преступниками. Дело, описанное в разделе M 86 «Безопасность» указывает на то, что киберпреступность использует бизнес-модель, где роли распределены между различными членами группы, которыми управляют администраторы для того, чтобы синхронизировать действия, и где используются законные счета «денежных мулов» для перевода средств со взломанных счетов.

Атаки на систему строились следующим образом:

- преступники заражали обычные сайты, используя вредоносные программы, создавая мошеннические рекламные сайты и публикуя соответствующие объявления на таких сайтах;
- пользователя, зашедшего на зараженный сайт, перенаправляют на сайт, с которого загружается конструктор (в настоящем примере «Eleonore Exploit Kit") на компьютер пользователя. Это дает возможность владельцу конструктора контролировать все, что загружается на компьютер пользователя и установить троянского коня[22]. Вредоносные программы настолько сложны, что лишь

20 Они соответствуют тем категориям преступлений, который должны быть криминализованы в соответствии с положениями Будапештской Конвенции (СДСЕ 185) и Дополнительным протоколом к Конвенции о киберпреступности о криминализации действий расистского и ксенофобного характера, совершенных с помощью компьютерных систем (СДСЕ 189)

21 Источник: M 86 «Безопасность» («Белая книга») «Киберпреступники нацелились на клиентов Интернет-банкинга (август 2010 г.). http://www.m86security.com/documents/pdfs/security_labs/cybercriminals_target_online_banking.pdf. Расследование, проводившееся как минимум еще в двух европейских государствах, позволило выявить похожие схемы. См. например Федеральная полиция Германии (2010): «Годовой отчет ПФР за 2009 г.». http://www.bka.de/profil/zentralstellen/geldwaesche/pdf/fiu_jahresbericht_2009.pdf

22 Троянский конь — это программа, которая кажется законной, но на самом деле имеет скрытый функционал для того, чтобы обойти меры безопасности и осуществить атаку. Троянский конь может представлять собой очень «симпатичную» программу, которую пользователь захочет загрузить и установить, не подозревая о ее скрытых задачах. Трояны обычно строятся на функциональности клавиатурных шпионов, шпионского программного обеспечения и иных методах, способных блокировать систему безопасности (Источник: ОЭСР (2007): «Вредоносные программы — угроза безопасности

немногие антивирусные программы могут выявить их.
- компьютер пользователя теперь является «ботом» («роботом» или «зомби»), с которого троян отправляет данные и на который получает инструкции с сервера управления и контроля (в данном случае сервер находился в Восточной Европе).
- пользователь вводит данные для доступа к своему банковскому счету, после чего троян передает данные о личности, дате рождения и номере безопасности на сервер управления и контроля.
- после того, как пользователь переходит в раздел операций данные для операции передаются на сервер, а не в банк.
- система сервера анализирует и дешифрует информацию и определяет соответствующий банковский счет денежного мула
-троян получает команду направить обновленные данные для перевода денежных средств на счет «мула»
-подтверждение из банка о переводе также направляется трояном на сервер контроля и управления.

2.2.2 Киберпреступность: инструменты и инфраструктура

27. Информация о сложившейся ситуации и тенденциях, а также основных технологиях и инфраструктуре, полученная в результате исследования, данных от частного сектора может быть обобщена следующим образом:

2.2.2.1 Вредоносные программы

28. Вредоносные программы[23] по прежнему остаются основным инструментом совершения преступлений. Вредоносные программы, по сообщениям многих, превратились в довольно крупный сектор со сложной экономической хорошо организованной инфраструктурой и финансированием преступными группировками[24]. Вирусы, черви и трояны «обезоруживают» антивирусные приложения, подгружают дополнительные вредоносные программы или крадут логин, данные о счетах, а также иные данные и считаются основными образцами враждебного кода[25].

Интернет -экономике». См. http://www.oecd.org/dataoecd/53/34/40724457.pdf)

23 Вредоносные программы — программное обеспечение, внедряемое в информационную систему для того, чтобы нанести вред этой и другим системам или для того, чтобы обеспечить доступ к ним лицам, не являющимся уполномоченными (Источник: ОЭСР (2007): «Вредоносные программы — угроза безопасности Интернет -экономике». См. http://www.oecd.org/dataoecd/53/34/40724457.pdf)

24 Отчет «Sophos" об угрозе безопасности (август 2010 г.), стр. 28: http://www.sophos.com/security/topic/security-report-2010.html

25 См. например Информационный бюллетень Symantec за апрель — июнь 2011 г.(http://www.symantec.com/business/threatreport/quarterly.jsp); Информационный отчет Microsoft по

Вредоносные программы развиваются быстро. Чтобы доказать данное утверждение «Symantec" сообщила о том, что разработала более 450,000 новых антивирусных кодов в период с апреля по июнь 2010 г. с тем, чтобы охватить новые вредоносные вариации. Но число компьютеров, зараженных вредоносными программами неуклонно растет.

29. Всемирная путина остается основным средством для вредоносных программ. В соответствии с данными "Sophos" Интернет-пользователи заманиваются на сайты, где вредоносная программа и атакует компьютер. Некоторые из них взламывают обычные сайты, в результате чего пользователи перенаправляются на вредоносный сайт. Во второй половине 2009 г. большинство таких сайтов было зарегистрировано в США (37,4%), затем идет Россия (12,8%) и Китай (11,2% по сравнению с 51,4% в 2007 г.)[26]. За обзорный период с апреля по июнь 2010 г. "Symantec" по количеству вредоносных программ отдала первое место США (около 21%), затем идет Индия (6%), Германия (5%), Китай (5%) и Бразилия (5%). Большая часть атак во всемирной паутине связана с вредоносной деятельностью в формате PDF[27]. Компания «Microsoft» в своем докладе за 2009 г. сообщила, что в части поражения от вредоносных и нежелательных программ США занимает лидирующее место (более 15%), затем идет Китай (около 8%) и Бразилия (около 6%). Китай (+19,1), Россия (+16,5) и Бразилия (+15,8) показывают значительный рост[28].

30. Что касается угроз, относящихся к электронной почте, то спам остается основным инструментом для мошеннических схем и распространения вредоносных программ. "Microsoft" сообщает, что объемы спама, связанного с авансовыми переводами денег за призы и азартные игры, значительно вырос во второй половине 2009 г. В США объемы рассылки спама составляют 27%, затем идет Корея (6,9%), Китай (6,1%), Бразилия (5,8%) и Россия (2,9%).

31. Большую часть потока обмена сообщениями составляет спам[29] и, как

безопасности, 2010 (http://www.microsoft.com/security/about/sir.aspx).

26 Отчет «Sophos" об угрозе безопасности (август 2010 г.): http://www.sophos.com/security/topic/security-report-2010.html

27 Информационный бюллетень Symantec за апрель — июнь 2010 г. http://www.symantec.com/business/theme.jsp?themeid=threatreport

28 Основано на данных, полученных в результате очистки компьютеров антивирусными программами компании "Microsoft". Информационный отчет Microsoft по безопасности, том 8, июль-декабрь 2009 г. http://www.microsoft.com/security/about/sir.aspx

29 По оценкам от 75% до более, чем 90% всех сообщений электронной почты, направляемых во всем мире.

оказалось, лишь ограниченное число бот-сетей вовлечено в рассылку спама[30]. В период с апреля по июнь 2010 г. «Symantec" просмотрела около 89 % спама от всего объема пересылаемых сообщений[31]. Компания «SPAMHOUSE" утверждает, что:

«80% спама, получаемого Интернет-пользователями в Северной Америке и Европы, можно отследить через псевдоимена, адреса, перенаправление ссылки, местонахождение серверов, доменов и серверов DNS, а также через данные о группе 100 известных спам-операторов, большинство из которых указаны в базе данных «ROKSO"[32].

2.2.2.2 Бот-сети[33]

32. Бот-сети остаются основной угрозой для информационной безопасности и совершения киберпреступлений. Они состоят из группы компьютеров, которые заражены вредоносной программой, которая превращает их в «роботов» (ботов) или «зомби»[34] и которые контролируются удаленно (владелец компьютера даже не подозревает об этом) владельцем бота с сервера управления и контроля. Вредоносная программа может выявить уязвимые места и размножить себя на другие системы.

33. В 2005 г. власти Нидерландов раскрыли бот-сеть, которая охватывала 1,5 миллиона зараженных компьютеров («ботов»)[35]. В декабре 2009 г.

Согласно данным, отраженных в Отчете компании «Commtouch» «О тенденции Интернет-угроз», за первый квартал 2010 г. число спама и фишинговых сообщенй превышает 183 миллиарда в день (www.commtouch.com/download/1679)

30 Информационный отчет Microsoft по безопасности, том 8, июль-декабрь 2009 г. Согласно данному отчету во второй половине 2009 г. на три бот-сети приходилось до 78,8% спама. Это "Rustock" (39,7%), "Bagle-cb" (28,6%) и "Cutwail" (10,4%). Такие бот-сети как, например, «Rustock" способны, по оценкам экспертов, направлять 30 миллиардов спам-сообщений ежедневно http://www.microsoft.com/security/about/sir.aspx. Таким образом, закрытие в ноябре 2008 г. «MColo", одного из поставщиков web-узлов в Сан-Фрациско, которая «приютила» крупнейшую в мире бот-сеть «Srizbi", на время сократила объемы всего спама на 50 % http://www.washingtonpost.com/wpdyn/content/article/2008/11/12/AR2008111200658_2.html?sid=ST2008111801165&s_pos

31 Информационный бюллетень Symantec за апрель — июнь 2010 г. http://www.symantec.com/business/theme.jsp?themeid=threatreport

32 Реестр известных спам-операторов («ROKSO") представляет собой базу данных, содержащую упорядоченную информацию и доказательства об известных профессиональных спам-операторах, деятельность которых приостанавливалась как минимум тремя Интернет провайдерами за совершение правонарушений, связанных со спамом. http://www.spamhaus.org/rokso/

33 См. Информационный отчет Microsoft по безопасности, том 9, январь - июнь 2010 г. с детальным анализом информации о бот-сетях

34 "Commtouch" сообщает, что в первом квартале 2010 г. ежедневно активировалось 305,000 «зомби». Большая их часть пришлась на Бразилию (14%), Индию (10%), Вьетнам (8%), Российскую Федерацию (7%) и Украину (4%) (www.commtouch.com/download/1679)

35 http://www.v3.co.uk/vnunet/news/2144375/botnet-operation-ruled-million

прекратила свою деятельность бот-сеть «Mariposa", которая состояла из 12 миллионов зараженных компьютеров[36]. Вредоносная программа «отслеживала» действия, совершаемые на зараженных системах для получения паролей, банковских данных и данных о кредитных картах[37].

34. Через бот-сети распространяется спам и парализуется работа сайтов. Они также могут быть использованы для распределенной атаки типа отказ в обслуживании (DDOS-атаки) для того, чтобы сорвать работу ключевой инфраструктуры. При этом очень сложно отследить атаки и тех, кто стоит за ними.

35. Уничтожение бот-сети «Rustock» в 2011 г. и последовавшее после этого подача иска в суд компанией «Microsoft" и другими компаниями показала новые правовые и правоохранительные возможности для сотрудничества государственного и частного сектора[38]. Вместе с технологиями отслеживания денежных средств также возможно определять преступников или преступные организации, связанных с ними[39].

2.2.2.3 Домены, используемые в преступных целях

36. Следующая составляющая киберпреступности — это использование доменов в преступных целях. Такие домены используются для бот-сетей и спама, а также для размещения детской порнографии и другого незаконного контента, а также для рекламы теневых услуг и товаров.

37. Использование доменов для преступных целей облегчается следующими факторами:

-некоторые домены или услуги web-хостинга предусматривают «пуленепробиваемый хостинг», то есть когда провайдер не сотрудничает с правоохранительными органами и относится снисходительно к деятельности своих клиентов или содержанию тех материалов, которые последние загружают или распространяют[40]. Как сообщается многие из тех,

36 Главные подозреваемые были арестованы в Испании в феврале 2010, а создатель вредоносной программы — в Словении в июле 2010 г.

37 http://en.wikipedia.org/wiki/Mariposa_botnet

38 http://www.wired.com/beyond_the_beyond/2011/03/microsoft-versus-rustock-botnet/ Для просмотра информации об иске, поданном компанией «Microsoft" см. http://krebsonsecurity.com/2011/03/homegrown-rustock-botnet-fed-by-u-s-firms/

39 http://krebsonsecurity.com/2011/03/microsoft-hunting-rustock-controllers/

40 Сообщается, что большинство «пуленепробиваемых доменов» находится в Восточной Европе и Дальнем Востоке. Например, для понимания ситуации в Европе, см. , например, отчет «Spamhouse" о доменах «Rock Phish", зарегистрированных на Nic.at (http://www.spamhaus.org/organization/statement.lasso?ref=7)

кто предлагал услуги «пуленепробиваемого хостинга» являются преступными организациями [41].

- В большинстве стран существуют правовые препятствия для закрытия доменов. Это особенно характерно для тех случаев, когда преступная деятельность осуществляется в другой стране, а не в той, где зарегистрирован домен.
- реестродержатели и регистраторы зачастую не выполняют свои функции по надлежащей проверке, когда регистрируют домены. Такие Интернет-ресурсы как доменные имена управляются соответственно Организацией по присвоению имени и адресов в Интернете (ICANN) и Региональными Интернет-регистраторами (RIRs) и их реестродержатеями (например, Интернет-провайдеры). Для доступа к этим ресурсам регистрирующееся лицо должно предоставить часть персональных данных в базу данных «Кто есть кто» (WHOIS). Согласно последнему отчету ICANN менее половины записей полностью точны (только 23%, если следовать жесткому определению «точности»)[42]. Также неточности были найдены в базе данных WHOIS RIRs. Это лишает правоохранительные органы возможности выследить тех, кто использует эти домены для преступной деятельности. Появление Интернет-протокола 6-ой версии, скорее всего, ухудшит эту ситуацию, поскольку большая часть IP-адресов будет распространяться в соответствии с существующей процедурой регистрации[43].
-даже если деятельность домена прекращена, то преступники могут перевести свою деятельность в другое место.

2.2.2.4 Теневая экономика

38. В течение последних нескольких лет зародилась «теневая экономика», которая предоставляет собой рынок товаров и услуг для совершения киберпреступлений, а также для продажи похищенных товаров и

41 Печально известным примером может служить «Russian Business Network" (http://www.washingtonpost.com/wpdyn/content/article/2007/10/12/AR2007101202461_pf.html; http://www.bizeul.org/files/RBN_study.pdf).

42 http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf

43 На конференции Совета Европы «Октопус» в 2010 г. было принято решение рекомендовать привести меры по надлежащей проверке, предпринимаемые ICANN, регистраторами и реестродержателями и соблюдению точности в базе данных WHOIS в соответствие со стандартами защиты информации. Также для достижения этих целей было рекомендовано одобрить «Изменения в Соглашение ICANN об аккредитации реестродержателей (RAA) и Рекомендации о надлежащей проверке, подготовленные правоохранительными органами» (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/2079_IF10_messages_1s%20provisional%20_24%20Apr%2010.pdf). http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/202/LEA_ICANN_Recom_oct2009.pdf

информации. Она представляет собой «единой экономическое пространство» для производителей, продавцов, поставщиков услуг, мошенников и клиентов[44]» и позволяет преступникам организовать свою деятельность. Согласно данным “Symantec”[45] на период с апреля по июнь 2010 г. самым рекламируемым товаром на «теневых серверах» являлись данные о кредитных картах (28%) и банковских счетах (24%).

39. Более того, такие платформы являются точками вброса украденных товаров и средствами обналичивания, то есть перевода виртуальных денег в реальные[46].

40. Такие товары и услуги представляют собой:

- информация о кредитных картах и иная информация для совершения мошенничества с использованием идентификационных данных;
- оффшорные банковские услуги и создание подставных компаний;
- «экспертные услуги», например, разработка вредоносных программ, восстановление данных и защита от экспертизы;
- рассылка спама, в том числе и для «выманивания» денежных средств;
- «пуленепробиваемый» хостинг;
- предложение в Интернете вредоносных программ и инструментов для облегчения или совершения других преступлений, таких как вредоносоные инструменты и поддельные анти-вирусные программы. Вредоносные инструменты позволяют лицу, не обладающему специальными техническими знаниями, создать и «развернуть» вредоносные программы, которые нацелены на дистанционные банковские услуги. Обычно она включает в себя такие компоненты как клавиатурные шпионы, формы захвата, а также программное обеспечение для бот-сетей «зомби».

2.2.2.5 Денежные мулы

41. «Денежные мулы» или «финансовые агенты» - это денежные курьеры, которые формируют основу для передачи преступных доходов от жертвы

44 Официальное описание “G Data” за 2009 г.: «Теневая экономика» (http://www.gdatasoftware.com/uploads/media/Whitepaper_Underground_Economy_8_2009_GB.pdf)

45 Информационный бюллетень Symantec за апрель — июнь 2010 г. http://www.symantec.com/business/theme.jsp?themeid=threatreport. См. также список товаров и услуг, доступных для продажи на теневых серверах (Корпорация “Symantec” 2010 г.) на http://www.symantec.com/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

46 Официальное описание “G Data” за 2009 г., стр. 17-18: «Теневая экономика» (http://www.gdatasoftware.com/uploads/media/Whitepaper_Underground_Economy_8_2009_GB.pdf)

преступнику[47]. Мулы могут и знать, и не знать о том, что они являются частью преступной цепочки. Их можно будет нанять разными способами: с потенциальными мулами могут связаться при помощи спама или когда он/она отвечает на вроде бы обычный сайт с объявлениями о работе, где рекламируются вакансии подставных компаний, например, «финансовый менеджер» «для надомной работы» и тому подобное. Мулы могут подписать настоящий трудовой контракт и предоставить копии паспорта и иных документов, удостоверяющих личность.

42. Их основная роль — это открыть счет или предоставить данные о своем уже открытом счете. После того как они получают денежные средства на свой счет им передаются инструкции о переводе этих средств на другой счет или за границу, используя электронный перевод, и, как следствие, облегчая отмывание денег, удерживая при этом комиссию.

43. Утверждается, что «денежные мулы» являются слабым звеном при совершении мошенничества при помощи компьютерных технологий. Кроме того, для использования похищенных кредитных карт и документов существующего количества денежных мулов явно недостаточно.

2.2.3 Новые платформы для киберпреступности

2.2.3.1 Социальные сети

44. Число социальных сетей и их пользователей значительно выросло за последние несколько лет[48]. Они также используются для распространения вредоносных программ, определяя цели для иных категорий киберпреступлений и ставят под угрозу безопасность. Согласно данным «Sophos"[49] социальные сети стали рентабельным и соблазнительным рынком для распространения вредоносных программ: при помощи программы Web 2.0 бот-сети воруют данные, выводят на экран ложные антивирусные сигналы тревоги и генерируют доход для преступников. Доля компаний, которые сообщили об атаках через спам и вредоносные программы с использованием социальных сетей увеличилось на 70% в 2009 г. Сотрудники, регистрируясь в социальных сетях, в результате

47 http://www.banksafeonline.org.uk/moneymule_explained.html

48 По данным «Facebook" на декабрь 2011 г. число только ее активных пользователей составило 845 миллионов (http://www.facebook.com/press/info.php?statistics)

49 Отчет «Sophos" об угрозе безопасности (август 2010 г.): http://www.sophos.com/security/topic/security-report-2010.html

подводят под удар информационные системы их компаний или учреждений, делая их доступными для спама, фишинга, вредоносных программ и утечки данных.

2.2.3.2 Облачная обработка данных

45. Развитие технологий сделало системы более уязвимыми для киберпреступности. Самой обсуждаемой тенденцией стала «облачная обработка данных», то есть перенос данных и услуг с определенного компьютера на сервер, который находится «где-то» в облаке. Это ведет к огромному количеству различных возможностей, но в то же время негативно влияет на безопасность. С одной стороны, отдельные компьютеры перестают быть такой уж соблазнительной целью, но с другой стороны «поскольку в Интернете храниться все больше важных данных […], то существует вероятность того, что системы безопасности будут взламываться все чаще, а большие объемы информации будут «уходить» быстрее, чем когда бы то ни было»[50].

46. Тот факт, что большая часть данных, необходимых для проведения расследования уголовного дела, будет храниться на сервере, находящемся на территории иностранного или неизвестного государства не способствует эффективной деятельности правоохранительных органов и наоборот, облегчает совершение киберпреступлений[51].

2.2.4 Предпосылки для киберпреступности

2.2.4.1 Организованная преступность

47. Экономическая преступность в течение многих лет оставалась основной

50 Отчет «Sophos" об угрозе безопасности (август 2010 г.), стр. 34: http://www.sophos.com/security/topic/security-report-2010.html. См. также http://www.sonicwall.com/downloads/SB_Security_Trends_US.pdf

51 http://www.eurodig.org/eurodig-2010/programme/workshops/workshop-1 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-resentations/2079_reps_IF10_reps_joeschwerha1a.pdf http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf/ Для того, чтобы решить вопрос о трансграничном доступе правоохранительных и судебных органов Комитет Конвенции против киберпреступности в ноябре 2011 г. принял решение о создании специальной группы, которая должна были предложить выход из создавшейся ситуации в виде Протокола к Будапештской Конвенции или иной документ, не носящий обязательный характер.

деятельностью организованных преступных группировок. Тенденция, наблюдаемая с 2004 г. такова, что преступники все чаще используют возможности Интернета и других информационных технологий, поскольку растет число как физических, так и юридических лиц, использующих такие технологии для своей экономической деятельности[52]. Основы для совершения киберпреступлений создаются еще и путем анонимности, деперсонализации и легкости общения, наличия возможностей для транснационального взаимодействия преступников для поиска новых жертв и отмывания денег, а также отсутствия связи между местом нахождения преступник и потерпевшего.

48. Сложные мошеннические схемы, сама инфраструктура киберпреступности (включая бот-сети и теневую экономику), уровень специализации и распределения ролей подтверждают наличие структурированных организованных преступных групп, которые действуют согласованно для совершения преступления и получения финансовых и иных материальных выгод[53].

2.2.4.2 Постоянные экономические и политические угрозы

49. Политические и экономические угрозы без получения немедленной экономической выгоды[54] такие как шпионаж, хактивизм (хакерство во имя политических или религиозных целей), терроризм[55], войны и конфликты, которые ведутся при помощи компьютерных систем, вызывают все большую озабоченность[56].

---

52 http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf, http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/Report2005E.pdf

53 Как определено в ст.2 Конвенции ООН против транснациональной организованной преступности

54 Также их называют «Передовые постоянные угрозы» или ППУ. Этот термин был придуман американской компанией «Mandiant", которая занимается вопросами безопасности (http://www.mandiant.com/services/advanced_persistent_threat/). Для краткого определения см.: http://www.damballa.com/knowledge/advanced-persistent-threats.php. Также: http://tominfosec.blogspot.com/2010/02/understanding-apt.html. Примеры приведены на http://www.businessweek.com/magazine/content/08_16/b4080032220668.htm

55 Использование Интернета для целей терроризма может включать в себя распределенные атаки типа отказа в обслуживании ключевой инфраструктуры, а также склонение, вербовку и обучение или использование информационных технологий для того, чтобы получить доступ идентификационным, коммуникационным и иным логистическим данным http://book.coe.int/EN/ficheouvrage.php?PAGEID=36&lang=EN&produit_aliasid=2221 http://www.mpicc.de/ww/en/pub/forschung/forschungsarbeit/strafrecht/cyberterrorismus.htm

56 Последние примеры это атаки на серверы «WIKI LEAKS" и наоборот на сайты, которые прекратили деловые отношения с «WIKI LEAKS" http://www.csmonitor.com/Business/new-economy/2010/1208/WikiLeaks-cyberattacks-now-involve-Visa-Facebook-Twitter-MasterCard, http://www.theglobeandmail.com/news/technology/wikileaks-faces-cyber-attacks-loses-paypal-account-

50. Проникновения и распределенные атаки типа отказа в обслуживании похожие на те, которые имели место в Эстонии в 2007 г.[57], Грузии в 2008 г.[58], США и Северной Корее в июле 2009 г.[59], взлом «Google" в декабре 2009 г.[60] или правительственных, деловых и учебных компьютерных систем в Индии в 2009 г., лишь показывают насколько сложно провести грань между преступностью, шпионажем[61], терроризмом и войной, поскольку такие атаки невозможно четко отнести какой- либо категории[62]. Поскольку данные преступления не направлены на извлечение прибыли, то в рамках настоящего исследования они рассматриваться не будут[63].

2.2.4.3 Финансирование терроризма

51. Террористические организации нуждаются в финансировании не только отдельных актов, но и для «покрытия длинного перечня оперативных расходов по развитию и поддержанию деятельности террористической организации, а также создания условий, позволяющих подпитывать их деятельность»[64].

52. Террористы могут собирать средства, используя законную предпринимательскую деятельность, благотворительные организации, или различные виды преступной деятельности с использованием Интернета, например, взлом он-лайновых банковских счетов, мошенничество и кражи, совершенные с помощью похищенных данных о кредитной карте, а также

---

fordonations/article1825485/, http://news.cnet.com/8301-31921_3-20024935-281.html

57 http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

58 http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

59 http://www.guardian.co.uk/world/2009/jul/08/south-korea-cyber-attack, http://en.wikipedia.org/wiki/July_2009_cyber_attacks

60 http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html

61 См. также «Тени в облаках: расследование кибер-шпионажа 2.0» апрель 2010 г. (http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0). Данное исследование отражает тот факт, что существует сложная экосистема кибер-шпионажа, включая кражу засекреченной и иной секретной информации. Сервер управления и контроля использует социальные системы для взлома компьютеров, а затем перенаправляют информацию и контролируют эти компьютеры с серверов, предлагающих услуги бесплатного Web-хостинга, находящихся в Восточной Азии.

62 Скотт Чартни (2009 г.): «Переосмысление кибер-угрозы: основы и последующие шаги («Microsoft") (http://www.microsoft.com/downloads/details.aspx?FamilyID=062754cc-be0e-4bab-a181-077447f66877&displaylang=en). См. также: http://garwarner.blogspot.com/2010/07/future-of-cyber-attackattribution.html

63 Было бы полезно использовать меры уголовно-правового воздействия и использовать (прежде чем вырабатывать новые) наилучшим образом такие инструменты, как Будапештская Конвенция, а в отношении терроризма — Конвенцию Совета Европы о предупреждении терроризма (СДСЕ № 196) (http://www.conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG)

64 Источник: ФАТФ (2008): «Финансирование терроризма» (http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf)

отмывание доходов через сайты азартных игр. Сообщается, что сайты благотворительных организаций также используются для сбора средств на террористические цели, он-лайновые платежные системы особенно уязвимы в части их использования террористическими организациями[65].

2.3 Преступления в Интернете, приносящие доход

53. Получение финансовых и иных экономических выгод — это была одна из мотиваций, которой руководствовались преступники с самого начала[66]. Однако эксперты единодушны в своем мнении, что основная цель киберпреступности в настоящее время — это получение дохода.

54. Очень тяжело оценить криминальные потоки денег в Интернете, а какие-либо надежные данные отсутствуют. Некоторые размышления могут навести на предположение о том, что киберпреступность, возможно, является самой доходным сектором:

- общество зависит от информационных и коммуникационных технологий;
- почти любое преступление может быть совершено более эффективно с наименьшими рисками через Интернет;
- более двух миллиардов, большое количество компаний, в частности, в финансовом секторе, государственные учреждения во всем мире связаны через Интернет[67]. Они потенциальные жертвы кибер-преступников;
- для киберпреступности не существует границ. Это снижает риск быть пойманным. Тот факт, что потерпевший находится на территории другого государства, значительно уменьшает «порыв» правоохранительных органов проводить расследование и осуществлять преследование. Кроме того, какие-либо риски для преступников снижаются также «благодаря» недостаточному уровню международного сотрудничества и несовершенного законодательства;
- киберпреступность, включая мошеннические схемы, все более

65 Майкл Якобсон «Финансирование терроризма и Интернет» Исследование конфликта и терроризма, 33:4, 353-363. Доступно на http://www.informaworld.com/smpp/section?content=a919769800&fulltext=713240928. Группа разработки финансовых мер борьбы с отмыванием денег «Уязвимость коммерческих сайтов и он-лайновых платежных систем для отмывания денег и финансирования терроризма (июнь 2008 г.) http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

66 См. «Der Spiegal" (Германия) за 22 января 1979 г. Ранние виды киберпреступлений включали в себя телефонное мошенничество в начале 1970-х (Говард Шмидт (2006): «Патрулируя киберпространство», «Larstan Publishing") .

67 В качестве примера: объем продаж или дохода от электронной торговли в США в 2008 г. составил 3,7 триллионов долларов (Источник:http://www.census.gov/econ/estats/2008/2008reportfinal.pdf).

автоматизированы и не нуждаются в присутствии человека;

– теневая экономика предоставляет доступ к недорогому инструментарию для совершения киберпреступлений. Теперь даже сверхсложные атаки не требуют особых знаний;

– для совершения киберпреступлений не нужно прибегать к насилию или заставлять человека и, таким образом не требуют личного контакта, человеческого участия.

55. Основываясь на этих суждениях, можно предположить, что экономический вред, который наносит киберпреступность, превышает наносимый просто экономической и организованной преступностью. Однако, экономический ущерб не равен криминальным потокам денежных средств в сети Интернет. Затраты на ремонт, потеря производительности, снижение доходов, потеря данных, потеря репутации, инфраструктуры, проведение корректировки и дальнейшее развитие, расходы на безопасность, правоохрану и иные аспекты могут стоить компаниям больше, чем денежный ущерб, нанесенный мошенничеством или кражей[68].

56. Приведенные ниже данные отражают те сумму, которые «стоят на кону», а также указывают на необходимость всеобъемлющего анализа и предоставления информации:

- из 146,663 жалоб, полученных и перенаправленных американским Центром приема сообщений об Интернет-преступлениях в правоохранительные органы в 2009 г., 100,206 жалоб содержали данные о материальном ущербе на сумму 559,7 миллионов долларов США[69].
- количество жалоб, сформулированных в базе данных жалоб потребителей Федеральной комиссии США по торговле[70], достигло 1.3 миллионов в 2009 г. размер выплат или потерь в результате реализации мошеннических схем составил в 2009 г. 1.7 миллиардов долларов США.
- В Германии данные об ущербе, причиненном киберпреступлениями ведутся Федеральной уголовной полицией, который в 2009 г. составил 36,9 миллионов евро[71].

68 Для типологии расходов на безопасность см. Михель Ван Этен/Йоханнес М.Бауэр/ Ширин Табатабай (2009): «Ущерб от нарушения безопасности в Интернете — основа и инструментарий для оценки экономических затрат на нарушение защиты. TU Delft (www.opta.nl/nl/download/publicatie/?id=3083)

69 Центр приема сообщений об Интернет-преступлениях. Отчет о киберпреступности за 2009 г. (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

70 База данных жалоб потребителей Федеральной комиссии США по торговле, данные за 2009 г. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf. Также включены данные IC3.

71 Согласно Федеральной уголовной полиции эта информация не включает в себя ущерб от фишинга или бот-

- в 2008 г. авиакомпании подсчитали, что они потеряли 1,4 миллиарда долларов США из-за мошеннического он-лайн бронирования[72].
- в 2008 г. потери от контрафактного программного обеспечения составили 53 миллиарда долларов США[73].
-обзор, содержащий информацию о 45 американских компаниях и опубликованный в июле 2010 г., содержит данные о том, что каждая компания хотя бы раз в неделю подверглась атаке, которая была успешна, затрачивая в среднем в год около 3,8 миллионов долларов США. Внешние издержки связаны прежде всего с кражей информацией (42%), нарушением деятельности и снижением продуктивности (22%), в то время как внутренние издержки связаны с выявлением и восстановлением[74].
- организация «UK Payments" подсчитала, что общая сумма ущерба по картам составила в 2009 г. 440,3 миллиона фунтов стерлингов[75]. Из них CNP – мошенничества. т. е. без физического наличия платежной карточки у преступников составляет 266,4 миллиона фунтов стерлингов.

57. Не все преступные деяния, совершаемые при помощи компьютеров приводят к получению преступного дохода. Следующие категории преступлений, направленных на получение дохода и, таким образом, являющихся предикатными преступлениями к отмыванию денег, особенно широко распространены.

2.3.1 Мошенничество

58. Основной категорией преступлений для получения прибыли в Интернете, как и в обычной жизни, является мошенничество, т. е. преднамеренный обман для того, чтобы лицо лишилось своего имущества, с последующим получением экономической выгоды[76]. Для того, чтобы обеспечить криминализацию не только обычного мошенничества, совершенного при помощи информационно-коммуникационных технологий, но и мошенничества, связанного с нарушением целостности компьютерных данных и систем, в текст Будапештской Конвенции было введено специальное положение о «мошенничестве, совершенном с

сетей, поскольку им не присваивается уникальный номер.
72 http://forms.cybersource.com/forms/airlinefraudpr
73 http://portal.bsa.org/Internetreport2009/2009Internetpiracyreport.pdf
74 http://www.arcsight.com/press/release/arcsight-and-ponemon-institute-release-first-annual-cost-of-cyber-crimestu/
75 http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/
76 Для схем от А до Я см. http://www.actionfraud.org.uk/a-z_of_fraud

использованием компьютерных технологий»[77].

59. Ответы на вопросник лишь подтверждают тот факт, что мошенничество остается основной категорией киберпреступлений в большинстве стран. Например[78]:

- Албания: сообщается, что объем мошенничества с кредитными картами и мошенничество через Интернет растет. С июня 2009 г. было выявлено восемь случаев мошенничества с кредитными картами и 5 — с мошенничеством через Интернет. Было возбуждено 15 уголовных дел из них:
  - 13 дел, связанных с компьютерным мошенничеством, включая восемь случаев мошенничества с кредитными картами и 5 — с мошенничеством через Интернет;
  - 1 случай воздействия на функционирование системы;
  - 1 случай распространения детской порнографии.

- Андорра: большая часть киберпреступлений связана с кредитными картами 53 расследования в 2009 г.), затем идет мошенничество в Интернете (12 расследований), клевета (10 расследований) и детская порнография (7 расследований).

- Эстония: зарегистрированное количество киберпреступлений увеличилось с 71 факта (2005 г.) до 501 факта (2009 г.), из которых 470 — это мошенничество, с использованием компьютерных технологий. Кроме того, данная категория мошенничества составляет большое количество осуществленных преследований (в 2009 г.: 353 из 368 дел, в отношении 148 лиц 159 осуществлялось преследование). При вынесении в 2009 г. шести

77 «Статья 8 — Мошенничество с использованием компьютерных технологий

Каждая Сторона принимает такие законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву — в случае совершения умышленно и неправомерно — лишения лица его собственности путем:

a. любого ввода, изменения, удаления или блокирования компьютерных данных;

b. любого вмешательства в функционирование компьютерной системы,

мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или другого лица».

Во многих странах положения о мошенничестве традиционно должны включать обман лица или введение его в заблуждение, но не охватывают «обман» компьютерной системы. В Германии, например, для соответствия положениям Будапештской Конвенции была введена специальная статья (Статься 263a – Компьютерное мошенничество) (см. Филипп Брунст/Ульрих Зибер (2010): «Законодательство для борьбы с киберпреступностью». В: Я.Базедов/У.Кишель/У.Зибер «Национальный отчет Германии на 18 Международном конгрессе по сравнительному правоведению», Вашингтон, 2010 г., стр.730-731.

78 Источник: ответ на вопросник, если не указано иное.

обвинительных приговоров за отмывание денег было установлено, что использовался Интернет.

-Германия: общая уголовная статистика немецкой полиции[79], отражающая информацию обо всех преступлениях, зарегистрированных в полиции, в 2008 г. содержала данные о 63,642 преступлениях, совершенных при помощи компьютерных технологий[80]. Самая большая категория преступлений (23,689 дел) — мошенничество с незаконно полученными ПИН-данными к дебетовым картам, затем идет мошенничество, совершенное с использованием компьютерных технологий, т. е. путем воздействия на компьютерные данные и системы (17,006 дел). К третьей категории преступлений относится неправомерный перехват или информационный шпионаж (7,727 дел), затем идет подлог с использованием компьютерных технологий (5,716 дел) и мошенничество, связанное с неправомерным доступом к услугам связи (5,244 дела).

В отдельных случаях сообщения об Интернет-преступлениях за 2009 г.[81] Федеральная уголовная полиция Германии (ВКА) выявила 50,254 дела, исключая мошенничества с кредитными картами:

– 22,963 случаев мошенничества с использованием компьютерных технологий (рост на 35% по сравнению с 2008 г.);
– 11,491 случай неправомерного перехвата/информационного шпионажа (рост на 48,7%);
– 7,205 случаев мошенничества, связанного с неправомерным доступом к услугам связи (рост на 37,4%);
– 6,319 случаев подлога с использованием компьютерных технологий (рост на 10,6%);
– 2,276 случаев воздействия на данные/выведение из строя (рост на 3,1%).

Ущерб составил 36.9 миллионов евро[82].

– Италия: компьютерное мошенничество является основным видом киберпреступлений; за период с апреля 2008 г. по апрель 2009 г. прокуратура Милана проводила расследование 1,753 дел, к которым привело расследование дел о незаконном доступе (541 дело). Что касается 1,653 дел,

79 Противоправные (преступные) деяния, с которыми приходится иметь дело полиции, включая попытки их совершения, за которые предусмотрено наказание, отражаются Уголовной статистике полиции
80 Похожие цифры и за предыдущие годы 62944 (2007), 59149 (2006), 62186 (2005), 66973 (2004).
81 http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf
82 Согласно Федеральной уголовной полиции эта информация не включает в себя ущерб от фишинга или бот-сетей, поскольку им не присваивается уникальный номер.

связанных с мошенничеством, то компьютерные технологии играли важную роль (например, мошенничество на Интернет-аукционах)[83].

– Литва: почти все дела о киберпреступлениях связаны с мошенничеством (4,586 дел зарегистрированных в 2009 г.), незаконным использованным средств платежа (2,376) и производством и незаконным владением электронными средствами платежа (881).

– Польша: в 2008 г. 94 новых дела о мошенничестве, переданные подразделением финансовой разведки в органы прокуратуры, содержали факты использования Интернета (для сравнения: 14 — в 2007 г. и 31 — в 2006 г.).

– Российская Федерация: Министерство внутренних дел усилило свою деятельность на данном направлении. В 2008 г. Управление «К» Министерства внутренних дел возбудило более 5,500 дел о незаконной деятельности в сфере информационных технологий, что отражает рост на 20% по сравнению с 2007 г. В январе 2009 г. Управление еженедельно начинало уголовное производство по 50-100 фактам.

– Словакия: статистика полиции не позволяет отдельно выявить дела,связанные с компьютерными системами, только если они не связаны с неправомерным использованием или разрушением данных на информационных носителях (включая незаконное использование логинов для Интернет-банкинга). В 2008 г. было выявлено 23 таки случая, а в 2009 г. - 28. Подразделение финансовой разведки выявило 128 случаев необычных сделок, связанных с фишингом и переводом денежных средств через соответствующие услуги по переводу денежных средств.

– Словения[84]: по 9 делам осуществлялось расследование и преследование. Дела были связаны с незаконным присвоением имущества и взломом компьютерных систем. По двум делам были осуждены два лица, снявшие деньги. Их признали виновными в отмывании денег по неосторожности. Одно дело об отмывании денег все еще рассматривается в суде, по другому ожидается обвинительное заключение. Возможный доход составил 128,500

83 Данные предоставлены прокуратурой Милана. Вслед за принятием Закона № 48 от 18 марта 2008 г., который ратифицировал Будапештскую Конвенцию, 29 прокуратур при районных апелляционных судах начали рассматривать дела о киберпреступлениях.

84 Сообщается, что вредоносные программы для бот-сети «Mariposa” были созданы в Словении. http://www.networkworld.com/news/2010/072810-alleged-mariposa-botnet-hacker-arrested.html

евро, но большая часть этих средств, заморожена Управлением по противодействию отмыванию денег или по решениям судов, по некоторым делам банки вернули денежные средства на банковские счета. Таким образом, реальные экономические потери не превысили 30,000 евро. Девять дел связаны со взломом информационных систем и созданием фальшивых Интернет-сайтов. На сегодняшний день два факта о взломе информационных систем привели к обвинительным приговорам за отмывание денег.

– Украина: ежегодно увеличивается количество дел, связанных с киберпреступлениями, которые передаются в суд: с 311 дел (226 из которых было передано в суд) в 2002 г. до 615 (364) в 2005 г., 691 (597) в 2008 г. и 707 (584) в 2009 г., из которых по 31 делу, связанному с воздействием на данные и систему, а также противозаконным использованием устройств, было проведено расследование. Эти дела переданы в суд.

– США[85]: американский Центр приема сообщений об Интернет-преступлениях IC3 в 2009 г. получил 336,655 жалоб, из которых 146,663 было передано в правоохранительные органы[86]. Большинство из них было связано с непоставкой товаров и непредставлением услуг (19,9%), кражей персональных данных (14,1%), мошенничеством с пластиковыми картами (10,4%) и мошенничеством на Интернет-аукционах (10,3%). Количество заявлений, формируемых в базе данных жалоб потребителей Федеральной комиссии США по торговле[87] в 2009 г. достигло 1.3 миллиона, из которых 54% - мошенничество, 21% - кража персональных данных и 25% иных заявлений. Схемы включали в себя:

– схемы знакомств по Интернету, реализованные мошенниками через сайты знакомств и электронную почту, они представлялись молодыми женщинами и вовлекали потенциальных жертв в личное общение, после чего просили перевести денежные средства для поездки к последнему. Для передачи денежных средств использовались лица, оказывающие услуги по переводу денежных средств. Это привело к многомиллионным потерям для граждан США.

– он-лайн кража из банка: проникновение и использование он-лайн номера банковского счета для отмывания денег, совершенное через цепочку

85 Список дел см. на http://www.justice.gov/criminal/cybercrime/cccases.html

86 Центр приема сообщений об Интернет-преступлениях (2010 г.). Отчет о киберпреступности за 2009 г. (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

87 База данных жалоб потребителей Федеральной комиссии США по торговле, данные за 2009 г. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf. Также включены данные IC3.

мулов, находившихся в США. Социальный инжиниринг (метод проникновения в защищенные системы, основанный на использовании социальной психологии — прим.переводчика) используется довольно часто (через компьютер или по телефону) для получения доступа к счету или облегчения такого доступа или получения ценной информации, например, адрес электронной почты лица для целенаправленной кражи персональных данных. Совершение преступлений может быть также связано с фишингом, перенаправление на «липовые» сайты, использование номера банковского счета в целях мошенничества и т. д.

– он-лайновые азартные игры через вербовку игроков, находящихся в США, и вовлечение международной банковской инфраструктуры (банковские чеки, электронные переводы, денежные переводы) для отмывания значительных денежных сумм с использованием сайтов, зарегистрированных в оффшорных юрисдикциях.

– производство и/или продажа поддельных документов, удостоверяющих личность (водительские права, паспорта, страховая карточка и т. д.) .

– он-лайн услуги по оказанию оффшорных банковских услуг, учреждению подставных компаний, web-хостингу, отмыванию денег, рассылке спама и т. д.

– распределенная атака типа отказ в обслуживании (DDoS), совершаемая по разным причинам, иногда для того, чтобы нанести офф-лайн удар по сайту соперника.

– изготовление или приобретение вредоносных программ, которые включали бы в себя клавиатурных шпионов, перехватчиков форм, бот-сети и т. д., для того, чтобы выявлять такие преступления как использование номера банковского счета в целях мошенничества;

– продажа поддельных антивирусных программ, пиратского программного обеспечения и фальсифицированных лекарств.

– мошенничество с кредитными картами и он-лайновое финансовое мошенничество путем кражи персональных идентификационных данных и использования е-продавцов, услуг по экспресс-доставке, банковских учреждений и он-лайновых платежных систем, например, «PayPal” и “Google Checkout”. Выявлены две крупные категории преступлений:

  – перегрузка украденных компьютеров, высоко-технологичного оборудования, модных аксессуаров и т. д. через разветвленную сеть специальных мулов, находившуюся в США для заказчиков-преступников, находившихся на территории оффшора;

– отмывание преступных доходов от продажи несуществующих товаров, например, программного обеспечения, видео-игр и т. д. через аукционы, на которых товар последовательно заказывается через е-продавцов с украденными идентификационными и финансовыми данными. Преступные доходы отмываются через он-лайновые платежи и счета финансовых учреждений в США и затем переводятся главарям, находящимся на территории офшора.

60. Другие схемы могут включать в себя налоговые мошенничества, когда преступники направляют сфальсифицированные заявления на льготы, на официальные он-лайновые системы используя формы для расчета налогов[88].

61. Поскольку большая часть случаев мошенничества совершается через Интернет, то трудно их классифицировать. Последние исследования указывают на то, что следующие явления превалируют.

2.3.1.1 Хищение персональных данных

Огромное количество случаев мошенничества, совершаемых через Интернет и иные информационно-коммуникационные технологии, связано так или иначе с хищением персональных данных, где последнее определено как «мошенничество или иное незаконное действие, когда персональные данные существующего лица используются в качестве основного инструмента без его согласия[89], «незаконное использование идентификационных данных (имени, даты рождения, адреса финансовой и иной персональной информации) другого лица, если оно не знает об этом или его согласие не получено» или «присвоение личности другого лица путем хищения персональных идентификационных данных (PII) для совершения мошенничества» или «кражи или присвоения уже существующих личных данных (или их значительную часть) с или без согласия лица, не зависимо от того живо оно или умерло».

88 Лицо было арестовано за отмывание 1 миллиона фунта стерлингов в результате он-лайнового налогового мошенничества. См. http://www.theregister.co.uk/2009/09/04/pceu_hmrc/

89 Определение, предложенное Берт-Жаап Купсом/Рональдом Линсом (2006 г.). См. http://www.fidis.net/fileadmin/fidis/publications/2006/DuD09_2006_553.pdf.
Следующее определение дано в Законе США «О краже персональных данных и сдерживании присвоения » (раздел 18, п. 1028 (а) (7), согласно которому наказывается лицо, которое «осознанно передает или использует, без законного на то права средства идентификации другого лица для совершения или содействия или подстрекательства к незаконной деятельности, которая является нарушением Федерального законодательства или тяжким преступлением в соответствии с федеральным или местным законодательством».

62. В принципе хищение персональных данных можно разделить на три стадии:

1. получение идентификационной информации, например, путем обычной кражи, поисковых систем, внутренних и внешних атак (незаконный доступ к компьютерной систем, трояны, клавиатурные шпионы, шпионские и иные вредоносные программы) или фишинга и иных техник социального инжиниринга.
2. владение и распоряжение идентификационными данными, включая продажу такой информации, что в настоящее время играет важную роль для инфраструктуры е-теневой экономики, где самым востребованным товаром является информация о кредитных картах, реквизиты банковских счетов, пароли и т. п.
3. использование идентификационной информации для совершения мошенничества и иных преступлений, например, путем присвоения личности иного лица для пользования банковским счетом и кредитными картами, открытия новых счетов, получения займов и кредитов, заказа товаров и услуг или распространения вредоносных программ.

63. Фишинг остается одной из основных технологий социального инжиниринга, используемого в Интернете для хищения персональных данных для последующего мошенничества. Разновидности его включают смишинг (обмен смс-сообщениями для получения информации), целенаправленные фишинг (персональные ложные сообщения, направленные на получение данных конкретного человека), фарминг (автоматическое перенаправление пользователя с легитимных на фальшивые сайты для того, чтобы последний раскрыл информацию о себе) и спуфинг (лицо или программа, выдающие себя за других с тем, чтобы «войти в доверие» и вынудить пользователя ввести свои данные на фальшивом сайте); финансовые учреждения, а также он-лайновые платежные системы и Интернет-аукционы — наиболее уязвимы[90]. Что касается отмывания денег, то каждый должен сообщать о фишинговых атаках, когда полученная информация используется для перевода средств с одного счета на другой.

90 Согласно данным «Ariva” больше всего фишинговым атакам в 2011 г. подвергался «PayPal”, затем идут другие (например, «Ebay”, «HSBC Bank” , “Chase Bank” и т. д. http://techblog.avira.com/2011/03/12/phishing-spam-and-malware-statistics-for-february-2011/en/

64. Антифишинговая рабочая группа сообщает, что за период с июля по декабрь 2009 г. произошло 126,700 атак[91]. За две трети из них ответственность взяла преступная фишинг — группа “Avalanche”, которая использовала технику и инфраструктуру, характерную для большинства фишинг-сайтов, нанеся удар по сорока финансовым учреждениям, он-лайн сервисам и рекрутинговым агентствам для получения идентификационных данных. Более того, ее преступная деятельность включала в себя и распространение вредоносных программ для дальнейшего хищения информации:

«Кроме того, преступники использовали инфраструктуру «Avalanche” для распространения печально известного трояна «Zeus” - части сложной вредоносной программы, который внедрялся в фишинг и спам. «Zeus” - это изначально вредоносная хакерская программа, созданная специально для автоматической кражи персональных данных и несанкционированных операций. Потенциальным жертвам присылается «фишинговая приманка», предлагающая обновление популярных программ, файлообменники, загружаемые формы от налоговых органов (например, Налоговое управление США, Королевская налоговая и таможенная служба в Соединенном Королевстве). Если получатель «заглатывает» эту приманку, то его компьютер заражен и преступники получают удаленный доступ к нему, воруют персональные данные, хранящиеся на нем, влияют на пароли и он-лайновые операции. Преступники могут даже войти в компьютер потерпевшего и осуществить банковские операции он-лайн, используя реквизиты его банковского счета. Для банков очень трудно отнести их к мошенничеству. Сочетание фишинга, вредоносных программ, дополненное спамом стало одним из злокозненных в Интернете»[92].

65. Таким образом, мошенничество, связанно с кражей персональных данных, основано прежде всего с воздействием на данные с тем, чтобы обмануть компьютерную систему.

66. Нет консолидированной информации о хищении персональных данных при помощи компьютерных технологий, однако некоторую информацию можно получить из национальных оценок [93]. Из 146,664 обращений,

91 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf
92 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf
93 УНП ООН: «Глобализация преступности: оценка угрозы, которую несет транснациональная организованная преступность» (2010 г.), см. http://www.unodc.org/documents/data-and-

полученных американским Центром приема сообщений об Интернет-преступлениях и переданных в правоохранительные органы в 2009 г., кража персональных данных шла на втором месте (14,1%) после непоставки товаров (19,9%)[94]. Согласно информации Федеральной комиссии США по торговле хищение персональных данных являлась основным видом жалоб в 2009 г. (21% или 278,078 из 721,418 полученных обращений). Основной формой хищения является мошенничество с кредитными картами (17%), мошенничество с правительственными льготами (16%), телефонное или иное коммуникационное мошенничество (15%) и мошенничество при устройстве на работу (13%).

67. Уголовная полиция Германии также отмечает, что помимо фишинга в части Интернет-банкинга (2,923 случая зарегистрировано в 2009 г.) используется и «кардинг», т. е. использование незаконно полученной информации о пластиковых карточках в целях мошенничества (53 случая), использование номера банковского счета, полученного в результате воздействия на данные для получения доступа к документам, удостоверяющим личность (617 случаев) и незаконное использование данных для доступа к телекоммуникационным системам (3,207 случаев)[95].

68. Кража персональных данных тесно связано с мошенничеством с платежными картами и незаконным использованием номеров банковского счета.

2.3.1.2 Мошенничество с платежными картами

69. Виды мошенничества с банковскими картами включают в себя:

– «Карточка физически отсутствует» (CNP) — это когда реквизиты настоящей карточки украдены и затем используются для совершения покупок через Интернет, телефон или почту. В Соединенном Королевстве на CNP-мошенничество приходится более половины ущерба от мошенничества с пластиковыми картами (266,4 миллионов фунтов стерлингов от общей суммы убытков в размере 440,3 миллионов фунтов стерлингов в 2009 г.); большая часть была совершена через

analysis/tocta/TOCTA_Report_2010_low_res.pdf

94 http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

95 http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf

Интернет[96];

- мошенничество при помощи поддельных карт, которые создаются на основании данных, считанных с магнитной полосы настоящей карты. В 2009 г. в Соединенном Королевстве данный вид мошенничества нанес ущерб на 80,9 миллионов фунтов стерлингов [97].
- потерянные или украденные карты, которые используются в магазинах, где не нужно вводить ПИН-код, или для совершения CNP-мошенничества;
- кража идентификационных данных карточки включает в себя открытие банковского счета на имя другого человека при помощи украденных или поддельных документов, удостоверяющих личность ("мошенничество при подаче заявления») или использование счета банковской карты другого лица, выдавая себя за настоящего владельца («использование номера банковского счета/карты в целях мошенничества»),
- мошенничество, связанное с неполучением по почте, т. е. это означает, что карточка была украдена в тот период времени, когда была отправлена компанией в адрес настоящего владельца.

70. С этим связаны следующее разновидности преступной деятельности:

- скимминг/клонирование, т. е. когда данные карточки скопированы («сняты») и проданы или изготовлены дубликаты («клоны»). Скимминг может происходить в нескольких местах: банкоматы или пункты продажи в результате технического взлома или преступного сговора с персоналом;
- утечка данных, когда персональная идентифицирующая информация (номера карт, имена, адреса и т. д.) крадется большими объемами у е-продавцов, экспедиторских компаний, кредитных организаций и иных он-лайновых систем;

96 См. Организация по предотвращению финансового мошенничества в Соединенном Королевстве 2010 г.: Мошенничество: факты 2010 г. - Полный обзор случаев мошенничества в платежной сфере и меры для его предотвращения (http://www.ukpayments.org.uk/files/fraud_the_facts_2010.pdf). Большая часть мошенничества с британскими картами совершается за границей (в 2009 г. 122.7 миллиона фунтов стерлингов из 440.3 миллионов фунтов стерлингов). Сообщается, что общий объем потерь снизился на 28% по сравнению с 2008 г. Не смотря на то, что данный отчет указывает на снижение уровня потерь от CNP-мошенничества на 19% по сравнению с 2008 г. подразделение компании «Visa" в Европе сообщает о постоянном росте уровня данного вида мошенничества, особенно если сравнивать с тем, что уровень потерь от иных видов мошенничества сокращается (источник: заседание Совета Европы 22 июля 2010 г.)

97 Организация по предотвращению финансового мошенничества в Соединенном Королевстве (2010 г.) (http://www.ukpayments.org.uk/files/fraud_the_facts_2010.pdf). Уровень указанного вида мошенничества снизился на 77% по сравнению с 2004 г.

- данные об украденных картах продаются партиями 1,000 долларов США за 100 номеров карт, что является обычной ценой;
- данные украденных карт зачастую используются для он-лайн покупок высокотехнологичного оборудования, компьютеров, ювелирных изделий, модных аксессуаров и т. д. Эти товары перегружаются мулами, действующими на территории различных государств, в адрес преступников;
- иное преимущество украденных реквизитов кредитных карт — это то, что можно создать на аукционе позицию дорогого товара, продающегося дешево. Победитель таких торгов оплачивает преступнику стоимость вещи, которую последний покупает или продает, используя реквизиты украденной карточки;
- преступный доход, получаемый в результате использования похищенных данных кредитных карт, отмываются через большое количества он-лайновых платежных счетов и счетов финансовых учреждений и затем при помощи электронного перевода передаются мулами преступникам.

2.3.1.3 Атаки на Интернет-банкинг, незаконное использование банковских счетов и их использование для мошенничества

71. Сообщается о большом количестве атак и незаконном использовании возможностей Интернет-банкинга.

72. Самым распространенным является фишинг. Общая схема фишинговых атак связана с тем, что клиента обманывают различными способами для того, чтобы он зашел на фальшивый сайт, который якобы принадлежит банку. Это можно сделать как по электронной почте, так и по телефону. Клиент вводит свои банковские данные для работы он-лайн на фальшивом сайте, которые и записываются преступниками, а затем используются для доступ к банковскому счету.

73. Большинство фишинговых атак спонтанны; они осуществляются путем рассылки большого количества спама. Однако имеют место и так называемый «целевой фишинг», когда атака совершается на конкретное наносится по конкретному лицу или небольшой группе лиц.

74. Существует и другая техника, называемая «фарминг», которая

перенаправляет клиента на фальшивый сайт. Эта деятельность связана с воздействием на процессы, используемые компьютером для определения IP-адреса конкретного сайта. Компьютер пользователя или широкополосный маршрутизатор может быть взломан и перепрограммирован на перехват запросов на сайт для дистанционного банковского обслуживания. Таким образом, клиент перенаправляется на фальшивый сайт.

75. Еще один способ — это использование троянов, созданных специально для банков, т. е. вредоносной программы, которая перехватывает сообщения между клиентом и Интернет-банком (атака с применением технологии «незаконный посредник»). Перехваченные банковские данные передаются преступникам. Кроме того, троян в ходе сессии обслуживания может выдать дополнительные инструкции. Это обманет компьютер банка, т. к. он получит разрешение на проведение операции, поскольку инструкции поступили, якобы, от клиента, не являющегося преступником.

76. Как только получены данные банковского счета клиента, преступники начинают использовать его для различных целей:
- деньги могут быть переведены со счета клиента. Для этого открывается новый счет (обычно мула) и денежные средства переводятся со взломанного счета клиента на счет мула;
- подается заявление на выдачу пластиковой карты. Для этого может быть использовано имя клиента, что ведет к снятию денежных средств или использования для покупок через торговые терминалы или Интернет с использованием взломанного счета;
- взломанный счет может быть использован и как счет мула.

77. И, наконец, несовершенство он-лайновой банковской инфраструктуры может быть использовано для взлома и получения доступа к данным клиента.

2.3.1.4 Мошенничество с использованием массового маркетинга

78. «Мошенничество с использованием массового маркетинга» - это «мошеннические схемы с использованием средств массовой коммуникации, включая телефоны, Интернет, массовую рассылку, телевидение, радио и

даже личный контакт для установления связи, оказания содействия или получение денег, активов и иных ценных вещей от большого количества потерпевших в одной и более юрисдикциях[98]. Это включает в себя авансовое мошенничество[99] или «мошенничество 419»[100], лотереи[101], призовые схемы и т. п.

79. Данный вид мошенничества может быть направлен на получение с большой группы лиц некрупных денежных сумм и наоборот. По оценкам экспертов, сумма ущерба составляет несколько миллиардов евро.

80. Указанный вид мошенничества совершается обычно целыми преступными сообществами с использованием информационных технологий, что позволяет им действовать и выбирать себе жертв по всему миру. Используемые ресурсы могут включать в себя законную деятельность (например, фирмы прямой почтовой рекламы), список контактов (например, от компаний, работающих без посредников), платежные системы, средства связи, фальсифицированные личные данные и подложные финансовые инструменты. Таким образом, данная категория мошенничества и кража персональных данных взаимосвязаны.

81. Международная рабочая группа по борьбе с мошенничеством с использованием массового маркетинга отмечает, что отмывание преступных доходов является важным компонентом для любых мошеннических схем. Потерпевшего могут попросить осуществить платеж при помощи наличных (чеки, почтовые переводы и т. п.). Инвестиционные мошеннические схемы обычно предусматривают использование банковских переводов, предусмотренных законодательством. В то же время группы из Западной Африки предпочитали электронные переводы, в результате которых денежные средства забирались при предъявлении поддельных документов, удостоверяющих личность. Платежи проводились по нескольким юрисдикциям. Это было сделано для того, чтобы исключить их отслеживание. Международная рабочая группа по борьбе с мошенничеством с использованием массового маркетинга также отмечает:

98 Согласно данным Международной рабочей группы по борьбе с мошенничеством с использованием массового маркетинга (июнь 2010 г.) http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf

99 Описание см. на: http://www.consumerfraudreporting.org/nigerian.php

100 Статья 419 Уголовного кодекса Нигерии криминализовала данное деяние. Для получения дополнительной информации см сайт Комисии Нигерии по борьбе с экономическим и финансовым мошенничеством (http://www.efccnigeria.org).

101 Описание см. на http://www.consumerfraudreporting.org/lotteries.php

«Рост использования данных потерпевших для получения денежных средств и последующего отмывания или получения и оплаты поддельных финансовых инструментов. Для осуществления данного вида мошенничества, могут наниматься люди, которые будут выполнять различные функции, например, собирать денежные переводы, размещать чек в банке для последующего инкассирования, передавать поддельные чеки иным потерпевшим, принимать поставки товаров, приобретенных при помощи украденных кредитных карт, передавать средства и товары за рубеж и служить в качестве агента лицевого счета для зарубежный компаний»[102].

82. Согласно данным американского Центра приема сообщений об Интернет-преступлениях авансовое мошенничество являлось третьей самой большой категорией правонарушений, по которым были получены жалобы в 2009 г. - 9,8%[103].

83. В Соединенном Королевстве ущерб от этой разновидности мошенничества составил 3,5 миллиардов фунтов стерлингов в 2006 г.; пострадало около 3,2 миллиона человек взрослого населения[104].

84. Мошенничество, связанное с переадресацией. Физические лица или небольшие компании путем обмана вовлекаются в пересылку товаров в страны со слабой правовой системой. Товары обычно оплачиваются при помощи украденной или поддельной кредитной карты[105].

2.3.1.5 Злоупотребление доверием, включая мошенничество на аукционах[106]

85. Мошенничество на аукционах в Интернете — это наиболее часто упоминаемые правонарушения[107]. Это включает как искажение данных о товаре, так и непоставку купленного и оплаченного товара. Обычно оплату требуют путем перевода наличных.

---

102 http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf, стр. 22.
103 http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf
104 Оценка угрозы организованной преступности в Соединенном Королевстве за 2009/2010 г., стр. 57, цитата из Отчета Антимонопольного управления. http://www.soca.gov.uk/about-soca/library
105 Для описания ситуации в каждом отдельном регионе см.: http://en.wikipedia.org/wiki/Internet_fraud
106 Описание см. http://www.consumerfraudreporting.org/auctionfraud.php
107 Американский Центр принятия сообщений об Интернет-преступлениях _____ относит жалобы о непоставке к самой обширной категории жалоб, переданных в правоохранительные органы в 2009 г. (19% от всех переданных жалоб) (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

2.3.1.6 Инвестиционное мошенничество, включая манипулирование на рынке ценных бумаг

86. Манипулирование на рынке ценных бумаг — это умышленная попытка нарушить свободную и честную деятельность рынка, создавая искусственные, ложные или вводящие в заблуждение данные о цене продаваемых активов. Примером манипулирования рынком ценных бумаг, совершаемого он-лайн является схема «накачка и сброс». Обычно такие схемы связаны с покупкой большого количества дешевых акций. Затем начинается массированная рассылки сообщений или реклама по телефону с тем, чтобы стимулировать людей на покупку именно этих акций. После того, как лица, стоящие за реализацией этой схемы, продадут все свои акции, «рекламная» кампания прекращается, цены стремительно снижаются, и инвесторы остаются с акциями, которые стоят гораздо меньше, чем они за них заплатили.

2.3.1.7 Пирамиды и сетевой маркетинг[108]

87. Сетевой маркетинг создается для продажи товаров и услуг через распространителей, которым обещано вознаграждение за их собственные продажи или продажи других лиц, которых удалось убедить присоединиться к сети. Такие схемы могут включать в себя продажу реальных товаров и услуг, но также и поддельных. Например, пирамиды или «схемы Понзи» предусматривают внесения финансовых инвестиций или иных платежей, которые будут возвращены, если удастся вовлечь большее число людей. Продавать товары и услуги при таком раскладе вовсе необязательно. Схема рушиться, когда к ней больше не присоединяются новые лица.

2.3.2 Иные категории преступлений в Интернете, приносящие доход

88. В дополнение к мошенничеству и финансовым преступлениям в Интернете могут совершаться и иные преступления, позволяющие получить доход тем или иным способом[109].

2.3.2.1 Материалы, содержащие факты насилия над ребенком

108 Описание см. на: http://www.consumerfraudreporting.org/MLMscams.htm

109 Начиная от торговли наркотиками и кончая вымогательством, торговлей людьми, скупка краденного и многие другие

89. Интернет, включая одноранговые системы обмена файлами, изменили методы распространения материалов, содержащих факты насилия над ребенком[110]. Теперь такие материалы доступны не только на ограниченном числе сайтов для педофилов. Распространение детской порнографии и иных материалов порождают все растущий спрос и, как следствие, сексуальную эксплуатацию детей[111]. Большинство таких сайтов являются коммерческими, то есть пользователю предлагается внести определенную денежную сумму зачастую после бесплатного «тура».

90. В ходе исследования, проведенного в Канаде в 2009 г.[112], было проанализировано 800 коммерческих сайтов, содержащих подобные материалы. 89,4% из них содержали изображения детей, не достигших 12 лет. Они были расположены на 1,091 обособленные IP-адреса. Более 70% находились в США, затем идет Канада (8,2%), Российская Федерация (3,7%), Соединенное Королевство (3,7%) и Германия (1,9%). Отмечается, что если сравнивать контент коммерческих и некоммерческих сайтов, то в Польше первая категория содержит на 80% больше материалов, содержащих факты насилия над ребенком, затем идет Бельгия (75%), Сингапур (61.5%), Турция (57,1%) и Италия (54,5%). В своем отчете за 2009 г. Британский Фонд наблюдения за Интернетом[113] отмечает, что 48% сайтов с изображениями насилия над детьми находятся в Северной Америке и 44% в Европе, включая Российскую Федерацию. Наиболее часто используемые доменные имена - это «.com" (41%) и «.ru" (20%).

91. Однако и эти данные могут быть неверными:

«И хотя точного подтверждения этому нет у Cybertip.ca есть все основания полагать, что сайты с изображениями насилия над детьми действуют на основании быстрых систем. То есть такие домены используют DNS-серверы, которые присваивают IP-адреса, сменяющиеся очень быстро.

110 Исследование содержит точку зрения, что в 1990-х законодательство по борьбе с детской порнографией было действительно эффективным и коммерческое распространение таких материалов было в большей степени незначительным (http://www.iptforensics.com/journal/volume4/j4_2_1.htm). Появление Интернета изменило ситуацию

111 Для того, чтобы такие материалы «не подпитывали» спрос в Будапештской Конвенции против киберпреступности в ст. 9 под понятие детской порнографии подпадает не только изображение несовершеннолетних, но и лиц «кажущихся несовершеннолетними», а также «реалистичное изображение несовершеннолетнего лица, участвующего в откровенных сексуальных действиях».

112 Канадский центр по защите детей 2009 г.: «Изображения, содержавшие сцены насилия над детьми» - анализ сайтов, проведенный Cybertip.ca (ноябрь 2009 г.) http://www.cybertip.ca/pdfs/Cybertip_researchreport.pdf

113 http://www.iwf.org.uk/media/news.285.htm

Обычно это IP-адреса, со взломанных компьютеров, которые подгружают соответствующий контент или действуют своего рода сервером-посредником для контента, находящихся на другой территории. Это означает, что в зависимости от региона просмотра, могут быть разные результаты. Даже если просмотр имел место 10 минут назад»[114].

92. То же самое канадское исследование содержит информацию о методах оплаты сайтов с детской порнографией. 56,4% сайтов принимают оплату по кредитной карте, 33,3% - при помощи он-лайн платежей. Около 24% - принимают платежи всеми возможными способами.

93. В 2009 г. Фонд наблюдения за Интернетом обработал 38,173 сообщения, из которых 8,844 касались сайтов с детской порнографией. В 2009 г. 461 неопределенная марка осуществляла свою деятельность для получения прибыли от детской порнографии[115].

94. Рассылка спама — это основная технология привлечения клиентов на сайты с детской порнографией.

2.3.2.2 Продажа фальсифицированных медикаментов[116]

95. Фальсифицированные медикаменты включают в себя лекарственные средства и медицинское оборудование в отношении, которых создается ложная информация об их характеристиках или источнике происхождения. Эта деятельность очень распространена в развивающихся странах, но масштабы проблемы разрастаются во всем мире[117]. Основная часть

114 Канадский центр по защите детей 2009 г.: «Изображения, содержавшие сцены насилия над детьми» - анализ сайтов, проведенный Cybertip.ca (ноябрь 2009 г.), стр 62 http://www.cybertip.ca/pdfs/Cybertip_researchreport.pdf. См. также http://wikileaks.org/wiki/An_insight_into_child_porn, который содержит описание использования специальных кодов для сокрытия контента серверов или сервера-посредника для того, чтобы скрыть обмен информацией между пользователем и сервером, т. е. сделать его анонимным и неотслеживаемым. Кроме того, можно взломать обычные сайты для размещения рекламы детской порногрфии или для того, чтобы перенаправлять пользователей на такие сайты. См. http://www.iwf.org.uk/documents/20100511_iwf_2009_annual_and_charity_report.pdf

115 http://www.iwf.org.uk/documents/20100511_iwf_2009_annual_and_charity_report.pdf

116 «Фальсифицированный медикаменты — это те, в отношении которых умышленно и обманным путем распространяются ложные сведения о характеристиках и/или источнике происхождения. Фальсификация может иметь место как в отношении запатентованных, так и непатентованных лекарственных средств. Поддельные лекарственные средства включают в себя те, в составе которых есть правильные ингредиенты и неправильные, те, в которых активные ингредиенты вообще отсутствуют или присутствуют в незначительном количестве или с поддельной упаковкой» (http://www.who.int/medicines/services/counterfeit/overview/en/)

117 Например, исследование 2009 г. о рынке фальсификата в 14 европейских государствах содержит информацию об обороте в размере 10,5 миллиардов евро каждый год. http://www.eaasm.eu/Media_centre/News/February_2010

фальсификата производится в Азии (из-за того, что производство оригинальных препаратов передано в этот регион). Фальсификат зачастую продается в промышленных масштабах через законную сеть распространения.

96. Развитие Интернета привело к значительному росту продаж и распространения поддельных лекарственных средств. Это происходит из-за высоких прибылей и широких возможностей, аутсорсинга, перепаковки и изменения цепочки распространения, низких рисков, возникающих в результате несовершенного законодательства, низкого уровня международного сотрудничества, а также вовлечения в эту деятельность организованных преступных групп, сопряженного с анонимностью, легкостью установления контактов и расширения международных границ, то есть все то, предлагает Интернет.

97. Что касается Интернета, то основными каналами являются:

– Интернет-аптеки. Исследование показывает, что большая часть е-аптек продают некачественные или поддельные или несертифицированные лекарства[118]. Деньги переводятся клиентами через он-лайновые платежные системы в банки, находящиеся за рубежом[119]
– спам или мошенничество при помощи массового маркетинга. Как установлено, сообщения о реализации лекарственных средств составляют 81% или 183 миллиарда спам-сообщений ежедневно[120] Деятельность фармацевтических спамеров основана на использовании бот-сетей и пуленепробиваемого хостинга[121], а также рассылке миллионов сообщений в день. Такие спамеры считаются самыми лучшими во всем мире[122]. Спамер может направить сообщение от конкретной е-аптеки или действовать как

---

http://www.pfizer.co.uk/sites/PfizerCoUK/Media/Pages/CrackingCounterfeitEurope.aspx. Последнее дело в США: http://news.hostexploit.com/cybercrime-news/4448-online-pharmacies-targeted-forillegally-distributing-drugs.html

118 http://v35.pixelcms.com/ams/assets/312296678531/455_EAASM_counterfeiting%20report_020608.pdf

119 См. типологическое исследование МАНИВЭЛ о взаимосвязи отмывания денег и фальсификации (2009 г.) http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2008)22RRepTyp_counterfeiting.pdf

120 Согласно отчету «Commtouch" "О тенденциях Интернет-угроз» 1 кв. 2010 г. (www.commtouch.com/download/1679)

121 Сообщается, что находится в Восточной Европе

122 Наибольшее число спам-сообщений в 2009 г. разослала «Canadian Pharmacy". Большая часть серого рынка продавцов медицинских препаратов специально метят свои сайты, как если бы они были канадскими на основании предположения о том, что многие американцы думают, что канадские лекарства дешевле, чем американские. В Соединенном Королевстве они могут позиционировать себя как «United Pharmacy". См. также «ГлавМед» (http://spamtrackers.eu/wiki/index.php/Glavmed).

заинтересованный рекламщик, получающий комиссию за каждое нажатие на спам-сообщение или от реальных продаж[123].

2.3.2.3 Нарушение авторских и смежных прав

98. Информационные технологии и Интернет облегчают цифровое воспроизведение и распространение материалов, охраняемых авторскими или смежными правами. Таким образом, Будапештская Конвенция (ст.10) требует от стран криминализовать такие нарушения, если они совершаются в коммерческом масштабе. Нарушения, связанные с авторскими и смежными правами, приносят большие суммы преступного дохода и зачастую имеют отношение к деятельности организованных преступных групп.

99. Например, что касается пиратского программного обеспечения в Интернете, то ущерб, нанесенный в 2008 г., оценивался в 53 миллиарда долларов США недополученного дохода. Эта цифра не включает ущерб от рисков, связанных с непригодным программным обеспечением, а также соотношение между вредоносным и пиратским программным обеспечением. Кроме того, она не учитывает недополученные доходы от поддержки, оказываемой законно, и услуг по продаже [124].

2.3.2.4 Он-лайн вымогательство

100. Преступниками используются различные методы вымогательства денег у жертв при помощи Интернета и других технологий. Например, информационная система государственного или частного учреждения целенаправленно угрожают или создается угроза опубликовать личную или опасную информацию о лице или учреждении[125]. Что касается коммерческой деятельности, то схемы вымогательства обычно включают в себя угрозу спровоцировать сбой в работе сетей и сайтов путем распределенной атаки типа отказа в обслуживании или похитить информацию. Также они включают в себя и репутационные угрозы, в т.ч. искажение внешнего вида сайта или предание гласности информацию о ненадежности IT-систем или ненадлежащей защите данных клиентов[126].

123 Сообщается, что «GlavNed" платило комиссию в размере 30-40% от продаваемых лекарств. http://www.networkworld.com/news/2009/071609-canadian-pharmacy-spam.html?hpg1=bn
124 http://portal.bsa.org/Internetreport2009/2009Internetpiracyreport.pdf
125 http://www.cas.sc.edu/socy/faculty/deflem/zInternetextort.html
126 http://us.mcafee.com/en-us/local/html/identity_theft/NAVirtualCriminologyReport07.pdf

Для передачи полученного от вымогательства дохода используются он-лайновые платежные системы. Такие операции включают в себя и отмывание денег, после получения выгодоприобретателем преступного имущества (т. е. доходов от вымогательства).

101. Некоторые примеры описывают использование антивредоносного программного обеспечения, когда пользователя склоняют к установке программы, которая тут же выбрасывает предупреждение о том, что компьютер заражен и нужно загрузить новую антивирусную программу[127] за отдельную плату и естественно не защищает, а наоборот содержит вредоносную программу или «схему-убийцу», т. е. жертве угрожают убить его/ее, членов семьи или друзей, если он/она не будут следовать инструкциями и не переведут деньги, используя услуги по переводу денег[128]. Отчеты отражают тот факт, что масштабы этого явления растут, зачастую к этой деятельности присоединяются организованные преступные сети. К сожалению, это одна из сфер, где ощущается недостаток данных и, как результат, нет достоверных данных о масштабах вымогательства.

2.4 Составление схемы картины рисков и «слабых» мест, связанных с киберпреступностью

102. Из-за быстрой скорости роста технического развития, платежные системы также очень быстро развиваются в части скорости операций, количества и видов поставщиков услуг, платежных методов, вариантов очистки и даже валют. Последний виток развития платежных систем предоставляет новые возможности для лиц, занимающихся отмыванием денег и делает практически невозможным выявление потенциальных подозрительных операций. Кроме того, кибер-преступники могут в рамках одной схемы смешивать традиционные и новые платежные методы, различные виды операций, включая наличные, банковские переводы, предоплаченные карты, системы денежных переводов, электронные деньги и иные электронные платежные системы.

127 http://www.usprwire.com/Detailed/Computers_Internet/Fake_antivirus_software_take_extortion_scams_to_the_21st_century_109371.shtml или см. также отчет «Symantec" о мошенническом программном обеспечении системы безопасности (2009 г.) http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr_rogue_security

128 Отчет IC3 о преступности в Интернете за 2009 г. стр.11 (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

103. Некоторые платежные системы представляют большие риски ОД/ФТ, чем другие в зависимости от степени анонимности переводов, места нахождения поставщика услуг, дробление на агентов и субагентов, взаимодействие с кредитными или финансовыми учреждениями в юрисдикции, которая соблюдает международные стандарты в сфере ПОД/ФТ или нет, качества надзора, наличия правил и руководств в сфере ПОД/ФТ и т. д. Различные «продукты» имеют различные характеристики и такие характеристики могут лечь в основу профиля риска.

104. ФАТФ в своем исследовании 2006 г. о новых платежных методах выделила четыре основных рисковых с точки зрения ОД/ФТ фактора в части платежных систем в Интернете: анонимные счета, анонимное направление и получение счетов (АТМ), высокие или несуществующие лимиты пополнения счета, поставщики услуг, находящиеся в офшорах и зачастую не соблюдающие законодательство других юрисдикций. Факторами, снижающими риск, являются достаточные требования и процедуры идентификации владельца счета, ведение записей об операции, в которых отражались бы данные о плательщике и получателе, контроль за операциями и сообщение о подозрительной деятельности, ограничения по сумме внесения денежных средств, реализация таких функций, как блокирование счета и ограничения доступа к услугам[129].

105. Что касается киберпреступности и отмывания денег, то ответ на вопросник позволил выявить риски, описание которых приведено ниже.

2.4.1. Технические риски

106. Широко распространенный доступ к быстрому и современному оборудованию и соединениям, повсеместная доступность соединений к Интернету дает возможность людям проводить ряд финансовых операций быстрее и дешевле. Техническая сторона вопроса больше не является препятствием для доступа пользователя в Интернет, как источнику ценной информации, но и как возможности для перемещения денежных средств между лицами или юрисдикциями. При этом развивалось и программное обеспечение, создавая дружественный интерфейс между потребителем и он-лайновыми финансовыми услугами. Таким образом, отсутствие специальных знаний и компьютерных навыков не является больше

129 ФАТФ-ГАФИ - «Отмывание денег с использованием новых платежных методов», стр. 18, октябрь 2006 г.

препятствием.

107. Компьютерная сеть и информационные технологии создают инфраструктуру для международных поставок товаров, оказания услуг, перевода средств между физическими и юридическими лицами. Но с другой стороны такая легкость является потенциальной угрозой совершения киберпреступлений и отмывания денег при помощи компьютерных технологий.

108. С другой стороны, информационные технологии применимы для проведения расследований правоохранительными органами и осуществления надзора, но в то же время они дают возможность преступникам быстрый доступ к дешевым, оперативным и практически анонимным платежным системам. Если и преступники, и правоохранительные органы могут выиграть от использования платежных систем в Интернете, то знания и легкость использования этих характеристик и составляют отличие.

109. Из ответов на вопросник, присланных странами, очевидно, что если в органах полиции и прокуратуры обычно функционируют специализированные подразделения, то иные правоохранительные органы, подразделения финансовой разведки и надзорные органы испытывают нехватку опыта и знаний о новых платежных системах. Также были отмечены недостаточный уровень надзора, сложности в сотрудничестве с Интернет-провайдерами (например, Интернет-кафе, локальные сети университетских городков).

2.4.2 Анонимность

110. При начале взаимоотношений с поставщиком, оказывающим услуги по осуществлению Интернет-платежей, прямого контакта между клиентом и оператором не происходит или он сведен к минимуму. В основе этих услуг лежит деятельность, осуществляемая без личного присутствия. Таким образом операторы практически не знают своих клиентов. Пользователи получают доступ к финансовым услугам в Интернете через компьютерный терминал, а внесение денежных средств или выведение их из системы производится через посредника, которым может являться агент или банк.

111. Если посредником является банк, то банк не обладает актуальной

информацией об операции. Единственное, что может увидеть банк, так это изменения на кумулятивном счету провайдера.

112. С другой стороны, поставщики финансовых услуг не знают реальную личность клиента или источник происхождения денег, поскольку они размещаются на основании идентификационного кода.

113. Если посредником является агент (например, розничные продавцы предоплаченных карт или кассовых чеков), то денежные средства вносятся в наличной форме и личность клиента еще более неизвестна.

114. Таким образом, риски, связанные с отмыванием денег, могут быть снижены путем снижения возможностей пополнения счета через агентов, на которых можно положиться в части того, что они принимают меры по НПК в соответствии со стандартами ФАТФ.

115. Уязвимость платежных систем в Интернете основана на том факте, что многие из операторов позволяют открывать анонимные счета и осуществлять переводы между различными поставщиками услуг. Сразу после открытия деньги могут быть переведены в любую точку мира, без использования традиционной банковской системы. Более того, пластиковые карты могут быть присоединены к такому счету.

116. В некоторых случаях предоплаченные карты дают их владельцу полную анонимность. Также они могут быть преданы третьему лицу, которое и становится бенефициарным владельцем.

117. Анонимное внесение средств, наряду с отсутствием надежных данных об идентификации клиента могут привести к недостаточности сведений об операции или происхождении денежных средств в случае проведения уголовного расследования, а также препятствовать проведению расследований, связанных с отмыванием денег и финансированием терроризма. При таких обстоятельствах, международные стандарты и соответствующие национальные требования в части «знай своего клиента» и НПК, а также обязательств по направлению сообщений в недостаточной степени выполняются финансовыми посредниками. И даже, если некоторые меры по НПК и «знай своего клиента» выполняются поставщиками он-лайновых платежных услуг, то все равно они реализуются не в полном объеме из-за того, что большая часть клиентов разовые и «история» их

взаимодействия с данной категорией финансовых учреждений очень коротка, чего нельзя сказать о банковской системе.

2.4.3 Ограничения в части лицензирования и надзора

118. В большей части поступивших ответов было указано на то, что деятельность поставщиков платежных услуг урегулирована в недостаточной степени или за ними осуществляется слабый надзор в части выполнения требований ПОД/ФТ. Слабый контроль со стороны регулятора или отсутствие такового — это ключевой фактор риска как для учреждений, так и для юрисдикций наряду с недостаточным санкционным режимом.

119. Одной из трудностей в части лицензирования и надзора является то, что юрисдикция регистрации и юрисдикция, где осуществляется основная деятельность, не совпадают. В некоторых случаях проблемой может стать отсутствие специального законодательства для поставщиков финансовых услуг.

120. Иногда, поставщики е-платежных услуг сознательно стараются избегать исполнения требований путем регистрации в юрисдикциях с «облегченным» правовым режимом, которые позволяют осуществлять финансовые операции в других странах.

121. Другая трудность в реализации должного надзора заключается в том, что такие поставщики услуг действуют виртуально. У них нет физического обменного пункта, магазина или пункта продаж. Роль выездных проверок надзорных органов очень велика для соблюдения честности финансовых посредников, включая посредников е-платжных услуг. Проблема заключается в том, как провести выездную проверку в отношении виртуальной предпринимательской деятельности. Кроме того, при проведении таких проверок у представителей надзорных органов должны быть на вооружении все новые технологические средства. При этом также должны проводиться специальные обучающие мероприятия для проверяющих для того, чтобы достигнуть эффективности проверочных мероприятий в части хранения данных, надлежащего анализа процедур внутреннего контроля и иных обязательств по ПОД/ФТ.

122. Еще одной проблемой, связанной с надзором, является правовая компетенция надзорного органа в отношении поставщиков услуг по оплате в

Интернете. Одним из решений может служить лицензирование и последующий надзор за коммерческим предприятием, оказывающим финансовые услуги в той стране, где находится сервер. Но эта опция ставит под вопрос уровень соответствия требованиям ПОД/ФТ той или иной юрисдикции. Другим решением является возложение на власти того государства, где финансовая организация предлагает Интернет-услуги, ответственности за надзор.

123. Проблемным вопросом остается и лицензирование Интернет-услуг, т. к. лицензия выдается соответствующим государственным органом той юрисдикции, где зарегистрирован поставщик услуг, даже если услуги он предоставляет абсолютно в других странах. Проблема становится еще более запутанной из-за международного характера оказываемых в Сети услуг. Должно быть выработано общее мнение по этому вопросу, т. е. вопросы лицензирования и надзора должны быть как-то распределены между юрисдикциями регистрации и юрисдикциями оказания услуг.

2.4.4 Географические или юрисдикционные риски

124. С распространением Интернета во всем мире расстояние перестало иметь значение. Чем больше географический охват платежной системы (он-лайновой или обычной), тем выше риски ОД/ФТ. Преступники знают об этих недостатках и находят все новые инновационные решения для получения выгоды.

125. Транснациональное функционирование предоставляет преступникам очень заманчивые возможности, т. е. они могут осуществлять свою деятельность с территорий тех юрисдикций, в которых недостаточно развит режим ПОД/ФТ и соответствующий надзор, а также, где они не станут субъектами расследования, проводимого иностранными правоохранительными органами[130].

126. Поскольку деньги переводятся с территории на территорию, то можно выявить и существующие тенденции перемещения денежных потоков. Анализ ответов показал, что некоторые страны являются пунктом отправления преступных доходов, что может служить показателем того, что пострадавшие от киберпреступлений находятся именно там. К таким

130 ФАТФ-ГАФИ - «Отмывание денег с использованием новых платежных методов», стр. 28, октябрь 2010 г.

юрисдикциям обычно относятся страны Западной Европы и Северной Америки.

127. Другая категория стран являются пунктами назначения для потоков криминальных денег. Хотя не всегда можно установить тот факт, что эта страна и есть конченый пункт назначения. Обналичивание совмещенное с использованием денежных мулов для того, чтобы запутать следы и скрыть деньги практически лишают возможности определить окончательный пункт назначения таких денег.

128. Однако из ответов на вопросник стало ясно, что некоторые страны используются как транзитные узлы, т. е. денежные потоки идут в эти страны, но в то же время денежные потоки из этих стран растекаются по другим направлениям, некоторые из них нехарактерны для кибер-атак.

129. Взаимосвязь между пунктом назначения денежных потоков и происхождения преступников была выявлена странами, участвующими в обзоре. Было выдвинуто предположение о том, что преступники переводят деньги обычно друзьям или родным в те страны, откуда они приехали. Было также выявлено, что преступники действуют в странах, находящихся по соседству со стороной их происхождения, а также в развитых странах, даже если они далеко от страны происхождения.

2.4.5 Сложность схем отмывания

130. В отличии от «традиционного» отмывания денег, для совершения которого используется банковская система, кибер-отмывание основано на использовании различных видов операций и поставщиков финансовых услуг, начиная банковскими переводами, внесением/снятием наличных, использованием электронных денег, и заканчивая денежными мулами и услугами по переводу денег. Таким образом, выявление и преследование преступных денежных потоков является очень сложной задачей для правоохранительных органов.

131. Обычно цепочка прерывается на операциях за наличные средства, совершаемую обычно денежными мулами, за которой следует использование традиционной платежной системы. Если соответствующий платежный сервис интегрирован с услугами по он-лайновым платежам, то деньги могут быть обменены на электронные и без промедления

практически анонимно переведены в другое государство.

132. Такие запутанные схемы бросают вызов мощному, но традиционному программному обеспечению для сбора данных в сфере ПОД/ФТ, основанной на поведении клиента, если часть отмывочной цепочки реализуется абсолютно в иной финансовой ситуации.

133. Методы осуществления платежей, лежащие в Интернете, могут также разделять источник, откуда поступили инструкции на проведение операции, от реального места проведения денежного перевода. Это является еще одним препятствием для правоохранительных органов в части выявления и преследования преступных средств.

2.4.6 Иные факторы риска

134. Определенные характеристики кибер-платежных систем могут являться факторами риска при некоторых обстоятельствах. Относительная легкость создания кибер-платежных систем наряду с низкими затратами на развитие такой деятельности порождает сомнения относительно собственника. Скорость, с которой проводятся операции, включая трансграничные переводы лишь способствуют отмывочным схемам. Низкая стоимость таких операций означает и низкие ставки для отмывания и стимулирует преступников на поиск незаконных источников получения прибыли. Легкая конвертация в реальные деньги и наличные может представлять возможность для отмывания денег во многих юрисдикциях.

3. Типологии и избранные примеры

3.1 Потоки «грязных»криминальных денег в Интернете и их отмывание денег

135. Предикатные преступления, совершаемые в Интернете для получения прибыли описаны в предыдущей главе. Зачастую Интернет — это то, место, где отмывание денег начинается. В ходе этого процесса доходы перемещаются от потерпевшего лица преступнику, а от последнего иным лицам, вовлеченным в отмывочную схему. Все это происходит до того, как преступник получает возможность распоряжаться этими доходами.

136. Появление киберпреступников и организованной киберпреступности — это новый вызов для правоохранительных органов и основных игроков. Что касается ИКТ, то либо появляются новые виды преступлений, либо получают развитие новые виды традиционных преступлений. Увеличение уровня проникновения новых технологий в социальную или экономическую жизнь любого государства обычно прямо пропорционально росту уровня киберпреступности. Адаптация правоохранительных техник к изменениям, привносимым новыми технологиями, а также основательные знания о компьютерных платежных системах являются важными факторами для поддержания следственных возможностей в новых условиях.

137. Киберпреступники используют Интернет для отмывания доходов от преступной деятельности независимо от ИКТ (деньги, полученные от уклонения от уплаты налогов могут быть отмыты с использованием электронных денег) или киберпреступлений. Примеры, полученные от стран, указывают на то, что преступные доходы от предикатных киберпреступлений отмываются с использованием различных технологий, начиная с использования традиционных методов (банковские системы или поставщики услуг по переводу денег) и заканчивая сложными Интеренет-переводами, которые зачастую связаны с организованными преступными сетями. Большинство доходов от киберпреступлений обрабатываются следующим образом:

– они обналичиваются в результате большого количества операций, включая привлечение денежных мулов для перевода наличных денежных средств или их эквивалента между платежными системами в Интернете, « обменников», мобильных платежных систем или открытие счета в

кредитном учреждении;

- они используются для покупки высоко ликвидных товаров, предоплаченных карт и т. д. для дальнейшей их перепродажи и получения наличных;
- они также могут быть использованы для совершения через Интернет покупок билетов, проездных документов, предметов обихода и иных товаров для дальнейшего их использования, возврата, перепродажи и получения наличных денежных средств;
- часть из них повторно инвестируются в развитие новых возможностей с тем, чтобы обойти системы безопасности.

138. Раздел, приведенный ниже, отражает наиболее часто используемые методы и инструменты для отмывания доходов от киберпреступлений, которые были выявлены странами, отвечавшими на вопросник. Кроме того, это своего рода попытка указать на уязвимые места мировой финансовой системы, характерные для этого вида отмывания денег. Однако не рассматривайте его как исчерпывающий перечень, поскольку он отражает только информацию, полученную и проанализированную на момент получения ответов для проведения данного исследования. Также он включает ряд дел, выявленных соответствующими подразделениями финансовой разведки или правоохранительными органами, отражая методы, используемые преступниками для маршрутизации преступных денежных потоков в Интернете при помощи как электронных платежных систем, так и традиционных платежных методов.

3.1.1 Услуги по переводу денежных средств

139. Большинство крупных традиционных поставщиков услуг по переводу денежных средств, например, «MoneyGram” и «Western Union” оказывают их он-лайн. Некоторые неофициальные сети по переводу ценностей, а также теневые банковские системы, такие как Хавала также действуют в Интернете. Исследование показало, что использование поставщиков услуг по переводу денежных средств — это обычный метод для отмывания доходов, полученных от киберпреступлений, поскольку 10 из 17 стран, участвовавших в исследовании указали на них в качестве самостоятельного метода или одного из этапов.

140. Поскольку большая часть денежных переводов, осуществляемая через

таких поставщиков, выплачивается наличными, то это дает возможность преступникам ввести в финансовую систему доходы, полученные незаконным путем. При этом абсолютное большинство законных операций с наличными денежными средствами, осуществляемых указанным способом предоставляет великолепную возможность для сокрытия отмывочной деятельности на стадии размещения.

141. Такие финансовые услуги имеют упрощенные обязательства по идентификации клиентов. Упрощенная процедура отправки/получения денежных средств дает возможность использовать их неограниченному кругу лиц: от лиц, отмывающих доходы от киберпреступлений, мулов или «финансовых агентов» до необразованных людей, которым очень тяжело взаимодействовать со слишком «зарегулированным» финансовым учреждением. Зачастую услуги по переводу денежных средств — это часть сложной схемы, в рамках реализации которой проводится хотя бы одна операция с наличными денежными средствами с тем, чтобы разрушить цепочку и скрыть след денег. Также в таких схемах осознанно или нет участвуют денежные мулы.

142. Поставщики услуг по переводу денежных средств оказывают их за небольшую плату и зачастую используют не такие жесткие комплайенс-программы в части ПОД, чем традиционные финансовые учреждения. Обычно такие поставщики заключают договоры с банками с тем, чтобы обеспечить безопасные и защищенные контактные точки со своими клиентами. Зачастую они лишь часть сложной схемы, в рамках реализации которой проводится хотя бы одна операция с наличными денежными средствами с тем, чтобы разрушить цепочку и «скрыть след» денег. Также в таких схемах участвуют денежные мулы.

143. Почти все страны отметили типологию, которая так или иначе совпадает с приведенной ниже:

- на почту пользователя приходит ложное предложение о работе (спам), заявителя вербуют по телефону или иным способом, исключающими личный контакт. Зачастую работа связана с финансовыми вопросами или работой на дому;
- доходы от киберпреступлений переводятся на счет денежного мула, который должен снять наличные денежные средства и затем направить их определенному получателю с использованием денежного перевода. Сумма

обычно ниже порогового значения с тем, чтобы избежать ее последующего отслеживания;

– такие денежные переводы используются для того, чтобы перевести наличные их конечному получателю.

144. Некоторые приведенные примеры, где были многократно использованы услуги лиц, переводящих деньги, вызывают озабоченность относительно сговора или проникновения организованной преступности в эту сферу деятельности с тем, чтобы организовывать и способствовать маршрутизации доходов[131].

145. Примеры указывают на то, что:

– поставщики услуг по переводу денег используются для отмывания доходов, полученных от киберпреступлений;

– они используются в отмывочных схемах совместно с денежными мулами

– они являются наиболее урегулированными посредниками, вовлеченными в отмывание денег от киберпреступлений и, таким образом, обладают всеми возможностями для передачи ценной информации в ПФР или правоохранительные органы для предотвращения киберпреступлений.

Пример 1. Кража информации о кредитной карте и отмывание денег

Были получены жалобы от Компании, выпускающей кредитные карты, относительно незаконного использования сотен кредитных карт.

Пунктом взлома оказался устройство поддержки пункта продаж продавца. Проверка системы выявила наличие клавиатурного шпиона. Была отслежена вся цепочка IP-адресов, удаленных серверов и адресов электронной почты. Она вывела на преступника в Румынии и клоны взломанных карточек, которые были использованы в США.

В Румынии по ходатайству прокурора судья вынес решение о безотлагательных мерах. В результате воздействия на данные было выявлено, что преступник собирал данные о кредитных картах, используя клавиатурного шпиона и коллектор адресов электронной почты. Клавиатурный шпион был усовершенствованной версией приложения, загружаемого бесплатно из

131 Отмывание денег через лиц, оказывающих услуги по переводу денег и обмену валют (МАНИВЭЛ, 2010 г.) см. http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/RepTyp_MSBs_en.pdf

Интернета. Кредитные карты были отобраны, а затем проданы по 1000 долларов США за 100 штук определенному лицу, находившемуся в США. Были найдены сообщения, отправленные по электронной почте, а также зашифрованные сообщения, направленные при помощи таких программ как «Messenger", ICQ и Skype.

Продавец в Румынии дал указание перевести деньги на различные имена в Румынию и Болгарию, используя «Western Union". В соответствии с инструкциями имя отправителя было ненастоящее для того, чтобы его не отследили. Также инструкции были даны сообщникам в США отправить деньги в он-лайновую платежную компанию, которая должна была произвести обмен и затем, получившуюся сумму перевести в «Western Union" в Болгарии.

В ходе производства обыска в доме были найдены компьютеры, которые использовались румынскими преступниками, документы из "Western Union" и наличные денежные средства. Было изъято 120,000 долларов США.

При проверке компьютера были обнаружены: использовавшийся клавиатурный шпион, базы данных с информацией о кредитных картах.

Румынским преступникам были предъявлены обвинения в незаконном доступе к компьютерной системе, незаконном воздействии на компьютерные связи, мошеннических действиях с кредитными картами и отмывании денег. Все при отягчающих обстоятельствах.

Источник: Румыния

Пример 2: СПО привело к аресту киберпреступников

ПФР получило два СПО от коммерческого банка относительно нескольких фактов снятия наличных денежных средств на небольшую сумму (500-1000 евро или суммы в иностранной валюте им равные), осуществленные физическим лицом «А» со своего банковского счета. До этого на этот счет были переведены средства, где в качестве целей перевода было указано, что это «подарок» или «денежное содержание». Переводы были осуществлены четырьмя разными лицами, находившихся в иностранных государствах.
За движением средств по счету лица «А» было установлено наблюдение, но

банк не выявил никаких иных видов операций.
В ходе проведения анализа ПФР запросило информацию о плательщиках из иностранных государств и получило ответ о том, что один из них был известен своими связями с преступными группами, занимающимися совершением преступлений с использованием компьютерных технологий. Главарем преступной группы значился мужчина, который проходил по базам данным полиции как «Самир». Он и его сообщники разыскивались правоохранительными органами. В результате совместных действий специальной группы были арестованы восемь человек, вовлеченных в совершение компьютерных преступлений.
В отношении арестованных были установлены следующие факты:
«Самир» проживал некоторое время в Италии, где, вступив в сговор с гражданином этой страны, он открыл на законных основаниях небольшую фирму по быстрому переводу денежных средств. Получив лицензию для своей компании, он также получил имя пользователя и пароль для отслеживания переводов (контрольные номера денежных переводов). Используя эти возможности, он получил следующие данные и информацию: имена плательщиков, их идентификационные данные, переводимые суммы, пункты отправки и назначения денег. Эти данные были использованы для поддели документов, удостоверяющих личность, и значительные денежные средства были сняты в пунктах назначения.
Кроме того, они скопировали операционные системы после присвоения лицензии и сертификата (на основании цифровой подписи), итоговая программа была установлена на два ноутбука с одинаковой конфигурацией (номер, модель, технические характеристики). Ноутбуки были проданы каждый за 100,000 евро, т. к. они давали возможность покупателям, как законным держателям лицензии, получить доступ к одной и той же информации о лицах, переводящих денежные средства. Дело передано в суд.

Источник: Румыния

Пример 3. Банковские переводы, подставные лица и денежные мулы для отмывания денег

ПФР анализировало обычное дело о фишинге/фарминге: преступник на ранней стадии незаконно получил доступ к банковскому счету потерпевшего,

используя дистанционное банковское обслуживание.
Для того, чтобы скрыть свою личность они связались с различными людьми, предлагая деньги за пользование их личными счетами для совершения операций.
В большинстве случаев подставные лица открывали новые счета специально для этих целей, и когда приходил перевод извне, то объявляли его своим.
Денежные средства затем переводились дальше на другие счета или обналичивались. Такие посредники зачастую используют услуги по переводу денежных средств.

Источник: Словакия

3.1.2 Электронные денежные переводы/ присвоение или открытие банковского счета

146. Не смотря на то, что новые технологии (например, он-лайновые платежные системы или электронные деньги) играют все возрастающую роль в экономической и социальной жизни общества киберпреступники все еще зависят от банковской и финансовой системы.

147. Электронные переводы — эффективный инструмент для лиц, отмывающих деньги, обычно используемый в начале отмывочного процесса, т. к. очень часто само преступление, совершаемое при помощи компьютерных технологий, заключается в извлечении денежных средств с банковского счета потерпевшего с использованием мошеннических методов. После этого этапа деньги переводятся на счет нанятого мула, с которого они либо снимаются, либо переводятся далее. Если денежные средства переводятся в другую юрисдикцию, то сумма такого перевода ниже порогового значения, чтобы не давать никаких разъяснений относительно их происхождения.

148. Сообщается о делах, в которых использовалась целая цепочка операций для того, чтобы скрыть незаконное происхождение средств. В некоторых случаях преступники пользовались несколькими он-лайновыми банковскими счетами. Иногда лица, занимающиеся отмыванием при помощи компьютерных технологий, проводили целый ряд бессмысленных операций по различным банковским счетам, в результате которых несколько раз снимались деньги. В таких случаях есть основания полагать, что все

операции, совершенные он-лайн, были проведены для того, чтобы скрыть тех, кто стоит за этими операциями, в то время как снятие денежных средств поручалось не очень важным лицам.

149. В других случаях преступник присваивал банковский счет, который мог быть использован для большей части операций как счет мула. Владелец счета может ничего и не подозревать.

150. Примеры указывают на то, что:

– в большинстве случаев главная цель киберпреступников — это банковская система. При этом она используется для отмывания денег;

– киберпреступники все еще зависимы от банковской системы. Усиление культуры ПОД в части предотвращения кибер-атак и отмывания, может также привести к снижению уровня преступности в этой сфере;

– электронные переводы используются совместно с другими методами.

Пример 4. Фишинг и отмывание денег с использованием банковского счета

Преступная группа собрала данные о пользователях и их пароли, используя вредоносные программы типа клавиатурного шпиона. Также широко были использованы бот-сети. При помощи украденных данных деньги были извлечены с банковского счет потерпевшего. После этого был осуществлен ряд банковских переводов; в конце цепочки преступники сняли со счетов денежные средства. В некоторых случаях деньги были переведены в электронные валюты и обратно.

Источник: Эстония

Пример 5. Хищение с банковских счетов

Две компании, незарегистрированные на территории государства, “Invest1” и “Invest2” переводили деньги небольшими суммами (100-200 долларов США) из страны Z на счет открытый в «Банке U» не-резидентом “Y”. «Помощь родственникам» была указана в качестве целей платежа.

После успешного перевода денежных средств со счетов компаний “Invest1” и “Invest2” были совершены переводы более крупных денежных сумм (200-300

тысяч). Эти средства были переведены на тот же банковский счет. Когда сумма на счете достигла довольно крупного размера клиент «Y” попытался снять деньги.

«Банк U” отслеживал все эти операции и попросил клиента “Y” предоставить дополнительные документы с тем, чтобы уточнить цель денежных переводов. Банк приостановил все текущие операции по счету на 2 дня. Также «Банк U” направил сообщение в ПФР.

Основываясь на результатах анализа ПФР приняло решение продлить приостановление операций по счету еще на 5 дней. В ходе проведения анализа было выявлено, что денежные средства были незаконно переведены со счетов компаний “Invest1” и “Invest2” и что имел место несанкционированный доступ к счетам этих компаний через их IP-адреса (место нахождения — страна «Z”). Было установлено, что у лица «Y” было несколько паспортов. Согласно полученной информации из банка, денежные переводы были осуществлены незаконно, и банк плательщика уже обратился с просьбой вернуть деньги. В течение данного периода времени «Банком U” было получено сообщение по электронной почте от неизвестного лица «N”, к которому прилагался договор, подтверждающий законность денежных переводов (договор финансовой помощи компаний “Invest1” и “Invest2”, оказываемой лицу «Y”). После анализа контракта, направленного «N” были установлены имя и фамилия отправителя, а также ник отправителя сообщения. Был установлен IP-адрес отправителя сообщения. Также при помощи социальных сетей было установлено, что «N” является другом сотрудника «Банка U”, было найдено его резюме и т. д. Кроме того, в ходе обмена информацией между всеми заинтересованными сторонами было установлено, что “N” подозревается в совершении мошеннических операций.

Проведя дальнейшее расследование ПФР получило информацию о том, что компьютеры компаний “Invest1” и “Invest2” были заражены вредоносной программой «Троян Спам», установившей необходимое программное обеспечение. Этот вирус был запущен для получения доступа к программному обеспечению компаний и контроля их он-лайновых счетов.

Источник: Украина

Пример 6: Интернет-мошенничество и отмывание денег через подставных лиц.

Данный пример описывает случай кибер-мошенничества и последующего отмывания денег, совершенные организованной группой, которая использовала Интернет для осуществления преступной деятельности и открытия банковских счетов в ряде стран ЕС.

Преступная группа создавала сайты для Интернет-продаж или использовала уже существующие (например, «E-Bay"), открывала личные банковские счета в финансовых учреждениях государств-членов ЕС, при условии предоставления последними услуг Интернет-банкинга, смс-оповещения и выпуска дебетовый карточек. Они продавали обычную для Интернета электронику: iPod'ы, мобильные телефоны, навигационные системы, подержанные автомобили, тракторы и фургоны. Подозрения возникли из-за низкой цены и ведению дел исключительно по электронной почте и использования предоплаченных сим-карт. Они также направляли поддельное банковское подтверждение. Преступники просили осуществить платеж на счет, открытый в другой стране ЕС. Эти счета были открыты в странах подставными лицами с низким социальным статусом.

После того, как платеж был осуществлен деньги снимались подставным лицом или без промедления переводились на счет другого члена преступной группы. После совершения нескольких операций счет закрывался, а подставное лицо, использовавшееся для открытия счета, менялось на другое.

Источник: Словакия

3.1.3 Снятие наличных со счета

151. Все большая прозрачность электронных переводов и услуг по переводу денежных средств являются тем фактором, который заставляет преступников рассматривать наличные в качестве ключевого элемента для перемещения активов и сокрытия преступных следов. В соответствии с ответами стран, полученными на вопросник, наличные денежные средства остаются частью цепочки отмывания доходов от киберпреступлений и их можно выявить на любой из трех стадий отмывания денег.

152. В некоторых случаях доходы от киберпреступлений (например, как в случае мошенничества с карточками) быстро снимались через банкоматы, суммы были невелики. С этого момента начинается процесс отмывания денег.

153. Похожая схема применяется в отношении «фишинговых переводов», которые осуществляются для аккумулирования на банковских счетах финансовых агентов. Агент снимает наличные за вычетом своей комиссии. Затем он покупает безымянные приходные ордеры Интернет-платежных систем на небольшую сумму (не более 500 евро), используя различные возможности (станции заправок, киоски/терминалы и т. д.) (Германия).

154. Другая выявленная типология указывает на то, что обналичивание происходит на стадии расслоения, когда вслед за электронными переводами идет снятие денежных средств, а оставшаяся часть отмывочной схемы продолжает реализоваться иными способами, например, при помощи поставщиков услуг перевода денежных средств обмен валют и т. д.

155. В других случаях деньги обналичивались после ряда операций, включая и те, когда использовались денежные мулы для перевода наличных денежных средств или их эквивалента между платежными системами в Интернете, «обменниками», мобильными платежными системами или открытие счетов в кредитных учреждениях (Российская Федерация).

156. Однако, вполне очевидно для киберпреступников, что наличные имеют ряд недостатков, например, необходимость прямого контакта между продавцами, крупные суммы в мелких купюрах или необходимость физического перемещения банкнот курьером при особых обстоятельствах через границу, где может осуществляться проверка таможенными органами и органами полиции. Еще одно ограничение связано с расстоянием между всеми участниками операций. Но самым важным снижающим риск фактором является то, что они не могут быть украдены киберпреступниками в виде банкнот. Кибер-атаки по определению направлены на более уязвимые виды ценностей, например, банковские счета, счета IPS, е-валюты и т. д. Киберпреступники не занимаются карманными кражами и не воруют бумажные деньги потому, что у них несколько иная сфера деятельности. Однако они используют наличные денежные средства, чтобы скрыть их след. Наличные от киберпреступлений представлены небольшими суммами

и используются в схемах отмывания денег в противовес смерфингу. С банковским счетов снимаются небольшие суммы денег или переводятся посредством соответствующих услуг с тем, чтобы быть перенаправленными на аккумулирующие счета.

157. Примеры указывают на то, что:

- операции с наличными денежными средствами — это обязательная стадия в схеме отмывания денег;
- очень часто используются банкоматы для того, чтобы избежать общения с сотрудниками банка;
- основная задача использования наличных денежных средств в отмывочных схемах — это «замести» следы.

Пример 7. Международные фишинговые атаки с использованием банковских счетов и обналичивания

Прибегнув к фишинговым атакам и иным способам похищения данных о кредитных картах, преступники переводили небольшие суммы денег со взломанных счетов на свои личные счета или счета компаний, подконтрольных им или тех компаний, от имени которых они были уполномочены совершать финансовые операции в другой стране. После этого преступники быстро снимали деньги через банкоматы в других юрисдикциях, а не в той, откуда переводились украденные деньги. Он мог совершить и ряд других операций для того, чтобы не удалось отследить движение наличных денежных средств.

Источник: Болгария

Пример 8. Организованная преступная группа, специализировавшаяся на мошенничестве с использованием систем денежных переводов, фишинге, незаконном использовании информации о кредитных картах и их подделке

Анализ полицейской информации привел к выявлению организованной преступной группы в большом городе, специализировавшейся на манипулировании с банкоматами и мошенничестве. Первичная информация была подтверждена дополнительно информацией, полученной от атташе ФБР относительно мошеннических переводов, совершенных при помощи электронных платежных систем.

Как следствие крупнейший банк и его клиенты стали жертвами фишинг-атаки, заключавшейся в снятии наличных денежных средств через банкоматы в двух крупных городах. При этом анализ информации, полученной полицией, и специальный полицейский осмотр позволил выявить скимиинг- устройство, установленное на банкомат в третьем по величине городе. Полученная информация позволила сделать вывод о том, что преступники принадлежали различным преступным группам, но в некоторых случаях работали сообща.

В ходе расследования было установлено, что преступная деятельность групп заключалась в фишинге (были выявлены цели и используемый инструментарий), мошенничестве с использованием систем денежных переводов, незаконном использовании информации о кредитных картах и их подделке, производстве скимминг-устройстви их использовании для получения личных идентификационных данных и паролей.

Источник: Румыния

3.1.4 Системы Интернет-платежей

158. Выражение «системы Интернет-платежей» (IPS) используется для описания переводов в Интернете, подобных банковским (платежные сервисы, основанные на привязке к банковскому счету; Интернет используются только для передачи распоряжения о переводе денежных средств от плательщика получателю), а также иных платежных услуг, предоставляемых небанковскими платежными институтами, действующими исключительно в Интернете и не связанными с банковским счетом напрямую).

159. В случае если IPS привязана к банковскому счету, то перевод является такой же банковской операцией. Единственной особенностью является то, что клиент находится перед своим компьютером, а не в офисе банка.

160. IPS, не привязанная к банковскому счету (например, «PayPal”), предлагает своим клиентам широкий спектр услуг по переводу денежных средств, включая трансграничные, он-лайн магазины, участие в он-лайн аукционах и т. д. Такие IPS позволяют клиентам иметь счета. В этом случае они могут объединить средства клиентов на едином банковском счете, открытом на имя поставщика услуг. В этом случае банк, в котором открыт

счет IPS, может не иметь прямых взаимоотношений с клиентом платежной системы. В этом случае меры по НПК в отношении таких лиц не могут быть реализованы.

161. Полученные ответы указывают на то, что роль и масштабы деятельности IPS возрастают . Таким образом, встает вопрос и о повышенных рисках их использования для ОД/ФТ и определённой уязвимости в части ОД на стадиях размещения и расслоения. Очень часто конвертация с использованием электронных платежных систем является важной составляющей частью на стадии расслоения. Такие услуги позволяют клиентам отправлять и получать деньги на виртуальные счета, доступ к которым обеспечивается через Интернет. Для таких услуг характерна высокая степень анонимности. Кроме того, растет их объем для перевода средств от лица другому лицу.

162. IPS — это очень дешевый, анонимный и быстрый способ перевести деньги за рубеж. К ним не применяются такие же требования в части ПОД/ФТ и надзор как к кредитным и финансовым учреждениям, что увеличивает риск их использования. для отмывания денег. Даже если IPS предлагает финансовые услуги своим клиентам, то не все поставщики подпадают под регулирование в целях ПОД/ФТ.

163. Одна из систем отмывания денег с использованием Интернет-платежей сводится к тому, что доходы, полученные от различных киберпреступлений переводятся на банковский счет финансового агента или денежного мула, после чего деньги снимаются. После чего могут быть куплены приходные ордеры системы Интернет-платежей. При этом продавец не обязан идентифицировать покупателя. В этом случае реальные деньги переводятся в виртуальные. Финансовый агент отправляет номер ордера по электронной почте другому лицу вместе с инструкциями. После чего ПИН может использован для оплаты в Интернете товаров и услуг, ставок при игре в покер, казино и иных развлекательных сайтах. Несколько ордеров на мелкие суммы могут быть использованы вместе. Также возможна конвертация в иные электронные валюты с использованием различных обменников в Интернете (Германия).

164. Иногда преступные доходы размещаются на счетах определенных лиц, а затем используются для покупки различных товаров и услуг на Интернет-аукционах. И хотя платежные системы гарантируют безопасность, операции

все равно представляют риск для совершения мошенничества из-за обезличенной природы Интернет-торговли и из-за слабого регулирования в той ил иной юрисдикции (Польша).

165. Развитие IPS в последнее время привело к тому, что они стали взаимодействовать с иными новыми и традиционными платежными сервисами. Деньги теперь можно переводить, используя разнообразные платежные методы, включая наличные, денежные переводы, электронные деньги, электронные переводы или кредитные карты. Более того, поставщики IPS стали выпускать предоплаченные карты для своих клиентов, таким образом давая им возможность снимать наличные денежные средства по всему миру при помощи банкоматов[132].

166. В зависимости от правовых требований того государства, где зарегистрирована IPS, они могут регулироваться как поставщики услуг по переводу денег и, таким образом, должны иметь все процедуры и правила в части ПОД/ФТ, хранить информацию об операциях и направлять сообщения о подозрительной финансовой деятельности.

167. Примеры указывают на то, что:
- счета IPS могут быть использованы для совершения мошенничества и отмывания денег точно также как используются банковские счета;
- учитывая, что счета IPS схожи с банковскими счетами, то превентивные меры, предпринимаемые банками, могут иметь значение и для IPS;
- использование небольших сумм — характерная черта для мошенничества и отмывания денег, совершаемых при помощи данной технологии.

Пример 9. Кража персональных данных и отмывание денег

Счет «PayPal" был открыт в филиале иностранного банка. Со счета были осуществлены денежные переводы на счета различных получателей (в соответствии с полученными распоряжениями).

В основе преступной деятельности лежало изменение серединных (т. е. с 12-ой по 17-ую) цифр счета, контрольных сумм (контрольных цифр), имен получателей их адресов в то время как остальные девять цифр оставались и банковский код (цифры с 3-ей по 11-ую) оставались неизменными.

132 «Отмывание денег при помощи новых платежных методов» - исследование ФАТФ, октябрь 2010 г.

Осуществлялось всего несколько операций (максимум 10), сумма не превышала 3000 злотых (т. е. 1000 долларов США).

По прошествии нескольких дней полученные средства переводились на счета организаторов или обналичивались.

Было установлено, что средства, полученные с американских счетов “PayPal», принадлежали другим лицам. Украв их персональные данные, преступники открыли счета на «PayPal” от их имени. Позже от имени потерпевших было отправлено заявление об открытии кредитной линии. Материалы были переданы в прокуратуру.

В результате банк применил систему автоматической верификации счетов получателей в отношении входящих переводов. Эти превентивные меры заставили преступников изменить образ действия. Преступники стали открывать в различных банках счета с доступом через Интернет (рекордсменом считается лицо, которое открыло один основной счет и 261 дополнительный). На эти счета поступали безналичные переводы со счетов «PayPal”. Аккумулированные средства переводились на счета организаторов, с которых они впоследствии и снимались.

Полученные материалы были направлены в прокуратуру, 48 счетов, принадлежащих одному из преступников, было заблокировано. Полиция установила, что этот преступный бизнес был организован и контролировался лицом, разбиравшемся в банковской и IT-системах. Остальные члены преступной группы жили в том же районе и были известны местной полиции. Что касается технической стороны дела, то для кражи персональных данных были использованы бот-сети.

Источник: Польша

Пример 10. Использование цифровых товаров, полученных обманным путем, который в конечном итоге позволил преступникам получить напрямую законные средства

Потерпевшие: владельцы кредитных карт, компания, занимающаяся е-

платежами, и VoIP-компания.

Схема: мошенники владели несколькими компаниями, предлагавшими телефонные номера премиум-класса. Они создали большое количество узлов по всему миру, большую часть в странах, где слабое регулирование, и стали звонить на эти узлы с компьютеров-зомби, используя счета VoIP, пополняемые при помощи поддельных карт, используемых для е-платежных систем.

Комментарии: звонки генерировали поступления для реальных поставщиков номеров премиум-класса. Эти компании могли утверждать на законных основаниях, что у них не было возможности проверить эти звонки до конечного пункта на предмет того, являются ли они мошенническими или нет. Кроме того, если звонки поступали со всего света, то очень сложно найти какие-либо общие черты.

Е-платежная система отразила операции с поставщиками VoIP, но не было возможности установить являются ли они мошенническими или нет за пределами ее обычной проверки на противодействие мошенничеству. VoIP-компания видела только узлы, но не конечные пункты. Если система узлов построена очень осторожно и продуманно, то риск выявить мошенников практически равен нулю.

Что касается ОД/ФТ, то у нас имеется в наличии доходы от преступления, кража данных о кредитных картах, которые были введены в законную экономику страны, без прохождения финансовой системы и были предоставлены для контроля в части противодействия отмыванию денег.

3.1.5 Денежные мулы

168. Денежные мулы являются важным элементом большого числа преступных операций в Интернете, на что указало значительная часть ответов на вопросник. Согласно полученным данным «мул» - это лицо, которое нанимают через Интернет с тем, чтобы оно открыло банковский счет, в отношении которого он/она выступали бы посредником для получения наличных и средств, полученных в результате кибер-пиратства (фишинг, клавиатурные шпионы и мошенничество). Затем мул переводит оставшиеся деньги на другие счета или за границу при помощи безналичных переводов, удерживая комиссию. Мулы получают на свои

банковские счета средства, например, со взломанных он-лайновых банковских счетов и могут их перевести на другие счета или обналичить их, используя иные средства, такие как системы по переводу денег или электронные деньги. Мул удерживают комиссию, являющейся частью операции.

169. Очень часто мул и потерпевший, чей банковский счет взламывается, живут недалеко друг от друг. За проведение каждой операции мул удерживает комиссию в размере от 5% до 10% от общей суммы отмываемых средств (что тоже помогает преступникам «размывать» связи) и переводит оставшиеся денежные средства через он-лайновые платежные системы. Однако некоторые примеры указывают на то, что размер комиссии увеличился — от 30% до 50% - возможно из-за повышения вероятности быть пойманным в результате эффективного взаимодействия правоохранительных органов или, как указали некоторые, из-за трудности в вербовке достаточного количества мулов.

170. Мула обычно описывают как доверчивое лицо, которого ввели в заблуждение профессиональные контакты со своим «работодателем» и который полагает, что он/она работают в компании, не занимающейся чем-либо противозаконным. Но этот наивный образ все чаще ставится под сомнение и представителями правоохранительных органов, и сотрудниками банков. т. к. есть достаточное количество примеров, когда мул знал о том, что занимается противоправной деятельностью.

171. Существует несколько сценариев того как счета мулов используются для маршрутизации доходов от преступлений. Владелец счета может быть полностью осведомлен об истинной природе средств и настоящей цели предпринимаемых действий, а может быть и нет. В случае если лицо не знало, то с мулом обычно связываются с сайта, где предлагаются вакансии «финансового менеджера» или «работа на дому». Рассылка спам-сообщений также используется для привлечения потенциальных мулов.

172. После вербовки мула деньги переводятся на его/ее счет с последующими различными поручениями. Им может быть поручено перевести деньги на счет, находящийся за рубежом, перевести деньги на временный счет в том же банке на выходные, получить наличные в банкомате, используя карточку

в течение часа, и перевести деньги в конечный пункт[133].

173. Количество мулов увеличивается пропорционально объемам Интернет-мошенничества. Если «работодатель» расценивает работу мула не как «специалиста по отмыванию денег», то он воспользуется его/ее услугами несколько раз и прибыль последнего не превысит 3,000 долларов США.

174. Однако некоторые примеры указывают на то, что операции денежных мулов могут отличаться сложностью в части структуры, когда задействованы несколько уровней мулов и реализации ими своих обязательств. Также в отличие от «одноразовых» мулов, т. е. лиц искренне верящих в то, что они занимаются надомной работой, появился и растет класс профессиональных мулов, которые специально развивают это направление деятельности.

175. Примеры и полученная информация указывают на то, что:
- деятельность денежных мулов является частью более сложных схем отмывания денег; связь с отмыванием денег от киберпреступлений очень невелика;
- их деятельность может быть выявлена и связана для выявления транснациональных преступных операций, а также бот-сетей и серверов, используемых в преступных целях;
- их деятельность имеет характерные черты, что делает их уязвимыми для идентификации сотрудниками банков в результате тщательной проверки, т. к. суммы операций малы;
- вербовка денежных мулов идет во многих странах, а не только в развивающихся как это было раньше. Эта тенденция объясняется различными факторами (например, убеждение, что операция, проводимая лицом/денежным мулом из развитой страны привлечет меньше внимания, мировой финансовый кризис, отсутствие достаточного количества денежных мулов);
- международные финансовые расследования, проводимые параллельно с расследованиями в сфере высоких технологий с использованием компьютерной криминалистики являются наиболее эффективным способом для достижения целей.

Пример 11. Мошенничество при помощи Автоматизированной клиринговой палаты (АКП) и отмывание денег с помощью бот-сетей и

133 Венгрия

денежных мулов

В марте 2009 г. в США были совершены проникновения в два школьные компьютерные системы округа, которые на первый взгляд невозможно было увязать друг с другом (система казначейства округа и система колледжа округа). Был нанесен ущерб более, чем на 790 долларов США, о чем и было отправлено сообщение в Центр приема сообщений об Интернет-преступлениях (IC3).
В первом случае деньги были переведены семи лицам, в отношении которых подтвердилась информация о том, что они являются денежными мулами, которые были наняты через сайты, публикующие информацию о вакансиях, которые заслуживают доверия. Дальнейший анализ, проведенный IC3, позволил выявить порядка 200 жалоб в отношении этих мулов.
Дополнительный анализ, проведенный Американским национальным альянсом по компьютерной криминалистике и подготовке (NCFTA), указал на то, что IP-адреса, с которых был осуществлен доступ к компьютерам потерпевших были частью бот-сети «Лигат». Это позволило установить связь между этими делами, а также иными проникновениями, когда использовались похищенные персональные данные жертв для осуществления операций через АКП. Дальнейший анализ IP-адресов, входящих в бот-сеть «Лигат», выявил связи с фармацевтическими спам-оперциями для того, чтобы заразить компьютер и установить вредоносное программное обеспечение, а также с подпольными карточными форумами и «свалками» кредитных карт .

Следующие методы были использованы в этом деле о мошенничестве через АКП:
- цель: мелкий бизнес, школы, агентства городов, округов и штатов;
- компьютеры были заражены вредоносными программами через полученный спам, направленный через бот-сеть «Лигат», после чего они также становились частью этой бот-сети;
- украденные персональные данные были использованы для осуществления операций на АКП;
- деньги переводились на счет мулов;
- мулам предлагалась работа после того, как они размещали свои резюме на специальных сайтах, заслуживающих доверия,
- подставные компании предлагали работу на дому;
- переводы через АКП осуществлялись семи из девяти мулов на сумму ниже 10,000 долларов США;

- затем мулы осуществляли безналичные переводы в адрес двух или трех лиц; каждый перевод был на сумму ниже 3,000 долларов США. Переводы осуществлялись раз за разом в одни и те же страны (например, Чешскую Республику, Молдову, Россию, Таджикистан и Украину);
- у мулов был доступ к «системе управления поручениями»;
- «менеджер по поручениям» указывал мулу, какое учреждение использовать для перевода, какой банковский счет открывать, а также имена и пункты, куда переводить деньги.

Источник: государственный сектор

Пример 12. Банковское мошенничество и отмывание денег при помощи бот-сетей, мулов и VIOP

Банк предлагал своим клиентам дистанционное банковское обслуживание с тем, чтобы последние могли осуществлять операции со своими счетами с домашнего компьютера. У некоторых клиентов счета были взломаны. Денежные средства с их счетов были переведены на счета в других странах. Компьютеры жертв были заражены вредоносными программами, что позволило украсть реквизиты счетов и иные персональные данные (возможно, как часть бот-сети). Международное расследование, проводимое представителями всех заинтересованных государств, позволило выявить большую и сложную систему связей денежных мулов, которая охватывала по меньшей мере порядка десяти стран и огромные суммы похищенных средств.

Мулов вербовали на разных языках при помощи рассылки сообщений, предлагавших легкий способ заработать деньги. С теми, кто «клюнул» связывались по телефону или посредством Протокола передачи голоса через Интернет (VOIP), который очень сложно отследить и за использование которого оплата осуществлялась при помощи карточек-клонов или украденных дебетовых карт. Мулам «первого уровня» давалось указание открыть банковский счет. По прошествии нескольких дней на их счета поступали деньги. Затем с ними снова связывались и отдавали распоряжения перевести их денежные средства в страны Восточной Европы. В Бельгии такое явление считается отмыванием денег.

Мулы «второго уровня» (если брать этот пример, то находившиеся в

большинстве своем в странах Восточной Европы) снимали их со счета и отдавали наличные третьим лицам - «сборщикам денег». Мулы обоих уровней ничего не знали об источнике происхождения этих денег. Сборщика денег информировали по электронной почте о сумме, которая должна быть получена, коде операции, осуществленной поставщиком услуг по переводу денег. Также сообщались имена и адреса мулов первого и второго уровня. Сборщик денег передавал деньги четвертому лицу, е-банкиру, который переводил их в электронные деньги. В расследуемом деле через сборщика денег прошло 150,000 долларов США два месяца.

Все эти процессы были хорошо организованы и доведены до автоматизма. Это дает основание полагать, что к организации приложил руку менеджер, имевший широкий доступ к данным или лицо, подобное ему.

Комментарии:

- дело связано с воздействием на компьютерные данные и системы, незаконным доступом, подделкой и мошенничеством и организованной преступностью;
- факт, что заведомо, как казалось, несвязанные между собой дела о мошенничестве при помощи он-лайновых операций, оказались на самом деле связанными. Более того, они оказались частью сложной транснациональной организованной преступной деятельности, которую удалось выявить, когда несколько прокуроров и сотрудники правоохранительных органов, проводивших свои расследования, связались со своими коллегами за рубежом. В этой связи деятельность совместных следственных групп (например, в рамках Евроюста) может быть очень полезна;
- в Бельгии состоялся обмен контактами и информацией между органами прокуратуры, правоохранительными органами, подразделением финансовой разведки, поставщиками услуг по переводу денег, банками и Европолом. Информация была собрана и проанализирована командой следователей, специализирующихся на расследовании финансовых преступлений и преступлений в сфере высоких технологий;
- расследование деятельности мулов считается одним из перспективных направлений для раскрытия всей преступной деятельности;
- отслеживание денежные следов, т. е. проведение финансовых расследований очень важная задача наряду с проведением расследований в сфере высоких технологий и компьютерной криминалистикой. Сочетание обоих приносит успех;

- не смотря на то, что VOIP очень тяжело отследить, такие компании как «SKYPE" могут располагать сведениями о фиксированных телефонных линиях или адресах, на который высылается счет на оплату, который, в свою очередь связан со счетом VOIP;
- кроме того, должно быть проведено расследование в отношении серверов, на которых создавались криминальные сайты. В этом конкретном примере в Бельгии проводилось расследование в отношении сервера, который направлял преступников на другие сайты, на которых предлагались средства для взлома компьютерных систем отдельных банков и список возможных мулов, ответивших на спам.

Источник: Бельгия

3.1.6 Международные переводы

176. Международные переводы могут рассматриваться как разновидность банковских переводов. Но с развитием новых платежных технологий международные переводы можно осуществлять при помощи банковского счета, а также электронных денег, IPS равно как и при помощи традиционных поставщиков услуг по переводу денежных средств. Несмотря на используемый платежный метод международные переводы имеют свои особенности, которые делают их уязвимыми для отмывания денег. Данная разновидность переводов была выделена странами, участвующими в исследовании, в отдельную категорию.

177. Одной из ключевых проблем в отношении международных переводов остается трудность для правоохранительных органов вернуть преступные активы, т. к. встает юрисдикционный вопрос.

178. Международная «отправка» денег обычно имеет место на стадии расслоения и следует после того, как, например, были использованы денежные мулы[134].

179. Что касается международных переводов, то в предварительных договоренностях участвуют несколько стран. В результате очень тяжело вычислить именно того преступника, который и «ведет игру», который разработал схему и координирует денежные переводы[135].

134 Венгрия
135 Эстония

180. Кроме того, очень сложно отследить те денежные средства, которые уже ушли за границу. Особую озабоченность вызывают ряд юрисдикций в части мошеннических платежей с последующими переводом денежных средств на счета компаний, зарегистрированных в офшорных зонах[136].

Пример 13.

ПФР проводило расследование в отношении мошеннической схемы, которая была придумана неизвестным лицом, занимавшимся присвоением денежных средств при помощи компьютеров. Присвоенные средства были переведены в пользу определенных физических лиц. Доступные средства на счете Компании X (Страна W) были переведены неизвестным лицом, получившим доступ к он-лайновым банковским счетам пострадавшей компании при помощи логина, путем международного перевода на счета физических лиц в украинском банке.

Со счета Компании X (Страна W) были осуществлены международные платежи в пользу физических лиц в Украине. Несанкционированные международные переводы были осуществлены незизвестным лицом, получившим доступ к он-лайновым банковским счетам пострадавшей компании при помощи логина. Общая сумма операций составила 577,000 долларов США.

Банк плательщика в Стране W выявил несанкционированные переводы и проинформировал об этом украинский банк. Средства в размере 284,000 долларов США были успешно возвращены. Более того, имели место и еще два несанкционированных перевода со счета Компании Z, каждый на сумму 98,000 долларов США, совершенные в пользу тех же физических лиц в Украине.

ПФР выявило признаки мошеннических операций в ходе финансового анализа, осуществленного с использованием информации, полученной от зарубежных коллег.

Источник: Украина

136 Словакия

3.1.7 Электронные деньги

181. Электронные или цифровые валюты относятся к системам обмена ценностей, которые осуществляются электронно. Электронная валюта это зашифрованный код, представляющий собой некую стоимость, привязанный к определенному счету, т. е. как и обычные бумажные банкноты, обладающие определенными характерными чертами, позволяющими перевести их в символьную ценность. Некоторые говорят, что электронные деньги — это реальные деньги, такие же, как и банкноты, но степень их ликвидности ниже, чем у наличных. Электронная валюта может быть использована только в определенных обстоятельствах (например, нужны доступные технические средства), в то время как наличные могут быть использованы в любых операциях.

182. Международные услуги по переводу электронных денег доступны во всем мире и дают возможность перевести средства из одной страны в другую страны без промедления, иногда не оставляя следов. Используя электронные валюты физические и юридические лица могут отправлять и получать денежные средства в режиме реального времени. Платежи могут осуществляться круглосуточной без выходных очень быстро, анонимно, за низкую плату и не покидая дом.

183. В настоящее время появляются поставщики электронных денег, которые стараются привязать свои «валюты» к различным драгоценным металлам или к другой категории, которая не очень явно увязывает их с драгоценными металлами. Обе категории стараются придать своему бизнесу образ законного и заручиться поддержкой через Международную ассоциацию цифровой валюты, торговую ассоциацию дилеров, занимающихся электронными валютами и обменом, для саморегулирования. Ассоциация ведет рейтинг членов и выступает в качестве посредника для урегулирования споров. «Однако Устав Ассоциации не содержит упоминание о политике и процедурах ПОД или того, что они придерживаются международных стандартов в сфере ПОД, например распространяемых ФАТФ[137].

184. Как уже было указано выше электронные валюты и анонимные платежные системы бывают двух видов: основанные на доверии и на

137 Оценка риска США — Министерство финансов, декабрь 2005 г.

драгоценных металлах. Первый случай касается доверия между продавцом и покупателем. «Обменного курса» для таких валют не существует и для других она не представляет какой либо ценности за исключением физических и юридических лиц, которые используют их[138].

185. Вторая категория имеют гарантию в виде драгоценных металлов и привязана к стоимости золота для того, чтобы установить обменный курс, например, “Egold” и “Pecunix”. После конвертации средства и счет невозможно отследить. Кроме того, некоторые компании предлагают привязать счет электронных денег к дебетовой карте для того, чтобы использовать в магазинах и автоматах, указанных «Interac”[139]. “Cirrus”, “Maestro” и “Plus”, например “GetEMoney”[140].

186. Киберпреступники и лица, отмывающие деньги, обычно используют системы цифровых или электронных валют, которые предлагают различный уровень анонимности, и дают возможность осуществлять мгновенные безналичные расчеты и небольшой шанс возврата или даже отсутствие такового. Некоторые системы почти всегда используются преступниками, включая, но не ограничиваясь только ими, например, «e-Gold”, “WebMoney.ru”, “Liberty Dollar”, “Pecunix”, “Liberty Reserve” “Fethard” и «E-Bullion”[141].

187. При этом товары, обеспеченные альтернативными валютами, такими как свободный доллар, также привлекательны практически по тем же причинам. Легкая конвертация в различные виртуальные валюты и счета, выполняемая т. н. «менялами» предоставляет преступникам замечательную возможность скрыть средства[142].

188. Среди Интернет-сайтов и форумов, которые чаще всего посещали киберпреступники, значатся «e-gold” и «Webmoney”. В некоторых юрисдикциях они не подпадают под требования о ПОД/ФТ (направление СПО и сообщений об операциях свыше определенного порогового значения, выполнение мер по НПК).

189. Во многих юрисдикциях электронные платежи осуществляются

138 Например, «WebMoney” « WMZ », и UKASH http://www.ukash.com/fr/fr/home.aspx
139 http://www.interac.ca/fr/about.php (Канада)
140 http://www.getemoney.com/atmcard.aspx
141 США
142 Германия

анонимно. Также необходимо отметить, что оборот электронных денег осуществляется вне банков и, как результат, вне банковской системы надзора. Банки выступают в качестве агентов, которые вводят деньги в электронную платежную систему или выводят их из нее, а в некоторых случаях как эмитенты электронных денег[143].

190. Есть примеры юрисдикций, где законодательство о ПОД/ФТ не относит электронные платежные системы к организациям, осуществляющим операции с денежными средствами или иным имуществом, в результате чего они не подпадают под требования о ПОД/ФТ. Эти пробелы позволяют использовать электронные деньги для легализации доходов от мошеннических операций, совершенных в Интернете (например, финансовые пирамиды, кража персональных данных Интернет-пользователей, у которых есть банковские карточки или электронные кошельки с возможностью их дальнейшего использования для незаконных финансовых операций), незаконного распространения несертифицированных товаров в Интернете, хищения денежных средств с банковских счетов (путем взлома банковских программ) и электронных кошельков пользователей он-лайновых платежных систем, незаконной деятельности вне Интернета (присвоение бюджетных средств, незаконная деятельность и т. д.).

191. Организаторы е-платежных систем не осуществляют виртуальный контроль за деятельностью своих клиентов, предлагающих товары и услуги он-лайн. Это создает благоприятные условия для незаконной и сомнительной деятельности в Интернете.

Пример 14

Министерство внутренних дел получило информацию от компании «WM Transfer" о том, что неидентифицированный пользователь их системы нарушил контракт с администрацией сайта и похитил 60,000 долларов США со счета компании. Затем в США была открыта платежная система «E-GOLD". Преступник пополнял счет при помощи банковской карты с использованием платежной системы «WM Transfer", а затем обналичивал средства.

Сотрудники правоохранительных органов задержали лицо, которое пыталось

143 Российская Федерация

получить деньги в банке в размере 14,000 долларов США, используя паспорт и платежную карту другого лица. Были конфискованы паспорт, сим-карты к мобильному телефону, банковские платежные карты. Был выявлен IP-адрес, с которого осуществлялся незаконный доступ в Интернет и использовалось компьютерное оборудование. Оборудование было использовано для присвоения чужого имущества (т.е. кошелек обменного пункта) путем мошенничества.

В результате расследования Министерство внутренних дел возбудило уголовно дело по статье 361, Раздел 2 Уголовного кодекса. Были задержаны двое подозреваемых: один — выходец из Кавказа, который организовал снятие наличных через банкоматы с использованием поддельных и утерянных паспортов граждан Украины, другой был осужден на 3,5 года за совершение подобных преступлений, но был освобожден условно-досрочно. Уголовное дело вместе в обвинительным актом было передано в суд.

Источник: Украина

3.1.8 Покупки в Интернете

192. Взаимоотношения между он-лайновыми платежными системами и он-лайн магазинами носят двусторонний характер. Развитие платежный систем — это ответ на требование рынка совершать покупки в Интернете. В ответ он-лайн магазины также расширяют свою деятельность из-за легкого доступа через Интернет, осуществляя ее при помощи он-лайновых платежных систем.

193. Лица, желающие совершать Интернет-покупки или участвовать в Интернет-аукционах, могут использовать существующие банковские счета, кредитные карты, безналичные переводы и даже наличные, чтобы пополнить счет Интернет-посредника, который и осуществит платеж. Некоторые платежные системы существуют для осуществления операций в адрес сайтов с азартными играми или сайтов «для взрослых», т. е. те,которые другие посредники обычно просто не будут осуществлять[144].

194. Использование преступниками виртуальных денег на виртуальном рынке является логическим последствием. Обычно этот метод используется в

144 Оценка риска США — Министерство финансов _____, декабрь 2005 г.

конце отмывочной схемы, на стадии интеграции, но также может иметь место на стадии расслоения, когда за покупкой сразу идет продажа.

195. Интернет-аукционы — это популярный способ покупки дорогих товаров (Российская Федерация) или для покупки билетов на самолет (Албания). Отдельными пунктами незаконных покупок в Интернете идут поддельные лекарственные средства и продажа товаров, представляющих высокий риск и незаконные товары (наркотики, огнестрельное оружие и и детская порнография), сетевой маркетинг (пирамиды или схемы Понзи), эскорт услуги, продажа табака, прекурсоров, украденные кредитные карты и информация о кредитных картах. Денежные переводы, совершаемые для таких операций особенно уязвимы для ОД. Также, определенный риск отмывания денег существует в связи с азартными играми и платежами в адрес таких сайтов.

3.1.9 Компании — оболочки

196. Также ответы стран указали на вовлечение компаний - оболочек в описанную выше деятельность. Такие компании предлагают широкий спектр возможностей для киберпреступников и обычно используются на стадии расслоения. Компании- оболочки - это компании, не осуществляющие предпринимательскую деятельность, не обладающие активами и правосубъектностью. Но у такой компании есть счет в банке, который обычно удачно расположен в офшоре. Их задача -это обеспечить основание для перевода денег из банка плательщика, а также скрыть маршрут денег.

197. Обычно у компаний-оболочек есть только адрес, почтовый ящик и лицо, которое уполномоченное совершать операции с банковским счетом. Такие компании могут использовать как традиционные платежные системы, так и он-лайновые. Если операция осуществляется через банковскую систему, то единственная трудность заключается в том, чтобы доказать, что компания действительно являлась «оболочкой». Если операция совершается через менее урегулированный сектор, то компании- оболочки могут осуществлять свою деятельность в течение продолжительного периода времени и оставаться не выявленными.

198. Примеры указывают на то, что:

- компании — оболочки использовались и используются в схемах

киберпреступников и отмывания денег;
- если компанию- оболочку используют для совершения киберпреступлений и отмывания денег, то суммы переводов обычно выше, чем обычно;
- использование компаний-оболочек часто связано с офшорами.

Пример 15:Использование компаний-оболочек для международных переводов средств, полученных в результате мошенничества.

ПФР получило СПО на основании требований Закона о ПОД/ФТ относительно мошенничества/мошеннических действий. 1,000,000 долларов США поступил на банковский счет офшорной компании, у которой был открыт счет в венгерском банке. Деньги были переведены с частного банковского счета, открытого в другой стране ЕС.
Что касается операции на сумму в 1,000,000 долларов США, то венгерский банк получил СВИФТ от банка-отправителя, в котором последний указывал на наличие мошеннической деятельности и попросил венгерский банк заморозить счета получателя и вернуть средства обратно в банк-отправитель. Получателем оказалась компания- оболочка.
После того как средства поступили на счет в венгерском банке, часть денег была переведена дальше, а вторая — снята наличными представителем компании, находившейся в офшоре.

Источник: Венгрия

Пример 16. Мошенничества через ПОС-терминалы

Дело о мошенничестве и отмывании денег было возбуждено в отношении иностранных физических лиц, которые попросили разрешение на постоянное проживание для ведения предпринимательской деятельности в стране для чего позже создали компанию, которая была официально зарегистрирована в Реестре компаний. Иностранных граждан зарегистрировали в качестве владельцев и лиц, входящих в состав орган, предусмотренного Уставом, и Компания начала свою деятельность с оптовой продажи модных товаров. В то же время эти лица открыли счет компании в банке, находящемся на территории их родного государства. На счет были внесены крупные суммы наличными.
Физические лица, представляющие компанию, попросили банк предоставить им мобильные POS-терминалы для получения постоянного дохода от

клиентов.
Указанные лица также открыли личные банковские счета в банках у себя на родине и внесли большие суммы денег на них.

Поскольку система ПОС-терминалов и предварительной авторизации действовали как и было задумано, то они решили выпустить свои платежные карты для пользования ими в ПОС-терминалах. Компания дала указания об осуществлении операции на основании предварительной авторизации, которая не списывалась с личного счета, но обрабатывалась. Сразу после истечения срока предварительной авторизации денежные средства снимались со счетов указанных лиц. После этого средства зачислялись на счет компании, затем без промедления обналичивались, после чего вносились на новый личный счет и переводились за рубеж. Баланс на личных счетах лиц всегда был отрицательный с большой суммой задолженности.

В настоящее время в прокуратуре рассматривается дело о совершении тяжких преступлений, а именно о мошенничестве и отмывании денег. Это особый случай из-за того, что были тщательно проработаны деталей и вложены собственные средства, точный подбора сферы деятельности, сложного способ действия, который требовал глубоких знаний банковской системы и сроков окончания.

Источник: Словакия

3.1.10 Предоплаченные карты

199. Предоплаченные карты появились относительно недавно в мире потребительских электронных платежей. Начало им было положено в виде электронной формы бумажных подарочный карт. Очень большое количество товаров предлагается оплатить предоплаченными картами без проведения идентификации или ее минимальном проведении. На эти карточки можно перевести средства, после чего они могут быть проданы или использованы. В отличии от предоплаченных банковских карт этот процесс может быть выполнен при помощи магазинной кредитной карты и предоплаченных мобильных телефонов.

200. В памяти предоплаченной карты хранится сумма, которая была внесена на нее ранее компанией или агентом, выпустившей ее. Так называемые

подарочные карты (закрытая система) позволяют держателю покупать товары и услуги в рамках одной определенной коммерческой цепи. Они могут куплены и использованы анонимно. Такие карты могут быть куплены на Интернет-аукционах («e-bay") по сниженной стоимости.

201. При открытой системе предоплаченные карты выпускаются банками или иными кредитными/финансовыми учреждениями, и они могут быть использованы для покупок во всех точках розничной торговли, где принимают обычные кредитные карты. Они могут быть использованы для снятия наличных и связаны с он-лайновым счетом.

202. Предоплаченные карты могут быть использованы преступниками для перевода преступных доходов из одной юрисдикции в другую (стадия расслоения) или для покупки товаров и/или услуг для получения преступной выгоды (стадия интеграции). Предоплаченные карты введены в ряде стран, но в большинстве стран, согласно представленным ответам, они используются реже, чем в США[145]. Исследование Бостонской консалтинговой группы предсказывает, что на США придется 53% всех предоплаченных карт, выпускаемых в мире. Кроме того, в нем подтверждаются данные о том, что Италия является наиболее перспективным рынком предоплаченных карт в Европе, в то время как Соединенное Королевство считается устоявшимся рынком, а рынки Германии и Австрии описываются как находящиеся в зачаточном состоянии. Однако использование и распространение предоплаченных карт выросло за последние годы. Согласно данным Базельского комитета по платежам и расчетного обсулуживания. количество выпущенных карт с функцией электронных денег выросло со 106,7 миллионов в 2004 г. до 275,28 миллионов в 2008 г. в ряде стран[146].

Пример 17. От фишинга до конвертации цифровых валют

Номера операций были изначально перехвачены Трояна. «Фишинговый перевод» был осуществлен на банковский счет финансового агента. Финансовый агент снял деньги, удержав свою комиссию. Затем он купил приходные ордеры он-лайновых платежных систем у различных эмитентов, через например, заправочные станции, киоски на максимальную сумму в

145 ФАТФ- ГАФИ - «Отмывание денег с использованием новых платежных методов», октябрь 2010 г.

146 Бельгия, Франция, Германия, Италия, Япония, Голландия, Сингапур и Швейцария

размере 500 евро. Покупки были анонимными без идентификации. Таким образом, реальные деньги были переведены в виртуальные. Финансовый агент направлял номер ордера (называемый «готовый для использования» ПИН-код) по электронной почте лицу, которое давало поручения. ПИН-код использовался для оплаты товаров и услуг в Интернете, а также для оплаты ставок в казино и азартных играх. Несколько ордеров на небольшие суммы могли использоваться вместе. Также могла быть использована конвертация в иные электронные валюты. Правоохранительные органы не могли отследить каналы, по которым проводились операции.

Источник: Германия

Пример 18. Кража данных, отмывание денег и использование предоплаченных карт

В отличии от организаций, созданных по типу мафиозных, действующих на определенной территории, существуют отдельные преступные группы, которые действуют совместно только в случае необходимости. Некоторые функционировали несколько лет, другие - в течение короткого период времени. В отношении компании «TJX" были совершены мошеннические действия в период с 2005 г. по 2007 г., в результате которых были украдены номера кредитных карт 94 миллионов клиентов из Северной Америки и Великобритании. В августе 2008 г. 11 человек было арестовано (3 — гражданина США, 1 — Эстонии, 2 — Китая, 1 — Белоруссии, 3 — Украины [147]). СМИ сообщили о том что все они являлись членами международной преступной организации, занимавшейся пиратством. Среди них были и те, кто взламывали сети вай-фай и те, кто координировал деятельность группы на самом высоком уровне. Все они постоянно встречались на карточных форумах, созданных по модели «CarderPlanet", объединяя членов со всего мира.

Кроме информации о кредитных картах продавцы предлагали поддельные документы (паспорта), дорожные чеки и даже лицензии на обучение. В 2009 г. был выявлен еще один факт кражи 130 миллионов единиц банковской информации.

147 «Retail Hacking Ring" были предъявлены обвинения в хищении и распространении номеров кредитных и дебетовых карт одного из основных американских елей розничной торговли: http://www.usdoj.gov/criminal/cybercrime/gonzalezIndict.pdf

Атаку совершили те же лица, что и в отношении компании «TJX”.

Для того, чтобы разработать такую же мошенническую схему как и в отношении компании «TJX”, были нужны навыки преступных групп, которые специализировались на использовании поддельных карт. Эти преступные группы либо объединялись, либо работали порознь, если это было необходимо.

В марте 2007 г. полиция Флориды проводила расследование в отношении члена одной из преступных групп и произвела несколько арестов. В основе схемы лежало использование предоплаченных карт (подарочных карт) для покупки дорогих товаров роскоши в магазинах электроники и ювелирных магазинах. Предоплаченные карты приобретались на поддельные кредитные карты, поставляемые другими членами преступной группы. Этот метод позволил им отмыть 225,000 долларов США[148].

Торговля похищенными данными является высоко прибыльными. У пользователей возникают дополнительные риски, но и доходы преступников высоки. Что касается последних случаев, то использовались два способа: покупки совершались на сайтах, на которых требовались только выставить счет или предоставить адрес доставки или использовались поддельные карты с магнитной полосой в тех странах, где они еще используются.

Источник: СМИ

3.1.11 Платформы для он-лайн игр и он-лайн торговли

203. Хотя исследование не содержит отдельных примеров использования платформ для он-лайн игр и он-лайн торговли для обмена иностранной валюты и иных финансовых рынках, ряд стран также подняли вопрос об отмывании денег с использованием этих техник.

204. Такие платформы также уязвимы для кибер-атак или мошенничества, направленного прежде всего на средства клиентов и представляют особые риски ОД/ФТ, которые были проанализированы в ходе другого исследовании[149].

148 Расследование по факту кражи данных у компании TJX привело к раскрытию схемы отмывания денег: http://www.usatoday.com/money/2007-06-11-tjx-datatheft_N.htm

149 Для дополнительной информации о рисках ОД/ФТ при использовании платформ для Интернет-торговли см.,например, исследование ФАТФ «Отмывание денег и финансирование терроризма в секторе

205. Программное обеспечение, распространяемое организаторами он-лайн игр позволяет перемещать и аккумулировать крупные денежные суммы, вносить и снимать призовые путем банковских переводов или различных электронных платежных систем. Отмечается тенденция систематического использования букмекерских контор, у которых есть зарегистрированные игровые сайты (Болгария), при помощи которых совершается отмывание денег, сокрытие активов и уклонение от уплаты налогов. Активы зачастую используются для финансирования преступных групп, открытия новых игорных заведений, коррупции и других преступлений.

3.2 Индикаторы возможного отмывания денег: показатели риска отмывания денег

206. Что касается кибер-отмывания, то индикаторы аномального поведения могут быть такими же, что и для традиционных платежных систем, но в тоже время могут обладать и отличительными чертами. Появление одного или нескольких таких индикаторов должно служить предупреждающим знаком необычного поведения, которое может быть связано с отмыванием денег или финансированием терроризма. Приведенный перечень не является исчерпывающим, а лишь отражает те способы действия преступников, которые были указаны в ответах на вопросник. Операции или вид деятельности, указанные в списке, необязательно являются признаком отмывания денег, если они связаны с законным бизнесом клиента. Сообщающие организации должны концентрироваться на выявлении подозрительной деятельности, а не на выяснении того факта, действительно ли операции связаны с отмыванием денег, финансированием терроризма или иным определенным преступлением:

- у лица слишком много аккаунтов у одного и того же Интернет-провайдера;
- отличие между предоставленной идентификационной информации о клиенте и IP-адресом;
- подозрительные IP-адреса и подозрительные имена пользователи (ники, клички, имена ICQ) могут помочь в выявлении преступных потоков;

ценных бумаг (2009 г.) на http://www.fatf-gafi.org/dataoecd/32/31/43948586.pdf. Для подробного описания рисков ОД/ФТ, связанных с он-лайн играми и методах ОД/ФТ МАНИВЭЛ проводит отдельное исследование, результаты которого будут опубликованы в начале 2012.

- логины и попытки введения логинов с непроверенных IP-адесов или идентификационных данных, которые якобы содержали информацию о подозрительной деятельности; попытка размещения того, что ранее было определено как вредоносные cookies-файлы;
- необычные условия или сложность операции: высокая частота денежных переводов в течение небольшого периода времени, большое количество разнообразных источников происхождения средств и платежных методов;
- в случае если речь идет о клиентах юридического лица, то отсутствие явной взаимосвязи между операцией и характером деятельности клиента;
- отсутствие точной информации о предпринимательской деятельности клиента или использование он-лайновых платежных систем вместо традиционных (обычных для компаний и деловых платежей);
- для физического лица (например, менеджера компании) — отсутствие а данных о профессиональной сфере деятельности; для компании — если в сфере деятельности указано «инвестирование», «международный», «международный инвестор», «любые виды экспорта-импорта»;
- подставные сотрудники, владельцы образцов или очевидные схожести, связанные с адресами, деятельностью, связанной с консультированием или финансами;
- внешность лица или его поведение не соответствует характеру совершаемой операции или поведение лица не заслуживает доверия;
- лицу нужна помощь в заполнении документов или оно не может их заполнить;
- лицо не осведомлено о характере деятельности юридического лица, которое он представляет;
- лицо не может объяснить необходимость оказания кредитным или финансовым учреждением той или иной услуги;
- лицо требует предоставить необычайно высокие лимиты (особенно для дальних переводов, которые не соответствуют обороту лица, предыдущему его финансовому поведению или социальному представлению о нем;
- лицо требует выдать ему две и более банковских карт, что не соответствует природе деятельности лица или его обороту;
- лицо не обладает информацией о настоящих бенефициарных владельцах юридического лица, которое он/она представляет, месте нахождения или не располагает контактными данными;
- лицо не может указать партнеров юридического лица и/или сферу его деятельности;

- лицо хочет открыть счет в филиале банка в одном округе/городе, в то время как адрес и местонахождения представителя или юридического лица — в другом месте, и не предоставлено вразумительного объяснения этому факту;
- внесение средств на счет лица/компании, у которой низкий уровень прибыли или не было никого значительного роста объемов прибыли;
- международные переводы, получаемые/отправляемые за рубеж, что не соответствует профили клиента;
- получены средства из за рубежа, после чего произошло их снятие или перевод в другое место;
- операция не соответствует предыдущим операциям клиентов;
- постоянные операции на сумму ниже порогового для избежания декларирования источника происхождения; крупная сумма переведенных активов;
- счет он-лайновой платежной системы используется только для снятия наличных;
- средства вносятся в основном наличной форме или инструментами, похожими на наличные (например, предоплаченные карты); сумма ниже порогового значения;
- внесение средств осуществляется неизвестной третьей стороной после чего идет незамедлительное их обналичивание или перевод;
- операции, осуществляемые в/из иностранных государств, в сочетании с неподтвержденными данными о внешних получателях, плательщике или источнике происхождения активов;
- установление длительных коммерческих отношений или осуществление операции путем электронного извещения, электронного документа, подписанного электронной цифровой подписью и иными способами без личного присутствия клиента;
- корпоративное накопление (переводы между банковскими счетами связанных между собою лиц или пожертвования без видимой на то причины);
- телеграфные переводы от организации - донора в адрес компаний, находящихся в налоговых гаванях;
- операции с активами из офшорных юрисдикций, а также стран, не реализующих международные стандарты ПОД/ФТ и т. д.;
- операции или снятие денежных средств (наличные, чеки, телеграфные переводы и т. д.) по счетам, в отношении которых не применяются

предыдущие условия о депозите;

- операции, связанные с большим количеством входящих/исходящих переводов без логической или видимой цели, осуществляемые в/из «рисковых юрисдикций» (т. е. стран, в отношении которых введены санкции, не сотрудничающие страны и страны, поддерживающие терроризм);
- необъяснимые клиринговые операции или операции по контракту с использованием чеков третьих лиц или их депозитами на счетах в иностранном банке;
- использование большого количества счетов для получения средств и для их дальнейшего перевода в адрес одних и тех же иностранных получателей;
- схемы со списанием наличных, при которых депозиты (например, в США) прямо ведут к снятию наличных через банкоматы в проблемных странах. Обратные операции также являются подозрительными;
- выдача чеков, платежных поручений и иных финансовых инструментов последовательно увеличивается, которая имеет место в отношении одного и того же лица или компании или лица или компании, чьи имена/наименования созвучны;
- предприятие с незначительным оборотом или вновь созданное мероприятие поучают переводы на значительные суммы, что не соответствует его профилю;
- счета открываются не резидентами, которые не имеют никакого отношения к юрисдикции, в которой оказываются платежные услуги;
- частые иностранные поступления на банковский счет, за которыми следует их обналичивание или перевод с использованием поставщиков услуг по переводу средств, он-лайновых платежных систем, валютных систем, располагающихся на сервере, который находится в стране или среде, в отношении которой имеются озабоченности в части ОД/ФТ, как это определено ФАТФ, региональными РГТФ или соответствующими национальными органами;
- деятельность денежных мулов является индикатором отмывания денег и должна стать поводом для ПФР предпринять соответствующие действия.

4. КОНТРМЕРЫ

207. В ответ на рост объемов потоков преступных денег в Интернете, государственный и частный секторы предприняли ряд мер, примеры которых приведены ниже.

208. Эти меры могут служить хорошим примером. Кроме того, они могут стать частью более системных подходов и стратегий, направленных на противодействие отмыванию денег и финансированию терроризма, а также на розыск, изъятие и конфискацию доходов от преступлений, совершаемых в Интернете:

- механизмы сообщения о мошенничестве и иных преступлениях в Интернете, направленных на извлечение прибыли;
- предотвращение и повышение осведомленности;
- регулирование, управление рисками и надлежащая проверка;
- создание правовой базы на основании международных стандартов;
- создание специализированных подразделений для борьбы с преступностью в сфере высоких технологий;
- взаимодействие между государственным и частным секторами;
- обучение.

209. Перед обобщением практики и предпринимаемых мерах, было бы полезно представить обзор того, что уже есть в наличии у государственных и частных учреждений, хранящих важную информацию и которые должны быть вовлечены в:

Учреждение	**Обязанности:**	**Характер, хранящейся информации**
Анти-отмывочная система		
Институты финансового сектора, на которых лежит обязанность направлять информацию	- обеспечение соответствия положениям о противодействии отмыванию денег и финансированию терроризма; - реализация надлежащей проверки; - направление сообщений о	- данные о клиентах и бенефициарных собственниках; - данные о финансовых операциях

	подозрительных или необычных операциях в ПФР	
Подразделения финансовой разведки (ПФР)[150]	- национальный центр, ответственный за получение, анализ и передачу в компетентные органы информации о подозрительных операциях и иной подозрительной деятельности, которая возможно связана с отмыванием денег и финансированием терроризма; - сотрудничество и обмен информацией между ПФР посредством Группы «Эгмонт»[151]	- информация о подозрительных или необычных операциях и проведенном в отношении них анализе
Службы, занимающиеся возвратом активов/финансовыми расследованиями[152]	- осуществляют финансовые расследования в отношении преступлений, связанных с преступными доходами; - предпринимают дальнейшие действия по информации, полученной от ПФР; -осуществляют предварительные меры для ареста и замораживания активов, которые могут являться доходами от преступлений.	- данные о расследовании определенной категории уголовных дел; - разведывательные данные
Прокуроры и судьи	-преследование и вынесение судебного решения;	-данные о расследовании определенной категории

150 См. http://conventions.coe.int/Treaty/EN/Treaties/Html/198.htm
151 http://www.egmontgroup.org/
152 Информацию о службах, занимающихся возвратом активов см. информацию на сайте «CARIN”: http://www.europol.europa.eu/publications/Camden_Assets_Recovery_Inter-Agency_Network/CARIN_Europol.pdf

	-надзор за расследованиями по уголовным делам; -выдача разрешений на проведение следственных действий, включая розыск, изъятие и замораживание активов; -международное судебное сотрудничество	уголовных дел
Надзорные органы и регуляторы	- предотвращают использование финансовой системы для отмывания денег и финансирования терроризма; - обеспечивают соответствие деятельности учреждений финансового сектора требованиям ПОД/ФТ	-данные об учреждениях финансового сектора; - информация о регулировании
Органы международного мониторинга[153]	- Мониторинг соответствия международным стандартам борьбы с отмыванием денег и финансированием терроризма	Информация о национальном регулировании и функционировании системы ПОД/ФТ
Органы, занимающиеся противодействием киберпреступности		
Специализированные подразделения в органах прокуратуры	- осуществление преследования по киберпреступлениям; -надзор за следствием и разрешение на проведение следственных действий; -международное сотрудничество	-данные о расследовании определенной категории уголовных дел

153 См. МАНИВЭЛ (http://www.coe.int/t/dghl/monitoring/moneyval/) и Группа разработки финансовых мер борьбы с отмыванием денег (www.fatf-gafi.org).

Подразделения по борьбе с преступлениями в сфере высоких технологий	- проведение расследование киберпреступлений; - сбор и анализ информации; -поиск по компьютерным системам; -оказание содействия иным полицейским подразделениям при проведении расследований по киберпреступлениям; - сбор разведывательной информации; - обмен информацией с подобными органами иностранных государств; - международное сотрудничество между органами полиции и оказание содействия международному сотрудничеству между судебными органами	-данные о расследовании определенной категории уголовных дел; - разведывательные данные
Компьютерно-технические лаборатории	- исследование электронных улик/доказательств для расследования по уголовному делу	- данные об электронных доказательствах/уликах
Создание контактных центров 24/7 для международного сотрудничества для борьбы с киберпреступностью[154]	-обеспечение сохранности данных при осуществлении международного сотрудничества; - сбор доказательств; - определение места нахождения подозреваемых;	-данные о расследовании определенной категории уголовных дел

154 См. Статью 35 Будапештской Конвенции против киберпреступности http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG. См.также: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf

	-содействие сотрудничеству между судебными органами	
Финансовый сектор (он-лайн)		
Платежные карты	- он-лайновые платежи, совершаемые клиентами	-данные о клиентах и операциях; -данные о мошенничестве и попытке совершения мошеннических действий; - индикаторы и критерии для выявления мошенничества
Дистанционное банковское обслуживание (Интернет-банкинг)	- управление счетами самими пользователями	- данные о клиентах и операциях; - данные о мошенничестве и попытке совершения мошеннических действий; - индикаторы и критерии для выявления мошенничества
Платформы для он-лайновых платежей	- он-лайновые платежные услуги и решения для физических лиц и компаний; соответствие требованиям о ПОД/ФТ и иным положениям, регулирующим деятельность финансового сектора	- данные о клиентах и операциях; - данные о мошенничестве и попытке совершения мошеннических действий; - индикаторы и критерии для выявления мошенничества

Контент-провайдер[155]	- предоставление услуг он-лайн, включая аукционы, магазины, социальные сети	- информация о клиентах; - данные о мошенничестве и иных зловредных действий в отношении их услуг или клиентов
Услуги по переводу денег	- перевод денежных средств он-лайн в любую точку земного шара	- данные о клиентах и операциях
Поставщики Интернет-услуг (ISP)		
Поставщики телекоммуникацион-ных услуг	- предоставляют доступ к телекоммуникационным каналам и высокоскоростному широкополосному Интернету и иные услуги; - «общественный перевозчик» электронных сигналов (не несет ответственности за содержание)	
Поставщики доступа в Интернет	- предоставляют пользователям доступ в Интернет по требованию; -обычно «общественный перевозчик» электронных сигналов (не несет ответственности за содержание); -условия для доступа и допустимые условия использования помогают справиться с	- информация о пользователях; - данные, связанные с Интернет-траффиком (регистрационные файлы, данные о IP); данные о содержании; - могут фильтровать спам, вредоносные программы или детскую порнографию; - проверка

155 Учитывая появление «Web 2.0”, то необходимо проводить разделение между профессиональными и непрофессиональными контент-провайдерами, поскольку любой пользователь может в результате стать контент-провайдером

	злоупотреблениями	благонадежности.[156](хотя шифрование, использование прокси-серверов, туннелирование зарубежных мульти-протоколов и т. п. сокращает возможности ISPs для DPI).
Хостинг-провайдер	- регистрация и размещение доменов; -хостинг серверов; хостинг почтовых служб	- информация о пользователях; - незначительные знания о размещаемом контенте до тех, пока не возникают проблемы
ICANN, регистраторы и реестродержатели[157]		
ICANN[158]	- координирует распределение доменных имен (Система имен доменов), адресов Интернет-протоколов (IP) и номеров автономных систем, а также номера частей и параметры протоколов	-Информация о регистраторах и реестродержателях
Регистраторы[159]	-управление общими доменами высшего уровня (gTLD)(например, «.com”, “.org”);	- база данных «WHOIS” («телефонная книга Интернета»), включая имена, почтовый адрес,

156 В то время как такие проверки позволяют улучшить системы безопасности это также позволяет ISPs отслеживать Интернет -траффик и возможно собирать и анализировать данные о миллионах пользователей. Это довольно проблематично из-за обезличенности Сети и отказа от дискриминации, фильтрации содержимого, свободы слова, пиратства и защиты персональных данных. http://www.deeppacketinspection.ca/
http://userpage.fu-berlin.de/~bendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf
http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf

157 Описание функционирования системы дано в отчете, подготовленном проектной группой Совета Европы о киберпреступности http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter1.pdf

158 Организация по присвоению имен и адресов в Интернете

159 Для Европы см. http://www.ripe.net/

	-управление страновыми доменами высшего уровня (ccTLDs) (например, “.fr”, “.uk”; -распределение и присвоение Интернет ресурсов, например, IP адресов, номеров в автономной системе (группы IP-сетей) и т. д. организациям	номер телефона, адреса электронной почты
Реестродержатели (ISP)	- получает доменное имя от регистратора в соответствии с Соглашением о регистрации реестродержателя (RRA); -предоставляет конечному пользователю услуги по получению доменного имени за вознаграждение	- информация о зарегистрировавшихся для базы данных «WHOIS». В соответствии с RRA такая информация должна быть полной и точной[160]
Институты, наблюдающие за деятельностью в Интернете		
CERT/CSIRT	Группы реагирования на компьютерные инциденты в сети Интернет (CERTs) или Группа реагирования на инциденты, связанные с компьютерной безопасностью (CSIRTs) являются институтами государственного или частного сектора, которые изучают уязвимые места и отвечают на инциденты, предоставляя технические решения и консультационные услуги[161]	- информация об инцидентах, связанных с компьютерной безопасностью

160 Что не соответствует действительности

161 Для CERT координационный центр — Университет Карнеги-Меллонов http://www.cert.org/. Для правительственных CERT см. http://www.us-cert.gov/ или https://www.bsi.bund.de/cln_156/DE/Themen/CERTBund/certbund_node.html. Для неофициальных групп правительственных CERTs в Европе см. https://www.bsi.bund.de/cln_156/ContentBSI/Themen/CERT_Bund/InternatKooperation/egovcert_en.html

Индустрия, научно-исследовательские институты, инициативы по борьбе с киберпреступностью[162]	- мониторинг системы имен доменов; - мониторинг протоколов пограничной маршрутизации (протокол BGP); -мониторинг злоупотреблений; -участие в расследовании преступной деятельности; -содействие сотрудничеству и выработки мер для борьбы с мошенничеством и иными категориями киберпреступлений	- информация о противоправных действиях в Интернете и взломанных машинах; -информация о бот-сетях и иных разновидностей атак; -информация о подозреваемых[163]

4.1 Сообщение о Е-преступлениях

210. Ограниченный объем данных и знаний о мошенничестве и иных видах киберпреступлений считается основным препятствием для предотвращения и контроля за киберпреступностью и преступными

162 Такие инициативы частного сектора ведут накоплению больших объемов информации, которая может быть использована для выявления злонамеренных деяний и таким образом обладают огромным массивом _____ информации, которая практически не используется правоохранительными органами.

Примеры:
http://mynetwatchman.com/
http://www.team-cymru.org/Services/
http://www.spamhaus.org/organization/index.lasso
http://eval.symantec.com/mktginfo/enterprise/white_papers/bwhitepaper_emea_Internet_security_threat_report_xv_04-2010.en-us.pdf
http://www.messagelabs.com/resources/
Перечень инициатив см.:
http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/networks/Networks_en.asp
При меры инициатив по борьбе с мошенничеством:

- Анти-фишинговая рабочая группа (http://www.antiphishing.org/) – международная панпромышленная и правоохранительная ассоциация, которая концентрирует свои усилия на борьбе с мошенничеством и хищении персональных данных в результате фишинга, фарминга и спуфинога всех видов

- Лондонский план действий (http://www.antiphishing.org/) развивает международное сотрудничество по борьбе со спамом и пытается решать связанные с ним проблемы, например, он-лайновое мошенничество, фишинг, и распространение вирусов. Участники оставили открытым План действий для других заинтересованных правительственных и общественных организаций, а также представителей частного сектора, для того, чтобы расширить сеть учреждений, вовлеченных в борьбу со спамом.

- Рабочая группа по обмену информацией о борьбе со злоупотреблениями_____ (MAAWG) объединяет представителей индустрии, занимающихся обменом сообщениями и успешно разрешает вопросы, связанные со злоупотреблением в этой сфере, например, спам, вирусы, атака типа отказа в обслуживании и т.п.

163 См., например база данных “ROKSO” на “Spamhouse” http://www.spamhaus.org/rokso/

денежными потоками на что и сослались страны в своих ответах. Возможности анализировать случаи Интернет-мошенничества и связанные с ним потоки денежных средств практически отсутствуют. Отсутствует понимание и осведомленность о том, что организованная преступность может стоять за мелким мошенничеством. Даже если подозрительные денежные потоки и выявляются, правоохранительные органы и частный сектор зачастую не могут сопоставить данные, для того, чтобы получить полную картину о преступной деятельности и выявления схем.

211. Примеры полезного опыта, связанные с сообщениях об Интернет-преступлениях уже доступны или нарабатываются.

4.1.1 Центр приема сообщений об Интернет-преступлениях (IC3)[164]

212. IC3 было создано в качестве партнерства между Федеральным бюро расследований и Национальным Центром по борьбе с беловоротничковой преступностью. Он получает он-лайн обращения лиц, которые полагают, что в отношении них были совершены мошеннические действия, или третьих лиц по отношению к жалобщику, после чего обращения перенаправляются в правоохранительные органы для проведения дальнейшего расследования. В соответствии с заявлением о целях:

> IC3 служит средством получения, изучения и передачи обращений о совершении преступлений в сфере компьютерных технологий, объем которых растет постоянно. IC3 предоставляет потерпевшим в результате совершения киберпреступления удобный и понятный механизм направления сообщений, которые предупреждают власти о наличии подозреваемых или нарушении гражданских прав. Для правоохранительных органов и регуляторов на федеральном, государственном, местном и международном уровнях IC3 предоставляет механизм направления обращений о преступлениях, совершенных в Интернете.

213. В 2009 г. IC3 получил 336,655 жалоб, 146,663 из которых были переданы в

164 http://www.ic3.gov/default.aspx

правоохранительные органы[165]. Большинство из них было связано с непоставкой товаров и услуг (19,9%), кражей персональных данных (14,1%), мошенничеством с пластиковыми картами (10,4%) и мошенничеством на Интернет-аукционах (10,3%).

214. Новая классификация, введенная в 2009 г., включает в себя 79 категорий преступлений. Помимо мошенничества в них входят незаконная торговля наркотиками, шантаж, порнография, терроризм и иные преступления, которые могут совершаться посредством Интернета[166].

215. Такая система позволяет правоохранительным органам выявлять не только отдельные преступления, но целые тенденции, а также проводить анализ киберпреступности более всесторонне.

216. IC3 публикует ежегодные отчеты о киберпреступности, а также познавательные и обучающие материалы, направленные на борьбу с мошенничеством и иными видами Интернет-преступлений.

4.1.2 MELANI[167]

217. В Швейцарии в 2004 г. было создано «Melde – und Analysestelle Informationssicherung" (MELANI). Это центр для направления сообщений и анализа данных о безопасности информационных систем, который содержит информацию об угрозах и контрмерах, аналитические отчеты о складывающейся ситуации, угрозах, тенденциях и возможностях направления сообщения.

218. MELANI поддерживает GovCERT.CH, Федеральная служба разведки (NDB) и Федеральное стратегическое подразделение по информационным технологиям (ISB).

219. На 1 января 2010 г. MELANI уже было наделено полномочиями для того, чтобы при наличии определенных обстоятельств блокировать доменные имена, в отношении которых есть подозрения, что они замешены в хищение персональных данных (фишинг) или распространении вредоносных программ.

---

165 Центр приема сообщений об Интернет-преступлениях (2010 г.). Отчет о киберпреступности за 2009 г. (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

166 (См. Центр принятия сообщений об Интернет-преступлениях _____ (2010 г.). Отчет о киберпреступности за 2009 г. (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).

167 http://www.melani.admin.ch

4.1.3 Национальный центр по сообщениям о мошенничестве[168]

220. В 2010 г. Соединенное Королевство создало «Action Fraud» как национальный центр, куда можно направить сообщение о мошенничестве в любое время.

221. Управляют “Action Fraud” Национальное подразделение по борьбе с мошенничеством — исполнительный орган Генеральной прокуратуры. Среди партнеров значится полиция Сити, Национальное бюро по борьбе с мошенничеством (NFIB), Ассоциация руководителей полицейских служб и Министерство внутренних дел. Сообщения о свершившихся фактах регистрируются и предаются в NFIB для дальнейшего расследования или разведывательных целей. Кроме того «Action Plan» предоставляет предупреждающую информацию и оказывает содействие потерпевшим.

4.1.4 Он-лайн система приема сообщений об Интернет-преступлениях (I-CROS)[169]

222. Вопрос о создании I-CROS в Европоле был инициирован в 2010 г. при поддержке Европейской Комиссии. Это позволит государствам- членам Европейского Союза и со временем третьим странам направлять в Европол сообщения о преступлениях, совершаемых в Интернете. Основные усилия будут сконцентрированы на тех преступлениях, которые указаны в статьях со 2 по 8 Будапештской Конвенции против киберпреступности[170].

223. I-CROS — это европейский механизм так называемой Европейской тревожной системы, создаваемой для получения сообщений о правонарушениях, совершаемых в Интернете, в соответствии решением Совета Европейского Союза о создании таких систем как на национальном, так и на европейском уровнях (24 октября 2008 г.). Ее дополняют национальные системы, которые должны быть созданы на территории государств-членов. Сообщения от граждан и частного сектора для начала поступают в национальную систему. Где они обрабатываются, а затем в случае необходимости направляются в иные государства-члены и Европол для перекрестной проверки в I-CROS.

168 http://www.actionfraud.org.uk/home

169 Информация предоставлена Европейской Комиссией

170 Проект Рамочной программы ЕС о борьбе с атаками на информационные системы (COM(2010) 517 final) в статье 15 содержит обязательство для всех государств-членов хранить, вести и предоставлять статистические данные о преступлениях, совершенных при помощи компьютерных технологий.

224. I-CROS является частью Европейской системы по борьбе с киберпреступностью (ECCP), которая также включает в себя исследовательскую рабочую программу «Киборг», которая делает упор на преступные группы, действующих в Интернете, а также Форум судебных и Интернет-экспертов (IFOREX) для обмена техническими данными и проведения обучения по вопросам борьбы с киберпреступностью для правоохранительных органов. ECCP — это первый шаг для применения более последовательного и эффективного подхода для борьбы с преступностью в Интернете на уровне ЕС.

4.1.5 Signal Spam[171]

225. «Signal Spam" - это государственно-частное партнерство во Франции, которое позволяет Интернет-пользователям направлять информацию о спаме, которые фиксируются в отдельной базе данных и затем могут быть использованы при проведении расследований по уголовным или административным делам, а также в ходе исследований, что в конечном итоге позволяет повысить безопасность сети и улучшить доставку почты.

226. Членами партнерства являются ассоциации (например, AFA- Французская ISP-ассоциация, Союз французских рекламодателей, Альянс производителей коммерческого программного обеспечения и другие), частный сектор (CERT-LEXI, "eBay"/"PayPal", "Microsoft", "Orange" и другие) и национальные органы (Национальная жандармерия, Подразделение французской полиции по борьбе с преступлениями в сфере высоких технологий, Французское бюро по защите данных CNIL, Следственная группа для борьбы с мошенничеством в сфере информационных технологий и другие).

4.1.6 Сообщение о Е-преступности: использование обычного формата данных

227. Данные, которые имеют отношение к проводимым расследованиям киберпреступлений, обычно очень объемны, рассеяны до разным странам и местами хранятся в таких форматах, которые делают невозможным обработку и обмен информацией.

171 https://www.signal-spam.fr/

228. Для того, чтобы разрешить эту проблему Анти-фишинговая рабочая группа разработала схему на основе XML для получения сведений о технической стороне фишинга, мошенничестве и иных формах компьютерных преступлений.

229. APWG разработала ряд расширений для Формата обмена описаниями случайных объектов (IODEF), а также стандарт направления сообщений по инцидентам в Сети, принятый на вооружение Группой специалистов по разработкам в Интернет[172]. Это даст возможность использовать обычный формат сообщений и предоставлять данные об источниках мошенничества и целях атак, о том какие серверы задействованы, какие вредоносные программы используются, доменные имена и информацию о регистраторе, файлы, имеющие силу доказательств, и другие.

230. В качестве обычного формата эта схема позволит обмениваться данными между государственным и частным сектором и создаст предпосылки в будущем для выявления Е-преступлений.

4.2 Предотвращение и осведомленность общества

231. Образованность и осведомленность общества, а также другие меры являются важными элементами для предотвращения мошенничества и иных видов преступлений, в том числе и отмывания денег и незаконных денежных потоков в Интернете.

232. В это связи предлагается принять меры по повышению осведомленности, начиная от общественных сайтов с общей информацией или материалами о предотвращении мошенничества[173] или образовательными материалами/курсами[174] и заканчивая рекомендациями для сотрудников государственные учреждений и учреждений частного сектора или специальными ресурсами о снижении рисков в каждом отдельном секторе[175] или для оказания помощи потерпевшим[176].

172 http://www.rfc-archive.org/getrfc.php?rfc=5901&tag=Extensions-to-the-IODEF-Document-Class-for-Reporting-Phishing
http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_if09_pres_APWG_ADVISORY_Reporting_eCrime_via_IODEF.pdf

173 http://www.ic3.gov/preventiontips.aspx
http://www.stoppbetrug.ch/4/fr/1prevention_methodes_descroquerie/40201ventes_aux_encheres.php

174 См., например, http://www.polizei-nrw.de/koeln/Vorbeugung/kriminalitaet/Internet-und-datenkriminalitaet/

175 См., например, ресурсы для продавцов для предотвращения мошенничества с платежными картами

233. Например, комбинированная система сообщений об активности бот-сетей информирует пользователей о том, что их система заражена, оказывает помощь в очистке систем и мерам предупреждения. Система разработана Информационным центром по борьбе с бот-сетями www.botfrei.de, которая является инициативой государства и частного сектора, Федерального бюро по информационной безопасности и ассоциацией поставщиков услуг ECO. Система доступна на нескольких языках.

4.3 Меры регулирования и надзора

4.3.1 Меры по управлению рисками и надлежащей проверке

234. Финансовые учреждения должны разрабатывать и применять соответствующие меры для снижения возможных рисков отмывания денег в отношении определенных товаров, услуг или клиентов на основании оценки рисков. Такие меры требуют инвестиций как с точки зрения ресурсов, так и времени с тем, чтобы выявить и записать данные, связанные с определенной категорией рисков. Такие меры могут включать в себя один и более из следующих пунктов:

– повышенная осведомленность учреждения о высоко рисковых сценариях, связанных с тем или иным видом финансовых услуг/продуктов/клиентов;
– соответствующий уровень знания своих клиентов (“KYC”) или усиленные меры по надлежащей проверке;
– получение разрешения старшего руководства на установление отношений или открытие счета;
– хранение информации;
– усиленный мониторинг операций; и
– повышенный постоянный мониторинг и пересмотр взаимоотношений;

235. В то время как появлялись общие руководства о риск-ориентированном подходе для управления рисками отмывания денег[177], отдельное руководство по рискам в Интернете только разрабатывается для финансовых организаций, оказывающих услуги в Интернете.

---

http://www.visa.ca/en/merchant/fraud-prevention/index.jsp
176 См., например, http://www.actionfraud.org.uk/home
177 http://www.wolfsberg-principles.com/risk-based-approach.html

236. Одним из примеров служит Рекомендация 1 от 10 февраля 2009 г. Совета Управления финансового надзора Венгрии о рисках для Интернет-безопасности[178].

237. У финансового сектора есть перечень необходимых мер, например:

- централизованная база данных об операциях, которая может быть использована для того, чтобы соотносить операции, осуществлять анализ, выявлять подозрительные операции, создавать индикаторы и отслеживать преступную деятельность как в финансовом учреждении, так и между финансовыми учреждениями;
- анализ поведения и мониторинг активности по счетам мулов;
- стоп-лист известных или подозрительных счетов;
- обмен информацией между финансовыми учреждениями;
- принятие на вооружение целостный подход в отношении всех перемещений денежных средств в рамках одного финансового учреждения;
- реализация мер защиты для дистанционного банковского обслуживания, включая два варианта аутентификации TAN (номер авторизации транзакции) и MTAN (мобильный TAN);
- проверка документов или требования о предоставлении дополнительных документов для подтверждения личности клиента;
- требование о том, чтобы первый платеж был осуществлен между счетами, открытыми внутри страны или в другую предварительно одобренную страну;
- мониторинг и анализ выписки об операциях, совершаемых при помощи банковских карт;
- установление лимитов денежных средств, которые могут быть переведены при помощи банковских карт;
- анализ и поиск связей между банковской картой и банковским счетом, с которого/на который переводятся средства с карты;
- мониторинг операций по картам и фиксирование данных о подозрительной деятельности;
- отказ от анонимных, закодированных или номерных счетов в электронных системах или Интернете, а также счетов, предлагаемых через Интернет-банкинг банками, находящимися в офшорах.

178 Рекомендация 1 от 10 февраля 2009 г. Совета Управления финансового надзора Венгрии о рисках для Интернет-безопасности

238. Коммерческие сайты и он-лайновые платежные системы взяли на вооружение активный риск-ориентированный подход, который включает в себя применение надлежащей проверки клиентов на основании оценки риска, построение и использование моделей и программного обеспечения для выявления необычной или подозрительной деятельности на основании индикаторов, пересмотр инструкций о подозрительных операциях, приостановление операций, ведение журнала регистрации событий[179].

239. Отдельные меры, предпринятые сектором, выпускающим платежные карты, включают реализацию стандартов безопасности продавцами, процессинговыми центрами и финансовыми учреждениями[180] или руководства для продавцов об управлении рисками[181].

4.3.2 Надлежащая проверка для регистраторов и реестродержателей

240. Использование доменов в преступных целях, например, операции с бот-сетями является строительным элементом инфраструктуры для совершения киберпреступлений. Процесс регистрации доменов[182] создает возможности для предотвращения и снижения риска незаконного использования доменов преступниками.

241. Ряд рекомендаций по надлежащей проверке были подготовлены правоохранительными органами для ICANN[183].

242. Они предусматривают, что:

– ICANN осуществляет расследования и надлежащую проверку всех регистраторов и реестродержателей;
– ICANN вносит изменения в Соглашения об аккредитации регистраторов (RAA) для того, чтобы последние собирают точную и полную информацию о тех, кто регистрирует доменные имена;

179 См. меры, предпринимаемые сектором в исследовании Группы разработки финансовых мер борьбы с отмыванием денег: «Уязвимость коммерческих сайтов и он-лайн платежных систем для отмывания денег и финансирования терроризма» (июнь 2008 г.). Они обсуждались в ходе подготовки данного типологического исследования

180 Например, Стандарты безопасности данных в сфере платежных карт (PCI DSS) и связанные с ними требования https://www.pcisecuritystandards.org/security_standards/index.php

181 http://usa.visa.com/download/merchants/visa_risk_management_guide_ecommerce.

182 Для лучшего понимания этого процесса см.доклад Вольфганга Кляйнваэхтера, подготовленный для проекта Совета Европы по борьбе с киберпреступностью http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter1.pdf

183 Организация по присвоению имени и адресов в Интернете (www.icann.org)

– информация, о том кто есть кто для всех общих доменов высшего уровня (gTLD), точная и подробная и может быть предоставлена правоохранительным органам;
– ICANN требует, чтобы все те, кто перепродает доменные имена, а также третьи лица, получающие их подпадали под те же требования, что и регистраторы и реестродержатели.

243. Проект рекомендаций обсуждался на различных форумах[184] и получил поддержку Правительственным консультативным комитетом ICANN в июне 2010 г. В коммюнике ПКК (Брюссель, июнь 2010 г.) помимо всего прочего говорится о том, что:

«ПКК призывает Совет, Рабочую группу по вопросам RAA и регистраторов работать вместе с правоохранительными органами для разрешения своих проблем и внести необходимые изменения без промедления»[185].

244. К декабрю 2011 г. был достигнут прогресс лишь по некоторым рекомендациям[186].

4.4 Единая правовая система, основанная на международных стандартах

245. Создание правовой системы для криминализации деяний, связанных с перемещением преступных доходов в Интернете, эффективных расследований киберпреступлений, отмывания денег и финансирования терроризма, а также конфискации преступных доходов осуществления международного сотрудничества считается крайне важным. Положения и Будапештской, и Варшавской Конвенций помогают странам справиться с этой проблемой.

4.4.1 Реализация положений Будапештской Конвенции о киберпреступности

246. Многие страны отмечают, что реализация положений Будапештской Конвенции о киберпреступности является важной мерой,обеспечивающей

184 Включая Конференцию Совета Европы «Октопус» в 2010 г. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Ws%202/LEA_ICANN_Recom_oct2009.pdf
185 http://gac.icann.org/system/files/Brussels-communique.pdf
186 http://www.icann.org/en/announcements/announcement-2-12dec11-en.htm. Изменения будут отражены путем внесения изменений в Соглашение об аккредитации регистраторов (RAA) и иных актах. Дальнейшие обсуждения пройдут на заседании ICANN (Коста-Рика, март 2012 г.)

правосудие:

- принятие значительных положений уголовно-правового законодательства в соответствии со статьями 2-12 означает криминализацию различных деяний, когда мошенничество и иные правонарушения совершаются в Интернете. Особое значение имеют ст.2 (незаконный доступ), ст. 3 (незаконный перехват), ст. 4 (воздействие на данные), ст.5 (воздействие на систему), ст. 7 (подлог с использованием компьютерных технологий) ст.8 (мошенничество с использованием компьютерных технологий);

- реализация процессуальных мер (описанных, например, в статьях 16 и 17, т. е. оперативное обеспечение сохранности хранимых компьютерных данных, статье 18 - распоряжение о предъявлении, статье 19 - обыск и выемка, статьях 20 и 21 - перехват данных о содержании) позволяет правоохранительным органам зафиксировать изменчивые электронные доказательства наиболее оперативно. Также оговаривается сотрудничество между поставщиками услуг при проведении расследований;

- Стороны Конвенции могут использовать настоящий договор как основу для международного сотрудничества, когда одна из Сторон может попросить другую Сторону обеспечить сохранность данных, которые хранятся в компьютерной системе, расположенной на территории последней (ст.29) и для оказания оперативной международной взаимной правовой помощи (статья 31).

- Будапештская Конвенция помогает гармонизировать законодательство между странами, что является важной предпосылкой для развития международного сотрудничества. Многие страны используют этот международный инструмент в качестве руководства для доработки своего национального законодательства.

247. Среди стран, которые приняли или изменили свое законодательство — Эстония, Германия и Португалия. Пример Румынии очень полезен поскольку она очень точно следует положениям Будапештской Конвенции о киберпреступности[187].

187 Описание законодательств стран в сфере противодействия киберпреступности см. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp

4.4.2 Реализация положений Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма188

248. Положения Варшавской Конвенции содержат требование для государств-членов предпринять ряд мер, включая:

- конфискацию (статья 3), следственные и предварительные меры (статья 4), замораживание, арест и конфискацию (статья 5), управление замороженным или изъятым имуществом (статья 6), полномочия и техники для проведения расследования (статья 7);
- криминализация преступления отмывания денег (статья 9);
- создание подразделения финансовой разведки, т.е. ПФР (статья 12);
- предупредительные меры (статья 13);
- приостановление подозрительных операций внутри страны;
- международные запросы о предоставлении информации по банковским счетам (статья 17), о банковских операциях (статья 18), о мониторинге банковских операций (статья 19), реализации предупредительных мер (статьи 21 и 22), о конфискации (статьи 23 и 24).
- сотрудничество между ПФР (статья 46).

249. Реализация положений настоящей Конвенции дает возможность государственным органам предпринимать эффективные меры для выявления, изъятия и конфискации преступных доходов, для предотвращения и снижения объемов отмывания денег и финансирования терроризма и международного сотрудничества.

250. У Конвенции есть свой механизм мониторинга, который осуществляется через Конференцию Сторон с тем, чтобы гарантировать, что ее положения выполняются эффективно[189].

4.5 Создание специализированный подразделений для борьбы с преступлениями в области высоких технологий[190]

188 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=198&CM=8&DF=&CL=ENG

189 http://www.coe.int/t/dghl/monitoring/cop198/default_en.asp

190 Для того, чтобы получить информацию относительно специализированных подразделений, собранную в 2011 г. см. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

251. Многие государства создали специализированные подразделения для борьбы с киберпреступностью. Например[191]:

- Албания: в Государственной полиции, подчиняющайся Управлению по расследованию финансовых преступлений, есть два специализированных подразделения, одно из которых отвечает за расследование преступлений, совершенных при помощи компьютерных технологий (Сектор по расследованию киберпреступлений), а второе- за отслеживание преступных доходов;

– Беларусь: были созданы Департамент по финансовому мониторингу Государственного контрольного комитета (ДФМ), Подразделения по борьбе с преступлениями в сфере высоких технологий в Министерстве внутренних дел и Государственном комитете по безопасности;

– Китай: в Министерстве общественной безопасности было создано специальное подразделение для борьбы с киберпреступностью (Бюро кибербезопасности). Китайский центр по борьбе с отмыванием денег отслеживает потоки преступных денежных средств, включая и Интернет.

– Венгрия: созданы Подразделения по борьбе с киберпреступлениями Национальной бюро расследований полиции Венгрии; Управление по финансовой экспертизе HFSA, а также национального механизма по управлению инцидентами — CERT-Венгрия;

– Румыния: подразделение по борьбе с киберпреступностью было создано в Директорате по расследованию дел, связанных с организованной преступностью и терроризмом Генеральной прокуратуры при Высшем кассационном суде. Функции подразделения определены в Законе № 161/2003. Специальное подразделение по борьбе с компьютерными преступлениями осуществляет свою деятельность при Генеральной инспекции полиции Румынии (Директорат по борьбе с организованной преступностью), начиная с 2003 г.

– Словакия: Департамент по борьбе с киберпреступностью при Бюро

191 Источник: ответы, полученные на вопросник

судебной и криминальной полиции Президиума Полиции Словацкой Республики работает над методологией, тенденциями и делами, связанными с киберпреступлениями на национальном уровне;

– Бывшая югославская республика Македония: управление по борьбе с киберпреступностью и контрафактом было создано в 2005 г. как часть Сектора по борьбе с организованной преступностью. С 2008 г. данное Управление является специальным подразделением по борьбе с с киберпреступностью.

– Украина: в 2001 г. было создано специализированное управление по борьбе с преступлениями в сфере интеллектуальной собственности и компьютерных систем при Министерстве внутренних дел. Кроме того, соответствующие подразделения Службы безопасности Украины также отвечают за противодействие киберпреступлениям, в частности по противодействию шпионажу в Управлении по защите государственной экономики; подразделения Главного управления по борьбе с коррупцией и организованной преступностью Службы безопасности Украины борется с потоками преступных денег в Интернете/компьютерных системах.

252. Подразделения по борьбе с преступностью в сфере высоких технологий полицейского типа обычно выполняют следующие задачи[192]:

- Расследование киберпреступлений:
  - проведение расследований для борьбы с киберпреступлениями;
  - сбор и анализ данных и информации;
  - осуществление технической деятельности для поиска по компьютерным системам;
  -составление внутренних правил и процедур для проведения расследований киберпреступлений;
  - оказание содействия иным полицейским управлениям при проведении расследований;
  - осуществление деятельности для оказания международной судебной помощи по уголовным делам, как на международном, так и на национальном уровне;

192 Источник: Совместный проект Совета Европы/ЕС по борьбе с киберпреступностью в Грузии (2009 г.): предложения по созданию подразделения по борьбе с преступлениями в сфере высоких технологий. Документ подготовлен Найджелом Джонсом (Соединенное Королевство) и Верджил Спиридон (Румыния).

- осуществление деятельности по повышению осведомленности общества о предотвращении преступлений в сфере компьютерных технологий.

- Исследования:
  - осуществлять качественную исследовательскую деятельность относительно выявления тенденций, которые в последующем могли бы стать требованиями для борьбы с киберпреступлениями;
  - работать во взаимодействии с научными кругами и частным сектором для выработки механизмов и техник для поддержания усилий для борьбы с киберпреступлениями.

- Сбор информации:
  - осуществлять международное сотрудничество и обмен информацией с иностранными подобными органами;
  - осуществлять анализ, изучение и оценку преступных проявлений;
  - собирать информацию из открытых источников и скрытых источников в Интернете.

- Обучение:
  - разработка профессиональных обучающих программ для специалистов в сфере компьютерной криминалистики и следователей, занимающихся расследованием киберпреступлений, чтобы обеспечить рост соответствующих знаний и навыков.

253. В 2010 г. Европейский Союз создал Специальную группу ЕС по борьбе с киберпреступностью, состоящую из глав специализированных подразделений всех государств-членов ЕС. В 2011 г. эта Группа и Совет Европы совместно разрабатывали проект документа о специализированных подразделениях по борьбе с киберпреступлениями[193].

4.6 Межведомственное сотрудничество

254. Сотрудничество между ведомствами, ответственных за проведение расследований и конфискацию активов, меры по борьбе с отмыванием денег и киберпреступностью являются важным условием для успешной борьбы с преступными потоками в Интернете. Ответы на вопросник содержат ряд примеров.

193 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

4.6.1 Германия: проектная группа «Электронные платежные системы»

255. Федеральная уголовная полиция Германии (ВКА) создала проектную группу по вопросам «электронных платежных систем», ответственность за деятельность которой возложена на подразделение финансовой разведки при ВКА при участии пяти Управлений уголовной полиции (LKAs). Она состоит из экспертов в области проведения финансовых расследований, преступности в Интернете и компьютерных системах и конфискации активов, а также эксперты из Федерального управления финансового надзора (BAFIN). Перед группой стояли следующие задачи:

- выявить и проанализировать дела, связанные с электронными платежными системами путем проведения проверок национальными органами полиции;
- описание проблемных областей, с точки зрения полиции;
- описание правоприменительных подходов с точки зрения полиции и надзорных органов.

256. Проектная группа издала следующие рекомендации для использования:

- информационное письмо об общих основах функционирования электронных платежных систем для того, чтобы повысить осведомленность сотрудников полиции в Германии;
- данная тема должна затрагиваться в ходе проведения обучающих программ для офицеров полиции, занимающихся финансовыми расследованиями, расследованиями преступлений в Интернете и компьютерных системах и конфискации активов;
- ПФР также опубликовало Информационное письмо, разместив его на своем сайте;
- тесное взаимодействие с провайдерами услуг он-лайновых платежей также играет важную роль, как и наличие контактных точек;
- сотрудничество между полицией и надзорными органами должно быть также усилено; то же самое касается и существующего сотрудничества между BAFIN и ВКА/ПФР;
- обмен информацией между надзорными органами между надзорными органами играет важную роль, например, для выдачи совместных запретов в отношении поставщиков услуг он-лайновых платежей, которые не проводят авторизацию;
- международный надзор за провайдерами должен быть усилен. Это не та проблема, которая может быть решена на национальном уровне.

- Данный вопрос должен обсуждаться международными органами, например, ФАТФ.

257. Более того, ВКА создала информационный фонд по электронным платежным системам, которые органы полиции могут оценить на национальном уровне. Однако создание и ведение такой базы данных на международном уровне было бы более целесообразно.

4.6.2 Албания: меморандумы о сотрудничестве

258. В Албании два меморандума о сотрудничестве были заключены между органами прокуратуры, полиции, таможни, налоговой службы, банком и Главной инспекцией по декларированию и аудиту активов, подразделением финансовой разведки и Национальной разведывательной службой. Было создано семь специальных групп по борьбе с коррупцией и финансовыми преступлениями в следующих округах: Тирана, Дуррес, Шкодер, Фиер, Влора, Корча и Гирокастра.

4.7 Сотрудничество между государственным и частным сектором и обмен информацией

259. Сотрудничество между государственным частным сектором, а также обмен информацией является, возможно, одной из мер, имеющих сильное влияние на предотвращение и контроль потоков преступных доходов в Интернете. Это разрешает одну из ключевых проблем, а именно ограниченный информационный обмен между финансовыми учреждениями внутри страны, а также между финансовыми учреждениями и правоохранительными органами.

260. Таким образом, большое количество примеров было приведено в ответах на вопросник и других источников не случайно большая часть примеров описывает взаимодействие и обмен информацией на национальном уровне. Было бы желательно усилить взаимодействие и обмен информацией между обоими секторами на международном уровне.

261. Дальнейшее сотрудничество между государственным и частным сектором может помочь решить основную проблему для всех видов киберпреступлений, а именно отнести конкретное преступное деяние к

конкретному человеку.

4.7.1 Форум по борьбе с преступлениями в области высоких технологий Федерации ирландских банкиров (ФИБ)

262. Форум состоит из лиц, занимающих руководящие должности и на которых возложены обязанности по обеспечению информационной безопасности, управлению рисками и борьбе с мошенничеством, представляющих все розничные банки, осуществляющие свою деятельность в Ирландии, и предлагающие услуги по дистанционному банковскому обслуживанию:

- Ирландская полиция;
- Полиция Северной Ирландии;
- Организация Ирландии по платежным услугам;
- Ассоциация Интернет-провайдеров Ирландии;
- Центр Университетского колледжа Дублина по расследованию киберпреступлений (UCD CCI)

263. Форум по борьбе с преступлениями в сфере высоких технологий собирается один раз в два месяца для обмена информацией о последних и зарождающихся угрозах, а также для того, чтобы сформулировать подход для борьбы с угрозами в сфере высоких технологий при оказании он-лайновых банковских услуг в Ирландии;

264.Одним из главных успехов Форума стала совместная попытка полиции Ирландии и UCD CCI выявить угрозы для банковских и платежных услуг, которые имеют место в других юрисдикциях для того, чтобы оценить угрозу возможных атак и защититься от них до того, как банки, осуществляющие свою деятельность в Ирландии, не понесли убытки. Регулярные отчеты о появляющихся угрозах направляется в адрес Форума.

265. Важным достижением Форума стало установление доверия между всеми участниками, что дало им возможность обмениваться информацией. В то же время члены форума должны осознавать, что вопросы борьбы, с киберпреступностью, выявление данной категории преступлений и реагирования на них не является вопросами конкуренции.

266. Также должно быть общее понимание того, что даже если под ударом находится один из членов Форума, то это может также случиться и с

другими в любое время.

267. Иной аспект передового опыта, реализованного Форумом по борьбе с преступлениями в области высоких технологий ФИБ, это работа на упреждение зарождающихся кибер-угроз. UCD CCI проводит исследование от имени Форума. Члены форума определи аспекты, которые вызывают к у них озабоченность, а также приоритетные направления исследования, установленные правоохранительными органами, а UCD CCI в свою очередь проводит исследование. Это процесс, состоящий из:

- вовлеченности всех членов Форума;
- советов правоохранительных органов и получения указаний относительно направления;
- использования опыта UCD CCI;
- проведения на территории огромного количества исследований.

268. Основная цель исследования, проводимого UCD CCI для Форума, - это выявление новых рисков в других юрисдикциях, до того как они появятся в Ирландии с тем, чтобы ирландские банки смогли оценить риски и предпринять соответствующие превентивные меры до того, как кто-нибудь понесет потери.

269. UCD CCI также пытается изучить то как реагирует частный сектор на угрозы, появившиеся несколько месяцев назад с тем, чтобы определить те места, где необходимо более тесное сотрудничество между членами.

4.7.2 Венгрия: Рабочая группа по управлению инцидентами

270. В Венгрии рабочая группа по управлению и наблюдению за инцидентами в Интернете была создана при участии банков, правоохраны (Национальное бюро расследований), Группы реагирования на нарушения компьютерной защиты в сети Интернет (CERT-Венгрия[194]) и Управления финансового надзора Венгрии (HFSA)[195]. Ситуация анализируется по меньшей мере четыре раза в год; также оцениваются новые способы совершения преступлений для выработки адекватных превентивных мер.

194 http://www.cert-hungary.hu/en
195 http://www.pszaf.hu/en/

Раз в году проводятся практические занятия, симулирующие атаку и реагирование на нее.

271. Профессиональный протокол реагирования на фишинг-атаку (в случае атаки: с кем связаться в полиции и финансовом учреждении, как сотрудничать, виды и структура информации, которой необходимо обменяться и т.д.) был разработан при участии полиции и экспертов кредитных учреждений для обеспечения быстрого и эффективного реагирования.

4.7.3 Американский национальный альянс по компьютерной криминалистике и подготовке NCFTA[196]

272. Основная цель созданной в 1997 г. NCFTA - это выявление преступников, ответственных за кибер-атаки. Это канал для обмена информацией между частным сектором и правоохранительными органами, включая предприятия малого и среднего бизнеса.

273. Отдельные инициативы включают в себя:

- CyFin – форум по борьбе с он-лайновыми схемами манипулирования на фондовом рынке;
- Решиппинг - инициатива по борьбе с сокрытием настоящих получателей товаров, приобретенных при помощи украденных персональных данных ;
- Цифровой фишнет - сбор информации о значимых и сложных фишинговых схемах;
- Аптека – нейтральный форум для обмена информацией между частным сектором и правоохранительными органами о незаконных он-лайн продажах медикаментов и иных угрозах;
- Система оповещения о мошенничестве в Интернете центральная клиринговая палата и механизм тревоги для сообщения о взломанных персональных данных.

4.7.4 Центры анализа и обмена информации (ISAC) для финансовых служб

274. В США «Финансовые услуги — Центры анализа и обмена информации»

196 http://www.ncfta.net/

(FS-ISAC)[197] - это американский форум для сотрудничества по важным (материальным и виртуальным) угрозам безопасности финансового сектора. Он собирает и анализирует информацию и предупреждает организации-члены об опасности и атаках для того, чтобы финансовый сектор смог подготовиться к ним. Для этого FS-ISAC сотрудничает с Министерством финансов США и является оперативным подразделением Координационного совета сектора финансовых услуг (FSSCC).

275. Виды информационных бюллетеней:

- информационный бюллетень для частного сектора о мошенничестве: присвоение и использование счетов компании (октябрь 2010 г.)[198];
- информационный бюллетень для потребителей о мошенничестве: участие в преступных схемах через надомную работу (октябрь 2010 г.)[199];
- распределенная атака типа отказа в обслуживании (DDOS): обзор и анализ (июнь 2010 г.) [200].

277. Подобные центры были созданы и в других странах[201].

278. Например, в Голландии в 2006 г. было создано подразделение по типу ISAC - «Обмен информацией о киберпреступности». Оно было создано как часть Национальной базы по борьбе с киберпреступностью (NICC), которая в свою очередь является государственно-частным партнерством[202]. Первым, кто присоединился к информационному обмену, были финансовые службы (FI-ISAC)[203]. Это создало основу для обмена информацией между Агентством национальной полиции (KLDP), Главной службой разведки и безопасности (AIVD), Правительственной группой реагирования на компьютерные угрозы (GOVERT.NL), банками, и банковской ассоциацией Голландии и NICC как координатором. Проводится около восьми встреч в году, в ходе которых участники обмениваются информацией, разбирают предпринимаемые меры, а также осуществляют мониторинг, в случае наличия угроз.

197 http://www.fsisac.com/
198 http://www.fsisac.com/files/public/db/p265.pdf
199 http://www.fsisac.com/files/public/db/p264.pdf
200 http://www.fsisac.com/files/public/db/p244.pdf
201 Для анализа угроз, которыми занимается ISACs, см. http://www.unixworks.net/papers/wp-017.pdf . См также http://www.surfacetransportationisac.org/SupDocs/Library/ISAC_Products/isac_role_in_cip.pdf
202 http://www.samentegencybercrime.nl/
203 http://www.samentegencybercrime.nl/Informatie_knooppunt/Sectorale_ISACs/FIISAC?p=content. Центры других секторов: Водный-ISAC, Энергетический-ISAC, Ядерный-ISAC и т.д.

279. Создание FI-ISAC на европейском уровне обсуждается с 2008 г.[204]

4.7.5 Европейская финансовая коалиция против коммерческой сексуальной эксплуатации детей в Сети[205]

280. Европейская финансовая коалиция была учреждена в 2009 г. в качестве партнерства между финансовыми, технологическими и Интернет-корпорациями и органами полиции для «выявления, разрушенияи конфискации активов» тех, кто извлекает прибыль из распространения материалов, содержащих сцены насилия над детьми. 14-ти месячный пилотный проект финансировался при поддержке Европейского Союза.

281. Было создано пять рабочих групп:

– Рабочая группа по взаимодействию между правоохранительными органами;
– Рабочая группа по выявлению платежных систем и их мониторингу [206];
– Правовая рабочая группа;
– Рабочая группа по Интернет-технологиям;
– Рабочая группа по предотвращению и повышению осведомленности.

282. Помимо всего прочего был подготовлен документ, содержащий передовой опыт по предотвращению появления и выявлению изображений со сценами насилия над детьми в коммерческих целях[207].

4.7.6 Специальные группы по борьбе Е-преступностью (секретная служба США)[208]

283. В октябре 2011 г. сеть Специальных групп по борьбе с Е-преступлениями, а также Рабочие группы были созданы в США на федеральном уровне,

204 http://www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/presentations/wim http://www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/copy_of_agenda-of-theinformation-sharing-workshop http://www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/copy_of_agenda-of-theinformation-sharing-workshop

205 http://www.ceop.police.uk/EFC/Public-Library/Latest-News/Conference-Roundup/

206 В этой группе сопредседательствуют «Visa» и “MasterCard”. В нее входят представители ряда ключевых компаний, обрабатывающих платежи. Эта рабочая группа должна обобщить передовой опыт Европы, описывающий те правила и процедуры, который не позволяет преступникам воспользоваться платежными системами. Группа также старается определить пути улучшения взаимодействия и информационного обмена между финансовыми учреждениями и правоохранительными органами.

207 http://www.ceop.police.uk/Documents/Finan%20Best%20Pract2010_080910a.pdf

208 http://www.secretservice.gov/ectf.shtml

уровне штатов и местном уровне для предотвращения, снижения числа и расследования атак на финансовые и важные инфраструктуры. Они объединили правоохранительные органы, органы прокуратуры, частный сектор и научные круги.

284. Расследование было сосредоточено на приоритетных делах, которые отвечали следующим критериям:

– значительные экономические и социальные последствия;
– участие организованных преступных групп, включая те, которые охватывают несколько округов или действуют на международном уровне;
– схемы с использованием новых технологий.

4.7.7 Европейская группа по борьбе с Е-преступностью (EECTF)[209]

EECTF была создана в июне 2009 г. в результате соглашения между Почтой Италии, Полицией Италии и Секретной службой США. Определены следующие задачи:

«Содействие в проведении анализа и разработки передового опыта по борьбе с киберпреступностью в странах Европы путем создания стратегического союза правоохранительных органов, научных и правовых кругов, а также учреждений частного сектора».

Ряд европейских правоохранительных органов, финансовый сектор, учреждения, занимающиеся вопросами безопасности в Интернете, а также научные институты присоединились к этой группе за это время.

4.7.8 Инициатива против киберпреступности для частного сектора и правоохранительных органов (CICILE)[210]

285. CICILE — защищенная Интернет-платформа, созданная Европейской Комиссией для обеспечения обмена и распространения информации о предотвращении киберпреступлений и борьбы с ними между основными участниками, то есть правоохранительными, государственными органами, частным сектором и НПО. Поскольку деятельность сообщества

209 В феврале 2011 г. EECTF опубликовало «Обзор киберпреступности в Европе, который в большей части касался кибер-мошенничества.
См. http://www.gcsec.org/sites/default/files/doc/CYBER_CRIME_survey.pdf
210 Информация предоставлена Европейской Комиссией

финансируется Европейской Комиссией, то оно доступно только для государств-членов.

286. CICILE создана на основе платформы SYNAPSE. SYNAPSE — это Интернет-платформа, предлагающая механизм оптимального использования опыта в разработке стратегий ЕС и управления ими (образование сетей консультативных органов, оказание содействия экспертным группам, проведение специальных/общественных обсуждений и е-дебатов и т. д.). SYNAPSE — это общественная услуга, предоставляемая Европейской Комиссией. SYNAPSE позволяет создать «е-Сообщества», которые позволяют группам членов и организаций со схожими интересами обмениваться информацией в определенной обстановке , которая предусматривает персонализацию и связь с сайтом инициатора.

4.7.9 Руководства по сотрудничеству между правоохранительными органами и ISP для борьбы с киберпреступностью

287. Сотрудничество между правоохранительными органами и Интернет-провайдерами играет важную роль при проведении расследований киберпреступлений.

288. В 2008 г. в ходе Конференции «Октупус», организованной Советом Европы и Международным проектом по борьбе с киберпреступностью были приняты руководящие принципы[211] для того, чтобы помочь правоохранительным органам и ISPs построить свое сотрудничество более структурировано. Они:

- включают в себя общие руководства для правоохранительных органов и провайдеров, а также отдельные для каждой из сторон;
- не нацелены на замену законодательства или иных нормативных требований, а лишь дополняют и помогают их реализации на практике;
- основаны на доступном полезном опыте;
- могут быть адаптированы под определенные условия каждой страны.

289. На практике представители правоохранительных органов и провайдеров любой из стран могут создать рабочую группу для достижения понимания

211 http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

или заключения официального соглашения о сотрудничестве. Руководства могут служить предварительным планом или просто основой для обсуждения.

290. После принятия этих руководств в апреле 2008 г.:

- Европейский суд по правам человека в своем решении по делу К.Ю. ротив Финляндии (заявление №2872/02) сослался на них, а особенно на необходимость «культурного взаимодействия» между правоохранительными органами и ISPs[212];
- в 2008 г. Совет министров юстиции и внутренних дел Европейского Союза[213] рекомендовал Европейской Комиссии осуществлять свою деятельность на основании руководств, принятых Советом Европы, и принял к сведению восемь отдельных рекомендаций;
- в январе 2009 г. Правительство Румынии приняло решение о том, что судебные, правоохранительные органы и регуляторы должны использовать эти руководства. Они были размещены на сайтах Министерства юстиции, Генеральной прокуратуры, Министерства внутренних дел и др.;
- Министерство внутренних дел Франции и Ассоциация Интернет-провайдеров Франции (AFA) разработали проект соглашения на основании руководств;
- в июле 2009 г. в Украине была создана рабочая группа для того, чтобы заключить соглашение между правоохранительными органами и провайдерами;
- в Индии руководства были представлены правоохранительным органам и частному сектору (март 2009 г.) для того, чтобы внести изменения в Закон «Об информационной технологии», принятый Парламентом в декабре 2008 г. (см. презентацию);
- в мае 2010 г. в Грузии был подписан меморандум о взаимопонимании между Министерством внутренних дел и ISPs.

4.8 Обучение

212 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/1429_ECHR_CASE_OF_K.U._v%20Finland.pdf
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp
Для интересных примеров саморегулирования см. Интернет-сборник полезного опыта Австралии http://iia.net.au/images/resources/pdf/icode-v1.pdf

213 http://www.eu2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf

4.8.1 Европейская группа по образованию и обучению для борьбы с киберпреступностью (ECTEG)[214]

291. У Группы есть зарегистрированные обучающие материалы по борьбе с киберпреступлениями, разработанные для различных программ Европейского Союза обучения правоохранительных органов, включая:

- двухнедельный вводный курс основных навыков для судебных следователей;
- криминалистика и NTFS;
- Сетевые расследования;
- Интернет-расследования;
- программа Linux как важный инструмент проведения расследования;
- беспроводная ЛВС и протокол VoIP;
- криминалистика и мобильные телефоны;
- криминалистика и оперативная информация (на стадии разработки);
- создание сложных сценариев (на стадии разработки);
- проведение расследований и вредоносные программы (на стадии разработки);
- криминалистика и “Visa” (должна была быть разработана в 2010 г.);
- сбор данных и базы данных (должна была быть разработана в 2010 г.);
- усложненный уровень курса «Криминалистика и мобильные телефоны».

292. Университетский колледж Дублина (Центр по расследованию киберпреступлений) продолжает лицензировать обучающие программы, которые реализуются под патронажем ECTEG.

4.8.2 Центр Университетского колледжа Дублина по расследованию киберпреступлений (UCD CCI)

293. UCD занимается гармонизацией обучающих программ для правоохранительных органов в сфере борьбы с киберпреступлениями с 2001 г. CCI был официально создан в 2006 г. Среди его задач:

- разработка, распространение и внедрение сертифицированных обучающих программ для следователей, занимающихся расследованием

214 http://www.ecteg.eu/

киберпреступлений, и специалистов по вопросам безопасности, в обязанности которых входит предотвращение и расследование преступлений в сфере высоких компьютерных технологий;

- проведение практических и теоретических исследований по вопросам киберпреступности и публикация результатов для использования следователями, занимающимися расследованиями киберпреступлений, и специалистами по вопросам безопасности, в обязанности которых входит предотвращение и расследование преступлений в сфере высоких компьютерных технологий;
- сотрудничество с стальными участниками процесса для предотвращения совершения киберпреступлений и их выявления.

294. CCI успешно взаимодействует с правоохранительными органами и частным сектором как на национальном, так и на международном уровне.

295. Одним из реальных результатов является взаимодействие правоохраны на уровне магистров наук при проведении расследований киберпреступлений и судебной обработки данных, проводимой UCD CCI. На сегодняшний день прошли обучение или зачислено на курсы 110 слушателей из Ирландии, Соединенного Королевства, Германии, Франции, Италии, Греции, Испании, Норвегии, Швеции, Голландии, Румынии, Дании и Кипра. Кроме слушателей из Европы были студенты из Ганы, ОАЭ, Китая, Японии, США, Канады, Новой Зеландии, Сингапура и Гонконга. Это было кульминацией усилий, предпринимаемых последние 15 лет, по гармонизации обучения для правоохранительных органов. Одним из достижений этой программы является сообщество выпускников, а также тот факт, что сотрудники правоохранительных органов иных государств содействуют международному сотрудничеству.

296. Предполагается, что правоохранительные органы любого государства должны иметь минимальные возможности для реагирования на киберпреступления. Обучающие программы — это необходимое условие.

4.8.3 Юго-восточная Европа — стратегии обучения для правоохранительных органов

297. В рамках реализации совместного проекта Совета Европы и Европейского Союза CyberCrime@IPA странам оказывается содействие в разработке всеобъемлющих стратегий обучения правоохранительных

органов в части проведения расследования по преступлениям, совершенным с использованием компьютерных технологий и обучению компьютерной криминалистике [215].

4.8.4 Концепция программы Совета Европы по обучению судей и прокуроров

298. Одним из уроков, вынесенных в результате реализации стратегий противодействия отмыванию преступных доходов и финансированию терроризма, стала необходимость обучения судей. Основываясь на предположении, что необходимо приложить усилия для того, чтобы судьи и прокуроры осуществляли преследование и выносили решения по делам о киберпреступлениях, а также использовали электронные доказательства через обучение, объединение в сети Совет Европы при поддержке Международного проекта по борьбе с киберпреступностью и Лиссабонской сети по обучению судей в 2009 г. принял «концепцию программы обучения судей и прокуроров»[216].

299. Ее цель — помочь организациям, осуществляющим обучение судей, разработать программы по борьбе с киберпреступностью и работе с электронными доказательствами для судей и прокуроров и интегрировать ее регулярную первоначальную программу обучения, а также программу повышения квалификации. Элементы концепции включают в себя:

- внедрение первоначального обучения;
- внедрение повышения квалификации;
- стандартные и воспроизводимые курсы/модули;
- доступ к обучающим материалам, а также материалам для самостоятельного обучения;
- пилотные центры для первоначального и углубленного обучения;
- углубление знаний через создание сетей;
- взаимодействие государственного и частного секторов.

300. В настоящее время концепция реализуется, например, в странах Юго-

215 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf

216 http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Training/default_en.asp

Восточной Европы при поддержке CyberCrime@IPA[217].

217 См. www.coe.int/cybercrime

5. Результаты

301. Поскольку киберпреступность получает широкое распространение и создает условия для получения больших сумм преступных доходов, то исследование и полученная информация указывает на то, что данных об отмывании денег и примеров успешных расследований недостаточно. Кибер-отмывание — это все еще проблема для правоохранительных органов. Эти результаты приводятся для того, чтобы помочь лицам, вырабатывающим стратегии, и регуляторам определить те проблемы, которые могут быть разрешены через принятие законодательных мер, осуществление надзора, эффективные меры и руководства для их реализации. Они также предназначены для того, чтобы правоохранительные органы и подразделения финансовой разведки вносили свой значимый вклад в анализ, выявление и расследование случаев отмывания преступных доходов от киберпреступлений. Кроме того, они призывают усилить сотрудничество между государственным и частным сектором.

5.1. Киберпреступность и криминальные денежные потоки

302. Киберпреступность с учетом определения, данного в Будапештской Конвенции, состоит из (a) преступлений против компьютерных систем и данных и (b) преступлений, совершенных при помощи компьютерных систем и данных.

303. Основные инструменты и инфраструктура киберпреступности включает в себя вредоносные программы, бот-сети, незаконное использование доменов, теневую экономику, предоставляющую товары и услуги, в частности, денежных мулов, которые являются важной частью движения преступных активов и отмывания денег в Интернете. Социальные сети и облачные компьютерные услуги создают новые основы для киберпреступности и новые проблемы для правоохранительных органов. Сложные мошеннические операции и такая инфраструктура указывают на участие организованных преступных групп.

304.Может показаться, что извлечение прибыли — основная цель киберпреступлений и что большие объемы преступных денежных средств вращаются в Интернете. Мошенничество — это то киберпреступление, о

котором сообщается наиболее часто. В частности, оно включает в себя мошенничество, совершенное при помощи украденных персональных данных (с использованием фишинга и других методов социального инжиниринга для кражи информации), платежных карт, атак на он-лайн-банкинг, незаконное использование номера счета, массового маркетинга, аукционов и иных видов злоупотребления доверием, инвестиционного мошенничества, а также пирамид и иных сетевых схем. Помимо мошенничества существует коммерческое использование материалов со сценами насилия над детьми, подделка медикаментов, преступления, связанные с нарушением авторских прав, мошенничества на сайтах знакомств, незаконные азартные игры, вымогательство и иные преступления, распространенные в физическом мире, приносящие доход, который потом перемещается и отмывается.

305. Можно ожидать, что если общество и дальше будет полагаться на всемирные информационные технологии и сети, то все преступления, особенно направленные на получение прибыли станут окончательно транснациональными и будут привлекаться такие технологии и электронные доказательства тем или иным образом, то будут расти объемы преступных потоков и отмывания денег в Интернете. Общество (государственные учреждения и учреждения частного сектора) должны быть готовы к этому.

5.2. Отмывание денег и вопросы киберпреступности

306. Что касается киберпреступности и отмывания денег, то основные выводы можно изложить следующим образом:

- финансовые последствия киберпреступности и размер соответствующих доходов (которые отмыты или снова инвестированы в развитие новых инструментов и техник для преступных целей) невозможно определить количественно, т. к. отсутствуют проверенные данные и исследования;
- примеры указывают на то, что доходы от киберпреступлений отмываются через сложные схемы с использованием как традиционных (безналичные переводы, снятие наличных, переводы денежных средств), так и новые платежные технологии (е-валюты, он-лайновые платежные системы);

- поскольку он-лайновые платежные услуги неизбежно используют хотя бы один элемент традиционно финансовой системы (наличные, банки, кредитные карты и т. д.), то киберпреступность и кибер-отмывание так или иначе негативно влияют и на традиционную финансовую систему. Однако преступники нашли способ для передачи товаров или выпуска их в оборот, минуя традиционную финансовую систему;
- Интернет-системы по переводу денежных средств наряду ч традиционной банковской системой используются для кибер-мошенничества и отмывания денег. Поставщики услуг по переводу денег как традиционные, так и он-лайновые часто становятся жертвами атак, но в то же время их услугами пользуются для отмывания денег. Некоторые он-лайновые платежные методы более уязвимы для отмывания денег, чем другие;
- преступники предпочитают переводить ценности между лицами в различных странах в виде битов и байтов, а не банкнот. Контрабанда наличных денежных средств практически не упоминается или просто не выявляется. Денежные мулы используются для того, чтобы «прервать цепочку» чаще, чем для трансграничного перемещения наличных;
- данные указывают на то, что в отличии от «традиционных» организованных преступных групп, которые довольно стабильны по своей структуре, группы киберпреступников - «пластичны». Случайные группы, сети или краткосрочные союзы создаются без привязки к какой-либо местности или специализации преступника. Услуги, предлагаемые на теневом рынке, приводят к тому, что преступникам нет необходимости обладать какими-либо специальными знаниями или навыками;
- в странах, принимавших участие в исследовании, уровень осведомленности о рисках, связанных с новыми платежными системами, услугами, и связанным с отмыванием денег, низок;
- наиболее уязвимые услуги и секторы для кибер-атак — это платежные сервисы и финансовые учреждения. Они подпадают под основной удар, т. к. и физические, и юридические лица все больше полагаются на он-лайновые системы в своей ежедневной жизни;
- очевидно, что существует риск того, что не выявление киберпреступлений или низкий уровень их выявления в странах, участвовавших в исследовании, связан прежде всего с невысоким уровнем осведомленности или репутационных факторов. Все это напрямую влияет на отсутствие информации о финансовых расследованиях или

расследованиях отмывания денег;

- недостаточное количество положений, криминализирующих киберпреступления[218], может привести к исключению киберпреступлений из квалификации по отмыванию денег ;
- хотя стратегии ПОД/ФТ является важным элементом для отслеживания преступных доходов, национальные стратегии ПОД/ФТ могут не сочетаться со стратегиями по борьбе с киберпреступлениями, разделяя таким образом предпринимаемые усилия для предотвращения кибер-отмывания и борьбы с ним;
- расследование и преследование по делам об отмывании денег и киберпреступлениях сложны и длительны. Учитывая большое количество составляющих, трудности в сопоставлении мелких дел для выявления крупных преступных сетей, трудности в получении электронных доказательств, находящихся на территории другого государства, то можно сделать вывод о том. Что существует огромное количество препятствий для проведения финансового расследования. Во многих странах разрешается проводить расследование дела о совершении киберпреступления, только если отбрасывается финансовый аспект или аспект, связанный с отмыванием денег. Это может объяснить низки уровень расследований дел об отмывании денег от киберпреступлений;
- отсутствует соответствующих правил в сфере ПОД/ФТ, регулирующих деятельность он-лайновых платежных систем. Законодательно закрепленные требования, адресованные всем он-лайновым платежным системам, в сфере ПОД/ФТ в части «знать своего клиента», НПК и обязательств по направлению сообщений, может снизить риски ОД в этом секторе;
- не только слабое законодательство, но различные подходы, применяемые в той или иной юрисдикции, способствуют использованию он-лайновых платежных сервисов для отмывания денег;
- различные источники (ФАТФ, ФИНСЕН, МАНИВЭЛ, ответы стран) ссылаются на различные электронные или он-лайновые платежные системы методы, используя разную терминологию (е-платеж, Интернет-платежные системы, е-валюта, новые платежные методы и т. д.). Очевидно, что не существует общей терминологии, поэтому иногда приходится упоминать лидера рынка или известного провайдера, чтобы понять, о каком

218 Для общих минимальных стандартов криминализации каждым государством соответствующих преступлений см. Конвенцию Совета Европы против киберпреступности (СДСЕ 185) на http://conventions.coe.int

конкретно платежном сервисе идет речь;

– что касается правоохранительных органов и органов прокуратуры, то необходима специализация сотрудников, что и делается в некоторых юрисдикциях. Но это в большей степени исключение, чем правило. В случае ПФР целевые программы по киберпреступности и кибер-отмыванию, включая изучение механизмов, стоящих за он-лайновыми платежными системами , должны носить обязательный характер.

5.3 Выводы и направления развития

307. В части контрмер документ с полезным опытом уже доступен и взят на вооружение как государственным, так и частным сектором. Это должно стимулировать другие страны и учреждения защитить своих граждан и финансовую инфраструктуру. Следующие области имеют потенциал для наращивания дальнейших усилий и внесения вклада в усилия, предпринимаемых для предотвращения отмывания денег и борьбы с ним:

308. *Адекватная исследовательская работа и меры для предотвращения или снижения рисков ОД/ФТ, а также кибер-рисков*. Существует срочная потребность провести капитальное исследование, которое охватывало бы и отмывание денег и киберпреступность, с должным рассмотрением всех аспектов, включая природы и масштабы, характерные черты преступников и вспомогательные средства, а также «слабые места» и зарождающиеся угрозы. Заполнение пробелов за счет будущих исследований также поможет выявить соответствующие стратегии и меры, необходимые для предотвращения или снижения рисков ОД/ФТ от киберпреступлений, соотносясь с существующими рисками. Это также приведет к повышению осведомленности представителей частного сектора и государственных учреждений об инструментах, техниках и операциях, чтобы определить те, которые в первую очередь уязвимы с точки зрения ОД/ФТ, что в результате повысит возможности для выявления как по делам о киберпреступлениях, так и по делам об отмывании денег. Управление рисками в частном секторе должно быть расширено с тем, чтобы охватить риски, связанные с Интернетом.

309. *Стратегии ПОД/ФТ и борьбы с киберпреступлениями*. Взаимосвязь между национальной стратегией в сфере ПОД/ФТ, в частности отмыванием денег от киберпреступлений и он-лайновыми платежными системами

также была указана для направления усилий особенно для тех стран, которые пострадали от этого. Положения многих стратегий по компьютерной безопасности указывают на то, что финансовый сектор, является важной частью инфраструктуры, которую нужно защищать от кибер-атак. Однако они не охватывают вопрос преступных доходов. По этой причине было принято решение сделать финансовые расследования и меры борьбы с отмыванием денег финансовой частью стратегии по противодействию киберпреступности[219].

310. *Принятие и реализация всеобъемлющего законодательства и международных стандартов в данной сфере.* Также важно в этом контексте обновлять национальное законодательство с тем, чтобы охватить киберпреступность, отмывание денег и процессуальные меры с тем, чтобы обеспечить сохранность, поиска и изъятия электронных доказательств, а также содействовать международному сотрудничеству в соответствии с положениями Будапештской Конвенции (СДСЕ 185) и Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма (СДСЕ 198). В этой связи нужно уделить должное внимание реализации пересмотренных Рекомендаций ФАТФ, особенно тех, которые имеют отношение к оценке рисков, новым технологиям, переводам денежных средств и ценностей, безналичным переводам и т.д.[220]

311. *Создание четких механизмов и стимулов для того, чтобы общество сообщало о мошенничестве и иных преступлениях, совершаемых в Интернете и направленных на извлечение прибыли или о киберпреступности при этом учитывая требования о защите частной жизни и ответственности.* Такой механизм направления сообщений позволит определить не только общие тенденции и угрозы, но и проанализировать преступную деятельность и схемы преступных денежных потоков и отмывания денег, а также предпринять действия со стороны судебных органов и подразделений финансовой разведки для проведения расследования по таким делам и осуществления преследования.

219 См. предложения, внесенные Международным проектом Совета Европы по борьбе с киберпреступностью http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

220 См. www.fatf-gafi.org

312. *Руководства и типологии*. Руководства для финансовых и нефинансовых учреждений, которые подпадают под требования о ПОД/ФТ сообщать о подозрительных операциях или операциях с денежными средствами, в отношении которых есть основания полагать, что последние получены от преступной деятельности и могут содержать в себе элементы киберпреступлений, что ведет к обязанности направлять сообщение в соответствии с национальным законодательством (т.е. авансовые мошенничества, взлом компьютеров, кибер-вымогательство, кража идентификационных данных, продажа краденных или поддельных товаров через Интернет, мошенничество с кредитными картами, кибер-отмывание и т.д.), специальные руководства по индикаторам риска и определения подозрительного поведения, примеры, техники и типологии ОД/ФТ, выявленные на национальном уровне и любая информация, которая может помочь сообщающим организациям выполнить свои обязательства в сфере ПОД/ФТ. В рамках финансового учреждения должно уделяться вниманиям таким методам, как описание поведения, мониторинг движения денежных средств по счетам денежных мулов, стоп-листы известных или подозрительных счетов, которые могут помочь выявить преступные денежные потоки.

313. *Создание специализированных подразделений по борьбе* с *киберпреступностью*. Во многих странах в течение последних десяти лет были созданы специальные подразделения по борьбе с преступлениями в сфере высоких технологий и подразделения кибер-экспертизы. Значимость таких подразделений и нагрузка на них возрастет, и им понадобятся ресурсы.

314. *Межведомственное взаимодействие особенно через проведение параллельных расследований киберпреступлений* и *отмывания денег*. Киберпреступления и отмывание денег затрагивает обязательства ряда институтов. Межведомственное взаимодействие, в частности, между органами, проводящими финансовые расследования, расследования преступлений в сфере высоких технологий, и подразделениями финансовой разведки играет важную роль особенно в части преступлений, направленных на извлечение преступных доходов. Должен быть рассмотрен вопрос об участии следователей в деятельности постоянных и временных следственных групп, специализирующихся на расследовании

киберпреступлений и возвращении активов[221]. У подразделения финансовой разведки могут иметь не только доступ к информации и разведывательным данным, но и проводить анализ возможностей, что привнесет дополнительный вклад и заполнит информационные пробелы в ходе проведения расследования дел об ОД, связанных с киберпреступлениями и незаконными денежными потоками[222]. Возможности подразделений финансовой разведки в этой связи в части обмена информацией с иными участниками процесс или сотрудничества может подпасть под ограничения, национального законодательства и должны быть пересмотрены, особенно в таких юрисдикциях, которые подвержены этому явлению[223]. Во многих юрисдикциях прокуроры могут играть главную роль в координации деятельности различных органов при проведении расследований.

315. *Развитие сотрудничества между государственным* и *частным сектором* и *обмена между ними информацией*. Исследование показало, что эта та сфера, где может быть достигнут значительный прогресс. Должен быть рассмотрен вопрос о создании надежных площадок для обмена обычной и разведывательной информацией между финансовым сектором, органами правосудия «антиотмывочными» органами.

316. *Обучение представителей органов правосудия, «антиотмывочных» органов аспектам, связанным* с *противодействием киберпреступности* и *сбором электронных доказательств*. Учитывая возрастающее количество киберпреступлений и электронных улик, то они должны быть включены в программы обучения для правоохранительных и судебных органов. Необходимость обучать судей – это ключевой урок, который был усвоен при проведении расследований по делам об отмывании денег и финансировании терроризма. Кроме того, должно проводиться дополнительное обучение по преступным денежным потокам в Интернете для основных участников, включая ПФР.

317. *Международное сотрудничество*. Связь между мерами противодействия отмыванию денег и финансированию терроризма/финансовыми

[221] В дополнение к Рекомендации 30 ФАТФ (пересмотренные в феврале 2012 г.)

[222] Рекомендации 30 и 31 (пересмотренные в феврале 2012 г.) призывают сотрудничать и обмениваться информацией между ПФР и правоохранительными органами, включая следователей, расследующий преступления, совершенные с помощью компьютерных технологий

[223] Как изложено в Рекомендации 31 (пересмотренные в феврале 2012 г.)

расследованиями и расследованиями киберпреступлений и компьютерной криминалистикой дает дополнительные возможности для международного сотрудничества. Международные стандарты, например, Конвенция Совета Европы СДСЕ 198, Рекомендации ФАТФ или Будапештская Конвенция против киберпреступности создают основы для сотрудничества, которые не используются в полном объеме[224]. Например, дополнительные меры для международного сотрудничества при проведении расследования по делам об отмывании денег и финансировании терроризма (статьи 21 и 22 Варшавской Конвенции) могут быть дополнены мерами обеспечения сохранности электронных доказательств не только Интернет-провайдерами, но и иными физическими и юридическими лицами (Будапештская Конвенция – статьи 16 и 17 для обеспечения сохранности на национальном уровне, статьи 29 и 30 – на международном). Это также применяется и к иным формам сотрудничества. 40 Рекомендаций ФАТФ призывает страны «разрешить их компетентным органам обмениваться информацией косвенно с не-партнерами»[225]. Это должно позволить обмениваться информацией между ПФР и подразделением по борьбе с компьютерными преступлениями в другой стране как через ПФР, так и напрямую.

[224] См Рекомендацию 36 (пересмотренные в феврале 2012 г.)
[225] См. параграф 17 Пояснительной записке к Рекомендации 40 (пересмотренные в феврале 2012 г.)

6. Приложение

6.1 Концепция исследования

Концепция[226]

Наименование: Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками

Проводит: Российская Федерация и Секретариат Совета Европы (Секретариат МАНИВЭЛ, Проект по киберпреступности и Проект МОЛИ-РУ)

Описание:

Настоящее исследование проводится на изучения потоков незаконных денежных средств и методов отмывания денег через информационно-коммуникационные технологии (ИКТ), включая Интернет. При этом помимо всего прочено планируется разработать документ, который содержал бы в себе описание мер, направленных на конфискацию преступных доходов и предотвращение.

Вопросы:

Киберпреступность нацелена на извлечение прибыли с использованием различных видов мошенничества и экономических преступлений (например, фишинг и иные виды кражи персональных данных, мошенничество с кредитными картами, мошенничество на аукционах, мошенничество при розничной торговле в Интернете, он-лайновые азартные игры, мошенничество с лотереями, правонарушения в сфере авторских и смежных прав, манипулирование на бирже, авансовые мошенничества, вымогательство, шпионаж, инсайд, электронная торговля похищенными или поддельными товарами и многое другое), совершаемые путем незаконного доступа, воздействия на данные, перехвата данных и систем при помощи вредоносных программ, включая бот-сети и спам. Интернет и информационно-коммуникационные технологии облегчают отмывание денег и финансирование

[226] Одобрена Комитетом экспертов Совета Европы по оценке мер противодействия отмыванию денег и финансированию терроризма (МАНИВЭЛ) в сентябре 2009 г.

терроризма. Как указывает ФАТФ коммерческие сайты и он-лайновые платежные системы уязвимы для отмывания денег и финансирования терроризма[227]. Преступники могут получать денежные средства на свои счета или счета, которые находятся под их контролем, с которых они могут снять их или переводить их, используя счета бенефициарных собственников в разные страны, или е-деньги или они могут отмыть используя е-золото, е-казино, Интернет-аукционы и иные способы. Все эти преступления по своей природе являются транснациональными.

Широкий круг участников вовлечен в реализацию мер по борьбе с такими преступлениями не только из государственного сектора, но и из частного. И хотя приводятся примеры предпринятых совместных действий, общие усилия все еще остаются точечными. Инициативы по борьбе с мошенничеством в Интернете должны исходить не только подразделений финансовой разведки или правоохранительных органов, ответственных за проведение финансовых расследований.

Знания о методах, используемых при совершении мошенничества, отмывании денег и финансировании терроризма через Интернет, можно усовершенствовать пути обмена информацией, между соответствующими представителями государственного и частного сектора, что поможет проводить расследования, приостанавливать и конфисковать активы, предотвращать мошенничество, отмывание денег и финансирование терроризма.

Цель исследования:

При проведении исследования ставятся следующие цели:
- исследовать определенные риски ОД/ФТ, а также тенденции и типологии;
- выработать индикаторы для выявления потоков преступных денежных средств и отмывания денег в Интернете;
- выработать возможные решения для действий, предпринимаемых участниками, носящих превентивный характер, а также для изъятия и конфискации преступных активов и проведения расследования по делам об отмывании денег и финансировании терроризма в Интернете.

[227] Группа разработки финансовых мер борьбы с отмыванием денег: Уязвимость коммерческих сайтов и онлайновых платежных систем для отмывания денег и финансирования терроризма (июнь 2008 г.). В проекте также учитывается и текущая работа ФАТФ над рисками ОД и ФТ в результате использования новых платежных технологий .

Необходимые ресурсы:

Проектная группа в идеале будет включать в себя представителей ПФР, следственных подразделений, отвечающих за финансовые расследования и расследование преступлений в сфере высоких технологий. Будут проводится консультации с ключевыми представителями частного сектора, чтобы они смогли привнести свой опыт в проект.

Проектной группе будут оказывать содействие один или два эксперта (один по вопросам противодействия отмыванию денег/проведению финансовых расследований, а другой, специализирующийся на преступлениях в сфере высоких технологий), которые будут помогать руководителю проекта и Секретариату в координации процессов и обобщении получаемой информации.

Взаимодействие между МАНИВЭЛ, Проектом Совета Европы по киберпреступности и Проектом МОЛИ-РУ позволит использовать дополнительные ресурсы и опыт, а также предоставит доступ к различным участникам.

Планируемый результат:

Проектная группа составит отчет, состоящий из двух частей:
- типологии: в этой части будет содержаться описание выявленных методов и тенденций ОД через Интернет, на основании примеров, полученных от стран,. Также буду выработаны индикаторы риска;
- полезный опыт: вторая часть будет описывать полезный опыт в части контр-мер, т.е. стратегий, политик и техник проведения расследования. Этот раздел должен содержать информацию и руководство по мерам, предпринимаемым основными участниками, включая подразделения финансовой разведки, финансовых следователей, подразделения по борьбе с преступлениями в сфере высоких технологий, а также частный сектор (ИКТ, финансовый сектор и т.д.)

Если у Вас возникли какие-либо вопросы по проекты, то свяжитесь с:

Александр Сегер
Подразделение по борьбе с экономическими преступлениями
Генеральный директорат по правам человека и верховенству права
Совет Европы
F-67075 Страсбург СЕДЕКС
Тел.: +33-3-9021-4506
Факс: +33-3-9021-5650
Эл.почта: alexander.seger@coe.int

Ливия Стойка Бехт
Секретариат МАНИВЭЛ
Директорат мониторинга
Генеральный директорат по правам человека и верховенству права
Совет Европы
F-67075 Страсбург СЕДЕКС
Тел.: +33-3-9021-4260
Факс: +33-3-8841-3017
Эл.почта: dghl.moneyval@coe.int

6.2 Ссылки[228]

Филипп Брунст/Ульрих Сибер (2010 г.). Законодательство о противодействии киберпреступности. В: Дж. Базедов/У.Кишель/У. Сибер (eds). Немецкий национальный отчет на 18 Международном конгрессе сравнительного законодательства. Вашингтон, 2010 г.

Федеральная уголовная полиция Германии (2010 г.): Ежегодный отчет ПФР за 2009 г. Висбаден

http://www.bka.de/profil/zentralstellen/geldwaesche/pdf/fiu_jahresbericht_2009.pdf

Федеральная уголовная полиция Германии (2010 г.): IUK-Kriminalitat – Bundeslagebild 2009 г. Висбаден
http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf

Мануэль Кастель (2000 г.): Расцвет сетевого сообщества. Молден/Оксфорд/Карлтон (второе издание)

Отчет «Commtouch» «О тенденции Интернет-угроз» за первый квартал 2010 г. www.commtouch.com/download/1679

Совет Европы (2002 г.): Отчет об организованной преступности за 2001 г. Страсбург (Комитет PC-S-CO).
http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/Report2001E.pdf

Совет Европы (2003 г.): Отчет об организованной преступности за 2002 г. Страсбург (Комитет PC-S-CO).

[228] Только избранный список. См. сноски по тексту исследования.

http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/PC-S-CO%20_2003_%207%20E%20OCReport% 202002-Provisional.pdf

Совет Европы (2004 г.): Отчет об организованной преступности за 2004 г. – Акцент на угрозах, которые несет киберпреступность (программа «Октупус») http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf

Совет Европы (2005 г.): Отчет об организованной преступности за 2004 г. – Акцент на угрозах, которые несет экономическая преступность (программа «Октупус») http://www.coe.int/t/dghl/co-operation/economiccrime/organisedcrime/Report2005E.pdf

Совет Европы (2005 г.): Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и от финансирования терроризма (СДСЕ 198). http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=198&CM=8&DF=05/12/2010&CL=ENG

Совет Европы (CyberCrime@IPA) (2011 г.): Стратегии обучения сотрудников правоохранительных органов. Страсбург http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Cyber%20IPA%20reports/2467_LEA_Training_Strategy_Fin1.pdf

Совет Европы (Международный проект по борьбе с киберпреступностью) (2008 г.): Руководство для сотрудничества между правоохранительными органами и Интернет-провайдерами для противодействия киберпреступности. Страсбург http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

Совет Европы (Международный проект по борьбе с киберпреступностью) (2010 г.): Процесс регистрации доменного имени – от регистрации до ICANN Страсбург. Доклад подготовлен Вольфгангом Кляйнвётером. http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter1.pdf

Совет Европы (Международный проект по борьбе с киберпреступностью) (2010 г.): Обучение судей и прокуроров аспектам, связанным с киберпреступностью – Концепция. Страсбург

http://www.coe.int/t/dghl/co-operation/economiccrime/cybercrime/Documents/Training/default_en.asp

Совет Европы (Международный проект по борьбе с киберпреступностью) (2011 г.): Стратегия борьбы с киберпреступностью. Страсбург http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

Специальная группа по борьбе с киберпреступностью EC/CyberCrime@IPA/Международный проект по борьбе с киберпреступностью (2011 г.): Специализированные подразделения по противодействию киберпреступности – Исследование полезного опыта, Совет Европы. Страсбург http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

Deutsche Gesellschaft fur Technische Zusammenarbeit (GTZ) (1998 г.): Наркотики и развитие в Азии (Eschborn). http://www2.gtz.de/dokumente/bib/99-0026.pdf

Европол (2007 г.): Преступления в сфере высоких технологий в ЕС: старые преступления- новые иснтрументы, новые преступления- новые инструменты. Оценка угроз в 2007 г. Гаага http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf

Группа разработки финансовых мер борьбы с отмыванием денег (2008 г.): Уязвимость коммерческих сайтов и он-лановых платежных систем для отмывания денег и финансирования терроризма (июнь 2008 г.). Париж http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

Группа разработки финансовых мер борьбы с отмыванием денег (2010 г.): Отмывание денег при помощи новых платежных технологий. Париж http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf

Противодействие финансовому мошенничеству в Соединенном Королевстве (2010 г.): Факты о мошенничестве – Детальный обзор случаев мошенничества в платежной индустрии и меры по его предотвращению. http://www.ukpayments.org.uk/files/fraud_the_facts_2010.pdf

Томас Л.Фридман (2006 г.) Мир – это квартира. Лондон

Официальное описание “G Data” за 2009 г.: «Теневая экономика»

(http://www.gdatasoftware.com/uploads/media/Whitepaper_Underground_Economy_8_2009_GB.pdf)

Обзор информационных войн/ финансирование теневых серверов (2010 г.): Тени в облаках – расследование кибер-шпионажа 2.0
http://www.nartv.org/mirror/shadows-in-the-cloud.pdf

Центр по приему жалоб на Интернет –преступления (2010 г.) Доклад о преступности в Интернете за 2009 г.
http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

Берт-Жаап Купс/Рональд Линс (2006 г.): Кража идентификационных данных, мошенничество с ними и иные преступления. В Datenschutz und Datensicherheit 30 (2006 г.) 9.
http://www.fidis.net/fileadmin/fidis/publications/2006/DuD09_2006_553.pdf

М 86 «Безопасность» («Белая книга») «Киберпреступники нацелились на клиентов Интернет-банкинга (август 2010 г.).
http://www.m86security.com/documents/pdfs/security_labs/cybercriminals_target_online_banking.pdf.

Информационный отчет Microsoft по безопасности, том 9, январь- июнь 2010 г. http://www.microsoft.com/security/sir

ОЭСР (2007): «Вредоносные программы — угроза безопасности Интернет - экономике». См. http://www.oecd.org/dataoecd/53/34/40724457.pdf)

Говард Шмидт (2006): «Патрулируя киберпространство». Северный Потомак

Александр Зегер (2007 г.): Кража идентификационных данных и Конвенция о киберпреступности. В Демостенис Хриссикос, Никос Пассас, Кристофер Д.Рам: Аастущая угроза преступлений с идентификационными данными: борьба с мошенничеством и незаконное использование идентификационных данных и их подделка (UN ISPAC) http://www.ispac-italy.org/pubs/ISPAC%20-%20Identity%20Theft.pdf

Отчет «Sophos" об угрозе безопасности (август 2010 г.), стр. 28: http://www.sophos.com/security/topic/security-report-2010.html

УНП ООН: «Глобализация преступности: оценка угрозы, которую несет транснациональная организованная преступность» (2010 г.), см. http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf