Министерство внутренних дел Российской Федерации
Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра оперативно-разыскной деятельности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: Использование специального программного обеспечения в оперативно-розыскной деятельности

Выполнил:
Кибатов Максим Сергеевич,
40.05.02 Правоохранительная деятельность, набора 2014 г.,
041 уч. группа

Руководитель:
кандидат юридических наук, доцент, доцент кафедры оперативно-разыскной деятельности
Музеев Айдар Иршатович

Рецензент:
Начальник отделения ЭБиПК УМВД России по г. Набережные Челны
майор полиции
Шайдуллин Эдуард Накипович

К защите _______
(допущена, дата)
Начальник кафедры _____

Дата защиты: "___" _____2019 г. Оценка _____

Казань 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

За последние 10 лет резко возросло количество преступлений в сфере и с применением высоких технологий. Только за первое полугодие 2017 года их количество выросло на 67% по сравнению с аналогичным периодом 2016 года. При этом, согласно статистике ГИАЦ МВД, количество расследованных уголовных дел в этой сфере год за годом снижается. К примеру, в 2012 г. Расследовано 6142 преступления, а в 2016 г. – 2470.

Значимость данной темы обусловлена тем, что по мере развития высоких технологий, растет и преступность в этой сфере. Новые способы совершения преступления, а также технологий анонимизации требуют совершенствования методики противодействия злоумышленникам.

Исследованию данной темы в уделяли внимание в своих трудах Бельский В.А., Образцов А.И., Волеводз А.Г., Гаврилин Ю.В., Абдульманов А.А., Василенко В. и другие ученые.

Объектом исследования является: совершенствование методики деанонимизации преступников, скрытного получения доказательственной базы.

Предмет исследования: практические возможности, а также правовые основы использования специального программного обеспечения в борьбе с преступлениями в сфере высоких технологий.

Целью данной дипломной работы является наиболее полное изучение правой основы использования технических средств для негласного получения информации, а также наркотических веществ в оперативно розыскной деятельности, и на основе полученных выводов, обосновать легальность использования предлагаемого программного обеспечения:

1. Изучить актуальные механизмы совершения преступлений в сфере высоких технологий.

2. Проанализировать механизмы анонимизации преступников;

3. Изучить правые основы использования технических средств для негласного получения информации, а также наркотических веществ в оперативно розыскной деятельности;

4. Обосновать возможность применения предлагаемого специального программного обеспечения в правовом плане.

При изучении данной темы нами были исследованы различные нормативные акты и ряд учебной литературы. В своей работе мы использовали труды известных ученых Образцова Р.С., Михеева А.Г., Третьяка Т.В. и других авторов. Среди источников правового регулирования использовались ныне действующие нормативные акты такие как Конституция Российской Федерации, Федеральный закон «О связи», Федеральный закон «Об Оперативно-розыскной деятельности», Уголовно-процессуальный кодекс Российской Федерации, Уголовный кодекс Российской Федерации, приказы МВД России.

Структура работы предопределяется задачами исследования и включает: введение, три главы, заключение и список литературы.

ГЛАВА 1. ОСНОВНЫЕ НАПРАВЛЕНИЯ И МЕХАНИЗМЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

§ 1. Основные направления совершения хищений в сфере высоких технологий

Эксперты международной компании Group-IB, специализирующейся на предупреждении и расследовании киберпреступлений, считают, что основными преступными деяниями, образующими рынок киберпреступности в России, являются:

1) мошенничество в системах интернет-банкинга;

2) фишинг;

3) хищение электронных денег;

4) услуги обналичивания иных нелегальных доходов;

5) спам (информация о медикаментах и различной контрафактной продукции, поддельном программном обеспечении, сфере услуг, образования, туризма и др.);

6) продажа трафика;

7) продажа эксплойтов;

8) продажа загрузок;

9) анонимизация;

10) DDoS-атаки.[1]

В развитии своих хакерских наборов атакующие уделяют внимание не только Windows платформам, но и MacOS, а также мобильным операционным системам. Все больше интереса хакеры проявляют к уязвимостям в домашних маршрутизаторах. Финансовая оценка активности

[1] Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации. // Юридическая наука и правоохранительная практика - Иркутский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации, 2016. - 1 (35) – 55

кибер-преступников является ярким индикатором смены приоритетов хакеров. Большая часть атакующих следуют за деньгами и, если они находят новые более эффективные способы заработка, они инвестируют время и средства именно туда, создавая новые инструменты, услуги, схемы проведения атак.

Поскольку основным объектом противозаконной деятельности преступников в сети Интернет являются материальные ценности, рассмотрим более подробно актуальную ситуацию в сфере высокотехнологичных хищений, в России и в мире.

Согласно статистике компании - лидера в сфере информационной безопасности, Group-IB, основную долю совершаемых в России кибер-хищений составляют:

1. Хищения у юридических лиц с использованием вирусов «Троян» для ПК

2. Хищения у физических лиц с использованием вирусов «Троян» для смартфонов на базе операционной системы «Android».

3. Целевые хакерские атаки на банки.

4. Хищения путем фишинга.

Полная статистика количества и сумм хищений, зафиксированных за 2017-2018 год представлена в Таблице 1.1

Таблица 1.1

Полная статистика количества и сумм хищений, зафиксированных за 2017-2018 год.[1]

Сегмент рынка в России	Кол-во групп	Успешных атак в день	Средняя сумма хищений в день (в RUR)	Средняя сумма хищений в день (в RUR)	H2 2017 - H1 2018 (в RUR)	H2 2017 - H1 2018 (в USD)	Процент изменения
Хищения у юридических лиц с троянами для ПК	3	2	1 100 000	2 200 000	547 800 000	9 130 000	-12%

[1] Group-IB. Hi-Tech Crime Trends. 2017. С. 22.

Сегмент рынка в России	Кол-во групп	Успешных атак в день	Средняя сумма хищений в день (в RUR)	Средняя сумма хищений в день (в RUR)	H2 2017 - H1 2018 (в RUR)	H2 2017 - H1 2018 (в USD)	Процент изменения
Хищения у физических лиц с Android-троянами	8	110	7 000	770 000	191 730 000	3 195 500	-77%
Целевые атаки на банки	3	-	118 000 000	-	1 303 900 000	21 731 667	-20%
Фишинг	26	108	1000	1 008 000	250 992 000	4 183 200	6%
Обналичивание похищаемых средств	-	-	-	1 336 500	919 543 500	15 325 725	-34%
Итого:				3 114 500	3 213 965 500	53 556 092	-32%

Разделим хакерские атаки по направленности в имущественном секторе:

1. На банки.
2. На клиентов банков.

1. Целенаправленные атаки на банки.

На текущий момент существует 4 группы, которые представляют реальную угрозу и задают тренды в атаках на банки: они способны не только проникнуть в сеть, добраться до изолированных финансовых систем, но и успешно вывести деньги через SWIFT, АРМ КБР, карточный процессинг и банкоматы. Речь идет о группах Cobalt, MoneyTaker, Silence, состоящих из русскоговорящих хакеров, а также о северокорейской Lazarus. В среднем в России каждый месяц киберограблениям подвергались 1-2 банка. Средний ущерб от одного успешного ограбления составляет 132 млн рублей ($2 млн). Количество целенаправленных атак на банки с целью хищения через SWIFT увеличилось в три раза. Если за прошлый прошлый период было всего три атаки в Гонконге, Украине и Турции, то в этом произошло девять успешных атак в Непале, Тайване, России, Мексике, Индии, Болгарии и Чили. Для межбанковской системы SWIFT представляют угрозу только две преступные группы: Cobalt и Lazarus. При совершении хищений через SWIFT и Cobalt,

и Lazarus тщательно готовили схему обнала. Вероятно, для оптимизации связанных с обналичиванием затрат хищения проводились сразу из двух банков. Как и в предыдущих атаках на SWIFT, вывод большей части похищенных средств удалось остановить. Выводом денег через АРМ КБР (автоматизиро- ванное рабочее место клиента Банка России) занимается только MoneyTaker — если в ноябре 2017 года им удалось вывести всего 7 млн рублей, то уже летом 2018 года они успешно похитили из «ПИР Банка» 58 млн рублей.

В 2017 и 2018 году хакеры из групп Cobalt и Silence игнорировали российскую систему межбанковских переводов АРМ КБР даже в тех случаях, когда им удавалось получить к ней доступ. Сейчас их внимание привлекают более надежные схемы хищений через банкоматы и карточный процессинг. Вместе с тем, Cobalt интересуется локальными системами межбанковских переводов за рубежом. Атаки на карточный процессинг остаются одним из основных способов хищений и проводятся группами Cobalt, MoneyTaker, Silence. В результате такой атаки в феврале 2018 года группе Silence удалось снять с карточек через банкоматы партнера банка 35 млн рублей. Фокусировка атак на банкоматах и карточном процессинге привела к уменьшению среднего ущерба от одной атаки. Однако такие атаки несут меньше рисков для преступников и более безопасны для «дропов», обналичивающих украденные деньги: атакующие находятся в одной стране, их жертва (банк) в другой, а обналичивание происходит в третьей. В анализируемом периоде атаки на платежные шлюзы проводила только группа Cobalt. При этом в 2017 году преступники похитили деньги у двух компаний, а в 2018 не сделали ни одной попытки.

В результате реагирования на один из инцидентов специалисты Group-IB установили, что помощь им оказывали участники группы Anunak, которая не осуществляла подобных атак с 2014 года. Несмотря на арест в Испании лидера группы весной 2018 года, Cobalt по-прежнему остается одной из самых активных и агрессивных группировок, 2-3 раза в месяц атакуя финансовые организации в России и за рубежом. Атаки с целью заражения банкоматной

сети проводят Cobalt, Silence, а также группа MoneyTaker, которая провела первую атаку такого рода в мае 2018 года.

Тренд на снижение угроз со стороны банковских троянов для ПК в России продолжается с 2012 года. Атаки на физических лиц ушли в прошлое, а ущерб для юридических лиц по итогам отчетного периода сократился еще на 12% и составил 547 млн. рублей ($8,3 млн.). Только три группы — Buhtrap2, RTM, Toplel — похищают средства со счетов юридических лиц в России. Основным способом хищения является удаленное управление или автоматические переводы через системы бухгалтерского учета 1С.

Во второй половине 2017 года тактика атакующих изменилась: вектором распространения троянов стала не традиционная вредоносная рассылка и не взломанные популярные сайты, а создание новых тематических ресурсов, на которых злоумышленники размещали код, предназначенный для загрузки троянов. После нескольких лет интенсивного роста рынок хищений с помощью Android-троянов в России значительно сократился. Это связано и с обновлениями операционной сети от Google, и с понижением лимитов на переводы по СМС, и с внедрением банками систем раннего обнаружения фрода с функционалом детектирования активности вредоносных программ на устройстве клиента. Количество проводимых ежедневных хищений с помощью Android-троянов в России снизилось почти в три раза. Стоит отметить и сокращение среднего размера хищений. Если в прошлом отчетном периоде он составлял 11 тысяч рублей, то в этом он опустился до 7 тысяч.

Новых крупных Android бот-сетей для атак в России не создавалось, за исключением вредоносной программы «Банки на ладони». Троян был замаскирован под финансовое приложение, выполняющее роль «агрегатора» систем мобильного банкинга ведущих банков страны.

Веб-фишинг — единственный метод хищений, который показал рост ущерба в России в отчетном периоде: с его помощью удалось похитить 251 млн. рублей, что на 6% больше показателя прошлого года. Этот сравнительно простой способ атаки привлекает все больше новичков: количество групп,

которые создают фишинговые сайты под российские бренды выросло с 15 до 26. Ежедневно им удается провести в среднем 1274 мошеннические транзакции. Средняя сумма одного хищения не изменилась и равна 1000 рублей. Большую популярность получил фишинг, связанный с переводом с карты на карту. В некоторых случаях атакующие брендируют такие страницы под конкретный банк, но есть и абсолютно независимый от брендов банков фишинг.

2. Атаки на клиентов банков

Более активное использование троянов с функцией самораспространения позволит атакующим поднять эффективность проведения атак с помощью банковских троянов для ПК, а также POS-троянов.

Основным методом проникновения в сети ресторанов и магазинов с POS-терминалами может стать бесплатный Wi-Fi, раздаваемый уязвимыми роутерами. Мы ожидаем начала атак на мобильный банкинг для юридических лиц в России. Основным методом методом распространения может стать контекстная реклама в поисковых системах. Ущерб от фишинга в России продолжит расти. Для повышения эффективности таких атак могут использоваться домашние роутеры, перенаправляющие пользователей на такие сайты. Владельцы бот-сетей Toplel и RTM могут отказаться от хищений у юридических лиц и начать проводить целенаправленные атаки на банки в России и СНГ. После распространения исходных кодов основной угрозой для банкоматов без компрометации банковских сетей станет вредоносная программа «Котлета» (Cutlet). BackSwap и IcedID могут стать значимыми банковскими угрозами в дополнение к Dridex, Trickbot и Gozi. Банковские Android-трояны будут захватывать мировой рынок и продолжат вытеснять банковские трояны для ПК.

Таким образом, исходя из изложенных выше данных мы можем полагать, что большая часть кибер-хищений затрагивает сферу предоставления банковских услуг. Однако, это – не единственное направление работы хакеров. Рассмотрим подробнее рынок высокотехнологичных хищений в России.

§ 2. Оценка рынка высокотехнологичных хищений в России

Финансовая оценка активности кибер-преступников является ярким индикатором смены приоритетов хакеров. Согласно данным Group-IB, большая часть атакующих следуют за деньгами и, если они находят новые более эффективные способы заработка, они инвестируют время и средства именно туда, создавая новые инструменты, услуги, схемы проведения атак. За прошедший период полностью ушли со сцены трояны для ПК, а хищения с помощью Android-троянов после нескольких лет взрывного роста резко сократились благодаря обновлениями операционной сети от Google, понижению лимитов на переводы по SMS, и с внедрением банками систем раннего обнаружения фрода с функционалом детектирования активности вредоносных программ на устройстве клиента. На подъеме фишинг – относительно простая тактика атак привлекает на рынок все больше злоумышленников. Основной угрозой для российских банков остаются хорошо подготовленные группы с практикой успешных целевых атак. В среднем в России каждый месяц они грабили 1-2 банка. Впрочем, в 2018 году было 4 месяца, когда не было зафиксировано ни одного ограбления (январь, февраль, май и июнь).

На графике ниже показаны группы, которые проводят целенаправленные атаки на банки с целью хищений. На текущий момент, по данным Group-IB, существует всего четыре группы, которые способны взломать банк, добраться до изолированных финансовых систем и вывести деньги. Каждая из этих групп имеет более глубокую историю, на графе отмечены моменты начала и завершения попыток ограбить именно банки. Группы, которые занимаются саботажем и шпионажем, на иллюстрации не представлены. Cobalt, MoneyTaker, Silence состоят из русскоговорящих финансово-мотивированных хакеров, Lazarus принято считать спонсируемой Северной Кореей. Именно эти

группы являются центром инноваций и формируют тренды в сложных атаках на банки. По каждой из этих киберпреступных групп Group-IB выпускала отчеты, результаты которых отражены на рисунке 1.1.

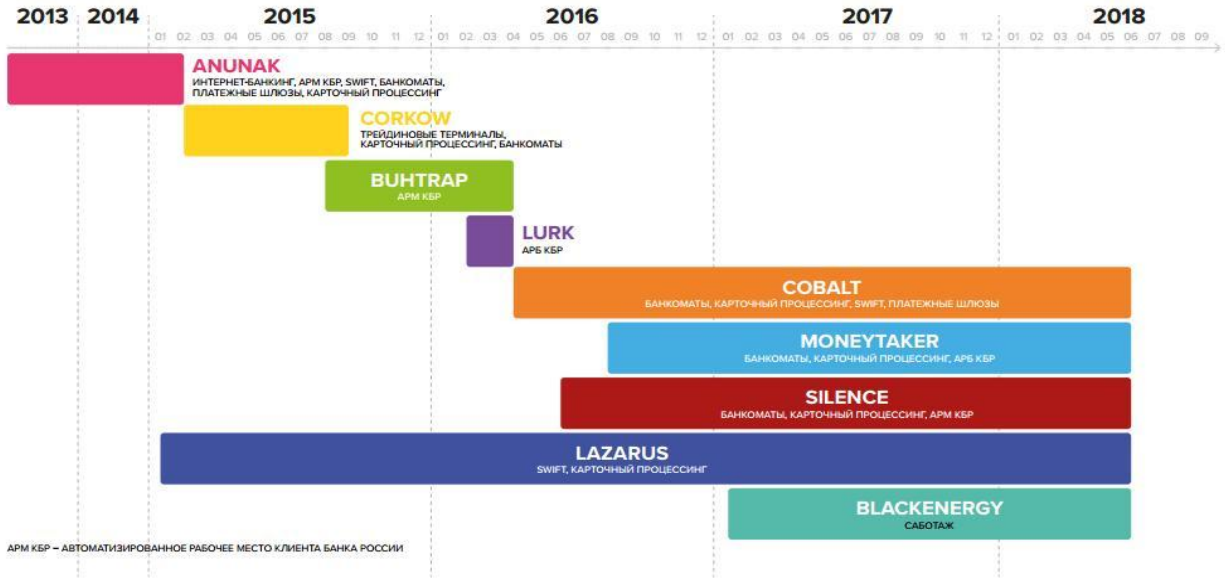

Рис. 1.1 Тренды в сложных атаках на банки.

В 2016 году основную угрозу для банков в России представляли атаки на АРМ КБР (Автоматизированное рабочее место клиента Банка России). Однако в 2017 и 2018 году хакеры из групп Cobalt и Silence игнорируют данные системы даже в том случае, когда успешно получают к ним доступ. Сейчас их внимание привлекают более надежные схемы хищений через банкоматы и карточный процессинг. И только группа MoneyTaker сделала одно успешное хищений в ноябре 2017 года через АРМ КБР. Тогда сумма ущерба составила всего 7 миллионов рублей, а в 2018 они успешно вывели из другого банка уже 58 миллионов рублей. В начале июля 2018 пользователь под псевдонимом Bobby.Axelrod опубликовал на подпольных форумах фреймворк Pegasus для автоматизации атак на АРМ КБР путем автоматической подмены платежных реквизитов. В архив также входили инструкции и исходные коды. Этот фреймворк использовался группой Buhtrap в 2016 году и все данные

из архива относятся к тому периоду. Ранее часть исходных кодов, используемых Buhtrap, уже утекали в сеть. Стоит отметить, что реализованная в данном фреймворке автозамена платежных реквизитов уже не актуальна для последних версий АРМ КБР, однако архив представляет большую ценность для автоматизации других шагов по компрометации банковских сетей.

Атаки на карточный процессинг по-прежнему являются одним из основных способов хищений и проводятся группами Cobalt, MoneyTaker, Silence. Этот метод обеспечивает самый безопасный способ обналичивания и максимальную финансовую выгоду. Рекордсменом в этой области стала группа Cobalt: в 2017 году в московском банке они попытались похитить 250 миллионов рублей. В других регионах суммы ущерба как правило значительно ниже. Эта схема хищений начала набирать популярность в 2016 году. В сентябре 2016 года группа Cobalt получила доступ в один из банков Якутии и начала подготовку к новому для них типу хищений — через карточный процессинг. Процесс изучения занял 2 месяца, и в ноябре они успешно похитили около $600 тыс. С тех пор Cobalt — лидер по количеству успешных атак этого типа. Параллельно вместе с ними схему атак на карточный процессинг начала прорабатывать и группа MoneyTaker. Самая первая атака, с которой мы связываем эту группу, была проведена весной 2016 года, когда в результате получения доступа к системе карточного процессинга STAR компании FirstData был ограблен National Bank of Blacksburg (США). В январе 2017 этот банк подвергся еще одной успешной атаке, о чем стало известно только спустя 7 месяцев после публичного релиза нашего отчета об атаках этой группы.

В течение 2017 MoneyTaker взломала еще 9 банков в США. Группа Silence провела свою первую атаку на карточный процессинг только в марте 2018 года и сразу успешно похитила 35 млн. рублей в одном из банков в России. Для успешного хищения через карточный процессинг атакующим не нужен специализированный софт, как например для атак на банкоматы или для автоподмены платежей в системах межбанковских переводов. Поэтому этот

метод доступен всем преступным группам, у которых есть опыт проникновения в банковские сети.

Атаки на банки с целью заражения их банкоматной сети проводят Cobalt, Silence, а также MoneyTaker. Последняя группа начала тестировать новый уникальный троян в мае 2018 года. Cobalt В 2016 году группа Cobalt провела серию успешных атак на банки и их банкоматные сети в России и за рубежом. Однако с осени 2016 года по декабрь 2017 года все их усилия были направлены на хищения другими способами. После продолжительной паузы, в декабре 2017 года они снова провели атаки на банкоматы в России. При этом использовался все тот же троян ATMSpitter, которые преступники задействовали в атаках и на Тайване, и в Европе и в России. Никаких значимых изменений в код самой программы внесено не было. Она по-прежнему является консольной и использует стандартные функции по интерфейсу XFS через XFS Manager (eXtensions for Financial Services). На вход программе передаются параметры, описанные в таблице 1.2.

Таблица 1.2.

Параметры программного обеспеченияXFS Manager для банкоматов.

Параметр:	Описание:
ServiceLogicalName	Имя службы, которое будет использовано для функции WFSOpen. Например, Cash Dispenser Module.
Cassettes Count	Количество кассет в банкомате. Значение может быть от 1 до 15.
Cassette Number	Номер кассеты из которой надо выдать наличные. Значение может быть от 1 до 15.
Banknotes Count	Количество банкнот, которые надо выдать из кассеты. Значение может быть от 1 до 60.
Dispenses Count	Сколько раз операция выдачи должна повториться. Значение может быть от 1 до 60.

Для управления диспенсером банкоматов Silence использует уникальную программу Atmosphere. На протяжении всей видимой нам деятельности группы троян модифицировался, чтобы соответствовать требованиям атакующих. Так, троян изменил логику внедрения в процессы, автор добавил ему гибкий инжектор, что позволило расширить перечень поддерживаемых банкоматов, с которыми работала группа. В дальнейшем троян был избавлен от ненужных функций, которые мешали или не использовались при работе преступников. Например, в последней версии программа не обрабатывала команды с пинпада, а генерируемый лог стал меньше. На начальном этапе развития программу перекомпилировали множество раз, что, скорее всего, и привело к нескольким безуспешным попыткам извлечь наличность.

Хакеры удаленно устанавливают на банкомат Atmosphere.Dropper, в ресурсах которого содержится библиотека .DLL — основное тело трояна Atmosphere. После извлечения тела дроппер внедряет библиотеку в процесс с именем fwmain32.exe. Уже внутри управляющего процесса библиотека предоставляет возможность удаленного управления диспенсером. В первых версиях присутствовала возможность управления диспенсером с помощью пинпада, но позже эти функциональные возможности были удалены.

Таблица 1.3.

Пример команд трояна Atmosphere.

Параметр	Описание команды
«B»	Получает информацию о содержимом кассет ATM. Помимо этого в лог записывается строка «cash units info received».
«A»	Получает информацию о содержимом кассет без логирования.
«Q»	Получает информацию о содержимом кассет ATM.
«D»	Одноразовая выдача купюр конкретного номинала из банкомата.
«H»	Приостанавливает все потоки в процессе, кроме собственного, и при помощи функций GetThreadContext + SetThreadContext перенаправляет их выполнение "на собственную функцию.

Параметр	Описание команды
"M", "R", "S", "P", "T", "L"	Запись результата выполнения последней команды в файл «C:\intel\<chrs>.007» Эта команда также по умолчанию выполняется в конце любой другой.

Команды передаются программе через файлы с определенным расширением. После считывания и исполнения команд программа, по задумке автора, должна переписывать файл мусором и удалять его для затруднения работы форензик-экспертов. Однако логика программы содержит ошибку, вследствие чего мусор не пишется поверх файла, а дописывается в конец. В ходе мероприятий по реагированию на инцидент информационной безопасности в одном из банков, команда криминалистов Group-IB обнаружила порядка 11 программ Atmosphere, скомпилированных в разное время и с незначительными изменениями. В одной директории с программами были найдены сценарии для командного интерпретатора, а также отдельный Injector, который принимал на вход в виде аргументов путь до библиотеки DLL и идентификатор процесса, куда должен был внедрить указанную библиотеку. Однако сценарии передавали не идентификатор процесса, а имя целевого процесса, что в итоге привело к безуспешной попытке получить контроль над диспенсером.

Атаки с помощью троянов для ПК В России.

Тренд на снижение угроз со стороны банковских троянов для ПК в России продолжается с 2012 года. За прошедший период ущерб сократился еще на 12% и составил 547 800 000 руб. Как и за предыдущий год, не появилось ни одного нового банковского трояна для ПК для хищений в России. Более того, не осталось ни одной группы, которая бы занималась хищениями средств у физических лиц в России с использованием таких программ. Активность проявляют только группы, которые используют банковские трояны для хищений у компаний. Таких команд осталось всего три: Buhtrap2, RTM, Toplel. При этом ни одна из них не использует атаку «человек-в-браузере»

(Man-in-the-browser). Buhtrap2 В 2016 года бот-сеть Buhtrap была продана и теперь используется другими злоумышленниками. Основным методом распространения в первой половине 2017 года был метод Drive-by: преступники взламывали легитимные сайты финансовой тематики (например, www.glavbukh.ru), при посещении которых загружался JavaScript, после чего происходила эксплуатация уязвимости браузера. В результате запускался PowerShell-скрипт, загружающий и приводящий в действие загрузчик Buhtrap. Во второй половине 2017 года тактика атакующих изменилась: вектором распространения троянов стала не традиционная вредоносная рассылка и не взломанные популярные сайты, а создание новых тематических ресурсов, на которых злоумышленники размещали код, предназначенный для загрузки троянов. Владельцы этой бот-сети активно использовали автоматические переводы через системы бухгалтерского учета 1С. После того, как разработчики 1С реализовали защиту от атак этого типа, включив проверку замены реквизитов, хакеры изменили свой код. Новый Buhtrap способен обходить защиту «1С:Предприятие» «Контроль безопасности обмена с банком» путем сокрытия отображаемого предупреждения.

RTM Банковский троян RTM начал свою активность в 2016 году и остается востребован преступниками. В конце 2016 года мы видели, что при распространении трояна RTM использовался загрузчик из утекших исходных кодов Buhtrap. Такая связь нередко сбивает специалистов по информационной безопасности при атрибуции. Как и в случае Buhtrap2, основными способами совершения хищения являются удаленное управление или автоматические переводы через системы бухгалтерского учета 1С. Однако мы не видели атак, которые бы обходили реализованную «1С:Предприятие» защиту от автоподмены реквизитов, как это сделано в Buhtrap. Toplel Преступная группа Toplel была обнаружена специалистами Group-IB в феврале 2015 года. В результате исследования было установлено, что она действует минимум с августа 2014 года и использует доменные имена, регистрируемые в зоне .SU. На тот момент для совершения хищений злоумышленники задействовали

программу, известную как RDPdoor (xTerm). Она предоставляет злоумышленнику удаленный доступ к компьютеру, что позволяет совершать транзакции с рабочего места пользователя в тот момент, когда подключен токен с электронной цифровой подписью, необходимой для подтверждения переводов. Программа распространялась преимущественно через письма с вредоносным вложением. Основной целью злоумышленников были клиенты банков России и Украины. Модули трояна RDPdoor определяли следующие системы интернет-банкинга Ibank, bifit, Промсвязь, Альфабанк, Diasoft, Сбербанк, Комита, Tiny, Fobos, ClntW32, cbsmain, BCClient, Tival, cbs, Севергазбанк, Ibc, Interbank, RS. Кроме трояна RDPdoor, преступники работают с модифицированной версией вредоносной программы Pony, которая может быть использована для сбора логинов и паролей на системах, не имеющих отношение к интернет-банкингу.

Атаки с помощью Android-троянов.

После нескольких лет роста рынок Android-троянов в России вышел на плато, однако продолжает активно развиваться на мировой арене. Пять наиболее распространенных схем хищений, описанных Group-IB в отчете за 2016 год, остались прежними:

• Хищение через SMS-банкинг.

• Переводы с карты на карту.

• Переводы через онлайн-банкинг.

• Перехват доступ к мобильному банкингу.

• Поддельный мобильный банкинг.

Активность владельцев Android-троянов резко снизилась благодаря задержаниям в 2017 году владельцев крупнейших в России Android бот-сетей: Cron и Tiny.z. Кроме того, владелец другой крупной бот-сети Honli просто прекратил использование этого трояна. Как следствие, количество проводимых ежедневных хищений снизилось почти в три раза. Также стоит отметить и снижение среднего размера хищений с использованием Android-троянов. Если в прошлом году он составлял 11 тысяч рублей, то в этом году он

опустился до 7 тысяч. Самой активной в прошедшем году была бот-сеть Asacub на базе одноименного приватного трояна. В августе 2017 появилось предложение о продаже форка этой вредоносной программы, но уже в сентябре тема была закрыта. Вторая по активности бот-сеть Agent.BID долгое время совсем не использовалась, и лишь с начала 2018 года ее владельцы вернулись к активной работе.

Веб-фишинг — единственный метод хищений, который показал рост в России в 2018 году.

Основные направления высокотехнологичных преступлений, в основе свершения которых лежат механизмы фишинга продемонстрированы на рисунке 1.2.

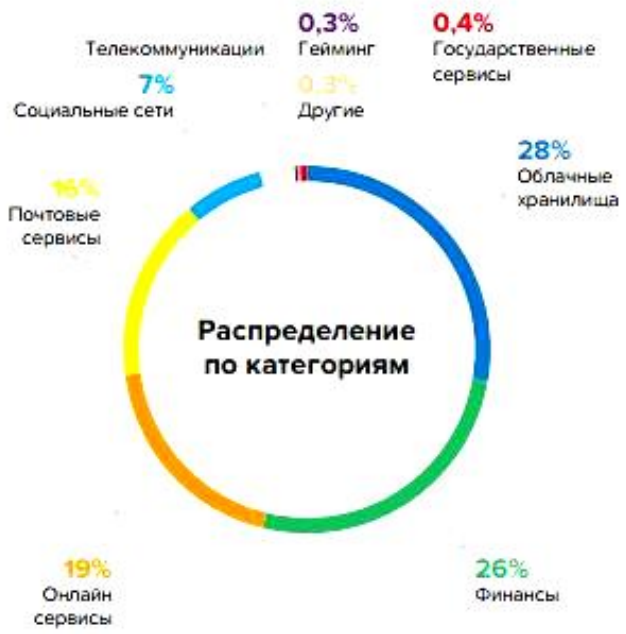

Рис. 1.2 Основные направления высокотехнологичных преступлений, в основе свершения которых лежат механизмы фишинга.

Количество групп, которые создают фишинговые сайты под российские бренды, выросло с 15 до 26. В России фишинг под банки и платежные системы автоматизирован и проходит в реальном времени, что позволяет обходить SMS подтверждения списания денег. Простота схем и широкий спектр инструментов для хищений привлекает на фишинговый рынок новых игроков. В этом году

с помощью веб-фишинга удалось похитить 251 миллион рублей, что на 6% больше, чем в прошлом году. Средняя сумма одного хищения не изменилась и составляет 1 000 рублей. Общее количество ежедневных успешных атак также выросло, но незначительно — до 1 274. Среднее количество жертв одной группы даже сократилось с 63 до 42. Основным фактором, сдерживающим рост количества атак, является активное выявление фишинговых сайтов и их оперативное закрытие, в том числе благодаря оперативному обмену данными между банками и ФинЦертом (FinCERT) Банка России. Основными способами привлечения пользователей на фишинговые страницы являются перенаправление посетителей со взломанных сайтов, а также в результате попадания в поисковую выдачу. В России, в отличие от многих других стран, под большую часть фишинговых сайтов регистрируется отдельное доменное имя. Большую популярность получил фишинг связанный с переводов с карты на карту. В некоторых случаях атакующие брендируют такие фишинговые страницы под конкретный банк, но есть и «небрендированный» фишинг.

Немаловажное место в совокупности высокотехнологичных хищений занимает кардинг. Рынок кардеров можно поделить на два основных сегмента: продажа текстовых данных о картах (номер, дата истечения, имя держателя, адрес, CVV) и «дампов» (содержимое магнитных полос карт). Текстовые данные собираются с помощью фишинговых сайтов, банковских троянов для ПК, Android, банкоматов, а также в результате взломов e-commerce сайтов. Дампы получают с помощью скимминговых устройств, а также с помощью троянов для компьютеров с подключенными POS-терминалами. Большая часть скомпрометированных карт продается на специализированных кардшопах. Системы GIB Threat Intelligence постоянно фиксируют и анализирует загружаемые на кардшопы данные. В среднем каждый месяц на них загружается 686 тысяч текстовых данных карт и 1.1 миллионов дампов. По данным Group-IB, 62% продаваемых данных карт относятся к дампам. Это означает, что POS-угрозы являются основным методом компрометации банковских карт. Кроме количественных показателей, компания Group-

IB фиксирует и стоимость каждого дампа, что позволяет измерять рынок кардинга. Текстовая информация о банковских картах стоит на кардшопах значительно дешевле: суммарно текстовые данные продавали всего за $95.6 миллионов, что составляет всего лишь 17% от общего рынка. Например, 19.9 миллионов дампов стоили уже $567.8 миллионов. Более подробная статистика рынка кардинга отражена в таблице 1.4.

Таблица 1.4.

Оценка рынка кардерских магазинов.

	Текстовые данные	Дампы	Всего
Общее количество	10 218 489	16 927 777	27 146 266
Размер рынка	$95 590 242	$567 791 443	$663 381 867
Минимальная цена	$0.75	$0.5	
Максимальная цена	$99.99	$295	
Средняя цена	$9.35	$33.54	

Основным методом получения дампов банковских карт является использование POS-троянов, которыми заражают компьютеры с подключенными POS-терминалами. Принцип работы всех POS-троянов остался неизменным: они собирают данные карт из оперативной памяти в тот момент, когда карты считывают через POS-терминал. Атакующие по-прежнему делятся на две категории:

• массово и случайно атакующие всех подряд в поисках возможности установить POS-троян;

• целенаправленно атакующие вендоров POS-терминалов или крупные сетевые организации, доступ в сети которых открывает возможность заражения сразу множества устройств.

Рынок POS-угроз достаточно динамичный. Отслеживая андеграундные форумы и участвуя в реагировании на инциденты, специалисты Group-IB регулярно наблюдают появление новых троянов, а также продажу и публикацию в открытом доступе исходных кодов уже зарекомендовавших в реальных атаках инструментов.

Некоторые группы не способны взломать сеть банка и заразить банкоматную сеть, но могут заразить отдельные банкоматы при наличии физического доступа. В прошедшем периоде для банковского сектора активными были две угрозы: Cutlet и Ploutus-D. Общая схема атаки «Jackpotting» включает 3 уровня злоумышленников:

• организатор / заказчик;

• разработчик ПО;

•дропы.

Главным в атаке является организатор, чаще всего он и заказывает разработку вредоносной программы. Основной целью организатора является получение денег с минимальными рисками. Для начала работы ему нужен полный набор инструментов. Есть два пути для их получения: заказать у разработчиков или перекупить у других злоумышленников. Далее организатор находит команду дропов (не менее 2-х человек) — людей, которым необходимо получить физический доступ к внутренней системе банкомата. Чтобы дропы не обманули организатора и не начали самостоятельную работу, в наборе вредоносных программ имеется специальный генератор ключей. Когда вредоносное ПО загружается в банкомат, оно требует ключ активации для дальнейшей работы. Такой ключ можно получить только из генератора ключей, который находится у организатора.

Для вскрытия банкомата злоумышленники высверливают, прорезают или прожигают отверстия на лицевой панели клавиатуры банкомата. Средний размер отверстия составляет 5 сантиметров. После этого они получают прямой доступ к шлейфу проводов. Злоумышленники отсоединяют диспенсер от USB-хаба или COM-порта (в зависимости от банкомата) и устанавливают на его

место специальную заглушку, которая имитирует работу диспенсера. Затем они подключают к USB/COM порту диспенсера микрокомпьютер с низким энергопотреблением. В этот момент дропы используют телефоны для взаимодействия с организатором и получения ключа активации. Средняя продолжительность действий злоумышленников, требуемых для хищения денежных средств, составляет около 8 минут. После получения наличности преступники заклеивали отверстие в банкомате с помощью наклейки.

В середине 2017 года появился новый комплект для атак на банкоматы, в том числе с новой вредоносной программой, которую назвали cutlet. Теперь вместе с набором инструментов шла максимально подробная инструкция по использованию с советами, как избежать проблем при работе. Впоследствии cutlet получила собственное приложение под Android, что позволяло злоумышленнику не использовать ноутбук, а обходится смартфоном.

25 января 2018 компания Diebold Nixdorf опубликовала отчёт «Potential Jackpotting US». В нём сообщается, что власти США предупреждают компанию о том, что на территории США впервые зафиксирована атака типа «Jackpotting» на банкоматы, произведенные их компанией. Ранее, в октябре 2017 года подобная атака была зафиксирована на территории Мексики. Также в СМИ появилась информация, что атаке могли под- вернуться банкоматы компании NCR Corp. Предположительно, злоумышленники для атаки использовали вредоносное ПО Ploutus-D. Ploutus-D – новая модификация более старой версии Ploutus. Эта программа впервые была замечена в Мексике в 2013 году. Тогда она распространялась при помощи CD-ROM. Первые упоминания Ploutus-D на андеграундных форумах датируются началом 2017 года. Однако ни одного положительного отзыва о работе или хотя бы проверке данного ПО нет, а все вендоры, которые создавали топики о его продаже, имеют плохую репутацию. Активных продаж программы на андеграундных форумах не замечено. Ploutus не уникальная разработка, в мире существует несколько различных реализаций примерно одной и той же схемы атаки. Различия между ними минимальны

и сводятся к специализации на определённом виде банкоматов, наиболее распространённых в регионе использования программы.

Атака на блокчейн. Эксплуатирование особенностей конкретных аспектов самой технологии блокчейн, как в «атаке 51%» или атаке повторного вывода средств.

Повторное использование учетных данных (Credentials reuse) Использование злоумышленниками известных им идентификаторов пользователя в других сервисах для получения доступа к кошельку (при условии их совпадения).

Взлом домена (Domain hijacking) Изменение данных регистрации домена. Например, хакеры изменяют А-записи и перенаправляют трафик веб-сайта на вредоносный сервер для сбора данных (логинов и паролей) или перевода средств.

Мошенничество изнутри проекта (Insider work) Использование доступа к информационным системам для кражи криптовалюты членом команды проекта или аутсорсным специалистом.

Вредоносное ПО (Malware). Атаки с использованием специально разработанного вредоносного программного обеспечения. Вредоносные программы используются не только для кражи приватных ключей или паролей пользователей, но и для доступа к машинам системных администраторов, а также создания бэкдоров в инфраструктуре биржи.

Фишинг (Phishing). Использование полной копии или имитации оригинального веб-сайта проекта, поддельных писем или сообщений от имени проекта для кражи конфиденциальной информации или загрузки вредоносного ПО на компьютеры жертв.

Уязвимость в исходном коде (Source code vulnerability exploitation) Использование логических ошибок или других уязвимостей в программном обеспечении, используемом на проекте.

Манипуляции на криптовалютных биржах – одни из самых распространенных незаконных схем хищений криптовалюты. Существует

множество различных схем манипуляций криптовалютным рынком. Например, схемы Pump&Dump (P&D). В таком случае трейдеры объединяются в группы в Telegram или Discord, число членов которых достигает нескольких тысяч человек. Затем они выбирают определенную криптовалюту, не имеющую особой ценности и перспектив (такие криптовалюты называют «shitcoin») и начинают одновременно скупать ее, тем самым искусственно взвинчивая курс. Этот этап называется «пампом», а следующий за ним этап, когда участники схемы продают свои позиции, – «дампом». Большинство мошеннических схем и инструментов атак, используемых для хищения криптовалют, аналогичны тем, что используются на традиционных рынках для хищения сведений о банковских картах и других пользовательских данных. Еще в 2016 году мы выпустили отчет о том, как хакерская группа Corkow взломала банк и, используя его брокерские счета, повлияла на обменный курс рубля. Аналогичное мошенничество, но с криптовалютой совершили неустановленные хакеры в начале 2018 года. Подготовка к атаке заняла более двух месяцев. Тактика действия атакующих на криптовалютном рынке была следующей:

1. В январе 2018 года неизвестная группа хакеров зарегистрировала домен, созвучный с брендом крупнейшей китайской криптобиржи Binance.

2. Ссылки на фишинговый ресурс начали рассылать трейдерам этой криптобиржи с целью получения их логинов и паролей.

3. Получив логины и пароли, атакующие смогли создать API-ключи, которые позволяют автоматизировать работу с биржей.

4. 7 марта 2018 года в течение двух минут атакующие автоматически, используя созданные ранее API-ключи скомпрометированных трейдеров, разместили множество заявок на покупку малоизвестной криптовалюты Viacoin.

5. Заявки на покупку привели к тому, что через 30 минут курс Viacoin подскочил на 143% с $2.80 до $6.79, по данным coinmarketcap.com.

6. После того как курс Viacoin вырос, атакующие начали продавать их за bitcoin с 31-го заранее подготовленного аккаунта.

7. После окончания торгов были отправлены запросы на вывод средств.

Атаки на ICO. В 2018 году количество проектов, выходящих на ICO снизилось, а их качество и уровень подготовки к кибератакам стали значительно выше. При этом объемы средств, которые вкладывают инвесторы, стали значительно больше, что привлекает внимание злоумышленников, за 2017 год «заработавших» на ICOболее $400 миллионов. Только за первое полугодие 2018 года ICO-проекты собрали почти $14 млрд — в два раза больше, чем за весь 2017 год ($5,5 млрд). В 2018 году атакам подверглись проекты, проводящие закрытый раунд ICO. Например, проект TON (Telegram Open Network), основанный Павлом Дуровым, подвергся фишинговой атаке, в результате чего злоумышленникам удалось украсть около $35000 в Ethereum. Все самое плохое, как правило, происходит именно в день старта продаж токенов в рамках проведения ICO. Шквал DDoS-атак одновременно с наплывом пользователей, лавина сообщений в в каналы Telegram и Slack, спам по списку рассылок.

Около 56% всех средств, украденных в ходе ICO, были похищены с помощью фишинговых атак. В разгар «криптовалютной лихорадки» все стремятся как можно быстрее купить токены (зачастую они продаются с большой скидкой) и не обращают внимания на такие мелочи, как подмененные домены. При этом фишинговая атака на ICO не требует серьезной подготовки и высокой квалификации. Схема атакующих осталась неизменной с 2016 года:

Злоумышленники отслеживают новые проекты, выходящие на ICO.

• Создают фишинговую страницу на доменном имени схожим с оригинальным. Основным отличием страницы является запрос секретного ключа или требование перевести криптовалюту на адрес мошеннического кошелька или смарт-контракта.

• На оригинальный сайт проекта начинается DDoS-атака, чтобы сделать его недоступным и спровоцировать инвесторов переходить на фишинговый ресурс.

• Одновременно с DDoS-атакой начинается SPAM-рассылка со ссылкой на фишинговый сайт.

• Кроме того, злоумышленники покупают контекстную рекламу в поисковых сетях, организовывают лавину сообщений в мессенджерах и любыми способами стараются нагнать трафик на фишинговый сайт, чтобы поднять его в топ поисковой выдачи. Если основной сайт проекта, выходящего на ICO, уязвим, то тактика меняется. Вместо создания фишингового ресурса непосредственно перед стартом ICO на оригинальном сайте заменяется адрес кошелька или смарт-контракта на мошеннические.

Фишинговые атаки на ICO-проекты не всегда проводятся с целью хищения средств. В этом году зафиксировано несколько случаев кражи баз данных инвесторов, участвующих в ICO. Такая информация затем может продаваться на андерграундных форумах или использоваться для шантажа.

Кража проекта Одна из особенностей проектов, выходящих на ICO, — полная открытость и прозрачность. Большая часть разработок и исходных кодов публикуется в открытом доступе. В первую очередь команда публикует White Paper, что открывает возможности для мошенничества.

• Злоумышленники находят новый не сильно раскрученный проект, но с хорошо проработанным описанием.

• Описание проекта полностью копируется и переводится на разные языки.

• Создается лендинг под новым брендом и с новой командой, но с ворованным описанием.

• Проект под новым брендом раскручивается в сети. Появляется контекстная реклама, ведутся обсуждения на специализированных площадках, чтобы привлечь внимание инвесторов.

У хакеров, которые могут профессионально провести целенаправленную атаку и похитить миллионы долларов появилась новая цель – криптобиржи. От их рук в 2016 году пострадали Bitfinex, Shapeshit, Gatecoin, Bitcurex. В 2017 и 2018 годах внимание хакеров к криптобиржам только возросло. Всего за 2017

год и первые 9 месяцев 2018 года было взломано 14 криптовалютных бирж, как минимум 5 из них были атакованфсеверокорейских хакеров из группы Lazarus, чьи жертвы преимущественно находятся в Южной Корее. Биржа YouBit (бывшая Yapizon) после второй атаки потеряла 17% своих активов и обанкротилась. Суммарно за 2017 и первые 9 месяцев 2018 года в результате взломов криптовалютных бирж было похищено $882 миллионов. в криптовалюте. 60% от общей суммы было похищено у японской биржи Coincheck.

Основным вектором проникновения в корпоративные сети криптобирж стал целевой фишинг. Злоумышленники отправляют вредоносные вложения, например, с темой «Engineering Manager for CryptoCurrency job», «Investment Proposal.doc», маскируясь под юридические компании и другие криптобирж. В случае запуска вредоносных файлов на компьютеры жертв устанавливается RAT, разработанный и постоянно обновляемый хакерской группой Lazarus. Далее злоумышленники исследуют локальную сеть и находят рабочие места или серверы, на которых осуществляется взаимодействие с приватными кошельками криптобирж.

Криптоджекинг – относительно новое направление, получившее наибольшее развитие в 2017-2018 гг. После загрузки специализированного вредоносного программного обеспечения вычислительные ресурсы компьютера используются злоумышленниками для добычи криптовалюты без ведома владельца. Программы для скрытого майнинга распространяются на тысячи компьютеров, образующих ботнет. Количество криптовалюты, получаемой в результате майнинга, напрямую зависит от совокупной производительности ботнета, поэтому вычислительные мощности в корпоративных сетях представляют для злоумышленников больший интерес, чем персональные компьютеры. Для массового распространения может использоваться, например, EternalBlue Exploit (CVE-2017-0144). Подобная уязвимость была использована при распространении шифровальщиков WannaCry в мае 2017 года и Petya в июне 2017 года. Так, операторы бот-сети намайнили при помощи трояна

Smominru, распространявщегося с помощью EternalBlue Exploit, приблизительно 8 900 Monero ($2.8-$3.6 миллионов). Каждый день ботнет добывал примерно 24 Monero, что на тот момент в среднем составляло $8500. Одной из первых успешных попыток разработки программного обеспечения для майнинга в браузере является решение Coinhive, заявившее о себе в сентябре 2017 года. Вслед за ним появились CryptoLoot, JSEcoin, Minr, CoinImp, ProjectPoi (PPoi), AFMiner, Papoto. Эти проекты предоставляли API, позволяющий владельцам веб-сайтов использовать вычислительные мощности компьютеров своих пользователей для майнинга криптовалюты. Такая модель сразу же привлекла внимание многих хакеров, которые обладают знаниями о том, как работать с нелегальным веб-трафиком. Можно выделить следующие векторы компрометации с целью встраивания вредоносных скриптов для майнинга:

1. Взлом веб-сайтов Взломы могут осуществляться разными способами: подбор паролей, эксплуатация уязвимостей в CMS или другом программном обеспечении, перехват паролей с помощью вредоносных программ или фишинговых сайтов. Поскольку майнинг осуществляется на компьютере посетителя и только в момент просмотра веб-сайта, залогом успеха является не количество взломанных сайтов, а их аудитория. Поэтому, как это было и с распространением обычных троянов методом Drive by download, сайты с высоким количеством посетителей ломаются целенаправленно.

2. Расширения для браузеров В 2017 году появилось расширение для Google Chrome под названием Active Poster. По некоторым оценкам, в скрытом майнинге участвовало более 100 тысяч пользователей. После нескольких жалоб в службу поддержки расширение было удалено. Аналогичные расширения были найдены и в браузере Mozilla Firefox.

3. Уязвимость третьей стороны (Third party services) Многие сайты используют сторонние JavaScript-библиотеки на своих страницах. Обычно это рекламные сети, аналитические или трекинговые сервисы. Операторы таких решений могут вставлять в свои скрипты майнинговый функционал специально

или в результате компрометации со стороны хакеров, как это было со скриптами Coinhive на YouTube.

4. Атаки Man-in-the-Middle Пользовательский трафик перенаправляется через промежуточные звенья, у которых зачастую есть доступ к контенту. Например, злоумышленники могут перехватывать незащищенный трафик, проходящий через точки доступа в публичный Wi-Fi, и вставлять в него к криптоджекинг-скрипты. Такие атаки уже были применены к сети Starbucks в Аргентине.

Незаменимым инструментом для проведения таких атак становятся бот-сети из домашних роутеров, например, Mirai и его аналоги. Заразив домашний роутер, можно манипулировать трафиком всех пользователей, которые его используют. В одном из последних случаев атакующему удалось найти 0-day уязвимость в маршрутизаторе MikroTik. С ее помощью он смог заразить около 200 000 устройств, которые встраивали в отображаемые страницы скрипт для майнинга от Coinhive.

АТАКА 51%. Как следует из названия, эта атака подразумевает установления контроля над 51% мощности системы. В роли атакующих может выступать как один майнер с крупным сосредоточением вычислительной техники, так и группа — пул. Однако получение контроля над 51% мощности не обязательно считать атакой, по крайне мере, до тех пор, пока владелец этой мощности не начнет целенаправленно использовать свое преимущество. Владея 51% мощности сети, атакующий может:

- заморозить работу системы;
- остановить подтверждение транзакций;
- приостановить майнинг;
- лишить других майнеров возможности подтверждать транзакции;
- списывать средства повторно.

Наибольшей опасностью для системы считается повторное списание средств (double spending). Так, атакующий может создать скрытый альтернативный блокчейн и использовать его для подтверждения собственных

транзакций. Двойное списание средств возможно и при меньшем контроле мощностей, но именно сосредоточение 51% предоставляет 100% гарантию, что верным блоком будет признан блок злоумышленника. О самой «атаке 51%» известно уже давно. Например, в 2016 году проекты Krypton и Shift подверглись атаке этого типа. В том же году известный в криптосообществе китайский предприниматель Чандлер Го заявил, что намерен при поддержке других майнеров осуществить «атаке 51%» на проект Ethereum Classic. И если в 2017 успешных атак этого типа не было, то в первой половине 2018 рынок столкнулся сразу с пятью случаями успешных атак:

• 4 апреля Сеть криптовалюты Verge подверглась «атаке 51%», которая стала возможной из-за бага в коде. Атака продлилась примерно три часа и, по оценкам одного из участников дискуссий, атакующий мог добыть криптовалюту на сумму более $1 миллион.

• 18 мая Директор по коммуникациям Bitcoin Gold Эдвард Искра впервые предупредил об атаке и указал, что майнер захватил по меньшей мере 51% хешрейта сети. Так, начиная с 16 мая на BTG-адрес атакующего поступило более 388 тысяч монет Bitcoin Gold. Таким образом, злоумышленник мог «заработать» около $18 миллионов.

• 22 мая Майнинговый пул SuprNova сообщил, что блокчейн криптовалюты Verge подвергся атаке 51% и все корректные блоки отвергаются. По их информации, проблема затронула все пулы и всех майнеров, поскольку злоумышленник на тот момент контролировал все блоки. Представители самого проекта ранее сообщили о вероятной DDoS-атаке на пулы и задержках с валидацией блоков.

• 3 июня Блокчейн ZenCash подвергся «атаке 51%», в результате которой неизвестные злоумышленники похитили более $550000 в эквиваленте криптовалюты ZEN. Злоумышленникам удалось реорганизовать 38 блоков, а сама атака продлилась менее четырех часов. по данным сайта Crypto51, который оценивает затраты на «атаки 51%», операция обошлась злоумышленникам в $30000.

• 6 июня Сеть недавно появившейся криптовалюты Litecoin Cash (LCC), которая является форком более известной криптовалюты Litcoin (LTC), также столкнулась с атакой 51%.

Таким образом, мы можем сделать вывод о постоянном совершенствовании инструментария преступных групп и об актуальности разработки методов противодействия их деятельности. Поскольку непосредственной задачей в противодействии деятельности преступников в сети Интернет является идентификация их IP-адреса, рассмотрим более подробно механизмы анонимизации кибер-преступников.

ГЛАВА 2. СРЕДСТВА АНОНИМИЗАЦИИ ПРЕСТУПЛНИКОВ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ИМ

§ 1. Средства анонимизации преступников

Сложность раскрытия преступлений в сфере высоких технологий заключается в умелой анонимизации преступников. Получение денег злоумышленниками в этом случае происходит через посредников, занимающихся обналичиванием незаконно добытых средств. В этом случае трудно определить не только мошенника, но и обнальщика, так как большинство денежных операций происходит в сети Интернет с использованием обезличенных виртуальных валют. Согласно отчету FATF наиболее востребованным видом криптовалюты является Bitcoin, разработанный неизвестным для широкой общественности программистом (или группой программистов), выступающим под псевдонимом Satoshi Nakamoto, под авторством которого в ноябре 2008 г. была опубликована «Белая книга» с описанием механизма функционирования Bitcoin и его протокола. Bitcoin – это децентрализованная P2P платежная сеть, обслуживаемая ее пользователями, функционирующая без органов управления и посредников на фоне отсутствия централизованного контроля. В основе сети Bitcoin лежит публичный реестр (Blockchain, или «цепочка блоков»), в котором хранится информация обо всех произведенных транзакциях пользователей сети между собой и тем самым подтверждается или опровергается факт проведения той или иной транзакции. В свою очередь, подлинность каждой транзакции защищена электронными подписями в соответствии с использованными в транзакции адресами, что позволяет пользователям иметь полный контроль над процессом передачи Bitcoin со своих Bitcoin адресов получателям.[1]

[1] Батоев В. Б., Семенчук В.В. Использование криптовалюты в преступной деятельности:

Также ни одно серьезное преступление в сфере высоких технологий не проходит без использования средств анонимизации. Анонимизация — процесс обеспечения анонимности. Анонимизация чаще всего заключается в изменении свойств сетевого профиля субъекта с целью обеспечения их несвязности с пользователем, либо же с целью использования более распространенных значений некоторых свойств.[1] Этот факт значительно затрудняет, а иногда делает невозможным установление реального IP-адреса кибер-преступника. Рассмотрим средства анонимизации преступников более подробно.

Одним из наиболее распространенных и эффективных ПО, маскирующих является браузер TOR. Он находится в свободном доступе для скачивания и установки. Скачав его, любой человек может замаскировать свой IP-адрес как минимум через 5 звеньев. Вышеуказанный браузер используется в основном рядовыми пользователями сети «глубокого Интернета» для получения доступа к сайтам, недоступным в обычных браузерах с доменными именами .onion. Основная цель массового использования Tor'a – покупка запрещенных законодательством товаров, таких как: наркотики, поддельные документы, оружие и т.д. Он так же подходит для осуществления профессиональной преступной деятельности.

Использование данного ПО делает невозможным вычислить преступника путем отправки запросов интернет-провайдерам и хостинг-компаниям в 99% случаев. В основном это обусловлено большим количеством времени, уходящим на расшифровку цепи IP-адресов, поскольку они становятся известны последовательно отправке запросов. Более того, отправка запросов в большинстве случаев не эффективна, поскольку владельцы серверов, через которых проходить интернет-трафик злоумышленника, как правило, находятся на территории и в правовом поле иностранного государства. Таким образом

проблемы противодействия // Труды Академии управления МВД России. 2017 - № 2 (42) – с 7.

[1] Тюрин К.А. , Болдырихин Н.В. Алгоритм вероятностной идентификации пользователей сетей//Издательство: Донской государственный технический университет - 2016 - с. 81-86.

получение компьютерной информации путем последовательной отправки запросов владельцам серверов, через которые проходил трафик злоумышленника не дает результатов, ведущих к идентификация мошенников при использовании ими браузера.

Для большей анонимизации преступники работают с TOR’ом через соединения VPN, шифрующие интернет-трафик.

VPN (англ. Virtual Private Network — виртуальная частная сеть). VPN – это обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии. В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

VPN-туннель – это виртуальное зашифрованное стойким алгоритмом соединение. Наглядно, его можно представить в виде непрозрачной трубы, а еще лучше этакого тоннеля, один конец которого упирается в компьютер рядового пользователя, а второй в специализированный сервер, находящийся, как правило, в удалении или даже в другой стране. Современные виды VPNподключения:

- PPTP (англ. Point-to-point tunneling protocol);
- OpenVPN;
- L2TP (англ. Layer 2 Tunneling Protocol).

PPTP (Point-to-point tunneling protocol) – это такой туннельный протокол типа "точка-точка", который позволяет компьютеру пользователя устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. Этот протокол (PPTP) стал известен, потому что, это первый VPN - протокол, который поддержала корпорация Microsoft. Все версии Windows, начиная с Windows 95

OSR2, уже включают в свой состав PPTP-клиент. Это самый известный и простой в настройке вариант подключения к VPN-сервису. Но, как говорится, есть здесь и отрицательный момент: многие интернет- провайдеры блокируют работу PPTP подключений.

OpenVPN – это свободная реализация технологии Виртуальной Частной Сети (VPN) с открытым исходным кодом для создания зашифрованных каналов вида "точка-точка" или сервер-клиенты между компьютерами. Она может устанавливать соединения между компьютерами, которые находятся за NAT-firewall без необходимости изменения его настроек. Но использование, этой технологии потребует установки дополнительного программного обеспечения для всех операционных систем.

L2TP (Layer 2 Tunneling Protocol) – это сетевой протокол туннелирования канального уровня, сочетающий в себе протокол L2F (layer 2 Forwarding), разработанный компанией Cisco, и протокол корпорацией Microsoft. Позволяет создавать VPN с заданными приоритетами доступа, однако не содержит в себе средств шифрования и механизмов аутентификации (для создания защищённой VPN и его используют совместно с IPSec). По отзывам экспертов, является наиболее защищенным вариантом VPN подключения, несмотря на трудность его настройки.[1]

Во избежание идентификации по личным аккаунтам в почтовых сервисах и социальных сетях, злоумышленники работают через виртуальную машину. И TOR и программы для подключения через VPN-туннели устанавливаются на чистую Windows, которая работает на основе программ VMware и VirtualBox. Такая комбинация действий исключает возможность подключений злоумышленника через IP-адреса, используемые для преступных действий.

[1] В.А. Артамонов, Е.В. Артамонова МНОО «Международная академия информационных технологий» (ООН) - 2016 – с. 3

Заканчивается цепочка анонимизации использованием 3G или 4G модема и симок, купленных на сайтах объявлений у неизвестных лиц. Визуально она показана на схеме 2.1:

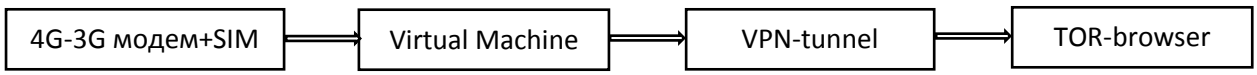

Схема 2.1 Последовательная цепь средств анонимизации преступников в Интернете.

При использовании вышеуказанной схемы анонимизации трафика, вычислить преступника путем наведения справок практически не представляется возможным. Также нельзя упускать из внимания, что данная схема не является каким-либо стандартом, или универсальным способом. Средств анонимизации и способов их применения бесконечное множество.

Однако, следует заметить что нельзя упускать из виду важную деталь - объект преступления, а именно – материальные ценности. В случае с совершением преступлений в сети Интернет этими ценностями чаще всего становятся электронные деньги, или криптовалюта. В большинстве случае, процесс обналичивания незаконно добытых денежных средств не происходит без использования криптовалют. Они считаются анонимными, хотя на практике это не всегда соответствует действительности. Рассмотрим преимущества применения криптовалюты Bitcoin в целях обезличивания денежных средств. Основные преимущества, которые привлекают преступников, это:

- Биткоин-адреса и протокол не требуют идентификации клиента.
- Криптобиржи не так строго регулируются, как обычные, которые по закону обязаны хранить надлежащую документацию своих клиентов.
- Такие устройства, как микшер или тумблер, смешивают несколько транзакций вместе, что затрудняет отслеживание определенного адреса.

- Транзакции могут выполняться через сеть TOR, которая направляет веб-трафик через несколько нод (составные части сети), тем самым скрывая реальный IP-адрес.
- Трудно определить, в какой юрисдикции должно проводиться уголовное расследование, если таковое имеется, поскольку сделка может распространяться по нескольким странам и организациям.
- Трудно определить, какой закон о противодействии отмыванию денег и соблюдение должны применяться, когда сделка идет по нескольким странам.
- В большинстве стран законы еще не разработаны.

Это делает Bitcoin почти анонимным платежным средством. Однако, использование вышеуказанной криптовалюты не единственный инструментарий в арсенали кибер-преступников.

Разберем некоторые способы цифрового отмывания денег, не только через биткоин:

- eCache: Некоторые виртуальные валюты, такие как eCache, полностью анонимны. По словам его операторов, eCache не связывает человека с транзакциями; он работает как сертификат цифрового носителя (DBC), который может быть передан другой стороне, как и любые другие данные в Интернете. Есть и другие анонимные криптовалюты. Для биткоина есть Dark Wallet: кошелек, который помогает BTC стать полностью анонимным.
- Crowdfunding можно использовать для отмывания денег несколькими способами. Например, эмитент может вступить в сговор с инвесторами для обмена денег на ценные бумаги. Согласно новому отчету FINCEN, в отчетах о подозрительной деятельности были выявлены случаи незаконного использования платформ сбора средств с толпы для отмывания денег, возможного финансирования терроризма, мошенничества с кредитными картами, кражи личных данных, схем фишинга и злоупотреблений со стороны компании.

- Схема — положить деньги на кредитные карты с подставными данными, открыть с них кошелек и делать покупки онлайн.
- Возврат акций в цифровой форме: облигации на предъявителя выпускаются как бумага и подлежат оплате держателем инструмента. Следовательно, их право собственности не регистрируется эмитентом, что удобно для преступников при перемещении средств.
- ММОРПГ игры: многие игроки используют виртуальные валюты в MMORPG. Преступники используют виртуальные валютные системы в этих играх для отправки виртуальных денег партнерам в другой стране. Популярные игры для такого типа схем — Second Life и World of Warcraft.
- Фирмы-консультанты: якобы покупаются информационно-консультационные услуги у иностранной фирмы.

Рассмотрев вышеуказаные средства анонимизации преступников на различных стадия совершения преступлений – от приготовления до легализации полученных доходов, мы можем делать вывод о том, что средства и методы совершения кибер-преступлений динамично развиваются и требуют симметричного развития методов противодействия со стороны сотрудников правоохранительных органов.

§ 2. Методы противодействия анонимизации злоумышленников и негласного получение доказательственной базы

Один из вариантов решения проблемы деанонимизации преступника – разработка и использование оперативными подразделениями специального программного обеспечения, направленного на вычисление реальных IP, MAC

адресов преступников, идентификации личности преступника по содержимому его компьютера.

Данная программа работает по типу троян-вируса в оболочке картинки, архива, файла-документа и т.д. Программа инициирует сбор информации об аппаратном и программном обеспечении с последующей записью её в отдельный файл. После чего данный файл отправляется по заранее определенному адресу. Обычным способом отследить отправку этой информации затруднительно, поскольку отправляемый трафик пользователя сети интернет не подотчетен провайдеру. Это повышает эффективность использования данного ПО.

Использование программы может проходить в 4 этапа:

1) Внедрение программы в файл-ловушку. При открытии файла, программа внедряется в ПК преступника.

2) Отправка файла злоумышленнику. Процесс должен проходить легендировано, от имени потенциальной жертвы, либо другим способом.

3) Внедрение программы в ПК преступника.

4) Получение данных об аппаратном и программном обеспечении злоумышленника.

Таким образом мы видим, что разработка и использование данного программного обеспечения является доступным и практически применимым в современных условиях.

Вышеописанное программное обеспечение может быть применимо в процессе оперативной разработки подозреваемых в совершении противоправных действий в сфере высоких технологий. Поскольку процесс использования программы предполагает создание условий оперативными сотрудниками, вводящих злоумышленника в заблуждение, и документирование их действий, данный процесс можно характеризовать как оперативно-розыскное мероприятие – оперативная комбинация.

Перечень этапов оперативной комбинации схож с алгоритмом использования предполагаемого программного обеспечения, изложенным выше.

Реалии современного законодательства не предполагают использование вышеописанного программного обеспечения в целях борьбы с преступностью. По характеру действия и целям применения оно входит в классификацию вредоносного ПО. Ответственность за создание, использование, распространение и модификацию вредоносного программного обеспечения предусмотрена ст. 273 УК РФ.

В то же время, запрещенные в обороте наркотические вещества и радиоэлектронных и специальных технических средств, изъятых из оборота или ограниченно оборотоспособных на территории Российской Федерации, используются в деятельности оперативных подразделений. По аналогии, программное обеспечение, содержащее в себе признаки вредоносных программ также, как и наркотические вещества со специальными техническими средствами, могут быть использованы в оперативно-розыскной деятельности.

Таким образом, мы можем сделать вывод о том, что механизмы способов противодействия преступникам в сфере незаконного оборота наркотических и психотропных веществ могут быть схожи с предложенными механизмами. Рассмотрим подробнее механизмы и правовые основы проведения оперативно-розыскных мероприятий с использованием вышеупомянутых средств.

ГЛАВА 3. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ, НАРКОТИЧЕСКИХ ВЕЩЕСТВ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ И МЕРЫ ПО ИХ СОВЕРШЕНСТВОВАНИЮ

§ 1. Правовые основы использования технических средств и наркотических веществ в оперативно розыскной деятельности

Применение предлагаемого программного обеспечения предполагает ограничения прав и свобод граждан, посколько его функционал несколько схож с функционалом компьютерного вируса. Использование вредоносного программного обеспечения влечет за собой ответственность в соответствии с действующим российским законодательством, что противоречит принципам и целям ОРД. Однако, если разобраться в специальной технической терминологии, содержимом УК РФ (а именно ст. 273), а также в нормативных правовых актах, регулирующих применение оперативными подразделениями ОВД средств, изъятых из гражданского оборота, мы увидим, что использование предлагаемого программного обеспечения не является нарушением закона. Его можно применять в ОРМ аналогично наркотическим веществам, псиотропным препаратам, а также специальным техническим средствам, предназначенным для негласного сбора информации.

Законом разрешено использование наркотических средств в оперативно-розыскных целях. Ответственность за приобретение, хранение, перевозка и сбыт наркотических веществ предусмотрена ст. 228 УК РФ. Однако, в соответствии со ст. 36 ФЗ-№3 «О наркотических средствах и психотропных веществах», при проведении контролируемых поставок, проверочных закупок, оперативного эксперимента, сбора образцов для сравнительного исследования, оперативного внедрения, исследования предметов и документов органам,

осуществляющим оперативно-розыскную деятельность, разрешается использование наркотических средств, психотропных веществ и их прекурсоров без лицензии.[1]

Наркотические средства используются правоохранительными органами в таком мероприятии, как проверочная закупка. Проверочная закупка – это оперативно-розыскное мероприятие, при котором с ведома и под контролем органов, осуществляющих оперативно-розыскную деятельность, допускается приобретение наркотических средств, психотропных веществ и их прекурсоров, а также инструментов или оборудования.[2]

Проводится путем заключения с лицом, подозреваемым в занятии незаконной деятельностью, мнимой сделки по возмездному приобретению предметов без цели их последующего потребления или сбыта. В соответствии со ст. 36 Закона о наркотиках данное мероприятие сотрудники оперативных подразделений могут проводить без лицензии. При этом исходя из буквального смысла закона «Об ОРД», оперативный сотрудник или иное лицо может выступать только в качестве покупателя наркотиков, а не их продавца, даже если данный способ изобличения в преступной деятельности будет более эффективный.

Для использования наркотических средств при проведении такого ОРМ, как проверочная закупка, необходимо постановление начальника оперативно-розыскного органа, а также постановление суда.

Вышеуказанная правая норма, регулирующая оборот наркотических средств и психотропных веществ, а также практика правоохранительных органов в использовании наркотиков при проведении ОРМ является примером того, как запрещенные законом предметы используются в оперативно-розыскных целях. Исходя из этого мы можем сделать вывод, что предлагаемое нами программное обеспечение может быть использовано по аналогии в

---

[1] Федеральный закон от 08.01.1998 N 3-ФЗ (ред. от 29.12.2017) "О наркотических средствах и психотропных веществах".

[2] Хачатрян Г. А. Тактика проведения проверочной закупки наркотических средств и психотропных веществ // Молодой ученый. — 2014 — №2 — С. 221-223.

оперативно-розыскной деятельности с наркотическими средствами. Однако, пример с использованием наркотических средств при осуществлении оперативно-розыскной деятельности – не единственный.

Еще одним примером использования оперативными подразделениями средств, ограниченных в гражданском обороте, является использование специальных технических средств для негласного получения информации. Разберем нормативно правовые основы, регулирующие их оборот и использование.

Федеральным законом № 420-ФЗ от 07 декабря 2011 г. «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» утверждена ч. 3 ст. 138 УК РФ, предусматривающая ответственность за незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации, утратила силу и появилась самостоятельная ст. 138 УК «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации». Ввоз и вывоз данных технических средств регламентируется Постановлением Правительства РФ от 10 марта 2000 г. N 214 "Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию".[1]

Постановлением Правительства Российской Федерации от 1 июля 1996 г. № 770 (ред. от 15.07.2002) «Об утверждении Положения о лицензировании физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством,

[1] Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию. [Поставновление Правительства РФ от 10 марта 2000 г. №214] // СПС Гарант.

реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности»[1] утвержден «Перечень видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности.»

Среди них указаны средства, предназначенные:

- для негласного получения и регистрации акустической информации;
- для негласного визуального наблюдения и документирования;
- для негласного прослушивания телефонных переговоров;
- для негласного перехвата и регистрации информации с технических каналов связи;
- для негласного контроля почтовых сообщений и отправлений;
- для негласного исследования документов и предметов;
- для негласного проникновения и обследования помещений, транспортных средств и других объектов;
- для негласного контроля за перемещением транспортных средств и других объектов;
- для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.

---

[1] Об утверждении Положения о лицензировании физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности. [Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 (ред. от 15.07.2002)] // СПС Гарант.

К техническим средствам для негласного получения информации, свободный оборот которых в Российской Федерации запрещен, относятся только специальные технические средства, предназначенные именно для целей негласного (т.е. тайного, неочевидного, скрытого) получения информации, тайна и неприкосновенность которой гарантированы Конституцией РФ.

Объективная сторона состава преступления, предусмотренного ст. 138 УК РФ, выражается в совершении незаконных альтернативных действий в виде производства, приобретения и (или) сбыта специальных технических средств, предназначенных для негласного получения информации.

Незаконность действий означает, что виновный, не будучи уполномоченным на то законом или подзаконными актами, производит, приобретает и (или) сбывает специальные технические средства, предназначенные для негласного получения информации.

Разберем правовые основы применения специальных технических средств.

Правовая основа применения специальной техники – это система законодательных и подзаконных актов, а также устанавливаемых ими принципов и правил, определяющих допустимость использования либо регламентирующих организацию, порядок, условия, способы и результаты использования технических средств в обеспечении правопорядка.

Законодательной основой правового регулирования применения специальной техники является Конституция Российской Федерации – основа всего федерального законодательства, ее нормы имеют прямое действие.

Требование ст. 23 Конституции РФ закрепляет право граждан на неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. Не допускается распространение информации о частной жизни лица (равно как и сбор, хранение, использование сведений) без его согласия (п. 1 ст. 24), жилище неприкосновенно (ст. 25).

Однако, ст. 55 Конституции РФ предусматривает ограничение прав и свобод человека и гражданина федеральным законом, но только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Следовательно, применение правоохранительными органами технических средств возможно не только для получения в рамках закона необходимой информации, но и защиты на законных основаниях информационных и имущественных прав и свобод граждан.

В Российской Федерации приняты и действуют законодательные акты, которые содержат нормы, допускающие использование технических средств и соответствующих приемов и действий в процессе осуществления правоохранительной деятельности.

В соответствии со ст. 11 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

Полиция предписано применять электронные формы приема и регистрации документов, уведомления о ходе предоставления государственных услуг, взаимодействия с другими правоохранительными органами, государственными и муниципальными органами, общественными объединениями и организациями.

Полиция использует технические средства, включая средства аудио-, фото- и видеофиксации, при документировании обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий, в том числе в общественных местах, а также для фиксирования действий сотрудников полиции, выполняющих возложенные на них обязанности.

П. 4 ст. 11, гласит, что Федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность использования

информационно-телекоммуникационной сети Интернет, автоматизированных информационных систем, интегрированных банков данных.

П. 56 ст. 12 Указа Президента Российской Федерации от 01 марта 2011 года № 248 «Вопросы Министерства внутренних дел Российской Федерации» к сфере полномочий МВД относит внедрение достижений науки, техники и положительного опыта в деятельность органов внутренних дел, а также развитие связи и автоматизированного управления в системе МВД России;[1]

Полиция имеет право осуществлять оперативно-розыскную деятельность в соответствии с Федеральным законом от 12 августа 1995 г. «Об оперативно-розыскной деятельности», который является базовым актом в вопросах применения специальных технических средств, предназначенных для негласного получения информации (оперативной техники). Ст. 6 ФЗ «Об ОРД» разрешает оперативным аппаратам правоохранительных органов (субъектов ОРД) использовать в ходе проведения оперативно-розыскных мероприятий информационные системы, видео- и аудиозапись, кино- и фотосъемку, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и вреда окружающей среде.

Статья 6 Федерального закона «Об оперативно-розыскной деятельности» позволяет использовать для решения задач оперативно-розыскной деятельности помощь специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе.

Указ Президента РФ от 01.09.95 № 891 «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» разграничивает полномочия Федеральной службы безопасности и МВД по проведению оперативно-розыскных мероприятий с использованием технических средств. Установлено, что контроль почтовых отправлений, телеграфных и иных сообщений в интересах органов,

[1] Вопросы Министерства внутренних дел Российской Федерации: Указа Президента Российской Федерации от 01 марта 2011 года № 248 // СПС КонсультантПлюс.

осуществляющих оперативно-розыскную деятельность, возлагается на органы федеральной службы безопасности.[1]

Оперативно-розыскные мероприятия, связанные с подключением к станционной аппаратуре операторов связи, в интересах органов, осуществляющих оперативно-розыскную деятельность, проводятся с использованием оперативно-технических средств органов федеральной службы безопасности. При отсутствии у органов федеральной службы безопасности на объектах связи необходимых оперативно-технических возможностей указанные мероприятия проводятся органами внутренних дел Российской Федерации, в том числе в интересах других органов, осуществляющих оперативно-розыскную деятельность.

Установлена юридическая ответственность физических и юридических лиц за незаконное использование специальных и иных технических средств, предназначенных для негласного получения информации.

Ст. 138 Уголовного кодекса РФ устанавливает ответственность за нарушение тайны переписки, телефонных переговоров, почтовых и иных сообщений. При этом объективная сторона преступления выражается как в незаконном ознакомлении с содержанием телефонных переговоров и почтово-телеграфной корреспонденции, так и в придании огласке сообщенных гражданами друг другу сведений.

Применение специальной техники представляет собой процесс поиска, сбора, хранения, обработки, предоставления информации, т.е. является информационной технологией. Правоотношения, возникающие при применении информационных технологий регулируются Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Помимо регулирования отношений, связанных с применением информационных технологий, он регламентирует процессы

[1] Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств: Указ Президента РФ от 01.09.95 № 891 // СПС Гарант.

поиска, получения, передачи, производства и распространения информации и обеспечении защиты информации.

Федеральный закон «О связи» от 07.07.2003 №126-ФЗ установил правовую основу деятельности в области связи, определил полномочия органов государственной власти по регулированию указанной деятельности, а также права и обязанности физических и юридических лиц, участвующих в указанной деятельности или пользующихся услугами связи. Законом определяются основные положения о связи в Российской Федерации.

Статья 16 посвящена сетям связи специального назначения, которые предназначены для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка. Порядок подготовки и использования ресурсов единой сети электросвязи Российской Федерации в целях обеспечения функционирования сетей связи специального назначения определен «Правилами подготовки и использования ресурсов единой сети электросвязи российской федерации в целях обеспечения функционирования сетей связи специального назначения» утвержденными Постановлением Правительства Российской Федерации от 22 февраля 2006 г. N 103.

Постановление Правительства Российской Федерации от 25 августа 2008 г. N 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» определяет, что оснащению аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS подлежат технические средства и системы, специальная техника, а также транспортные средства.

В отдельную группу таких документов входят ведомственные нормативные акты по вопросам технической политики органов внутренних дел, акты, утверждающие перечень новых образцов технических средств, принятых на их вооружение, а также нормативные документы, регламентирующие нормы табельной положенности подразделений правоохранительных органов техническими средствами, сроки их эксплуатации.

В оперативно-розыскной деятельности вышеупомянутые технические средства используются оперативными подразделениями при проведение ОРМ, связанных с негласным получением и фиксированием информации, в том числе и подразумевающих собой нарушение права граждан на неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. В этом случае мероприятие должно быть санкционированно постановлением суда.

Таким образом, вышеуказанные правовые нормы, регулирующие оборот наркотических средств и психотропных веществ, а также специальных технических средств, предназначенных для негласного получения информации, а также практика правоохранительных органов проведения ОРМ являются примером того, как запрещенные законом предметы и вещества используются в оперативно-розыскных целях.

§ 2. Меры по совершенствованию правового регулирования использования технических средств, предназначенных для негласного получения информации

Предлагаемое нами программное обеспечение предполагает скрытный доступ к личной информации преступника, а также её копирование и передачу на удаленный сервер / персональный компьютер ОВД. По характеру действия, способу внедрения в компьютер злоумышленника и перечню функций, она подпадает под характеристику вредоносной компьютерной программы.

Вредоносная программа — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с

целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путём копирования, искажения, удаления или подмены информации.

Рассмотрим статью 273 УК РФ.

Согласно ст. 273 УК РФ, уголовно преследуется создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Объективную сторону составляет факт создания компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Наиболее распространенными видами вредоносных программ являются компьютерные вирусы, черви, программы-сканеры, эмуляторы электронных средств защиты, программы управления потоками компьютерной информации, программы-патчеры.

С субъективной стороны преступление характеризуется виной в форме прямого умысла, о чем свидетельствует указание законодателя на заведомый характер деятельности виновного. В этой статье определено, что создание, использование или распространение вредоносных программ заведомо для виновного предназначено для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

В случае создания и использования программы в оперативно-розыскных целях, исключается и объективный, и субъективный состав.

1) Программа предназначена для получения доказательной базы, а также определения местонахождения преступника. В связи с этим, исключается виновный умысел и общественная опасность деяния.

2) Применение программного комплекса будет санкционированным, если его использование мотивированно отсутствием иных эффективных методов определения местонахождения преступника, а также получения доказательной базы. Санкционирование может быть произведено начальником оперативного подразделения, а также, в обязательном порядке судом, поскольку её применение затрагивает тайну личной жизни граждан.

Нами было проведено эмпирическое исследование в форме опроса сотрудников оперативных подразделений, которые в своей служебной деятельности сталкивались с раскрытием преступлений в сфере высоких технологий. Результаты исследования показали, что применение вышеупомянутого программного обеспечения сочли целесообразным 80% респондентов. 95% опрошенных сообщили, что с подобным способом решения оперативно-тактических задач не сталкивались. Причиной отсутствия опыта использования подобного программного обеспечения признали отсутствие нормативно-закреплённых механизмов использования программного обеспечения в ведомственных инструкциях 45% респондентов. Более подробный перечень вопросов и ответов изложен в Приложении 1. В виду этого мы полагаем, что основным препятствием в реализации предложенного нами метода является отсутствие нормативно-правовой базы работы оперативных сотрудников с программным обеспечением.

Большинство законодательных актов, упомянутых при детальном изучении правового регулирования использования специальных технических средств для негласного получения информации, можно использовать в качестве правовой основы легализации предлагаемого программного обеспечения. Для этого необходимо внести изменения в следующие нормативно-правовые акты:

1) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» - о разрешении

использования вредоносного программного обеспечения в целях оперативно-розыскной деятельности.

2) «Перечень видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности.», утвержденный Постановлением Правительства Российской Федерации от 1 июля 1996 г. № 770 (ред. от 15.07.2002) «Об утверждении Положения о лицензировании физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» - о включении программного обеспечения с предлагаемым нами функционалом в перечень специальных технических средств, предназначенных для негласного получения информации.

Таким образом, внеся необходимые изменений в вышеуказанные нормативно-правовые акты, мы сможем легализовать использование предложенного нами программного обеспечения в оперативно-розыскных целях.

ЗАКЛЮЧЕНИЕ

Мы изучили основные направления и механизмы совершения преступлений в сфере высоких технологий и выявили, что преступность в сфере высоких технологий является одной из самых динамично развивающихся, вслед за самой индустрией информационных технологий. Основным объектом выше указаных преступлений является информация, имеющая материальную ценность. Экономика в целом, и финансовые потоки в частности всё больше перетекают в информационное поле. Соответственно, растёт количество видов и способов хищения информации, представляющей материальную ценность. В связи с этим злоумышленники изучают, разрабатывают и тестируют всё больше способов совершения преступлений. Самые распространенные из них, это:

1. Атаки на блокчейн-проекты;
2. Кардинг;
3. Хакерские атаки с помощью Android-троянов;
4. Атаки банк-клиентов.
5. Фишинг;
6. Целевые атаки на банки.

В 2017 году произошел всплеск популярности инвестирования и использования криптовалют. Поскольку данные платежные средства в правовом поле разных стран мира регулируются слабо, или не регулируются вообще, они стали самым популярным объектом хищений в сети Интернет. Согласно приведенных выше данным, суммы, украденные у некоторых международных криптовалютных бирж за 2017-2018 годы существенно превышают суммы хищений фиатных валют банков. Данная ситуация обусловлена тем, что рынок криптовалют появился не так давно, и системы безопасности еще не успели довести до совершества. К тому же, криптовалюты

основаны на блокчейн-технологиях, большинство из которых являются open-source проектами и открыты к модификациям большого круга разработчиков по всему миру. Таким образом, ввиду колоссального роста технических возможностей кибер-преступников и медленного развития механизмов правового регулирования, правоохранительным органам требуются принципиально новые методы и средства борьбы с злоумышленниками.

Мы предложили использование программного обеспечения, позволяющего скрытно получать информацию с технических устройств (мобильный телефон, персональный компьютер). Однако, некоторые функции и способ внедрения программы злоумышленнику, могут быть схожи с признаками вредоносного программного обеспечения. В таком случая, действия сотрудника оперативного подразделения могут квалифицировать как преступление, предусмотренное ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ». Разобрав ст. 273 УК РФ, мы сделали вывод, что в случае применения вышеупомянутого программного обеспечения сотрудником правоохранительных органов в оперативно-розыскных целях, а именно - получение доказательств противоправной деятельности преступника, ни субъективного, ни объективного состава ст. 273 УК РФ не усматривается.

Также, рассмотрев нормативно-правовые акты, дающие основания для использования технических средств ограниченного гражданского оборота, мы можем сделать вывод, что использование предлагаемого нами программного обеспечения может быть аналогично возможно не только в практическом, но и в правовом плане. Однако, для полной легализации использования вышеуказанной программы, необходимо внести соответствующие изменения в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также «Перечень видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности.»,

утвержденный Постановлением Правительства Российской Федерации от 1 июля 1996 г. № 770 (ред. от 15.07.2002) «Об утверждении Положения о лицензировании физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности».

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации от 12.12.1993 (с изм. от 21.07.2014) // Собрание законодательства РФ. 2014. № 31. Ст. 4398.Уголовный кодекс Российской Федерации: [федер. закон: принят Гос. Думой 24 мая 1996 г.: по состоянию на 20 июля. 2016 г.]. // Собрание законодательства Российской Федерации 1996 N 25 Ст. 2954.

2. Уголовно-процессуальный кодекс Российской Федерации: [федер. закон: принят Гос. Думой 22 нояб. 2001 г.: по состоянию на 01 сен. 2016 г.]. // Собрание законодательства Российской Федерации 2001 N 52 (ч. I) Ст. 4921.

3. Об оперативно-розыскной деятельности. [федер. закон: принят Гос. Думой 12 августа 1995 г.: по состоянию на 25 июля. 2016 г.]. // Собрание законодательства Российской Федерации 1995 N 144 Ст. 12.

4. О связи. [федер. закон: принят Гос. Думой 7 июля 2003г.: по состоянию на 18 августа 2017 г.]. // СПС КонсультантПлюс.

5. Об информации, информационных технологиях и о защите информации. [федер. закон: принят Гос. Думой 27 июля 2006г.: по состоянию на 20 декабря 2017 г.]. // СПС КонсультантПлюс.

6. О наркотических средствах и психотропных веществах. [федер. закон:принят Гос. Думой 8 января 1998г.: по состоянию на 7 июля 2016 г.] // СПС КонсультантПлюс.

7. Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию. [Поставновление Правительства РФ от 10 марта 2000 г. №214] // СПС Гарант.

8. Об утверждении Положения о лицензировании физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности. [Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 (ред. от 15.07.2002)] // СПС Гарант.

9. Вопросы Министерства внутренних дел Российской Федерации: Указа Президента Российской Федерации от 01 марта 2011 года № 248 // СПС КонсультантПлюс.

10. Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств: Указ Президента РФ от 01.09.95 № 891 // СПС Гарант.

II. Монографии, учебники, учебные пособия

1. Group-IB. Hi-Tech Crime Trends. 2017. С. 22.

2. Василенко В. Пластиковые деньги.//Хозяйство и право 2015. – №10. – 38 с.

3. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации. // Юридическая наука и правоохранительная практика - Иркутский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации. 2016. - 1 (35) – 55 с.

4. Батоев В. Б., Семенчук В.В. Использование криптовалюты в преступной деятельности: проблемы противодействия // Труды Академии

управления МВД России. 2017 - № 2 (42) – с 7.

5. Тюрин К.А. , Болдырихин Н.В. Алгоритм вероятностной идентификации пользователей сетей//Издательство: Донской государственный технический университет - 2016 - с. 81-86.

6. В.А. Артамонов, Е.В. Артамонова МНОО «Международная академия информационных технологий» (ООН) - 2016 – с. 3

7. Тимофеева И. Мошенничество с помощью Интернета приобретает всё более широкий размах// Вечерний Новосибирск. – 2015. – №4. –123 с.

8. Бельский А.И., Бочарникова Л.Н. Мошенничество в сфере компьютерной информации // Противодействие преступлениям в сфере информационных технологий: материалы международной научно-практической конференции, 23 мая 2013 года. — Белгород, 2013. — 179 с.

9. Гаврилин Ю. В. Преступления в сфере компьютерной информации: квалификация и доказывание/ Учебное пособие. — М.: Книжный мир, 2013. — 245 с.

10. Сизов А.В. Причины и условия совершения преступлений в сфере компьютерной информации / А.В. Сизов // Информационное право. - № 2. - 2008. - С. 38-41.

11. Соловьев Л.Н. Расследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ. Автореф. дис. ... канд. юрид. наук. - Москва, 2003. – 25 с.

12. Старичков М.В. Понятие лица, имеющего доступ к ЭВМ, системе ЭВМ или их сети, в российском уголовном праве / М.В. Старичков // Деятельность правоохранительных органов и федеральной противопожарной службы в современных условиях: проблемы и перспективы развития. Материалы международной научно-практической конференции. - Иркутск, 2006. - С.131-133.

13. Степанов-Егиянц В.Г. Криминологическая характеристика личности компьютерного преступника / В.Г. Степанов - Егиянц// Российский следователь. - № 19. - 2014. - С.41-44.

14. Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств / В.П. Талимончик // Законодательство и экономика. - 2005. - №5. - С. 57-62.

15. Теоретические проблемы информационного права. Отв. ред. И.Л. Бачило. - М., 2018. -293с.

16. Тишутина И.В. К вопросу об источниках информации о противодействии расследованию организованной преступной деятельности // Актуальные проблемы современной юридической науки и практики: Материалы Международной научно-практической конференции. 25-26 мая 2017 года. - М., 2012. - С.220-222.

17. Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика). - Ростов-на-Дону, 2014. – С. 176.

18. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. - М.: Издат. группа «Юрист». 2010. - С. 12-20.

19. Ястребов Д.А. Вопрос о латентности неправомерного доступа к компьютерной информации в Российской Федерации / Д.А. Ястребов // Юридический мир. - 2015. - №10. - С. 36-39.

Справочная литература:

1. Апелляционное постановление Московского областного суда от 24.06.2014 по делу № 22к-3647/2014 // Справочно-правовая система «КонсультантПлюс» [дата обращения 29.05.2019].

2. Институт комплексных стратегических исследований / Центр Информационных технологий – Электрон.дан. – М.:2016. URL: http://www.icss.ac.ru, свободный. Загл. с экрана. – Яз.рус.англ.яп. [дата обращения 02.02.2016].

3. Электронный вестник / ЭТБ.; Царенко А.С.; – Электро.дан. – Электронный вестник Выпуск № 45. Август 2014 г. М.:2016. URL: http://ee-

journal.spa.msu.ru, свободный. Загл. с экрана. – Яз.рус.англ.нем. [дата обращения 10.02.2016].

ПРИЛОЖЕНИЕ 1

Результаты опроса практических сотрудников.

Вопрос:	Ответ:
1. Целесообразно ли создание данного программного обеспечения?	1) Да. (80%) 2) Нет. (5%)
2. К какому виду ОРМ можно отнести использование вышеуказанного программного обеспечения?	1) Оперативный эксперимент. (13%) 2) СИТКС. 3) Наведение справок. 4) Получение компьютерной информации. (87%)
4. При раскрытии какого вида преступлении использование ПО было бы востребовано больше всего?	1) Мошенничества в сфере высоких технологий. (15%) 2) Преступления, связанные с незаконным оборотом наркотиков. (27%) 3) 272 и 273 ст. УК РФ. (53%)
4. Реализовывались ли подобные решения задач ОРД на практике?	1) Да. (5%) 2) Нет. (95%) 3) Не сталкивались с задачами этого типа. (0%)
5. В чем причина отсутствия опыта использования подобного программного обеспечения?	1) Отсутствие нормативно-закреплённых механизмов использования ПО в ведомственных инструкциях. (45%) 2) Отсутствие технической возможности разработки ПО. (10%) 3) Высокая стоимость создания ПО, а также нецелесообразность этих затрат. (35%) 4) Отсутствие аналогичного опыта работы в этом направлении в других подразделениях. (5%) 5) Отсутствие квалифицированных кадров. (5%)