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: **ОРГАНИЗАЦИЯ И ТАКТИКА БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ, СОВЕРШАЕМЫМИ С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ**

Выполнил: **Набиев Руслан Рамилевич**
(фамилия, имя, отчество,
слушатель группы №021, обучающийся по
№ группы специальность, год набора)
специальности 40.05.02- Правоохранительная
деятельность, 2012 года набора

Руководитель: к.ю.н. доцент кафедры оперативно-
(уч. степень, уч. звание, должность,
разыскной деятельности КЮИ МВД России
полковник полиции А.И. Музеев
специальное звание, И.О. Фамилия)

Рецензент: ____________________
(уч. степень, уч. звание, должность,
____
____
специальное звание, И.О. Фамилия)

К защите _*допущена*_______________________________

Начальник кафедры ОРД ____________ Е.П. Шляхтин

Дата защиты: «___» _________ 2017 г. Оценка _______________________

Казань – 2017

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования: В работе освещаются проблемы борьбы с относительно новыми, технически и организационно сложными преступлениями – хищениями денежных средств с банковских счетов, а также электронных денежных средств, совершаемыми с использованием специализированных вредоносных компьютерных программ, массово распространяемых в сети Интернет. В настоящее время такие преступления квалифицируются как мошенничество в сфере компьютерной информации, предусмотренное ст. 159.6 УК РФ, введенной в действие Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации».

Появление и рост количества таких преступлений обусловлены интенсивным развитием в последние десятилетия различных систем переводов денежных средств (платежей), осуществляемых с использованием компьютерных технологий и сетей передачи данных, и широким распространением доступа к сети Интернет.

Согласно данным официальной статистики МВД России, в настоящее время наблюдается серьезное сокращение числа преступлений, совершаемых в сфере компьютерной информации. Так, если в 2012 г. их было зарегистрировано 11636, то в 2013 г. – 7398. При этом в 2014 г. сокращение зарегистрированных преступлений названного вида составило 36,4%, а за 10 месяцев 2015 г. – 63,9%[1]. Вполне понятно, что приведенные показатели свидетельствуют не об уменьшении случаев совершения компьютерных преступлений, а о высокой латентности последних, о том, что выявлять их

[1] Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: http://www.mvd.ru/presscenter/statistics/reports дата обращения 20.11.2016 г.

стало гораздо сложнее. Тем более что ещё в 2009 г. фиксировалось увеличение числа зарегистрированных преступлений в сфере компьютерной информации на 29,1%.

Одной из причин сложившегося положения дел служит совершенствование противодействия проводимому расследованию данного вида преступлений со стороны, как виновных лиц, так и иных заинтересованных в сокрытии истины субъектов. На эффективность оказываемого расследованию противодействия указывает и падение раскрываемости преступлений в сфере компьютерной информации. Так, в 2014 г. раскрываемость данного вида преступлений уменьшилась на 39,8%, а за 10 месяцев 2015 г. – на 61,2%. Причём с января по декабрь 2009 г. наблюдался рост раскрываемости на 34,2%[1].

Таким образом, очевидно, что государство постепенно уступает инициативу в пользу криминализированных сообществ и индивидуально действующих лиц, не признающих каких-либо ограничений в сфере компьютерной информации. Между тем, это абсолютно недопустимо, поскольку компьютерные и иные высокие технологии становятся неотъемлемым компонентом механизма управления государством и обществом.

Объектом исследования является правоотношения возникающие в связи с преступлениями в сфере высоких технологий.

Предметом данной работы являются нормы российского и зарубежного законодательства, материалы статистки, следственно-судебной практики и специальная литература, отражающие вопросы обеспечения безопасности компьютерной информации.

Целью работы в изучении особенностей раскрытия преступлений в сфере компьютерной информации, анализ современного состояния и перспектив развития сферы высоких технологий, и на основании этого, выдвижение рекомендаций на законодательном уровне.

---

[1] Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: http://www.mvd.ru/presscenter/statistics/reports дата обращения 20.11.2016 г.

Для достижения поставленной цели были определены следующие **задачи**:

1. Изучить и проанализировать правовую регламентацию, статистику преступлений в сфере высоких технологий.

2.Раскрыть понятие и сущность компьютерной информации как объекта исследования.

3. Рассмотреть механизм образования и локализации компьютерных преступлений.

4. Дать характеристику преступлений, совершаемых в сфере высоких технологий.

5. Рассмотреть особенности взаимодействия сотрудников оперативных подразделений органов внутренних дел (далее ОВД) с подразделениями оперативно-технических мероприятий (далее ОТМ) органов внутренних дел в ходе производства оперативно-розыскных мероприятий и следственных действий;

6. Изучить вредоносные программы и компьютерные вирусы.

Методологическая основа представлена общенаучным методом диалектического материализма и частными методами научного познания: индуктивным и дедуктивным; анализа и синтеза; наблюдения, интервьюирования; историческим и сравнительным методами, и другими.

Теоретическая и практическая значимость Практическая значимость настоящей работы состоит в возможности использования содержащихся в ней выводов, предложений и рекомендаций в практической деятельности сотрудников органов внутренних дел. Отдельные положения работы могут способствовать более глубокому и всестороннему осмыслению особенностей раскрытия, а также, совершенствованию процессуальной деятельности органов предварительного расследования и оперативно-розыскной деятельности.

Теоретическую базу работы составили научные труды Андреев Б.В., Акопов Г.Л., Атаманов Р.С., Батурин Ю.М., Вехов В.Б., Ворошилова Т.В., Волженкин Б.В., Воробьев В.В., Горяинова К.К. , Головин А.Ю, Гульбин Ю.Ф., Мирошников Б.Н., Мельников Д.А., Попков Ю.С., Пущин В.С., Сорокин А.В., Скоромников К.С., Сейджман М .,Тищенко В.И., Жуков Т.И.

Нормативно-правовая база дипломной работы представлена нормами Конституции РФ, международного права, уголовно-процессуального, уголовного законодательства Российской Федерации, федерального закона «Об оперативно-розыскной деятельности», нормативными правовыми актами РФ, а также законодательством и практикой применения по данному виду преступлений.

Структура дипломной работы обусловлена целью и задачами исследования и состоит из введения, трех глав, заключения, списка использованных источников.

ГЛАВА 1. ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

§ 1.1. Понятие и сущность преступлений в сфере высоких технологий и правовая основа борьбы с ними

Компьютеризация всех слоев населения является социально значимым явлением, ее достижения могут быть использованы не только в хороших намерениях. Но и при совершении преступлений компьютерной направленности. Компьютерные преступления носят специфический характер, в настоящее время – это новации в системе уголовного права. Способы совершения компьютерных преступлений настолько многогранны и носят изощренный характер, что документирование и раскрытие данного вида преступлений порой вызывает определенные трудности. В связи с чем разрабатываются и внедряются новые формы и методы оперативно-розыскной деятельности.

Необходимо заметить, что одним из важнейших составляющих элементов методики раскрытия компьютерных преступлений является субъективная особенность личности преступника, которая на начальном этапе раскрытия преступлений представляется лишь скудной информацией, в связи с чем необходимо учитывать такие составляющие, как пол, возраст, социальное происхождение, уровень образования, род занятий, наличие специальности, семейное положение, социальный статус, уровень материальной обеспеченности, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре. Иными словами, немаловажное значение в раскрытии любого вида компьютерного преступления играет характерологическая особенность психологии личности преступника, которая позволяет при глубоком анализе определить и сузить круг подозреваемых лиц, мотив преступления, способ его совершения, а также выдвинуть версии, что естественно, приблизит оперативных сотрудников и следователей к проведению ОРМ и следственных действий, способствующих раскрытию данного вида преступлений.

Действующий уголовный закон в настоящее время защищает не только документированную информацию, но и ее разновидности, что расширяет возможности своевременно изобличить лиц, совершающих преступления данной направленности. Из проведенного анализа Уголовного Кодекса Российской Федерации (далее УК РФ) следует отметить, что отношения, возникающие в области компьютерной информации, в настоящее время подлежат специальной охране.

В главу 28 УК РФ о преступлениях в сфере компьютерной информации введены термины и понятия, которых ранее не было не только в уголовно-правовой терминологии, но и в законодательстве, регулировавшем информационные отношения.

Основным предметом посягательства является компьютерная информация, определяемая как документированные сведения о лицах, предметах, фактах, событиях, явлениях и процессах, хранящиеся на машинных носителях, в электронно-вычислительных машинах (далее ЭВМ), системе или сети ЭВМ, либо управляющие ЭВМ.

ЭВМ называется комплекс электронных устройств, позволяющий осуществлять предписанные программой (или пользователем) информационные процессы: сбор, обработку, накопление, хранение, поиск и распространение информации[1].

Понимая под системой любой объект, элементы которого находятся в упорядоченной взаимосвязи, систему ЭВМ можно определить как комплекс, в котором хотя бы одна ЭВМ является элементом системы, либо несколько ЭВМ составляют систему.

---

[1] Карчевский Н. В. Компьютерные преступления: определение, объект и предмет. - /Карчевский Н. В.- Режим доступа: http://www.ifap.ru/pi/05/karchev.htm

Целью системы является повышение эффективности работы ЭВМ. Сетью ЭВМ являются компьютеры, объединенные между собой линиями (сетями) электросвязи, т. е. технологическими системами, обеспечивающими один или несколько видов передач (телефонную, телеграфную, факсимильную передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио и проводного вещания). К машинным носителям компьютерной информации относятся устройства памяти ЭВМ, периферийные устройства связи, сетевые устройства и сети электросвязи.

Прогнозируя побудительные факторы совершения неправомерного доступа к компьютерной информации, обратимся к таблице, составленной Д.Уидомом, для 4-х видов мотивов, возможных преступников и предупредительных мер.[1]

Вместе с тем, основная сложность расследования данного преступления заключается, прежде всего, в необходимости доказывания факта «вредоносности программ». Отмечу, что на сегодняшний момент отсутствует четкое законодательное определение данного понятия, доктринальное его толкование довольно противоречиво.

В Уголовном кодексе РФ до ноября 2012 г. отсутствовал состав преступления, который можно было бы считать специализированным для хищений денежных средств, так как совершаются преступления в сфере высоких технологий совершаемых с использованием вредоносных компьютерных программ. Такой состав был внесен в УК РФ по законодательной инициативе Верховного суда РФ лишь недавно. В числе ряда новых форм мошенничества в соответствии с Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ» была добавлена ст. 159.6 «Мошенничество в сфере компьютерной информации».

---

[1] Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература., 1991. – С.43.

Таблица № 1.

Побудительные факторы, способствующие совершению киберпреступлений.

Номер мотива	Мотив	Предупредительные меры	Группы возможных преступников
1	Игнорирование этики	Общее предупреждение посредством информационной политики	Профессиональные нарушители режимов эксплуатации компьютеров
2	Корысть (личная нажива)	Создание неблагоприятных условий для готовящихся преступлений	Преступники – «любители» в «белых воротничках»
3	Корысть (коррупция)	Надзор	Высокопоставленные чиновники, эксперты
4	Другие антиобщественные мотивы	Контроль за доступом в компьютерные системы	Профессиональные преступники, хакеры, люди с психическими отклонениями

Согласно данной статье, таковым является «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации «информационно-телекоммуникационных сетей».

В профессиональном сообществе это нововведение вызвало в основном положительные отзывы, однако, отмечаются и некоторые недостатки новой статьи УК РФ. В частности, возникновение конкуренции норм со ст. 272 УК РФ, которой предусмотрен «причинивший крупный ущерб или совершенный из корыстной заинтересованности» «неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование компьютерной информации». Диспозиция ст. 159.6 УК РФ предусматривает дополнительные способы совершения преступления, такие как «ввод» компьютерной информации и «иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или «информационно-телекоммуникационных сетей». Кроме того, обеспечивается дифференциация уголовной ответственности за счет введения большего количества квалифицирующих признаков, предусмотренных ч. 2-4 ст. 159.6 УК РФ.

Несмотря на положительные качества новой статьи УК РФ, на практике остается до конца неясным разграничение сферы ее действия со ст. 272 УК РФ, хотя теперь такие действия, как уничтожение (удаление), блокирование и модификация компьютерной информации, предусмотренные и ст. 272 УК РФ, если они совершены с целью хищения чужого имущества, охватываются диспозицией статьи 159.6 УК РФ и дополнительной квалификации не требуют.

Как позитивный момент в литературе отмечается также и гуманизация уголовно-правовой политики за счет нововведении: санкции ч. 1 и 2 ст. 272 УК РФ строже, нежели санкция ч. 1 ст. 159.6 УК РФ. Более того, крупным ущербом в ст. 272 УК РФ, согласно примечанию, признается ущерб, сумма которого превышает один млн., руб.. В квалифицированных составах ст. 159.6 УК РФ (ч. 3 и 4) предусматривается совершение преступлений в крупном и особо крупном размерах. Согласно примечанию, к ст. 159.1, крупным размером признается стоимость имущества, превышающая один млн пятьсот тыс. руб., а особо крупным – шесть млн руб. [1]

Однако польза гуманизации законодательства в данном случае может быть поставлена под сомнение. До введения ст. 159.6 УК РФ наибольшее

---

[1] Гавршин Ю.В., Шипилов В.В. Особенности следообразованпя при совершении мошенничеств в сфере компьютерной информации. Российский следователь. М., 2013. № 23. С. 2-5.

количество уголовных дел по хищениям данной формы возбуждалось не только по ст. 272 УК РФ, но и одновременно по ст. 158 или ст. 159 УК РФ. Для последних, согласно примечанию, к ст. 158 УК РФ, крупным размером признается стоимость имущества, превышающая двести пятьдесят тыс. руб., а особо крупным – один млн руб.

В результате введения ст. 159.6 УК РФ фактически произошло снижение ответственности для наиболее опасной и квалифицированной части преступников. На практике это привело к переквалификации ряда уголовных дел в начале 2013 г. и даже в некоторых случаях к вынужденному изменению мер пресечения обвиняемым на не связанные с лишением или ограничением свободы.

Несмотря на отмеченные недостатки, статья 159.6 УК РФ сейчас более всего подходит для квалификации хищений, совершаемых с использованием вредоносных компьютерных программ. Законодатель явно отделил мошенничества в сфере компьютерной информации, сопряженные с воздействием на нее, от иных случаев мошенничества, в которых средства обработки компьютерной информации используются только в качестве вспомогательных средств совершения преступлений. Разумеется, перечисленные в диспозиции ст. 159.6 манипуляции с компьютерной информацией возможны не только при использовании вредоносных компьютерных программ для совершения хищений в системах дистанционного банковского обслуживания. Однако, учитывая относительную редкость нетипичных преступлений и устойчивый рост числа типовых хищений, можно полагать, что статистика по данной статье отображает в большей части именно интересующие нас хищения.

Понятие компьютерной информации является не менее многозначным, чем понятие информации. Ее место в системе правонарушений, возникающих в информационной среде, до сих пор является предметом научных дискуссий, которые пока не завершились формированием общепризнанного научного и законодательного определения, поскольку многообразие его толкования отображает весьма сложный характер реального мира.

Компьютерная информация может быть массовой, если она предназначена для неограниченного круга лиц, или конфиденциальной, если принадлежит определенному собственнику или ее распространение и доступ к ней ограничены специальной нормой права, например персональные данные о субъектах, государственная, коммерческая, врачебная тайна и т. п.

Доступ к такой информации ограничен и требует специального допуска. В противном случае доступ к такой информации является неправомерным.

В заключении параграфа необходимо сделать следующие выводы:

1. С учетом представленных позиций авторов понятие «компьютерной информации» как предмета преступления можно сформулировать как организационно упорядоченную совокупность сведений (сообщений, данных), зафиксированных на машинном носителе либо в информацинно-телекоммуникационной сети с реквизитами, позволяющие их идентифицировать, имеющую собственника либо иного законного владельца.

2.Уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее собственнику (владельцу, пользователю).

§ 1.2. Оперативная обстановка по линии преступлений, совершаемых в сфере высоких технологий

Как уже ранее было отмечено, компьютерными преступлениями по Уголовному кодексу Российской федерации являются ст. 272 «Неправомерный доступ к компьютерной информации», ст.273 «Создание, использование и распространение вредоносных программ для ЭВМ», ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети», так же особенно популярна ст. 159.6 «Мошенничество в сфере компьютерной информации». На основании вышеприведенных статей мы провели анализ статистки, который позволил обозначить четкую картину оперативной обстановки по данной линии преступлений

Центральный банк РФ занялся сбором статистики об инцидентах в области информационной безопасности при осуществлении переводов денежных средств сравнительно недавно. Согласно Указанию ЦБ РФ от 9 июня 2012 г. № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств», операторы обязаны ежемесячно предоставлять в ЦБ отчетность по двум формам: денежных средств», операторы обязаны ежемесячно предоставлять в ЦБ отчетность по двум формам:

- форме 0403202 «Сведения о выполнении операторами платежных систем, операторами услуг платежной инфраструктуры, операторами по переводу денежных средств требований к обеспечению защиты информации при осуществлении переводов денежных средств»;

- форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

Интерес для нас представляет отчетность по форме 0403203, предоставляемая операторами в Центральный банк РФ ежемесячно.

С момента выхода Указания № 2831-У ЦБ РФ опубликовал два аналитических обзора инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, подготовленных на основе результатов отчетности по форме 0403203, – за первое полугодие 2013 г. и за второе полугодие 2014 г.[1] В последующем аналогичные аналитические обзоры не выпускались, а в июне 2015 г. банком был опубликован существенно отличающийся по структуре и составу данных «Обзор о несанкционированных переводах денежных средств (2014 год)»[2].

Таким образом, за полгода общее количество включенных в отчетность инцидентов увеличилось на 35 %. По месяцам отмечается неустойчивая тенденция к росту.

Из опубликованных к настоящему времени обзоров можно сделать несколько выводов:

- количество совершенных хищений достаточно велико даже с учетом того, что сведения о них предоставляются только частью операторов по переводу денежных средств (в 2014-2015 гг. около 10 % операторов, за 2014 г. данные отсутствуют);
- более половины инцидентов (по данным 2014-2015 гг.) являются непосредственно несанкционированными переводами денежных средств (и попытками переводов);
- еще около 40 % инцидентов (по данным 2014-2015 гг.) с высокой вероятностью являются выявленными и пресеченными на ранних этапах приготовлениями к совершению хищений;
- большая часть хищений выявляется самими клиентами; так, в 2014 г. клиентами было выявлено 84 % несанкционированных операций;

---

[1] Защита информации при осуществлении переводов денежных средств. / http://www.cbr.ru/PSystem/?PrtId=sec (дата обращения 12.06.2017).

[2] Банк России. Обзор о несанкционированных переводах денежных средств (2014 год). URL: http://www.cbr.ru/psystem/P-sys/survey_2014.pdf (дата обращения 12.06.2017)

– наибольшее количество хищений совершается в отношении клиентов – физических лиц. В 2015 г. более 80 % от количества всех несанкционированных операций с использованием систем ДБО были связаны со списанием денежных средств со счетов физических лиц. В связи с этим наибольшее число несанкционированных операций было осуществлено в объеме от 10 до 50 тыс. руб. Вместе с тем при меньшем количестве хищений со счетов клиентов – юридических лиц – на них приходится больший объем денежных средств (более 73 % объема всех несанкционированных операций).

Представленные в обзорах ЦБ РФ сведения позволяют провести показательное сравнение количества хищений, отчеты о которых поступили от операторов, и количества преступлений по ст. 159.6 УК РФ, сведения о которых содержатся в учетах ГИАЦ. В то время как за весь 2013 г. по ст. 159.6 УК РФ было зарегистрировано 693 преступления, только за первое полугодие 2013 г. в Центральный банк РФ поступили сведения не менее чем о 4980 (46,8 % от общего количества инцидентов) несанкционированных переводах денежных средств. Даже если полагать, что все 693 зарегистрированных преступления являлись хищениями денежных средств с банковских счетов, совершенных с использованием вредоносных компьютерных программ, разница получается более чем в 7 раз только с учетом сведений за полгода.

В обзоре за 2014 г. содержится информация о 825 попытках и 4065 успешных хищениях в системах ДБО, большинство из которых были совершены с использованием вредоносных компьютерных программ. Кроме того, косвенно сообщается о большом количестве хищений электронных денежных средств, общая сумма ущерба от которых превышает 100 млн руб.

В 2015 году состояние оперативной обстановки в Республике Татарстан отражает статистка, предоставленная отделом «К» МВД по Республике Татарстан за 12 месяцев выявлено 82 факта совершения преступлений, из них по ст.138 УК РФ – 4, по ст.158 УК РФ – 9, по ст.159 УК РФ – 40, по ст.159.6 УК РФ – 3, по ст.183 УК РФ – 4, по ст.242 УК РФ – 1, по ст. 272 УК РФ – 11, по ст.273 УК РФ – 2, по ст. 163 УК РФ – 2, по ст. 128.1 УК РФ – 2, по ст. 137 УК РФ – 3, по ст. 207 УК РФ – 1.

В 2016 году Сотрудниками отдела «К» МВД по Республике Татарстан за 9 месяцев текущего года выявлено 113 фактов совершения преступлений (АППГ-49, +130%), из них по ст.158 УК РФ – 44, по ст.159 УК РФ – 47, по ст.242 УК РФ – 6, по ст.272 УК РФ – 8, по ст. 273 УК РФ – 1, по ст. 135 УК РФ – 4, по ст. 185.3 УК РФ – 1, по ст. 163 УК РФ – 1, по ст. 146 УК РФ – 1.

На лицо явное увеличение преступлений в сфере высоких технологий, использования сети Интернет.

Согласно полученным оценкам оперативных работников, следственными органами возбуждаются уголовные дела не более чем по 1 из примерно 20 сообщений о хищениях денежных средств с банковских счетов или из электронных кошельков. Однако и сами заявления, по мнению оперативных работников, подавались не более чем в половине случаев хищений денежных средств со счетов юридических лиц и не более чем в 1 из 3-5 случаев хищений денежных средств со счетов физических лиц.

В типовом случае обращения потерпевшего по факту хищения в правоохранительные органы в заявлении сообщается только о несанкционированном переводе денежных средств на неизвестный потерпевшему счет (или счета). Поскольку такие преступления происходят в условиях почти полной неочевидности, факт использования вредоносных компьютерных программ и несанкционированного доступа к электронным средствам платежа на момент обнаружения хищения, как правило, не может быть подтвержден. В случае успешного совершения хищения и применения злоумышленником достаточных средств и методов удаления или сокрытия следов — это событие однозначно выглядит как преступление только с точки зрения бывшего владельца похищенных средств. Причем сам владелец денежных средств обычно не понимает, каким именно способом совершено преступление[1].

Отсутствие осведомленности и правильного криминалистического определения ситуации, а также выработанного унифицированного подхода к проведению комплекса первоначальных проверочных мероприятий приводит к ошибочному выбору тактики раскрытия, выполнению тех или иных безрезультатных действий и, следовательно, к затягиванию процессуальных сроков рассмотрения сообщении о преступлениях». К сказанному остается добавить, что во многих случаях факт совершения хищения с использованием именно вредоносных компьютерных программ так и остается неизвестным как для сотрудников правоохранительных органов, так и для самих владельцев денежных средств, что исключает возможность установления и привлечения всех виновных лиц к уголовной ответственности[2].

Основные доказательства использования вредоносной программы, а также «неправомерного доступа к охраняемой законом компьютерной информации» (с декабря 2012 г. – «ввода, удаления, блокирования, модификация компьютерной информации») находятся на компьютере или мобильном устройстве потерпевшего. Подтвердить указанные факты можно только в результате сложного криминалистического исследования, которое провести на этапе проверки сообщения о преступлении весьма затруднительно.

Обратимся к примеру. В Управление «К» поступила информация о появлении на территории Российской Федерации нового вида вредоносного программного обеспечения – «Faketoken.b-ruStels2», целью которого являются устройства, работающие на платформе «Android».

Оперативникам удалось выйти на след участников преступной группы, в которую входило семь человек.

---

[1] Дуленко В.А, Мамлеев Р.Р., Пестриков В.А. / Преступление в сфере высоких технологий / Учебное пособие. – М.: ЦОКР МВД России, 2010. – 20-21 с.

[2] Шмонин А.В. Организация выявления и раскрытия хищений денежных средств с использованием дистанционного банковского обслуживания: сб. тр. конф. «Информатизация и информационная безопасность правоохранительных органов». М., 2014.

Программу, которую они использовали после установки на устройство, запрашивала баланс привязанной к номеру банковской карты, скрывала поступающие уведомления и начинала осуществлять переводы денежных средств с банковского счета на счета, подконтрольные злоумышленникам.

В результате проведенных обысков было изъято значительное количество компьютерной техники со следами распространения в сети Интернет вредоносного программного обеспечения, 25 мобильных телефонов, более 150 сим-карт, электронные носители информации и свыше 100 банковских карт, на которые производилось зачисление похищенных денежных средств.

В настоящее время участники преступной группы задержаны и дают признательные показания. В отношении 3-х активных фигурантов избрана мера пресечения в виде ареста. Им предъявлены обвинения по статье 158 УК РФ (Кража).

Сумма предотвращенного ущерба клиентам банка по предварительным оценкам составляет более 5 млн. руб.[1]

Ведется работа по установлению причастности данных лиц к десяткам аналогичных преступлений.

К сожалению, как показывает практика, не меньшее усердие в уничтожении следов совершения преступлений предпринимают и сами пострадавшие. По наблюдениям опрошенных сотрудников оперативно-розыскных подразделений, до половины пострадавших непосредственно сразу после выявления фактов хищений денежных средств (что часто сопровождается выведением из сгроя компьютеров) самостоятельно или силами сторонних специалистов производят восстановление вышедших из строя компьютеров, их проверку антивирусными программами (с обязательным удалением найденных вредоносных программ). Иногда – полную замену операционных систем, в том числе с переустановкой платежного программного обеспечения (если таковое

---

[1] Опрос оперативных сотрудников проводился в рамках преддипломной практики в отделе «К» при МВД по Республике Татарстан.

имеется), и даже замену носителей информации. После этого уже следуют обращения в правоохранительные органы.

В результате при рассмотрении заявлений по фактам совершенных хищений денежных средств правоохранительные органы в большинстве случаев не имеют подтверждений применения вредоносных компьютерных программ и несанкционированного доступа к электронным средствам платежа или их утраты, а, следовательно, и того, что вообще имел место неправомерный и несанкционированный перевод денежных средств. Предположение о том, что лицо, обратившееся по факту несанкционированного перевода денежных средств, таким способом на самом деле пытается отказаться от собственного легального перевода по каким-либо субъективным причинам, часто является основанием для принятия решения об отказе в возбуждении уголовного дела.

Однако даже если доводы пострадавшего и установленные обстоятельства происшествия оказываются достаточными для принятия решения о возбуждении уголовного дела, возникает проблема квалификации деяния.

В качестве вывода по параграфу необходимо отметить:

1. Отсутствие прямо подтвержденных «ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» (либо «неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации») вызывает затруднение при квалификации преступления по ст. 159.6 УК РФ или возможно альтернативным ст. 272 и 273 УК РФ. В отдельных случаях следствием могут быть усмотрены признаки кражи (ст. 158 УК РФ) или простого мошенничества (ст. 159 УК РФ).

2. Перспектива возбуждения дела с неопределенной квалификацией и возможной последующей переквалификацией, с отсутствующим или крайне затянувшимся экспертным исследованием, без выявленных лиц, без получателя

денежных средств и с весьма слабой в целом перспективой раскрытия воспринимается сотрудниками полиции негативно. Поэтому зачастую на практике используется любая возможность и любые основания для отказа в возбуждении уголовного дела по поступившим заявлениям, что оставляет данные преступления безнаказанными.

3. Статистика, предоставленная Отделом «К» по Республике Татарстан, говорит, об увеличение преступлений в сфере высоки технологий, что наталкивает на дополнительную разработку новых методов реагирования.

ГЛАВА 2. ОРГАНИЗАЦИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕНИХ ДЕЛ ПО БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ, СОВЕРШАЕМЫМИ С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ

§2.1 Организационно-структурное и информационно-аналитическое обеспечение борьбы с преступлениями, совершаемыми с использованием высоких технологий

Организация борьбы с преступностью – это комплекс мер, направленных на предупреждение, выявление, пресечение и раскрытие преступлений, установление причин и условий их порождающих, юридическое воздействие на лиц, совершающих преступления. Правоохранительная деятельность осуществляется специально уполномоченными государственными органами в строгом соответствии с законом. Задачей государства в борьбе с преступностью является максимально возможное уменьшение сферы ее распространения, снижение негативных проявлений и последствий, профилактика.

Борьба с хищениями денежных средств, совершаемыми с использование высоких технологий, является для правоохранительных органов особенно трудной задачей вследствие относительной новизны и высокой технической сложности таких преступлений, организованного характера преступной деятельности, территориальной распределенности преступных групп, межрегионального характера большинства совершаемых преступлений[1].

Существенные проблемы имеются в информационно-аналитической деятельности, подразумевающей регистрацию и изучение количественных и качественных показателей преступности; в деятельности по выявлению,

---

[1] В.И. Тищенко, Т.И. Жуков, Ю.С. Попков. Сетевые взаимодействия. Предмет исследования и объект моделирования. М.: Ленанд, 2014. С.3,4

предупреждению, пресечению и раскрытию преступлений, осуществляемой оперативными подразделениями; в деятельности следственных подразделений по расследованию преступлений. При этом, как уже было отмечено, вопросы борьбы с хищениями денежных средств с использованием высоких технологий пока еще недостаточно исследованы и освещены в научной литературе. Изучение данной темы, по сути, только начинается.

Основную работу по выявлению, предупреждению, пресечению и раскрытию преступлений в сфере компьютерной информации выполняют оперативные подразделения органов внутренних дел, такие как Управление «К» БСТМ МВД России, отделы «К» БСТМ МВД, ГУМВД и УМВД субъектов РФ, специализированные отделы ГУЭБиПК МВД России и подразделений экономической безопасности МВД, ГУМВД и УМВД субъектов РФ, а также некоторые подразделения уголовного розыска. Несмотря на успешное пресечение указанными подразделениями в течение последних лет преступной деятельности ряда групп, занимавшихся хищениями денежных средств с использованием вредоносных компьютерных программ, такая работа ведется, по сути, без надлежащего информационно-аналитического обеспечения.

Как справедливо указывает А.Н. Волощук, «оперативные подразделения правоохранительных органов, несмотря на активное стремление перестроить свою работу в сложившихся условиях, пока не в состоянии в полной мере контролировать складывающуюся обстановку из-за того, что возникают существенные трудности не только в выявлении, но и в комплексной систематизации сведений о криминальных процессах, происходящих в Интернет пространстве. Все это негативно влияет на уровень эффективности, поэтому требуются новые подходы, основанные на системно-масштабном анализе разнородной информации. И важную роль в этом процессе играет информационно-аналитическое обеспечение борьбы с Интернет преступностью»[1].Основными направлениями информационно-аналитической деятельности в борьбе с преступлениями, совершаемыми в сфере электронных платежей, по мнению С.В. Воронцовой[2], должны являться:

- формирование и анализ базы данных о таких преступлениях;
- комплексный анализ информации о состоянии борьбы с преступлениями в сфере оборота электронных расчетов и платежей в целях выработки решений;
- проведение целенаправленных криминологических и социологических исследований в целях оценки складывающейся оперативной обстановки и прогнозирования;
- подготовка на основе анализа разнообразных документов (материалов, докладов, оценок, проблемных записок, предложений н др.).

Формирование массивов данных должно производиться, в первую очередь, оперативными подразделениями. Большой объем разнородных сведений из различных источников, касающейся всех сторон преступной деятельности и сопутствующих процессов и событий поступает в оперативные подразделения при проведении оперативно-розыскных мероприятий, в ходе проверок по сообщениям о преступлениях, а затем и следственных действий по делам о преступлениях в сфере компьютерной информации. Однако эти данные в настоящее время в каких-либо централизованных базах данных не сохраняются и системному анализу не подвергаются. Большая часть информации, представляющей иногда весьма значительную ценность, остается в распоряжении лишь их непосредственных получателей – отдельных оперативных подразделений и их сотрудников. Через некоторое время информация фактически теряется, оставаясь в лучшем случае в материалах дел оперативного учета или уголовных дел. Информационный обмен не только

---

[1]Волощук А.Н. Информационно-аналитическое обеспечение борьбы с интернет-преступностью. Cyber Safety Unit, 1 июля 2013 г. С.45.

[2] Воронцова С В. Преступления в сфере электронных расчетов и платежей: правовые и организационно-тактические основы противодействия. М., 2010. С. 183.

между подразделениями, но и между сотрудниками одного и того же подразделения во многих случаях фактически не налажен.

Поскольку централизованной базы данных оперативно-розыскной информации по преступлениям в сфере компьютерной информации в органах внутренних дел в настоящее время не существует, рассуждать о модели данных, ее системе управления, аппаратной и сетевой инфраструктуре, а также о способах и порядке наполнения и использования можно только теоретически. Вероятно, такая база должна быть общей для всех преступлений указанной категории. Выделение данных, относящихся к хищениям денежных средств с использованием вредоносных компьютерных программ, должно производиться внутри общего массива в связи с особенностями характера и объема данных. Необходимо будет учитывать, что некоторые сведения, касающиеся хищений рассматриваемого типа, будут иметь особый правовой статус (сведения, составляющие банковскую тайну, персональные данные).

Для обеспечения эффективного информационно-аналитического обеспечения деятельности по борьбе с описываемыми хищениями должны сохраняться следующие данные:

1. Сведения обо всех переводах денежных средств, как состоявшихся, так не завершенных, в процессе совершения хищений. Сведения о счетах (банковских, карточных, остатках электронных денежных средств), имеющих отношение к совершению хищений: счетах законных владельцев денежных средств; счетах, используемых для вывода и обналичивания похищенных денежных средств; счетах, используемых участниками преступной деятельности для расчетов между собой и т. и.

2. Сведения о физических лицах (персональные данные, псевдонимы, приметы и т. п.), имеющих любое отношение к хищениям. Должны учитываться сведения об установленных и неустановленных участниках преступной деятельности; о законных владельцах денежных средств, в отношении которых совершались или планируются преступления; о владельцах

любых счетов, банковских карт, средств связи, учетных записей любого типа и т. д., задействованных любым образом при совершении хищений.

3. Сведения о юридических лицах, имеющих отношение к хищениям. Должны учитываться сведения об организациях, которыми открыты любые счета, а также которым принадлежат любые средства связи, учетные записи любого типа и т. д,, задействованные при совершении хищений.

4. Сведения о сетевых адресах (IP-адресах), с которых осуществлялись какие-либо соединения в процессе подготовки и совершения хищений и в целом в процессе осуществления преступной деятельности.

5. Сведения о доменных именах веб-сайтов, использовавшихся в процессе подготовки и совершения хищений. В частности: доменные имена управляющих серверов ботнетов; имена веб-сайтов, с которых осуществлялось распространение вредоносных программ; имена веб сайтов, используемых участниками преступной деятельности для общения, сбыта или приобретения криминальных товаров и услуг и т. д.

6. Сведения обо всех телефонных номерах, адресах электронной почты, аккаунтах систем мгновенного обмена сообщениями, почтовых и юридических адресах, MAC-адресах устройств, «юзер-агентах» (User Agent) сетевых приложений и т.д.[1]

Нетрудно заметить, что разработка и создание базы данных, необходимой для сохранения и обработки перечисленных сведений и медиа объектов, является исключительно сложной и трудоемкой комплексной задачей. Не будет преувеличением сказать, что для ее реализации необходимо проведение отдельного научно-практического исследования, участие в котором должны принимать сотрудники научных подразделений, представители технических подразделений, которые в дальнейшем будут обеспечивать функционирование необходимой аппаратной и сетевой инфраструктуры, а также представители оперативных подразделений будущих пользователей базы данных. В структуре

[1] Дуленко В.А, Мамлеев Р.Р., Пестриков В.А. / Преступление в сфере высоких технологий / Учебное пособие. – М.: ЦОКР МВД России, 2010. – С.22

МВД России в настоящее время существуют подразделения оперативно-розыскной информации (УОРИ, ЦОРИ), на которые должна быть возложена эксплуатация базы данных, а также ведение части аналитической работы. Указанные подразделения осуществляют свою деятельность в интересах оперативных подразделений МВД России.

Оперативные подразделения, занимающиеся борьбой с преступлениями в сфере компьютерной информации, должны будут обеспечивать наполнение базы данных. Для работы с ней потребуется организация непосредственного доступа к базе на рабочих местах сотрудников подразделений, так как внесение и получение сведений в бумажной форме невозможно в силу характера сохраняемой информации, а также для обеспечения оперативности. Создание и функционирование базы данных потребует соответствующих изменений в структуре как подразделений оперативно-розыскной информации, так и в структуре оперативных подразделений непосредственных пользователей базы данных. Вероятно, потребуется введение отдельных должностей для сотрудников, работающих с базой данных, так как ввод, поиск данных и проведение аналитической работы являются трудоемкими задачами, и их вряд ли возможно совмещать с выполнением иных трудовых обязанностей. На определенном этапе в составе оперативных подразделений, занимающихся борьбой с преступлениями в сфере компьютерной информации, потребуется создание отдельных аналитических подразделений, на которые в числе прочих задач будет возложена работа с рассматриваемой базой данных.

Подводя итоги данного параграфа, полагаем, что необходимо создание, наполнение и получение информации из такой базы данных которая позволят резко повысить эффективность борьбы с хищениями денежных средств, совершаемыми с использованием вредоносных компьютерных программ. К сожалению, в настоящее время все рассуждения о ее будущих возможностях имеют, как уже было сказано, чисто теоретический характер. Однако предъявляемые обществом требования повышения эффективности борьбы с преступлениями в сфере компьютерной информации рано или поздно приведут к осознанию руководством правоохранительных органов необходимости создания централизованного учета оперативной информации и налаживания информационно-аналитической деятельности.

§ 2.2. Особенности организации проведения ОРМ по документированию преступлений, совершаемых с использованием высоких технологий

Использование информационно-телекоммуникационных систем в качестве платформы информационного обмена сформировало инфраструктуру для сращивания различных видов преступности, способствовало ее расширению до транснационального масштаба и в конечном итоге определило создание угроз национальной безопасности. События в этих странах показали эффективность использования информационных технологий для организации массовых беспорядков, что, в ряде случаев, обеспечило захват власти радикальными силами и смену политических элит.

Использование современных информационно-телекоммуникационных систем в различных сферах общественной и финансово-хозяйственной деятельности привели к расширению источников социальной опасности, связанных с проявлениями криминального характера. Отмечается рост преступлений, совершенных с использованием современных информационных технологий и высокотехнологичных средств, и систем телекоммуникаций, в том числе сети Интернет. Преступность в Интернете приобретает все более опасные и организованные формы, получая при этом ярко выраженный международный характер. Так, отмечается усиление организованности криминальных структур, использующих возможности Интернета для осуществления международной организованной преступной деятельности, проявлений терроризма и экстремизма. Такие структуры широко применяют методы конспирации, используют распределенные информационно-телекоммуникационные системы для организации и управления преступной деятельностью, для сокрытия следов преступлений.

В то же время информационное пространство содержит значительные объемы информации, которая представляет интерес для оперативных подразделений органов внутренних дел. Она с успехом может использоваться для решения задач ОРД, в том числе противодействия экстремистским и террористическим угрозам, тяжким и особо тяжким видам преступности, движению денежных средств, полученных противоправным путем и криминальным источникам финансирования международных преступных группировок, экстремистских и террористических организаций[1].

Необходимо отметить, что действующая законодательная и нормативная база, в том числе и теоретические основы ОРД, позволяет с успехом выявлять экстремистские и террористические проявления в сети Интернет, осуществлять оперативное документирование преступных действий в целях привлечения к ответственности лиц, подготавливающих и совершающих квалифицированные преступления с использованием информационных технологий.

Специфика построения и функционирования современных информационно-телекоммуникационных систем, в том числе сети Интренет, дает возможность рассматривать в теории ОРД глобальные компьютерные сети не только в качестве технологической поисково-информационной системы, но и в качестве специфической социально-технологической среды.

В последнее время широкое распространение, в том числе и в теоретической базе ОРД, получает понятие *«сетевое информационное пространство»* (киберпространство)[2]. Под киберпространством понимается[1]

---

[1] Сундиев И.Ю., Смирнов А.А., Кундетов А.И., Федотов В.П. Теория и практика информационного противодействия экстремистской и террористической деятельности. – М.: 2014. С.247

[2] Грибанов Д. В. Правовое регулирование кибернетического пространства как совокупности информационных отношений: Автореферат дисс. к.ю.н. Екатеринбург, 2003.

социально-технологическая среда, возникающая в процессе использования глобальных информационно-телекоммуникационных сетей в процессе специфических форм социального взаимодействия и имеющая пространственные и коммуникативные свойства, в которой возможно осуществление различных видов деятельности. К ним может относиться деятельность в политической[2], общественной[3], преступной и противопоставляемой ей оперативно-розыскной[4] сферах.

Использование понятия сетевого информационного пространства позволяет рассматривать глобальные информационно-телекоммуникационные сети уже не только как систему телекоммуникаций, допускающую обмен данными и снятие информации с технических каналов связи, но и в качестве места осуществления ОРД.

В качестве нового вида социального образования, сетевого информационного пространства (киберпространство), сформировавшегося при использовании глобальных информационно-телекоммуникационных сетей, современные системы электросвязи базируются на сетевых технологиях и определяют специфику организационно-тактических форм проведения ОРМ в борьбе как с общеуголовной преступностью в Интернете, так и с сетевыми криминальными явлениями.

Исходя из этого, под ОРМ в информационных средах и, в частности, в информационно-телекоммуникационных сетях, понимают осуществляемую в соответствии с Законом об ОРД деятельность оперативных и специальных технических подразделений, направленную на поиск и реализацию оперативно-значимой информации о деятельности преступных групп и сообществ, лиц,

---

[1] С.В. Володенко. Интернет-коммуникации в глобальном пространстве современного политического управления. – М., 2015. - 72-73 с.

[2] Акопов Г.Л. Интерент и политика. Модернизация политической системы на основе инновационных политических интернет-коммуникаций. - М.,2014. -23-25 с.

[3] С.В. Кобзева. Противодействие распространению агрессивной информации. Мировой опыт. –М., 2009. -6-8 с.

[4] Теория оперативно-розыскной деятельности: Учебник.3-е изд.,перераб. и доп. // Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. – М.: ИНФРА-М, 2014. – 712 с.

подготавливающих и совершающих преступления, экстремистских и террористических организациях, задействующих информационные среды для своей деятельности или для подготовки массовых акций, угрожающих безопасности общества или направленных на дестабилизацию общественной жизни.

Поэтому осуществление ОРД в сетевом пространстве, обладающем особыми свойствами, предполагает специфические организационно-тактические формы оперативно-розыскных мероприятий.

Специфика сетевого пространства отражается на формах, проводимых в нем ОРМ, через ряд следующих факторов:

1. Дефицит времени на принятие решения и осуществление мероприятия при проведении ОРМ, характерный при осуществлении ОРД, увеличивается из-за недолговечности существования информационных объектов и логических каналов, динамичностью изменения структуры элементов информационных сетей.

2. Технологическая сложность большинства сетевых процессов и значительный объем данных, передаваемых, хранящихся и выявляемых в электронном виде, приводят к необходимости как привлечения к проведению ОРМ сотрудников, которые должны обладать специальными знаниями в области информационных технологий, так и к необходимости учитывать специфику информационных технологий для использования результатов ОРМ в глобальных компьютерных сетях.

3. На характере проводимых в сетевом информационном пространстве ОРМ сказывается специфика сформировавшейся в нем *социальной среды,* которую можно рассматривать как устойчивую совокупность личностей, участвующих в сетевых процессах, и возникающих между ними общественных отношений.

4. Сетевая социальная среда имеет крайне разнородный характер, а ее часть, использующая информационно-телекоммуникационные системы для

противоправной деятельности или распространяющая социально опасные взгляды, должна рассматриваться в ОРД в качестве криминогенной среды.

Важная для раскрытия преступлений информация концентрируется на сетевых криминогенных объектах в виде:

а) следов противоправной деятельности;

б) сообщений лиц, осведомленных об обстоятельствах подготовки и совершения преступлений;

в) ссылок на сетевые адреса размещения материалов, запрещенных к распространению.

Кроме того, искомая информация присутствует в коммуникационных действиях разрабатываемых лиц, реализуемых через сообщения электронной почты, сеансы прямой связи (IP-телефония, ICQ и т.п.), условные сигналы либо зашифрованные сообщения, размещаемые на общедоступных сетевых информационных ресурсах.

Таким образом, специфика ОРМ в информационно-телекоммуникационных системах обусловлена особенностями сетевого информационного пространства и сетевой среды, а противоправная деятельность преступных групп и сообществ, построенных по сетевому принципу и основывающихся на возможностях сетевых информационно-телекоммуникационных систем, существенно отличается от обычных форм подготовки и совершения преступлений или соучастия в нем[1].

Указанные особенности действующих в сетевом пространстве преступных групп и сообществ определяют необходимость корректировки организационно-тактических форм проведения ОРМ.

Исходя из вышеизложенного, необходимо сделать вывод о том, что на начальном этапе раскрытия преступлений в сфере телекоммуникаций и компьютерной информации немаловажное значение имеет своевременное получение информации о совершенном или готовящемся преступлении данной

---

[1] Дуленко В.А, Мамлеев Р.Р., Пестриков В.А. / Преступление в сфере высоких технологий / Учебное пособие. – М.: ЦОКР МВД России, 2010. – 25-27 с.

направленности. Полученная информация позволит избрать правильную линию поведения оперативным сотрудникам подразделений «К» с целью определения необходимого осуществления неотложных оперативно-розыскных, специальных технических мероприятий и следственных действий. Данное обстоятельство поможет с наименьшей затратой времени выйти на более точное оперативное сопровождение по установлению конкретных лиц, причастных к совершенному преступлению, и, как положительный результат, приведет к изобличению фигурантов с закреплением полученных в ходе документирования доказательств.

ГЛАВА 3. ТАКТИКА БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ, СОВЕРШАЕМЫМИ С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ

§ 3.1. Особенности выявления и оперативного документирования преступлений, совершаемых с использованием высоких технологий

В соответствии со ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» и ч. 1 ст. 272 УК РФ, «информация – это сведения (сообщения, данные) независимо от формы их представления»[1]. Что же касается определения компьютерной информации, то доцент кафедры криминалистики МГУ им. М.В. Ломоносова В. Крылов рассматривает компьютерную информацию как специальный объект преступного посягательства и считает, что компьютерная информация «есть сведения, знания или набор команд (программа), предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях – идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования».

Таким образом, правовой защите подлежит главным образом документированная информация (документ), зафиксированная на материальном носителе с реквизитами, т.е. информация, которая облечена в форму, позволяющую ее «идентифицировать»[2].

Кроме того, понятие «документированная информация» основано на «двуединстве – информации (сведений) и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. №149-ФЗ. - Ст.2.
[2] Крылов В.В. Информация как элемент криминальной деятельности // Вестник Московского университета. Сер. 11. – М.: Право, 1998. – № 4. с 23-24

материализация и овеществление сведений...»[1]. Отсюда можно сделать вывод, что информация становится объектом гражданского законодательства.

В последнее время в связи с повышением компьютерной грамотности общего числа населения РФ возросло и количество преступлений, совершенных в сфере высоких технологий.

Проведение мероприятий по преступлениям, связанным с неправомерным доступом к компьютерной информации и использованием вредоносного программного обеспечения, требует специальных познаний в области компьютерной информации и должно осуществляться в тесном взаимодействии с отделом «К» МВД по Республике Татарстан.

На первоначальном этапе признаки совершения подобных преступлений могут выражаться в следующем:

– потерпевшим самостоятельно не производились какие-либо сомнительные операции, связанные с переводом денежных средств с расчетных счетов;

– потерпевшему без его участия или участия владельца определенного Интернет-ресурса заблокирован доступ к собственной компьютерной информации, размещенной на компьютерной технике, современном устройстве сотовой связи, электронном почтовом ящике, персональной странице в социальной сети и т.п.;

– информация, размещенная на перечисленных ресурсах, уничтожена, модифицирована или скопирована без участия потерпевшего.

В случае выявления перечисленных признаков необходимо провести следующие первоначальные мероприятия:

1. Произвести подробный опрос потерпевшего с целью выяснения следующих обстоятельств:

---

[1] Копылов В.А. Информационное право. – М.: Юристъ, 1997. – С. 23.

– когда и при каких обстоятельствах обнаружен факт хищения, или когда и при каких обстоятельствах произошло уничтожение, блокирование, модификация либо копирование компьютерной информации;

– какие электронные платежные средства использовались потерпевшим при совершении финансовых операций с использованием расчетного счета, с которого были похищены денежные средства;

– какая компьютерная техника использовалась потерпевшим при совершении законных финансовых операций, а также отклонения от обычной работы данной техники (наличие сбоев, следов посторонних воздействий и т.п.);

– в случае уничтожения, блокирования, модификации либо копирования компьютерной информации, на какой компьютерной технике, современном устройстве сотовой связи или Интернет-ресурсе размещалась компьютерная информация;

– дата и время совершения противоправных платежных операций;

– осуществлялось ли дальнейшее использование компьютерной техники после обнаружения факта хищения, либо уничтожения, блокирования, модификации либо копирования компьютерной информации;

– проводились ли ремонтные, профилактические работы.

2. В обязательном порядке разъяснить потерпевшему необходимость сохранения компьютерной техники в неизменном виде (исключить дальнейшее использование, самостоятельное удаление вредоносного программного обеспечения).

3. По возможности изъять для приобщения к материалу проверки компьютерную технику в комплексе (системный блок, смартфон) либо накопитель информации (жесткий диск, флэш-карту и т.п.).

4. По изъятой компьютерной технике необходимо назначить компьютерное – техническое исследование с целью получения ответа на следующие вопросы:

– наличие на компьютерной технике вредоносного программного обеспечения или его следов;

– каким способом произведена установка на компьютерную технику вредоносного программного обеспечения;

– наличие следов деятельности или образцов вредоносного программного обеспечения (присутствие файлов, созданных вредоносным программным обеспечением и т.п.);

– иные сведения, представляющие интерес.

При назначении компьютерного -технического исследования постановку вопросов необходимо согласовывать с экспертом. В самом отношении необходимо указывать, что вопросы поставлены в редакции эксперта.

5. Организовать взаимодействие с отделом «К» МВД по Республике Татарстан по существу проведения дальнейших мероприятий;

6. Направить запрос и постановление суда в банк, или направить запрос в платежную систему, оператору связи, где обслуживается расчетный счет, на который были перечислены похищенные денежные средства.

7. При получении сведений от операторов электронных платежных систем, банков, операторов сотовой связи проанализировать полученные сведения и принять одно из следующих решений:

– если установлено место совершения преступления, направить материал проверки по территориальности;

– если установлено, что преступление совершено на обслуживаемой территории, принять решение о возбуждении уголовного дела;

– если место совершения установить не представляется возможным, принять решение о возбуждении уголовного дела;

– если отсутствуют основания для возбуждения уголовного дела, отказать в его возбуждении.

Анализ оперативной обстановки и имеющиеся оперативные данные свидетельствует о том, что в настоящее время на территории России существует обширный рынок сбыта вредоносных программ, широко развернута деятельность ряда глубоко законспирированных, либо с закрытым доступом, то есть требующих специального «инвайта», а также «открытых» и «полуоткрытых» Интеренет-ресурсов, на которых происходит рекламирование, распространение, обмен и продажа вредоносных программ, в том числе с участием несовершеннолетних. Также не стоит забывать и об Интренет-ресурсах бесплатных объявлений – излюбленное место распространителей вредоноса[1].

В настоящее время направлен в СУ УМВД России по Н-ской области материал проверки по факту распространения гражданином вредоносных компьютерных программ за денежное вознаграждение, собранный в рамках материалов ОРД в отношении фигуранта по признакам преступления по ст. 273 УК РФ.

Для наглядности используются материалы оперативных разработок, реализованных сотрудниками подразделения «К» БСТМ УМВД России по Н-ской области, а также материалы расследования уголовного дела (№ 2012-…) в отношении лица, обвиняемого в преступлении, предусмотренном статьей 273 УК РФ.

Работу по выявлению и пресечению фактов преступной деятельности фигурантов по распространению вредоносных компьютерных программ условно можно разделить на три взаимосвязанных и последовательных этапа:

- получение и проверка информации в целях установления фактов незаконного распространения вредоносного программного обеспечения, и лиц к ним причастных;

- оперативная разработка и документирование преступной деятельности фигурантов (с использованием имеющихся оперативных возможностей), подготовка и предоставление в следственные органы материалов ОРД, достаточных для возбуждения уголовного дела;

---

[1] Дуленко В.А, Мамлеев Р.Р., Пестриков В.А. / Преступление в сфере высоких технологий / Учебное пособие. – М.: ЦОКР МВД России, 2010. – 28-29 с.

- реализация материалов разработки и оперативное сопровождение расследования по уголовному делу, как правило, вплоть до рассмотрения дела в суде.

Обратимся к примеру : В марте 2014 года в отдел «К» БСТМ УМВД России по Н-ской области поступила оперативная информация, о том, что гражданин, имеющий ник в сети Интернет и в программе видеозвонков «Skype» «51» (предположительно Иванов Иван Иванович), в группе с неустановленными лицами занимается за денежное вознаграждение созданием и распространением вредоносных компьютерных программ, предназначенных для взлома и неправомерного доступа, а также обучает хакингу. Продажа вредоносных компьютерных программ «51» (Ф.И.О.) осуществляется с использованием возможности сети Интернет (в том числе через сайты объявлений), через форумы Интернет-ресурсов таких, как «Xakep.ru», «Forum. N-sk.ru», размещенные на ресурсах «Н-скета».

В целях конспирации «51» никаких контактных данных в сети не оставлял, кроме почты «51@gmail.ru» и ника в «Skype» «51». Регистрацию и доступ к вышеуказанным ресурсам осуществляет с использованием анонимайзера.

В целях проверки достоверности полученной оперативной информации была разработана оперативная комбинация, целью которой являлась попытка войти в доверие и получить дополнительные контактные сведения о распространителе программных продуктов посредствам переписки.

В целях установления причастности фигуранта к распространению вредоноса в сети Интернет проведён мониторинг (наблюдение), поиск и анализ информации, размещенной на сайтах, расположенных на информационных ресурсах Н-ских провайдеров сети Интернет, на англо- и русскоязычных сайтах России и иностранных государств. Получены образцы продукции для проведения сравнительного исследования.

Даны соответствующие задания (поручения) подсобному аппарату на установление фигуранта и его связей, причастных к распространению, написанию и распространению вредоносных компьютерных программ, а также конкретных фактов преступной деятельности.

Осуществлены необходимые проверки по оперативно-розыскным, справочно-вспомогательным и криминалистическим учетам УМВД России по Н-ской области и другим информационным базам данных.

Проведен сбор и анализ дополнительно полученной оперативной информации, по результатам которой был намечен последующий план действий по документированию и разоблачению преступной деятельности фигурантов (сбор характерных следов и установления способов совершения данного вида преступлений).

В ходе ОРМ были получены сведения об IP-адресе, с которого фигурант размещал объявления, а также установлен круг лиц, способных освещать деятельность фигуранта.

Также в ходе переписки, оформленной актом наблюдения в присутствии представителей общественности, с фигурантом посредством компьютерной программы «Skype» установлены контактные номера телефонов, а также назначена встреча для проведения ОРМ «проверочная закупка».

В ходе реализации намеченного плана действий оперативной комбинации на подготовительном этапе перед встречей был составлен ряд вопросов, при ответе на которые фигурант давал бы конкретные ответы, указывающие на осведомленность о нарушении законодательства РФ и достаточность своих знаний в технической части. В зависимости от складывающейся оперативно-розыскной ситуации определяется список необходимых вопросов:

1. Какое образование имеет фигурант?
2. Его уровень навыков владения компьютером.
3. Осведомленность об уголовной ответственности за распространение вредоносных программ.
4. Имело ли место создание им конкретно данной компьютерной программы? Если да, то при каких обстоятельствах.
5. Где, когда, при каких обстоятельствах имело место завладение данной

компьютерной программой?

6. Сколько раз и кому реализовывал фигурант распространяемую программу?

7. Какие функции выполняет интересуемая программа?

8. Осуществлял ли фигурант неправомерный доступ с использованием продаваемой программы? Если да, то в отношении кого именно.

9. Обучал ли кого-нибудь пользоваться данным программным продуктом?

После проведения первой проверочной закупки было назначено исследование в ЭКЦ УМВД России по Н-ской области закупленного образца компьютерной программы. На разрешение исследования поставлены следующие вопросы:

1. Содержатся ли на представленном для исследования USB-флеш-носителе какие-либо программные продукты? Если да, то, какие именно.

2. Является ли находящееся на представленном для исследования USB-флеш-носителе программное обеспечение вредоносным?

3. Детектируются ли антивирусным программным обеспечением программные продукты, содержащиеся на предоставленном USB-флеш-носителе? Если да, то, к какому семейству вредоносных программ относятся данные программные продукты.

4. Какими признаками вредоносности обладают компьютерные программы, находящиеся на представленном USB-флеш-носителе?

После проведения исследования закупленной компьютерной программы 15 апреля 2014 года на основании постановления заместителя начальника УМВД РФ по Н-ской области – начальника полиции о проведении ОРМ, в соответствии с ФЗ «Об ОРД» в установленном месте сотрудниками отдела «К» БСТМ УМВД России по Н-ской области произведена проверочная закупка образцов вредоносной компьютерной программы «Spy-Net 2.7» распространяемой фигурантом.

По итогам проведенного исследования собранного материала, где следы совершения данного вида преступления были задокументированы, выяснены обстоятельства, указывающие на преступную деятельность фигуранта, появились достаточные основания полагать, что в действиях разрабатываемого лица (разрабатываемых лиц) имеются признаки преступления, указанные в особенной части УК РФ в статье 273. Данный материал проверки был направлен в следственный орган для решения вопроса о возбуждении уголовного дела.

В заключении необходимо сделать вывод, что как бы ни складывалась та или иная оперативно-следственная ситуация, в любом случае сотрудники, наделенные правами документирования фактов, имеющих отношение к преступной деятельности разрабатываемых лиц, и последующего эффективного расследования уголовного дела, всегда должны знать о предпочтительной последовательности и нюансах практической реализации полученных следов, которые в дальнейшем можно будет приобщить к материалам уголовного дела в качестве вещественного доказательства. В ходе взаимодействия оперативных сотрудников ОВД со следователями при проведении оперативно-технических мероприятий иногда возникают и типичные ситуации, которые поддаются алгоритмизации и программированию. Однако все принимаемые решения должны носить законную правовую основу и содержать в себе обоснованность, мотивированность, своевременность и реальность их исполнения. Законность предполагает, что принимаемое решение предусмотрено действующим законодательством и полностью ему соответствует.

§ 3.2. Использование результатов оперативно-розыскной деятельности в доказывании по уголовным делам о преступлениях, совершенных с использованием высоких технологий

В динамичных условиях нашего времени общество постоянно сталкивается с проблемами различного характера, порождение которых зачастую вызвано стремлением к созданию более совершенных и эффективных моделей существования. Это в полной мере относится и к такой специфической сфере, которая все более быстрыми темпами внедряется в современную жизнь мирового сообщества, – как область применения электронной техники и информационных технологий.

Создание электронно-вычислительной техники последних поколений с огромными возможностями, их широкое распространение и применение в экономической, социальной и управленческой сферах, а также появление в быту значительного количества современного высокотехнологичного оборудования явились не только новым свидетельством технического прогресса, но и неизбежно повлекли за собой негативные последствия, связанные с различного рода злоупотреблениями при использовании средств компьютерной техники и информационных технологий.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы способны вызвать тяжелые и необратимые последствия, связанные не только с имущественным ущербом, но и с причинением физического вреда людям. Опасность компьютерных преступлений многократно возрастает, когда они совершаются в отношении действующих объектов жизнеобеспечения, транспортных и оборонных систем, атомной энергетики[1].

Первым зафиксированным фактом убийства, совершенного посредством компьютерных технологий, был случай, произошедший в феврале 1998 г. в США, где тяжело раненный свидетель преступления был спрятан в закрытом госпитале на территории военной базы. Преступники через Интернет изменили режимы работы кардиостимулятора и аппарата вентиляции легких, что привело к смерти охраняемого лица.[2]

Сотрудникам правоохранительных органов довольно сложно расследовать данную категорию дел по ряду объективных и субъективных причин. Так, например, сотрудникам, осуществляющим работу по своевременному раскрытию и дальнейшему расследованию выявленных преступлений, необходимо владеть знаниями компьютерных и информационных технологий, а также своевременно и тактически грамотно применять нормы уголовно-процессуального законодательства.

Прерогативой каждого сотрудника правоохранительных органов является то, что, не взирая на занимаемую должность, он ежедневно должен вносить свой вклад в недопущение противоправных действий лиц, которые склонны к совершению преступлений. Если преступление будет совершено или допущено, то в таком случае его необходимо своевременно раскрыть, расследовать, выяснить обстоятельства расследуемого преступления, установить лиц, причастных к его совершению, определить роль каждого участника. В предусмотренные законом сроки должны быть установлены все обстоятельства совершенного преступления, собраны доказательства виновности или невиновности лица и обеспечено своевременное назначение ему наказания или освобождение от него.

---

[1] В.И. Тищенко, Т.И. Жуков, Ю.С. Попков. Сетевые взаимодействия. Предмет исследования и объект моделирования. М.: Ленанд, 2014. - 52 с.

[2] Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. канд. юрид. наук: 12.00.08. – М., 2012. -. 20-23 с.

Специфика уголовно-правовых отношений, возникающих в связи с совершением общественно-опасных деяний, обусловливает особенности механизма осуществления как оперативно-розыскных, в том числе и специальных технических мероприятий, так и параллельное сопровождение их во время производства следственных действий и до окончания уголовного судопроизводства, а в исключительных случаях и на некоторое время, и после него.[1] В таких случаях, когда ведется уголовное преследование лица, предполагаемо виновного в совершении средней тяжести, тяжкого и особо тяжкого преступления, его привлечение к уголовной ответственности и возложение на него мер уголовно-правового воздействия принимает на себя государство в лице специально уполномоченных органов, а потерпевший же при этом выступает в качестве одного из участников уголовного судопроизводства на стороне обвинения. Так, до недавнего времени такое мероприятие, как прослушивание телефонных и иных переговоров проводилось только в рамках оперативно-розыскной деятельности, которую регламентировал Федеральный закон об ОРД от 1995 года, тогда как в настоящее время, в связи с выходом ныне действующего уголовно-процессуального кодекса РФ, данное мероприятие включено в разряд следственного действия и заложено в нормы ст.186 УПК РФ. Хотя некоторыми специалистами задолго до появления указанной статьи в российском уголовно-процессуальном законодательстве приводились не столько убедительные, сколько эмоциональные доводы против введения этого следственного действия[2].

Однако, возникшие требования правительства к компетентным органам по вопросу улучшения эффективности борьбы с преступностью оказались более высоким аргументом, чем мифическая угроза нарушения прав и законных интересов граждан. Более того, в настоящее время ведется дискуссия и о том,

---

[1] Алескеров В.И. Применение мер безопасности к участникам уголовного судопроизводства // Вестник Российской Правовой Академии Министерства Юстиции. – 2007, № 4. - С. 70 – 73.
[2] Савицкий В.М. Правосудие и личность.// Советское государство и право. 1983 г. № 5. С 58.

что в необозримом будущем данное следственное действие будет проводиться при возникновении необходимости по всем уголовным делам вне зависимости от степени их общественной опасности. Проведенный анализ действующего уголовно-процессуального законодательства Российской Федерации и опыт практического применения его норм свидетельствует о том, что охране прав и свобод личности при производстве по уголовным делам вообще и на предварительном следствии в частности придается весьма важное значение[1]. В связи с чем в целях обеспечения соблюдения конституционного права граждан на тайну телефонных и иных переговоров в УПК РФ была включена специальная статья. Данная статья является единственным следственным действием, производство которого допускается по возбужденному уголовному делу при наличии достаточных оснований полагать, что телефонные и иные переговоры могут содержать сведения, имеющие значение по уголовному делу. Данное следственное действие является настолько специфичным, что его производство требует помимо тщательной подготовки еще и задействование (подключение) соответствующих оперативных служб. В соответствии с п.11 ч.2 ст. 29 УПК РФ разрешение на производство данного следственного действия уполномочен давать суд в порядке, предусмотренном статьей 165 УПК РФ. Однако необходимо отметить, что при наличии угрозы совершения насилия, вымогательства и других преступных действий в отношении свидетеля, потерпевшего или их близких родственников, близких лиц, контроль и запись переговоров допускаются по их письменному заявлению, а при его отсутствии – на основании судебного решения, вынесенного по ходатайству следователя., Согласно нормам статьи 186 УПК РФ данное следственное действие не может осуществляться свыше шести месяцев и должно быть прекращено по постановлению следователя, но не позднее окончания предварительного расследования по уголовному делу.

---

[1] Шаталов А.С. Контроль и запись переговоров на предварительном следствии: правовые основания, тактические условия, технология проведения // Журнал Высшей школы экономики «Право» - 2009 - № 3 – С. 57-84.

При производстве такого действия, как контроль и запись телефонных и иных переговоров следователь имеет право в любое время истребовать от органа, их осуществляющего, фонограмму для просмотра и прослушивания. Фонограмма передается следователю в опечатанном виде с сопроводительным письмом, в котором должны быть указаны даты, время начала и окончания записи переговоров лица, интересующего следствие, а также краткие характеристики использованных при этом технических средств. О результатах осмотра и прослушивания фонограммы следователь с участием понятых и, при необходимости специалиста, а также лиц, чьи телефонные и иные переговоры записаны, составляет протокол, где должна быть дословно изложена та часть фонограммы, которая, по мнению следователя, имеет отношение к данному уголовному делу. Фонограмма в полном объеме приобщается к материалам уголовного дела на основании постановления следователя в виде вещественного доказательства. Ее хранение должно осуществляться в опечатанном виде в условиях, исключающих возможность ее прослушивания и тиражирования посторонними лицами и обеспечивающих, кроме того, сохранность и техническую пригодность фонограммы для необходимого последующего прослушивания.

Такова законодательная рекомендация порядка производства контроля и записи переговоров. Состязательный характер российского уголовного судопроизводства, жесткие требования законодателя к ходу и результатам предварительного расследования, а также к решениям, которые могут быть приняты судом по его итогам порождают необходимость разработки новых научных положений и основанных на них рекомендаций, относящихся к тактике проведения этого следственного действия и к определению наиболее целесообразной линии поведения осуществляющих его лиц[1].

---

[1] Шаталов А.С. Контроль и запись переговоров на предварительном следствии: правовые основания, тактические условия, технология проведения // Журнал Высшей школы экономики «Право» - 2009 - № 3 – С. 57-59.

Следует заметить, что определенная работа в этом направлении ведется специалистами в сфере оперативно-розыскной деятельности. В настоящее время методы и познавательные технологии, используемые сотрудниками оперативных подразделений, во многих случаях не позволяют сохранять процессуальную безупречность значимой информации, полученной при производстве оперативно-розыскных мероприятий с использованием технических возможностей. Иными словами, при производстве аналогичного оперативно-технического мероприятия не всегда удается добиться соблюдения всех требований, предъявляемых уголовно-процессуальным законом к доказательствам. В результате чего, собранные оперативными сотрудниками сведения о переговорах и других, в широком понимании этого значения, задокументированных действиях лиц могут признаваться судом недопустимыми в доказывании их преступной деятельности в ходе судебного рассмотрения и окончательного разрешения по уголовным делам.

В целях улучшения получения качества необходимой информации при ее документировании на протяжении всех последних лет ведется дискуссия с участием научных и практических работников, результаты которых доводятся до соответствующих служб правоохранительной системы Российской Федерации. В связи с чем, наряду с необходимой правовой базой правоохранительные органы Российской Федерации получают в свое распоряжение технические средства, специально созданные для обнаружения, фиксации, изъятия и проверки значимой информации путем производства оперативно-технических мероприятий, а также право на использование в этих целях любых средств коммуникации[1].

Следователь и сотрудники оперативно-розыскных подразделений заинтересованы в своевременном раскрытии подготавливаемых или уже совершенных преступлений и успешном расследовании уголовных дел, для

---

[1] Дуленко В.А, Мамлеев Р.Р., Пестриков В.А. / Преступление в сфере высоких технологий / Учебное пособие. – М.: ЦОКР МВД России, 2010. – 120-121 с.

чего им необходимо установить причастность разрабатываемого, подозреваемого, обвиняемого, а в ряде случаев и подсудимого лица (фигуранта) в совершенном преступлении. И когда возникает необходимость для проведения оперативно-розыскных мероприятий указанным должностным лицам необходимо поэтапно совершить следующие действия, а именно:

1) принятие решения о производстве необходимого мероприятия (действия) и согласование своего решения с руководителем органа;

2) получение разрешения на осуществление данного мероприятия;

3) поручение технического осуществления органу, уполномоченному на

4) производство конкретного специального технического мероприятия;

5) (получение) истребование полученных результатов;

6) осмотр полученных в ходе проведения ОРМ результатов;

7) оценка полученных результатов;

8) приобщение полученных результатов к материалам уголовного дела в

9) качестве вещественного доказательства.

После совершения всех вышеперечисленных действий у оперативного сотрудника появляется основание для использования полученных результатов в процессе доказывания по уголовному делу. Таким образом, анализ правовых оснований и тактических условий, рассматриваемых (проводимых) оперативно-технических мероприятий позволяет убедиться в том, что их суть заключается в организации практического осуществления контроля, как в процессуальном плане, так и в целях оперативно-розыскных мероприятий. Иными словами, при расследовании уголовных дел специально уполномоченными участниками уголовного судопроизводства создаются необходимые условия для целенаправленного собирания интересующей следствие криминалистической значимой информации. Необходимость ее получения, целесообразность и последующая результативность использования в доказывании по уголовному делу предопределены не только строгим соблюдением законодательных предписаний, имеющих прямое отношение к проведению оперативно-технических мероприятий, но и применением криминалистической технологии, учитывающей самые разнообразные закономерные связи. Она имеет универсальный характер и, в принципе, может применяться для познания каждого из обстоятельств, входящих в предмет доказывания по уголовному делу.

Рассмотрим пример, взятый из практической деятельности Управления «К» БСТМ МВД России.

Несколько участников группы, являясь действующими сотрудниками банка, копировали персональные данные клиентов и передавали их сообщникам. Злоумышленники, используя поддельные документы, получали доступ к банковским счетам жертв, и с помощью системы онлайн банкинга осуществляли переводы денежных средств на счета, открытые на подставных лиц, после чего обналичивали их через банкоматы в г. Москве и Московской области.

В ходе проведения оперативно-розыскных мероприятий выяснилось, что в состав группы входят 10 человек. Все они были задержаны.

В ходе обысков, проведенных по шести адресам, изъято 34 сим-карты, 26 мобильных телефонов, 2 ноутбука, 50 банковских карт, поддельная печать одного из нотариусов г. Москвы, пустые бланки доверенностей на замену сим-карт и поддельные бланки временного удостоверения личности.

Возбуждено уголовное дело по ч. 4 ст. 159 (мошенничество) УК РФ. В отношении подозреваемых лиц избрана мера пресечения в виде заключения под стражу. Указанная группа осуществляла свою преступную деятельность с 2012 года. Ущерб, нанесенный клиентам банка, превышает 20 млн. руб.

Не будем останавливаться на каждом виде оперативно-технических мероприятий, но при производстве любого из них всегда присутствует компонент негласности, дефицит протяженности во времени, за исключением контроля и записи переговоров. Оно выгодно отличается от любого вида ОТМ, и, естественно, обуславливает вполне определенную последовательность действий следователя и оперативного сотрудника для легализации средства доказывания. Технологическая цепочка оперативно-технических мероприятий начинается с принятия решения об их проведении. Однако все они имеют свою специфичную технологию, содержание которых должно быть представлено научными и разработанными на их основе рекомендациями об оптимальной линии поведения как оперативных сотрудников ОВД, так и следователей.

Целью взаимодействия, которых является получение, относимых, допустимых, достаточных и достоверных доказательств, которые имеют не только процессуальную, но и тактическую природу. Вместе с тем принятие решения о проведении одного из видов оперативно-технических мероприятий неминуемо влечет за собой определенные ограничения конституционных прав и свобод граждан, в связи с чем должны быть соблюдены все условия о недопустимости разглашения любых (полученных) данных, необходимых в дальнейшем с их практической реализацией в процессе доказывания преступной деятельности разрабатываемых лиц, подозреваемых в совершении преступления. Одновременно принятие такого решения и его дальнейшее производство связано с присутствием постоянного риска, как оперативных сотрудников, так и следователей на определенном этапе предварительного расследования[1].

В каждом конкретном случае решение о проведении оперативно-технического мероприятия порождает определенная оперативно-розыскная и следственная ситуация, обусловленная интересами раскрытия преступления, установления лиц, причастных к его совершению, для скорейшего продвижения процесса доказывания и эффективности расследования по уголовному делу.

Мы разделяем точку зрения авторов, которые говорят о том, что «проведенный анализ деятельности оперативных подразделений показывает, что подходы к получению, учету, анализу, документированию и представлению в следственные органы как самих данных, так и результатов ее обработки, в

---

[1] В.И. Тищенко, Т.И. Жуков, Ю.С. Попков. Сетевые взаимодействия. Предмет исследования и объект моделирования. М.: Ленанд, 2014. – 35-36 с.

разных следственных, оперативных и оперативно-технических подразделениях, в различных субъектах Российской Федерации значительно отличаются.

Отмечается неоднозначность в организации взаимодействия правоохранительных органов и компаний операторов связи, отсутствуют унифицированные алгоритмы взаимодействия между оперативными и оперативно-техническими подразделениями (далее ОТП), на которые возложены функции получения биллинговой информации для решения задач ОРД, не определено, в рамках каких ОРМ запрашиваются и предоставляются инициаторам данные об абонентах и оказываемых им услугах связи, а также другие сведения о работе информационно-телекоммуникационных систем, необходимые в ходе ОРД».

В заключении главы необходимо сделать следующие выводы:

1. В настоящее время методы и познавательные технологии, используемые сотрудниками оперативных подразделений, во многих случаях не позволяют сохранять процессуальную безупречность криминалистической значимой информации, полученной при производстве оперативно-розыскных мероприятий с использованием технических возможностей. Иными словами, при производстве одноименного оперативно-технического мероприятия не всегда удается добиться соблюдения всех требований, предъявляемых уголовно-процессуальным законом к доказательствам. В результате чего, собранные оперативными сотрудниками сведения о переговорах и других, в широком понимании этого значения, задокументированных действиях лиц могут признаваться судом недопустимыми в доказывании их преступной деятельности в ходе судебного рассмотрения и окончательного разрешения по уголовным делам.

2. Следователь и сотрудники оперативно-розыскных подразделений заинтересованы в своевременном раскрытии подготавливаемых или уже совершенных преступлений и успешном расследовании уголовных дел, для чего им необходимо установить причастность разрабатываемого, подозреваемого, обвиняемого, а в ряде случаев и подсудимого лица (фигуранта)

в совершенном преступление, необходима совместная и продуманная работа.

3. Целью взаимодействия, является получение, относимых, допустимых, достаточных и достоверных доказательств, которые имеют не только процессуальную, но и тактическую природу. Вместе с тем принятие решения о проведении одного из видов оперативно-технических мероприятий неминуемо влечет за собой определенные ограничения конституционных прав и свобод граждан, в связи с чем должны быть соблюдены все условия о недопустимости разглашения любых (полученных) данных, необходимых в дальнейшем с их практической реализацией в процессе доказывания преступной деятельности разрабатываемых лиц, подозреваемых в совершении преступления.

ЗАКЛЮЧЕНИЕ

Подводя итоги настоящей дипломной работы, хочется отметить, что деятельность оперативных подразделений, обеспечивающих раскрытие и своевременное реагирования на преступления в сфере высоких технологий, использованием вредоносных компьютерных программ, не достаточно проработана, но приобретает особую значимость в связи с компьютеризацией и глобальным использованием сети Интернет. В целом анализ статистических данных показывает, что, начиная с 2007 г. до настоящего времени прослеживается стойкая динамика увеличения количества и способов совершения данного вида преступлений.

Институт высоких технологий в настоящее время находится на этапе развития и требует пристального внимания и изучения, так как реализация правовой защиты нередко затруднена наличием большого количества пробелов, которые вызывают немало проблем в правоприменительной практике. Преодолеть указанное препятствие возможно посредством реформирования действующего уголовного, уголовно-процессуального и иного законодательства России по рассматриваемым аспектам.

Необходимо отметить, что автором приведенные рекомендации по устранению выявленных в ходе проведенного исследования законодательных коллизий и пробелов приведены с учетом современной ситуации, на основании статистики предоставленной отделом «К» по Республике Татарстан по преступлениям в сфере хищения денежных средств с использованием вредоносных компьютерных программ. В связи с этим работа может представлять интерес в качестве законодательной инициативы и практической значимость для ОВД, уголовного розыска. Так же данная работа представляет интерес и для теоретиков при проведении более узких исследований.

Основные выводы проведенного исследования, сделанные на основании анализа действующих правовых норм отечественного законодательства, теоретических положений, материалов оперативно-розыскной практики, а также мнения практических сотрудников, нашли свое отражение в следующих положениях:

1. С учетом представленных позиций авторов понятие «компьютерной информации» как предмета преступления можно сформулировать как организационно упорядоченную совокупность сведений (сообщений, данных), зафиксированных на машинном носителе либо в информационно - телекоммуникационной сети с реквизитами, позволяющие их идентифицировать, имеющую собственника либо иного законного владельца.

2. Уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее собственнику (владельцу, пользователю)

3. По нашему мнению отсутствие прямо подтвержденных «ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» (либо «неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации») вызывает затруднение при квалификации преступления по ст. 159.6 УК РФ или возможно альтернативным ст. 272 и 273 УК РФ. В отдельных случаях следствием могут быть усмотрены признаки кражи (ст. 158 УК РФ) или простого мошенничества (ст. 159 УК РФ)[1].

4. Перспектива возбуждения дела с неопределенной квалификацией и возможной последующей переквалификацией, с отсутствующим или крайне затянувшимся экспертным исследованием, без выявленных лиц, без получателя

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (с изм. от 23.05.2016) // Собрание законодательства РФ. – 1996. - № 25.- Ст. 2954.

денежных средств и с весьма слабой в целом перспективой раскрытия воспринимается сотрудниками полиции негативно. Поэтому зачастую на практике используется любая возможность и любые основания для отказа в возбуждении уголовного дела по поступившим заявлениям, что оставляет данные преступления безнаказанными.

5. Основную работу по выявлению, предупреждению, пресечению и раскрытию преступлений в сфере компьютерной информации выполняют оперативные подразделения органов внутренних дел, такие как Управление «К» БСТМ МВД России, отделы «К» БСТМ МВД, ГУМВД и УМВД субъектов РФ, специализированные отделы ГУЭБиПК МВД России и подразделений экономической безопасности МВД, ГУМВД и УМВД субъектов РФ, а также некоторые подразделения уголовного розыска. По нашему мнению, целесообразно проводить обучение, подготовку специалистов в направлении компьютерных преступлений для более эффективной работы подразделениями уголовного розыска, а именно создание специализированных курсов повышающих навыки в техническом направлении по преступлениям в сфере высоких технологий. Необходимо проводить заслушивания по данным делам в территориальных подразделениях с участием представителей или руководителей специализированных подразделений или консультантами отдела «К».

6. Отсутствует единая база, общая для всех преступлений указанной категории. Выделение данных, относящихся к хищениям денежных средств с использованием вредоносных компьютерных программ, должно производиться внутри общего массива в связи с особенностями характера и объема данных. Необходимо будет учитывать, что некоторые сведения, касающиеся хищений рассматриваемого типа, будут иметь особый правовой статус (сведения, составляющие банковскую тайну, персональные данные). Создание, наполнение и получение информации из такой базы данных позволят резко повысить эффективность работы оперативных подразделений в борьбе с

хищениями денежных средств, совершаемыми с использованием вредоносных компьютерных программ.

7. Для реализации и разработки единой базы данных необходимо проведение отдельного научно-практического исследования, участие в котором должны принимать сотрудники научных подразделений, представители технических подразделений, которые в дальнейшем будут обеспечивать функционирование необходимой аппаратной и сетевой инфраструктуры, а также представители оперативных подразделений будущих пользователей базы данных.

8. В работе приведен алгоритм реагирования оперативных подразделений на рассматриваемые преступления, проведение ОРМ на первоначальном и дальнейшем этапе, который в дальнейшем можно использовать как методические рекомендации для подразделений уголовного розыска.

9. На начальном этапе раскрытия преступлений в сфере телекоммуникаций и компьютерной информации немаловажное значение имеет своевременное получение информации о совершенном или готовящемся преступлении данной направленности. Полученная информация позволит избрать правильную линию поведения оперативным сотрудникам подразделений «К» с целью определения необходимого осуществления неотложных оперативно-розыскных, специальных технических мероприятий и следственных действий. Данное обстоятельство поможет с наименьшей затратой времени выйти на более точное оперативное сопровождение по установлению конкретных лиц, причастных к совершенному преступлению, и, как положительный результат, приведет к изобличению фигурантов с закреплением полученных в ходе документирования доказательств

10. Целью взаимодействия, является получение, относимых, допустимых, достаточных и достоверных доказательств, которые имеют не только процессуальную, но и тактическую природу. Вместе с тем принятие решения о проведении одного из видов оперативно-технических мероприятий неминуемо

влечет за собой определенные ограничения конституционных прав и свобод граждан, в связи с чем должны быть соблюдены все условия о недопустимости разглашения любых (полученных) данных, необходимых в дальнейшем с их практической реализацией в процессе доказывания преступной деятельности разрабатываемых лиц, подозреваемых в совершении преступления.

11. В настоящее время методы и познавательные технологии, используемые сотрудниками оперативных подразделений, во многих случаях не позволяют сохранять процессуальную безупречность криминалистической значимой информации, полученной при производстве оперативно-розыскных мероприятий с использованием технических возможностей. Иными словами, при производстве одноименного оперативно-технического мероприятия не всегда удается добиться соблюдения всех требований, предъявляемых уголовно-процессуальным законом к доказательствам. В результате чего, собранные оперативными сотрудниками сведения о переговорах и других, в широком понимании этого значения, задокументированных действиях лиц могут признаваться судом недопустимыми в доказывании их преступной деятельности в ходе судебного рассмотрения и окончательного разрешения по уголовным делам.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Конституция России от 12.12.1993 г. (в ред. от 04.08.2014) //Собрание законодательства РФ. – 2014.- № 31.

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (с изм. от 23.05.2016) // Собрание законодательства РФ. – 1996. – № 25.- Ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в ред. от 12.12.2016) // Собрание законодательства РФ, 2001. № 52. Ч. 1. Ст. 4921; Российская газета, 2016. № 1.

4. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (в ред. от 06.07.2016) // Собрание Законодательства РФ. - 1995.- № 33; Российская газета. -2016.- № 160.

5. О деятельности по приему платежей физических лиц, осуществляемой платежными агентами : Федеральный закон от 03.06.2009 № 103-ФЗ (ред. от 03.07.2016) // Собрание Законодательства РФ. -.2009- № 39.

6. О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 03.07.2016) // Российская газета .-2016.-№ 11

7. О банках и банковской деятельности :Федеральный закон от 02.12.1990 № 395-1 (ред. от 03.07.2016) // Собрание Законодательства РФ. - 2016.- № 223

8. О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России: приказ МВД РФ от 19.06.2012 № 608 // Российская газета. 03.08.2012. № 5850.

Книги, монографии, сборники научных трудов, учебные пособия

9. Андреев Б.В. Расследование преступлений в сфере компьютерной информации: учебное пособие / под ред. Б.В. Андреев. П.Н. Пак, В.П. Хорс. - М., 2012. - 152 с.

10. Атаманов, Р.С. Криминалистическая характеристика мошенничества в онлайн-играх / Р.С. Атаманов //. Российский следователь, 2011. - № 21. - 268 с.

11. Атаманов, Р.С. Некоторые вопросы расследования мошенничества в сети Интернет / Р.С. Атаманов. М., 2010. - № 4 (17). - 496 с.

12. Бурлаков, В.Н., Средства массовой информации и преступность (криминология СМИ) / В.Н. Бурлаков, Г.Н. Горшенков, С.В.Максина. М., 2012. - № 5. - 584 с.

13. Батурин Ю.М., Жодзишский А.М., Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин., А.М. Жодзишский - М.: Юрид. лит., 1991.

14. Быков В.М. Проблемы расследования групповых преступлений: автореф. дис. … д-ра юрид. наук. / В.М. Быков – М., 1992. – 262 с.

15. Воробьев В.В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис. … канд. юрид. наук. / В.В. Воробьев – Н. Новгород, 2010. – 200 с.

16. Вехов В.Б. Тактические особенности расследования преступлений в сфере компьютерной информации: учебное пособие / под ред. В.Б. Вехов, В.В Попова, Д.А.Илюшин., 2014. – 289 с.

17. Волженкин, Б.В. Прозрачность правосудия и информационная безопасность. / Б.В. Волженкин. – Режим доступа: law.edu.ru/doc/document.asp

18. Гаврилин Ю.В., Шипилов В.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации / Ю.В. Гаврилин, В.В. Шипилов // Российский следователь. 2013. №.23. С. 2-5.

19. Голубев, В.А. Вопросы международного сотрудничества в борьбе с транснациональной компьютерной преступностью / В.А. Голубев // – Режим доступа: http://www.crime-research.ru/articles/2011/

20. Гудзь, Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий / Е.Г. Гудзь // - Сб. докладов науч.-практ. семинара «Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств». - М., 2012. - 62 с.

21. Голубева В.А., Рыжкова Э.В., Компьютерная преступность и кибертерроризм: сборник научных статей / В.А. Голубева, Э.В. Рыжкова. // - Запорожье: Центр исследования компьютерной преступности, 2012. – Вып. 3. – 448 с.

22. Дикова Н.И. Осрбенности расследования преступлений, совершенных с использованием электронных платежных средств и систем : автореф. дис. … канд. юрид. наук. / Н.И. Диков - С., 2011.- 18-29 с.

23. Дворецкий, М.Ю. Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ: учебное пособие / под ред., М.Ю. Дворецкий, А.Н. Копырюлин. - Уголовное право, 2012. - №4. - 34 с.

24. Дуленко В.А. Преступление в сфере высоких технологий : учебное пособие / под ред., В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков - М.: ЦОКР МВД России, 2010. - 200 с.

25. Завидов Б. Д. Мошенничество в сфере высоких технологий: учебное пособие / под ред., Б.Д. Завидов, З.А. Ибрагимова. - Современное право, 2011. - № 4. - 44 с.

26. Карчевский Н.В. Компьютерные преступления: определение, объект и предмет /Н.В. Карчевский - Режим доступа: http://www.ifap.ru/pi/05/karchev.htm

27. Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в Российском сегменте сети Интернет: дис. канд. юрид. наук: 12.00.08. / Т.П. Кесареев -М., 2012.- 207 с

28. Крылов В.В. Расследование преступлений в сфере информации: учебное пособие / под ред., В.В. Крылов.- М., 2014. -164 с.

29. Крылов В. В. Расследование преступлений в сфере компьютерной информации: учебное пособие / под ред., В.В.Крылов. - М., 2012. - 615 с.

30. Маляров А.И. Объект преступления в сфере электронно-цифровой (компьютерной) информации и вопросы квалификации (российский и зарубежный опыт) / А.И. Маляров // - Общество и право, 2008. - № 2. -25 с.

31. Никифоров И., Уголовные меры борьбы с компьютерной преступностью: учебное пособие / под ред., И. Никифоров. - Защита информации, 2010. - № 5. - 258 с.

32. Номоконов В.А. Глобализация информационных процессов и преступность/ В.А. Номоконов // - Режим доступа: http://www.vkeys.kiev.ua/box/4/93.shtml

33. Номоконов В.А. Новые информационные технологии в борьбе с преступностью/ В.А. Номоконов // - Российский криминологический взгляд, 2012.- № 1. - 94 с.

34. Селиванов Н. А. Проблемы борьбы с компьютерной преступностью: учебное пособие / Н.А. Селиванов // - Законность, 2013. -№ 8. 37 с.

35. В.И. Тищенко, Т.И. Жуков, Ю.С. Попков. Сетевые взаимодействия. Предмет исследования и объект моделирования. М.: Ленанд, 2014. - 352 с.

36. Федоров В.А. Компьютерные преступления: выявление, расследование и профилактика: учебное пособие / под ред., В.А. Федоров. - Законность, 2011, № 6. - 43 с.

37. Черкасов, В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий: учебное пособие / под ред., В.Н. Черкасов. - Саратов, 2015. - 81 с.

38. Шмонин А.В. Организация выявления и раскрытия хищений денежных средств с использованием дистанционного банковского обслуживания: // А.В. Шомин / Информатизация и информационная безопасность правоохранительных органов». М., 2014.- 210 с.

Судебная практика

39. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27 декабря 2012 г. № 51 // Российская газета. - 2008. - № 4.- С. 7-8

Информационные ресурсы

40. http://www.mvd.ru/userfiles/file/2012/ban/mart/sb_1207.pdf
41. http://mvd.ru/presscenter/statistics/reports/item/804701/
42. http://mvd.tatarstan.ru/rus/index.htm/news/156697.htm
43. http://mvd.tatarstan.ru/rus/index.htm/news/154893.htm
44. http://mvd.tatarstan.ru/rus/index.htm/news/154410.htm5
45. http://www.symantec.com/ru/ru/security