МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
АКАДЕМИЯ УПРАВЛЕНИЯ

Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий

Учебное пособие

Часть 1

МОСКВА • 2019

УДК 343.8:004
ББК 67.401.213
Д 39

Одобрено редакционно-издательским советом Академии управления МВД России

Рецензенты: *В. Ф. Васюков*, профессор кафедры криминалистики и предварительного расследования в ОВД Орловского юридического института МВД России имени В. В. Лукьянова, доктор юридических наук; *В. Н. Береснев,* начальник ЛУ МВД России на ст. Москва-Ярославская.

Д 39

Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. / [А. В. Аносов и др.]. – М. : Академия управления МВД России, 2019. – Ч. 1. – 208 с.

ISBN 978-5-906942-87-6

Учебное пособие подготовлено в двух частях. В первой части учебного пособия рассмотрены особенности выявления признаков преступлений, совершенных с использованием информационно-коммуникационных технологий, их квалификации с учетом требований действующего законодательства и сложившейся правоприменительной практики, организации их расследования и предупреждения. Во второй части рассмотрены организационно-тактические основы оперативно-розыскной деятельности органов внутренних дел по организации выявления и раскрытия отдельных видов преступлений, совершенных с использованием информационно-коммуникационных технологий. Вторая часть содержит сведения, составляющие государственную тайну.

Учебное пособие предназначено для преподавателей, адъюнктов, слушателей (курсантов) образовательных организаций системы МВД России, а также для сотрудников органов внутренних дел, в компетенцию которых входит противодействие преступлениям, совершаемым с использованием информационных, коммуникационных и высоких технологий.

Нормативные правовые акты приведены по состоянию на 18 февраля 2018 г.

УДК 343.8:004
ББК 67.401.213

ISBN 978-5-906942-87-6

Авторский коллектив:

Гаврилин Ю. В., доктор юридических наук, доцент, профессор кафедры управления органами расследования преступлений Академии управления МВД России (введение, глава 2).

Аносов А. В., кандидат юридических наук, доцент кафедры уголовной политики Академии управления МВД России.

Баранов В. В., старший преподаватель кафедры информационных технологий Академии управления МВД России.

Васильченко Д. А., кандидат юридических наук, заместитель начальника кафедры оперативно-разыскной деятельности ОВД Омской академии МВД России.

Голяндин Н. П., кандидат юридических наук, доцент, профессор кафедры специальных дисциплин СКИ (ф) Краснодарского университета МВД России.

Гринченко В. С., заместитель начальника БСТМ ГУ МВД России по Московской области – начальник отдела «К».

Десятов М. С., кандидат юридических наук, доцент, начальник кафедры оперативно-разыскной деятельности ОВД Омской академии МВД России.

Кузьмин Н. А., кандидат юридических наук, доцент, начальник кафедры оперативно-разыскной деятельности и специальной техники Московского университета МВД России имени В. Я. Кикотя.

Лапунова Ю. А., кандидат юридических наук, доцент кафедры организации оперативно-разыскной деятельности Академии управления МВД России.

Любан В. Г., кандидат юридических наук, доцент кафедры оперативно-разыскной деятельности и специальной техники Московского университета МВД России имени В. Я. Кикотя.

Малахов А. С., кандидат юридических наук, доцент кафедры оперативно-разыскной деятельности ОВД Омской академии МВД России.

Парфенов А. В., кандидат юридических наук, заместитель начальника кафедры организации оперативно-разыскной деятельности Академии управления МВД России.

Прохоров Е. С., начальник отдела по раскрытию резонансных преступлений УУР ГУ МВД России по Алтайскому краю.

Рясов А. В., кандидат юридических наук, доцент, доцент кафедры оперативно-разыскной деятельности и специальной техники СФ Краснодарского университета МВД России.

Смольянинов Е. С., кандидат юридических наук, доцент, заместитель начальника кафедры уголовной политики Академии управления МВД России.

Третьяков М. А., заместитель начальника ЦПЭ УМВД России по Калужской области.

Филиппов А. Н., кандидат юридических наук, доцент, профессор кафедры оперативно-разыскной деятельности и специальной техники Московского университета МВД России имени В. Я. Кикотя.

Содержание

Введение

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[1] в качестве приоритетного направления внутренней политики определяет развитие информационных и коммуникационных технологий, формирование информационного пространства и соответствующей инфраструктуры.

Информационные технологии все глубже проникают в повседневную жизнедеятельность большинства граждан. Отмечается, что в 2016 г. в России на 100 человек приходилось 159,95 мобильных телефонов и из 100 человек 71,29 человека использовали мобильный доступ к сети Интернет. Средняя скорость в сети Интернет возросла на 29 %, что ставит Россию на один уровень с Францией, Италией, Грецией.

Примерно с середины 2000-х гг. электронные средства массовой информации, информационные системы, социальные сети, технологии беспроводного доступа в сеть Интернет, мобильная связь постепенно становились частью повседневной жизни россиян. Государство поощряет указанные тенденции: создана система предоставления государственных и муниципальных услуг в электронной форме, что позволяет гражданам направлять в электронной форме индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления.

В настоящее время активно продолжается процесс цифровизации практически всех сторон жизнедеятельности посредством внедрения технологий искусственного интеллекта, биометрической идентификации, работы с большими объемами данных, облачного хранения информации, дистанционного банковского обслуживания. Широко обсуждается перспектива использования технологии блокчейн, в том числе и в сфере оказания государственных и муниципальных услуг.

Все большее количество персональной информации пользователи помещают в информационные системы: посредством электронной почты пересылаются копии документов, удостоверяющих личность, на сервисы платежных систем направляются реквизиты банковских карт, в социальных сетях размещается информация о личной жизни, посредством мессенджеров передается иная конфиденциальная информация. Помимо этого интеллектуальные

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20. Ст. 2901.

системы поисковых сервисов на основе анализа запросов пользователя с высокой точностью формируют его социальный портрет, включая род занятий, круг интересов, уровень доходов, географию перемещений, социальные связи и пр.

Эти и другие глобальные изменения в сфере информационных процессов не могли не сказаться на состоянии преступности. По данным ГИАЦ МВД России, содержащимся в Отчетах о преступлениях, совершенных в сфере телекоммуникационной и компьютерной информации – «Форма 1-ВТ», утвержденная приказом МВД России от 1 апреля 2002 г. № 311, в 2017 г. в производстве правоохранительных органов находились уголовные дела о 105 645 преступлениях, совершенных с использованием информационно-коммуникационных технологий, что на 24,5 % превышает аналогичный показатель прошлого года – 79 704. Следует отметить, что подобная тенденция неуклонно сохраняется на протяжении последних лет.

Приведенные статистические показатели не отражают всю гамму преступлений, совершенных с использованием информационно-коммуникационных технологий. Так, в отчет, охватывающий около 10 составов преступлений (ст. 158, 159, 159.3, 159.6, 183, 272–274 УК РФ), не вошли такие преступления против личности, как доведение до самоубийства (ст. 110 УК РФ), склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110.1 УК РФ), организация деятельности, направленной на побуждение к совершению самоубийства (ст. 110.2 УК РФ), угроза убийством или причинением тяжкого вреда здоровью (ст. 119 УК РФ), принуждение к изъятию органов и тканей человека для трансплантации (ст. 120 УК РФ), клевета (ст. 128.1 УК РФ), понуждение к действиям сексуального характера (ст. 133 УК РФ), нарушение неприкосновенности частной жизни (ст. 137 УК РФ), нарушение изобретательских и патентных прав (ст. 147 УК РФ), вовлечение несовершеннолетнего в совершение преступления (ст. 150 УК РФ), вовлечение несовершеннолетнего в совершение антиобщественных действий (ст. 151 УК РФ), розничная продажа несовершеннолетним алкогольной продукции (ст. 151.1 УК РФ), вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (ст. 152.2 УК РФ), разглашение тайны усыновления (удочерения) (ст. 155 УК РФ) и иные преступления, совершаемые дистанционным способом, при которых непосредственный физический контакт между субъектом преступления и потерпевшим, а также соучастниками, осуществляется посредством сообщений в мессенджерах, социальных сетях, на специализированных сайтах.

Безусловно, развитие информационных и коммуникационных технологий открывает новые возможности для совершения перечисленных и иных преступлений прежде всего в сфере экономики, против общественной безопасности и общественного порядка и др., представляя собой вызов всей правоохранительной системе и общественной безопасности.

Анализ результатов деятельности органов внутренних дел по данному направлению деятельности свидетельствует о недостаточности принимаемых мер, что было отмечено в решении Координационного совещания руководителей правоохранительных органов Российской Федерации от 23 сентября 2016 г. № 2 «Об эффективности работы по выявлению, пресечению, расследованию и предупреждению преступлений, совершаемых с использованием информационно-коммуникационных технологий», а также в решении Коллегии МВД России от 24 октября 2017 г. № 3км «О мерах по совершенствованию раскрытия и расследования мошенничеств».

Ранее возникавшие проблемы правоприменения норм уголовного и уголовно-процессуального законов по данному направлению деятельности разъяснены Постановлением Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

В настоящее время не отвечает предъявляемым требованиям организация работы по проведению процессуальных проверок по сообщениям о преступлениях в сфере современных информационно-коммуникационных технологий: имеют место факты вынесения незаконных постановлений об отказе в возбуждении уголовного дела и направления сообщений о преступлениях по подследственности, приводящих к укрытию преступлений от учета. По большей части находящихся в производстве уголовных дел расследование приостанавливается в связи с неустановлением лиц, подлежащих привлечению в качестве обвиняемого. Данное обстоятельство вызвано низким качеством работы органов предварительного следствия, невыполнением требований законодательства, влекущими несоблюдение разумного срока уголовного судопроизводства. Зачастую не принимаются необходимые меры к возмещению ущерба, причиненного преступлениями.

Настоящее учебное пособие направлено на формирование у слушателей образовательных организаций системы МВД России знаний, умений и навыков по выявлению признаков преступлений, совершенных с использованием информационно-коммуникационных технологий, их квалификации с учетом требований действующего законодательства и сложившейся правоприменительной прак-

тики, организации их выявления, раскрытия, расследования и предупреждения.

За помощь в подготовке данного учебного пособия авторский коллектив выражает благодарность: Следственному департаменту МВД России и лично заместителю начальника контрольно-методического управления В. В. Кузьмину, а также следователю по особо важным делам контрольно-методического управления Д. В. Гусеву за предоставленные материалы следственной практики и организации расследования анализируемых преступлений; Экспертно-криминалистическому центру МВД России и лично заместителю начальника управления инженерно-технических экспертиз – начальнику отдела компьютерных и радиотехнических экспертиз О. В. Тушкановой за предоставленные материалы практики экспертно-криминалистического обеспечения расследования.

Глава I. Уголовно-правовые и криминологические основы противодействия преступлениям, совершенным с использованием информационных, коммуникационных и высоких технологий

§ 1. Уголовно-правовая характеристика преступлений, совершенных с использованием информационных, коммуникационных технологий и в сфере компьютерной информации

Активное применение компьютерных технологий во всех сферах жизни общества является неотъемлемой характеристикой современности. В настоящее время этот вектор развития общественной жизни объективно обусловливает и существенный рост количества совершаемых преступлений с использованием компьютерных технологий. В соответствии с отчетом об исследовании киберпреступности, предоставленным компанией «Нортон», в 2013 г. 85 % граждан России становились жертвами компьютерных преступников, а совокупный ущерб от киберпреступлений в мире составил 113 трлн долларов.

Это означает, что в ближайшем будущем Россия, вполне вероятно, столкнется со следующей ситуацией: повсеместное внедрение во все сферы жизни общества современных компьютерных технологий приведет к еще более значительному скачку компьютерной преступности, на который правоохранительные органы смогут адекватно отреагировать лишь при условии надлежащего правового обеспечения своей деятельности по противодействию преступности данного вида.

Не вызывает сомнений тот факт, что преступления, совершаемые с использованием современных компьютерных технологий, имеют существенную специфику. Применение технических новинок для совершения противоправных действий позволяет преступникам посягать на наиболее важные охраняемые законом общественные отношения в сфере прав и интересов личности, общества и безопасности государства. Сложность обнаружения действий компьютерного преступника и его возможности совершать преступления в киберпространстве, не имеющем государственных границ, многократно увеличивают степень общественной опасности таких деяний.

В то же время действующее уголовное законодательство Российской Федерации не в полной мере содержит достаточной нормативной правовой базы для реализации ответственности за пре-

ступления исследуемой группы в соответствии с их реальной общественной опасностью. Некоторые деяния, обладающие признаком общественной опасности, не криминализированы в рамках УК РФ. В современном российском законодательстве отсутствует нормативное закрепление понятий «преступление, совершаемое с использованием компьютерных технологий», «компьютерные технологии», «использование компьютерных технологий». Закрепленные в действующем российском уголовном законодательстве составы, регламентирующие ответственность за использование компьютерных технологий при совершении преступлений, не во всем соответствуют требованиям, предъявляемым международным сообществом для унификации на международном уровне, в частности Конвенции Совета Европы «О преступности в сфере компьютерной информации» (EST № 185).

Понятие и виды преступлений, совершенных с использованием информационно-коммуникационных технологий

Человеческая цивилизация находится в постоянном развитии. Новые технологические разработки позволяют сделать жизнь человека значительно комфортнее. Однако параллельно проходит и иной процесс: по мере появления технических достижений многие из них начинают использоваться для облегчения криминальной деятельности. Так, всеобщая компьютеризация играет значительную роль в деле технологического оснащения преступности. Кроме того, в современном обществе информация закономерно перешла на новую ступень развития, стала товаром, получившим реальную стоимость, в связи с чем стала распространенным предметом посягательства. Сложность обнаружения действий компьютерного преступника и одновременно возможность без существенных усилий осуществлять криминальную активность делают данную категорию преступлений достаточно притягательной для злоумышленников.

При этом развитие компьютерной преступности происходит по двум взаимосвязанным путям: с одной стороны, появляются новые неизвестные ранее преступления, с другой стороны, преступники используют компьютерные технологии при совершении деяний, ответственность за которые уже закреплена в «некомпьютерных» статьях УК РФ.

Кроме того, использование технических приспособлений позволяет преступникам эффективно координировать свои действия и избегать ответственности. Например, в преступных группах, создаваемых посредством сети Интернет, участники могут не иметь информации о других членах группы и никогда не встречаться друг

с другом, что существенно уменьшает риск быть обнаруженными. В то же время использование протоколов связи позволит им эффективно осуществлять совместные действия для достижения единого умысла.

Динамичность развития и распространенность преступлений, совершаемых с использованием компьютерных технологий, сделали их предметом исследования многих российских и зарубежных специалистов. Такие преступления изучаются с позиций уголовного права, криминологии, криминалистики, уголовного процесса, виктимологии и многих других наук. Однако столь разнородный взгляд на проблему приводит к существенным различиям в установлении авторами понятийного аппарата. Что же является преступлениями, совершаемыми с использованием компьютерных технологий, и каково соотношение данного понятия и понятий «киберпреступления», «компьютерные преступления», «преступления в сфере компьютерной информации»? В российской уголовно-правовой доктрине отсутствует единая точка зрения по данному вопросу. Основной проблемой является несовершенство действующего уголовного законодательства, в котором отсутствует регламентация ответственности за совершение преступлений с использованием компьютерных технологий, а официальное закрепление получила только ограниченная группа деяний, для которой используется термин «преступления в сфере компьютерной информации». В то же время данные проведенного нами опроса показывают, что 60 % респондентов считают современное уголовно-правовое регулирование ответственности за использование компьютерных технологий при совершении преступлений ненадлежащим, а 80 % опрошенных уверены в большей степени общественной опасности преступлений, совершаемых с использованием компьютерных технологий, по сравнению с «некомпьютерными» деяниями.

Существенное значение для изучения преступлений, совершаемых с использованием компьютерных технологий, имеет анализ истории их развития. Говоря о ретроспективе преступного использования компьютерных технологий и его законодательного ограничения, следует принимать во внимание, что динамика данных процессов существенно различалась в России и в странах, где компьютерные технологии стали частью общественной жизни значительно раньше. В нашей стране еще в период существования СССР компьютерные технологии в основном использовались для работы в правоохранительной и банковской сферах, в целях обеспечения обороноспособности страны и полного контроля государством, в то время как в зарубежных странах компьютер прак-

тически сразу стал существенной частью жизни обычных граждан. Таким образом, в мире проблема противодействия преступлениям, совершаемым с использованием компьютерных технологий, проявилась гораздо раньше и до конца 1990-х гг. стояла гораздо острее, чем в России.

Так, первенство в совершении киберпреступлений принадлежит США. В 1966 г. компьютер был впервые использован как инструмент для совершения кражи из Банка Миннесоты.

В истории развития криминального использования компьютерных технологий можно отметить следующие наиболее значимые события:

– в 1973 г. сотрудник Ситибанк с помощью служебного компьютера похитил 2 млн долларов;

– 1987 г. – первый случай заражения компьютерным вирусом в СССР;

– 1989 г. – вирус в сети Пентагона, блокировка 6 000 компьютеров;

– 1990 г. – группа хакеров на 24 часа саботировала работу сети NASA;

– 1995 г. – покушение на кражу 2,8 млн долларов из Ситибанка.

Постепенно единичные случаи стали системными, противоправное использование компьютерных технологий распространилось повсеместно, а ущерб от таких деяний стал исчисляться миллионами долларов. Так, например, в 2003 г. средние потери американских компаний от кражи конфиденциальной информации составили 2 699 842 $, от компьютерного саботажа – 214 521 $, повреждения информации – 199 871 $.

В соответствии с отчетом компании «Нортон» в 2011 г. убытки от совершения киберпреступлений составили 388 млрд долларов, а жертвами стали 341 млн человек. Как показывают данные проведенного нами опроса, 13,33 % респондентов сталкивались за последний год с противоправной деятельностью с использованием компьютерных технологий один раз, а 33,33 % – неоднократно.

Анализируя историю совершения преступлений с использованием компьютерных технологий, можно выделить закономерности их развития. Так, если на заре становления киберпреступности основной целью злоумышленника являлось личное обогащение, а компьютер использовался как инструмент хищения, то к 90-м гг. XX в. основной целью лица, совершающего преступление с использованием компьютерных технологий, стал «интеллектуальный вызов», т. е. стремление показать свое превосходство в знании компьютерных систем и обходе средств их защиты. В настоящее время

преступления с использованием компьютерных технологий часто становятся инструментом незаконного политического давления.

Например, в начале 2009 г. финансовые учреждения Индии, в том числе Государственный банк, подверглись атаке хакеров из Пакистана.

Весной 2013 г. банковская система Южной Кореи оказалась выведена из строя в результате кибератаки. Власти страны обвинили в этом государственных хакеров Китая и спецслужбы КНДР.

В мае 2013 г. компьютерным атакам со стороны «Сирийской электронной армии» подверглись интернет-представительства СМИ США и телекомпании ВВС. Кроме того, хакеры разместили в прессе информацию о взрыве в Белом Доме. Это вызвало обвал фондовых бирж США.

Как видно, компьютерное вмешательство может использоваться для причинения ущерба экономическим интересам либо безопасности страны, а также в качестве способа дестабилизации обстановки в обществе и даже провокации неконституционных политических процессов.

Межгосударственная интеграция, новые средства коммуникации, развитие международной электронной торговли породили такое негативное явление, как криминальную глобализацию, выражающуюся в том числе в высокотехнологичном мошенничестве, интеллектуальном пиратстве и отмывании преступных доходов, которые осуществляются международными преступными структурами с применением компьютерных технологий.

Таким образом, преступления, совершаемые с использованием компьютерных технологий, наряду с терроризмом и коррупцией, со временем стали представлять существенную угрозу не только отдельному человеку или государству, но и цивилизации в целом.

Киберпреступность и ее классификация

Разнородность правового закрепления составов преступлений с использованием компьютерных технологий в законодательстве различных государств ставит перед наукой и правообразующими структурами проблему унификации правового пространства на международном уровне. Исходной позицией по данному вопросу должен являться тезис о том, что для преступлений данного вида государственных границ в принципе не существует. Работы в данном направлении ведутся на универсальном, межгосударственном и региональном уровнях правового регулирования. Благодаря подписанию странами – участницами международных договоров устанавливаются единые основы юрисдикции и правила международно-

го сотрудничества государств в сфере противодействия преступности с использованием компьютерных технологий.

На наш взгляд, наиболее актуальными для исследования являются близкие Российской Федерации правовые пространства: международные документы, принимаемые в Европейском правовом пространстве и СНГ. Изучение и последующая имплементация предложенных в международных актах составов компьютерных преступлений в российское законодательство будут способствовать облегчению преследования лиц, совершающих преступления с использованием компьютерных технологий, на межгосударственном уровне.

Известно, что Совет Европы принимает значительные усилия по приведению к единообразию законодательств стран – участниц в сфере правового регулирования компьютерных преступлений.

Исторически первым нормативным актом Совета Европы, посвященным вопросам регулирования киберпреступности, была Рекомендация № R 89 (9) Комитета Министров стран – членов Совета Европы о преступлениях, связанных с компьютерами, принятая 13 сентября 1989 г. В соответствии с данным документом государствам – членам Совета Европы надлежит при разработке национального законодательства принять во внимание Отчет Европейского комитета по проблемам преступности о преступлениях, связанных с компьютерами. В рамках данного Отчета Комитет по проблемам преступности дал оценку явлению компьютерной преступности и представил руководящие указания для криминализации противоправных деяний в законодательстве стран – участниц.

По мнению ряда авторов, рекомендательный характер указанного документа не способствует разрешению возникающих на практике коллизий и не отменяет необходимости подписания полноценных международных правовых документов. С этим нельзя не согласиться, однако следует отметить и значение указанной Рекомендации – ее принятие стало первой вехой в деле унификации борьбы с преступлениями, совершаемыми с использованием компьютерных технологий, на международном уровне.

Отчет разделяет преступления, совершаемые с использованием компьютерных технологий, на два перечня: минимально необходимые к включению в национальное законодательство и дополнительные.

К минимально необходимым преступлениям отнесены:

1. Компьютерное мошенничество, которое определяется как ввод, изменение или удаление данных или программ компьютера или иное вмешательство в процессы обработки данных, влияющее на итоги обработки данных, которое причиняет экономический

ущерб или приводит к уничтожению собственности другого лица, совершаемое с целью получения незаконным путем экономической выгоды для себя или для другого лица.

2. Компьютерный подлог, т. е. ввод, изменение или удаление данных (программ) компьютера либо другое вмешательство в процесс обработки данных, совершенное способом или при условиях, установленных нормами национального законодательства, которыми эти деяния квалифицируются как подлог, и совершены в отношении традиционного объекта правонарушения.

3. Причинение ущерба компьютерным данным или компьютерным программам, т. е. незаконное удаление, причинение ущерба или ухудшение качества данных или программ компьютера.

4. Компьютерный саботаж: ввод, изменение или удаление данных или программ компьютера, или создание помех компьютерным системам с целью воспрепятствования работе компьютера или телекоммуникационной системы.

5. Несанкционированный доступ, представляющий неправомочный доступ к системе или компьютерной сети путем нарушения мер охраны.

6. Несанкционированный перехват, т. е. неправомерный и осуществленный с применением технических средств перехват сообщений, направленных в систему или сеть компьютеров, исходящих из системы или сети компьютеров и передаваемых в рамках системы или сети компьютеров.

7. Несанкционированное воспроизведение компьютерной программы, охраняемой авторским правом. Под ним понимается совершенное неправомерно распространение, воспроизведение или передача в общественное пользование компьютерной программы, охраняемой законом.

8. Несанкционированное воспроизведение микросхемы, т. е. совершенное неправомерно воспроизведение микросхемы изделия на полупроводниках, если она охраняется законом, либо неправомерное использование или импорт в коммерческих целях микросхемы или изготовленного с ее применением изделия на полупроводниках.

Дополнительный перечень правонарушений в соответствии с Отчетом включает в себя следующие составы противоправных деяний:

1. Неправомерное изменение данных или программ в компьютере.

2. Компьютерный шпионаж, который в соответствии с Рекомендацией определен как получение незаконными способами или раскрытие, передача или использование торговой или коммерче-

ской тайны лицом, не имеющим на это прав или какого-либо иного законного основания, с целью причинения экономического ущерба лицу, имеющему доступ к этой тайне, или получения незаконной экономической выгоды для себя или третьего лица.

3. Несанкционированное использование компьютера – это незаконное использование системы или сети компьютеров, которое совершается: а) лицом, которое имеет право использовать систему, с осознанием того, что действия этого лица увеличивают риск причинения ущерба системе или ее функционированию либо причиняют такой ущерб; б) любым лицом с целью причинения ущерба управомоченному пользователю системы, функционированию системы или самой системе; в) любым лицом с фактическим причинением ущерба системе в целом, функционированию системы или управомоченному пользователю системы.

4. Несанкционированное использование компьютерной программы, охраняемой законодательством: неправомерное использование охраняемой законом компьютерной программы либо воспроизведение без права на это, совершаемые с целью получения незаконной прибыли для злоумышленника или третьих лиц либо причинения правообладателю ущерба.

Несмотря на то что Рекомендация и Отчет носят необязательный характер для стран – членов Совета Европы, их положения можно гармонично использовать в российской правовой системе для законодательного установления ответственности за совершение преступлений с использованием компьютерных технологий.

Вторым существенным документом в исследуемой сфере является Конвенция Совета Европы о преступности в сфере компьютерной информации. Она содержит нормы статей материального уголовного права, регламентирующие преступления, связанные с использованием компьютерных технологий, в соответствии с которыми страны – участницы обязаны реализовать правовые нормы в собственном законодательстве.

Таким образом, использование компьютерных технологий при совершении преступлений является особой разновидностью общественно опасной и противоправной деятельности, в настоящее время получающей все большее распространение как в глобальном масштабе, так и в отдельных странах, в том числе и в России. Рассматриваемому виду преступлений присущи следующие объясняющие возрастающую стремительными темпами «популярность» в криминальной среде черты: высокий уровень латентности, который объясняется как всеобъемлемой компьютеризацией общественной и личной жизни, так и трансграничным характером преступной

деятельности и связанной с этим неуловимостью компьютерных преступников, а также сравнительная простота совершения преступлений.

Динамичность распространения компьютерных технологий и их метаморфозы обязывают законодателя и правоохранительные органы, противодействующие компьютерной преступности, увеличивать скорость реакции на появление новых способов противоправной деятельности с использованием компьютерных технологий. Наилучшим способом противодействия высокотехнологичной преступности можно считать реализацию опережающего правового регулирования.

Отсутствие единой международной нормативной правовой базы, существенные различия в национальных законодательствах стран, объединенных идеей совместной борьбы с компьютерной преступностью, и отсутствие единого подхода к определению понятийного аппарата рассматриваемой совокупности общественно опасных деяний существенно осложняют эффективное противодействие использованию компьютерных технологий при совершении преступлений.

Существует настоятельная продиктованная временем необходимость выделения преступлений, совершаемых с использованием компьютерных технологий, в качестве отдельной группы противоправных деяний в уголовном законодательстве. Потребность в этом обусловливается как возрастающей степенью общественной опасности деяний, так и особенностями их объекта.

§ 2. Особенности квалификации преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации

Стремительный рост информационных технологий закономерно обусловливает интерес исследователей к ним из разных областей науки. Право, в том числе уголовное, не является исключением. В настоящее время формируется отдельная отрасль права – информационное право. Несмотря на это, до сих пор в науке не выработаны единые подходы к анализу информационно-правовых явлений. В частности, отсутствует понятие информации, которое удовлетворяло бы большинство исследователей и которое можно было бы применять в уголовно-правовой сфере. Такое положение дел нельзя признать удовлетворительным.

В 1998 г. была разработана и одобрена Концепция государственной информационной политики Российской Федерации, одним из

предназначений которой является привлечение внимания государственных органов, средств массовой информации, всех заинтересованных лиц к вопросам подготовки государства, общества, личности в условиях жизни информационного социума. Согласно данной Концепции одной из основных задач государственной информационной политики является обеспечение информационной безопасности. Среди основных положений правового обеспечения государственной информационной политики – защита законными средствами личности, общества, государства от ложной, искаженной и недостоверной информации. В развитие положений Концепции в 2000 г. была утверждена Доктрина информационной безопасности Российской Федерации. В июле 2000 г. в Окинаве «восьмерка» приняла Хартию Глобального информационного общества, в которой устанавливаются основные принципы вхождения государств в такое общество. 27 июля 2006 г. принят Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Особенности квалификации преступлений, совершаемых с использованием информационно-коммуникационных технологий и в сфере компьютерной информации

Говоря о правовом регулировании преступлений с использованием компьютерных технологий в уголовном законодательстве Российской Федерации, не следует забывать о том, что понятия «преступления в сфере компьютерной информации» и «преступления, совершаемые с использованием компьютерных технологий» не идентичны по своему смысловому составу. Поэтому, на наш взгляд, необходимо рассматривать преступления в сфере компьютерной информации как составную часть преступлений с использованием компьютерных технологий. Также необходимо отдельно рассмотреть остальные преступления с использованием компьютерных технологий, закрепленные в иных главах УК РФ.

Общественная опасность преступлений в сфере компьютерной информации заключается в том, что неправомерный доступ или изменение компьютерной информации может нарушать деятельность различных систем обеспечения государства: обороны, энергетики, транспорта и повлечь не только материальный ущерб, но и человеческие жертвы.

Правовое регулирование преступлений в сфере компьютерной информации в УК РФ осуществлено путем закрепления в главе 28 «Преступления в сфере компьютерной информации» трех составов:

1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

Сущность запретов, отраженных в правовых нормах указанной главы уголовного закона, заключается в недопущении общественно опасных деяний, посягающих на безопасность компьютерной информации и систем обработки компьютерной информации. При этом сам компьютер выступает всегда как средство совершения преступления.

Расположение главы 28 в разделе IX УК РФ «Преступления против общественной безопасности и общественного порядка» позволяет определить родовой объект компьютерных преступлений. Им является общественная безопасность. Под общественной безопасностью понимается совокупность общественных отношений, установленных нормативными правовыми актами, обычаями и традициями, обеспечивающих достаточный уровень личной безопасности членов общества и самого общества в целом. Вместе с тем преступления в сфере компьютерной информации могут посягать и на иные объекты уголовно-правовой охраны. К ним относятся права граждан на обеспечение охраняемой законом тайны (семейной, личной, врачебной и др.), право собственности, безопасность государственной тайны и др.

Видовым объектом преступлений, ответственность за которые регламентирована главой 28 УК РФ, являются общественные отношения в сфере обеспечения безопасности компьютерной информации. Безопасность компьютерной информации распространяет свое действие на информацию в компьютерных устройствах и может быть рассмотрена как аспект информационной безопасности. Среди прочих видов безопасности информационная безопасность обладает наибольшей степенью неопределенности. Это объясняется ее свойствами, проистекающими из неопределенности информации, разнообразия ее носителей и наличия информационного аспекта во всех видах человеческой деятельности.

Отношения информационной безопасности возникают в процессе накопления, обработки и использования информации и включают в себя информацию, связанные с информацией процессы, автоматизированные информационные системы, информационные технологии, средства информационного обмена и т. д.

С учетом изложенного информационную безопасность можно определить как существующую в социуме совокупность обществен-

ных отношений, подразумевающих достаточную степень защиты процессов производства, накопления, сохранения, передачи и применения (использования) компьютерной информации, в которые вовлечены лица, являющиеся собственниками, владельцами или пользователями информации.

Информационная безопасность обеспечивается применением мер, направленных на уменьшение, предотвращение или поддержание на приемлемом уровне негативных последствий от неправомерного воздействия на объекты информационной сферы. Законодательное определение информационной безопасности содержалось в ст. 2 Федерального закона от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене». В данной статье под ней понималось состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

После утраты силы данного закона нормативное определение информационной безопасности было закреплено в Доктрине информационной безопасности Российской Федерации, утвержденной Президентом России 9 сентября 2000 г. Здесь это понятие определено как состояние защищенности национальных интересов России, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Непосредственный объект предусмотренных главой 28 УК РФ составов преступлений трактуется исходя из названий и содержания диспозиций конкретных статей. Но вместе с тем он производен от родового и видового.

При совершении преступления в сфере компьютерной информации, помимо посягательства на безопасность компьютерной информации, могут поражаться иные блага: неприкосновенность частной жизни, права личности, имущественные интересы, основы конституционного строя, общественная или государственная безопасность. Эти интересы личности, общества и государства, подлежащие правовой охране, являются дополнительным объектом посягательства для преступлений в сфере компьютерной информации. Незначительность ущерба этим охраняемым благам либо полное отсутствие такового может исключать уголовную ответственность в силу малозначительности совершенного деяния в соответствии с ч. 2 ст. 14 УК РФ.

Предметом закрепленных в главе 28 составов преступлений является компьютерная информация. Понятие компьютерной информации раскрывается в примечании 1 к ст. 272 УК РФ. Под ней понимаются сведения (сообщения, данные), представленные

в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Объективная сторона компьютерных преступлений может проявляться как в действии, так и в бездействии. В основном данные деяния совершаются путем действий. Однако нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) возможно также путем бездействия. Поскольку глава 28 УК РФ закрепляет в основном материальные составы преступлений (исключение составляет создание, использование и распространение вредоносных компьютерных программ (ч. 1 ст. 273 УК РФ, имеющее формальный состав)), действие либо бездействие должно влечь за собой последствия в виде причинения вреда законным правам или интересам личности, общества или государства. Между деянием и последствиями должна быть установлена причинно-следственная связь.

Временем совершения преступления в сфере компьютерной информации следует признавать момент нажатия управляющей клавиши компьютера, запускающей конечную команду. При этом не имеет существенного значения, через какой промежуток времени наступили предусмотренные опасные последствия. Разделяющий последствия и деяние промежуток времени может быть минимальным и составлять несколько мгновений, затраченных компьютером на анализ, принятие и исполнение загруженной команды. Напротив, при определенных условиях этот временной промежуток может быть весьма длительным, поскольку, например, в некоторые вредоносные программы изначально вносится условие, при котором они начинают функционировать не сразу, а через определенный промежуток времени. Вредоносный код может начать разрушительное действие только после совершения пользователем некоторых манипуляций, например, после запуска определенной программы или по истечении некоторого промежутка времени после работы с программой.

Гораздо сложнее определить место совершения компьютерного преступления. Большинство преступлений в сфере компьютерной информации совершается в компьютерных сетях. Это подразумевает, что место совершения противоправного деяния и место наступления общественно опасных последствий могут отделяться друг от друга многими километрами и даже находиться на территории разных государств.

Действующий УК РФ не закрепляет в правовых нормах место совершения преступления в сфере компьютерной информации.

Им может признаваться как место совершения деяния, так и место, в котором деяние окончено либо пресечено, либо место наступления общественно опасных последствий.

Существенное значение задача определения места совершения преступления приобретает в случае совершения действий, образующих состав преступления в сфере компьютерной информации на территории одного государства, когда последствия этих действий наступают на территории другого государства. Наглядным примером может служить дело В. Левина, который с помощью компьютера, находящегося в офисе фирмы в Санкт-Петербурге, вводил ложные данные в систему банка «Ситибанк», расположенного в США, в результате чего со счетов вкладчиков было похищено более 10 000 000 долларов. В. Левин скрывался от следствия и был задержан и осужден в Лондоне. При этом Великобритания отказала в выдаче преступника США и РФ, мотивируя это тем, что законодательство страны не регламентирует ситуацию, когда преступление совершено на территории одного государства, а последствия наступили на территории другого.

Субъект всех закрепленных в УК РФ преступлений в сфере компьютерной информации общий. Им является вменяемое физическое лицо, достигшее возраста наступления уголовной ответственности – 16 лет.

Субъективная сторона рассматриваемых деяний может характеризоваться как умышленной, так и неосторожной формами вины. Среди мотивов, характерных для всех компьютерных преступлений, преобладают два основных: корысть и «интеллектуальный вызов», т. е. стремление продемонстрировать собственный профессионализм.

Следует обратить внимание на то, что с момента вступления в силу действующего Уголовного кодекса в главу 28 УК РФ долгое время вносились только незначительные изменения, не касающиеся структуры и содержания статей. Так, используемые ранее в санкции для определения размера штрафа минимальные размеры оплаты труда заменялись на фиксированные суммы, производилось ужесточение санкций, одновременно их нижние пределы снижались до минимально возможных для определенных видов наказаний.

Ситуация изменилась с принятием Федерального закона от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». В соответствии с ним нормы, содержащиеся в главе 28 УК РФ «Преступления в сфере компьютерной информации», подверглись качественной переработке с учетом

накопленного практикой опыта. Во все статьи главы 28 УК РФ были внесены существенные изменения, затронувшие как структуру, так и содержательную часть содержащихся в них запретов.

Однако данные изменения не до конца решили общую проблему приведения законодательства в соответствие с требованиями действительности и, как следствие, не способствовали устранению частных проблем, возникающих в процессе правоприменительной деятельности. Дело в том, что определение в уголовном законе признаков объективной стороны преступлений, ответственность за которые предусмотрена статьями главы 28 УК РФ, и установление их на практике предполагает использование как законодателем, так и правоприменителем специальных технических знаний в сфере компьютерной информации и устройства компьютерных систем.

Наибольшему количеству изменений подверглась ст. 272 УК РФ «Неправомерный доступ к компьютерной информации».

До внесения поправок структурно статья состояла из двух частей. Первая часть предусматривала ответственность за совершение общественно опасного деяния небольшой тяжести, а вторая – с учетом особенностей субъекта устанавливала признаки квалифицированного состава, относящегося к преступлениям средней тяжести. На основании ч. 1 ст. 272 УК РФ в изначальной редакции наказуем был неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Квалифицированный состав преступления образовывало то же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Проблемы правоприменительной практики при квалификации преступлений, совершенных с использованием информационно-коммуникационных технологий

В ст. 272 УК РФ законодатель соединил в одном составе несколько деяний, являющихся самостоятельными преступлениями в зарубежном уголовном законодательстве.

Речь идет о незаконном доступе к компьютеру (компьютерной системе) и вмешательстве в систему или данные (ст. 2, 4 и 5 Конвенции о киберпреступности). Еще до принятия Конвенции некоторые зарубежные страны разграничили три указанных преступления.

В частности, ответственность за незаконный доступ предусмотрена в ст. 138а УК Голландии и ст. 197 УК Испании в главе против преступлений, посягающих на общественный порядок и неприкосновенность частной жизни; случаи вмешательства в систему (логического/компьютерного саботажа по УК Голландии) по голландскому УК и УК Испании отнесены к главе о причинении вреда.

Многие лица, получающие доступ к компьютерным системам и сетям, убеждены, что они не делают ничего противозаконного и уголовно наказуемого (а если исходить из действующего уголовного кодекса, то так оно и есть), даже если им приходится нарушать системы защиты, установленные пользователем. Однако для нормального функционирования компьютерных систем и обеспечения безопасности хранения и передачи информации уголовный закон должен защищать компьютер любого пользователя, пользующегося средствами защиты. Поэтому во многих зарубежных правопорядках незаконный доступ к компьютеру защищается наравне с незаконным проникновением в жилище, поскольку в обоих случаях преступник посягает на конституционные права граждан: на неприкосновенность жилища (ст. 25 Конституции Российской Федерации) и неприкосновенность частной жизни, личную и семейную тайну (ч. 1 ст. 23 Конституции Российской Федерации). Такой подход представляется оправданным, учитывая роль компьютеров в жизни современного человека, когда в нем может храниться большой объем сведений о человеке, касающихся разных сфер его жизни.

Но если компьютеры находятся не во владении частных лиц, а во владении каких-либо организаций, тогда сам факт доступа к ним может иметь негативные последствия. Как отмечает А. Г. Шипков, электронные вычислительные машины и их информационное содержание широко применяются в вооруженных силах, космонавтике, атомной энергетике, в наземных, морских, воздушных транспортировках и т. д. Неправомерный доступ в компьютерное обеспечение такой деятельности может причинить ущерб обороноспособности страны, повлечь аварийные ситуации, экологические катастрофы, гибель людей и многое другое.

Отметим одно обстоятельство, на которое российские ученые обычно не обращают внимание. Согласно УК РФ наказуемым является доступ к компьютерной информации, в то время как в Конвенции и УК многих зарубежных стран, в частности Голландии, речь идет о незаконном доступе к компьютерной системе в целом или ее части. Конечно, и в том и в другом случае предметом уголовно-правовой охраны будет неприкосновенность хранящихся в компьютере данных, однако представляется, что зару-

бежная формулировка является более удачной, поскольку она акцентирует внимание на том, что запрещенным является доступ прежде всего к компьютеру как к устройству, потенциально хранящему конфиденциальную информацию, т. е. в таком случае уголовно-правовой барьер переносится на более раннюю стадию незаконного доступа.

Можно представить ситуацию, когда в компьютере не содержится никакой иной информации, кроме обеспечивающей работу операционной системы. В таком случае лицо, незаконно проникнувшее в компьютер, не будет подлежать ответственности за незаконный доступ к информации, поскольку данная информация не является конфиденциальной и не охраняется законом. В то же время если уголовно-правовой запрет будет касаться незаконного доступа к устройству, то действия лица будут уголовно наказуемы.

Второй вариант криминализации представляется более предпочтительным.

Можно провести грубую аналогию с традиционными составами преступлений. Согласно ч. 1 ст. 158 УК РФ кража имущества запрещена. Кража с незаконным проникновением в хранилище указана в ч. 2 ст. 158, а самонарушение неприкосновенности жилища – в ст. 139 УК РФ. Таким образом, уголовный закон в равной степени охраняет как неприкосновенность жилища, так и имущество, которое может в нем находиться. Если выделить в самостоятельный формальный состав незаконный доступ, то он условно будет корреспондировать ст. 139 УК РФ. При этом незаконное копирование данных будет корреспондировать ч. 1 ст. 158 УК РФ, а незаконный доступ, повлекший незаконное копирование, – ч. 2 ст. 158 УК РФ. Данная аналогия не кажется такой уж нелепой, если вспомнить вышеупомянутые положения зарубежного законодательства.

Следует отметить, что не все специалисты поддерживают предложение о разделении ст. 272 УК РФ на несколько самостоятельных составов. По мнению Е. В. Красненковой, диспозицией ст. 272 УК РФ охватываются и изменение (модификация), и стирание, и подавление компьютерных данных (информации) или программ, и несанкционированный доступ к компьютерной информации, поэтому введение в УК РФ новых составов преступлений является нецелесообразным. Это будет способствовать тому, что в УК РФ появится довольно значительное количество статей, содержащих однотипные составы преступлений, которые в практической деятельности специалисту довольно сложно применять. Тезис исследователя о том, что ст. 272 УК РФ уже объединяет в себе несколько составов и поэтому не нуждается в изменениях, несостоятелен.

На основе многолетнего опыта борьбы с компьютерными преступлениями за рубежом пришли к выводу о необходимости формулировки самостоятельных составов доступа и саботажа, где практические работники не испытывают каких-либо проблем. Проблема, скорее, будет лежать в плоскости достаточной профессиональной квалификации правоприменителей, а не в особой сложности формулировок УК РФ.

Это свидетельствует о стремлении зарубежных стран, во-первых, унифицировать свое законодательство о компьютерных преступлениях, а, во-вторых, в равной мере защитить компьютерные системы от доступа к ним и вмешательства в хранящиеся там данные, в работу системы.

На данный недостаток обращают внимание также другие российские исследователи. В частности, С. Д. Бражник отмечает, что российский законодатель в 1996 г. ввел в УК РФ минимальное количество статьей о преступлениях в сфере компьютерной информации вопреки правилу, согласно которому одна статья УК должна быть посвящена одному составу. При этом была сделана попытка объединить различные по своему характеру деяния в одну статью. Возможно, подобное объединение было оправданным на первом этапе при небольшом количестве и разнообразии преступлений данного вида, но в настоящее время требуется расширение круга уголовно-наказуемых деяний главы 28 УК РФ.

Последствием принятого законодателем подхода в криминализации рассматриваемого деяния может быть следующее: если информация была скопирована, то все признаки состава преступления есть, а если она была просто прочитана – то нет. Как справедливо отмечает Т. Л. Тропина, чтение информации не менее опасно, чем ее копирование. В некоторых случаях злоумышленнику достаточно увидеть и прочитать информацию, и она теряет свою ценность или может быть применена им в дальнейшем безо всякого копирования. Кроме того, существуют иные способы сохранения данных для дальнейшего использования, например, фотографирование экрана компьютера. Данное утверждение Т. Л. Тропиной с позиции теории информации представляется не совсем корректным, поскольку фотографирование также должно являться частным случаем копирования информации в рамках ст. 272 УК РФ, поскольку осуществляется с использованием технических средств. А. М. Доронин в связи с этим предлагает свою редакцию ст. 272 УК РФ, которая в числе прочих негативных последствий неправомерного доступа включает визуальное ознакомление с информацией. Однако данное предложение, хотя и повышает эффективность рассматриваемой нормы, все же является недостаточным.

А. Е. Шарков также обоснованно полагает, что достаточным для криминализации является совершение самого незаконного доступа к специально охраняемой законом компьютерной информации. В связи с этим им предлагается исключить из диспозиции ч. 1 ст. 272 УК РФ указание на необходимость наступления последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ или их сети. Перечисленные последствия, по мнению ученого, должны влечь более строгую ответственность и могут быть сформулированы в качестве отягчающих обстоятельств. Следует отметить, что по подобной схеме построена ст. 138а УК Голландии, ч. 1 которой предусматривает уголовную ответственность за незаконный доступ, а ч. 2 – за незаконный доступ, если впоследствии информация была скопирована или записана. Однако последствия незаконного доступа в виде уничтожения, блокирования и модификации не включены голландским законодателем в ч. 2 ст. 138а. Думается, связано это с тем, что за рубежом юристы проводят более четкую грань между незаконным доступом и вмешательством в данные. С позиции теории информации такой подход представляется более эффективным, чем «наслоение» на основной состав в качестве квалифицирующего признака другого самостоятельного состава. Вместе с тем в тексте диспозиции ч. 1 ст. 272 УК РФ представляется необходимым оставить указание на копирование информации или совершение другого преступления как последствия незаконного доступа, убрав уничтожение, блокирование или модификацию информации. Без копирования информации или совершения иного преступления сам факт незаконного доступа в нынешних российских условиях не обладает большой общественной опасностью. Кроме того, на практике незаконный доступ осуществляется, как правило, с целью получения какой-либо информации или совершения с его помощью иного преступления. Так, в 2005 г. Красноярский краевой суд вынес обвинительный приговор в отношении А. и Б., которые совершили неправомерный доступ к охраняемой законом компьютерной информации информационных центров УВД г. Красноярска и ГУВД Красноярского края, повлекший копирование информации. В 2002 г. Сосновоборский городской суд Красноярского края вынес приговор по упомянутому выше в работе уголовному делу в отношении А., который, осознавая, что логин и пароль являются незаконно полученными, предвидя возможность наступления общественно опасных последствий в виде блокирования работы ЭВМ законного пользователя, а также причинения материального ущерба, имея безразличное отношение к наступлению последних, неоднократно осуществил без оплаты от себя лично выход в Интернет, при этом блокируя работу ЭВМ медицинского училища.

В последнем случае мы имеем дело с незаконным доступом к компьютерной информации, повлекшим наступление двух последствий. Как признаются сотрудники отдела «К», они не могут дать точного определения термину «блокирование информации». На практике данное понятие было истолковано как создание препятствий законному пользователю воспользоваться своим правом на распоряжение информацией применительно к случаям, аналогичным вышеизложенному. Представляется, что отсутствие правовой квалификации данного явления и изъятие из текста УК РФ термина «блокирование информации» не помешает квалифицировать незаконный доступ как преступление, если последствием его будет копирование информации или совершение иного преступления. Отсутствие в уголовном законе рассматриваемого термина позволит сделать УК РФ в этой части более понятным, лаконичным и соответствующим международно-правовым тенденциям борьбы с компьютерными преступлениями.

Таким образом, информация представлена прежде всего в объекте составов преступлений информационного характера, который является дополнительным и может быть определен как общественные отношения по обеспечению информационной безопасности. Информация также может являться предметом преступлений, а указание на информационное воздействие содержаться в описании объективной стороны составов преступлений.

Уголовное законодательство содержит большой массив преступлений информационного характера. Следует отметить, что число таких преступлений, по сравнению с УК РСФСР 1960 г., выросло примерно в 1,5 раза. Преступления информационного характера могут быть классифицированы по различным основаниям.

Общим моментом, объединяющим все преступления информационного характера, является использование в конструкции составов таких преступлений терминов, обозначающих различные информационные явления. Указанные термины должны употребляться, во-первых, корректно с точки зрения теории информации, во-вторых, единообразно во всем тексте уголовного закона. Нарушение этих требований будет означать несоблюдение таких принципов криминализации, как беспробельность закона и неизбыточность запрета, а также определенность и единство терминологии. На примере анализа состава преступления, предусмотренного ст. 183 УК РФ, показано, что законодатель не всегда учитывает названные принципы криминализации применительно к формулированию составов преступлений.

§ 3. Система противодействия преступлениям, совершенным с использованием информационно-коммуникационных технологий и в сфере компьютерной информации

Угрозы информационной безопасности и методы их реализации

Под угрозой вообще обычно понимают возможную опасность. В дальнейшем изложении *угрозой информационной безопасности АС* (автоматизированной системы) будем называть возможность воздействия на обрабатываемую в АС информацию, приводящего к ее модификации, уничтожению, копированию, блокированию, а также на компоненты АС, приводящего к утрате, уничтожению или сбою технических устройств и носителей информации.

Определение возможных угроз информационной безопасности приводится с целью задания полного перечня требований к разрабатываемой системе защиты АС. Эффективный анализ угроз возможен на основе их классификации по ряду признаков. При этом каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Как следствие, для защищаемой системы определяют не полный перечень угроз, а перечень классов угроз.

Классификация возможных угроз информационной безопасности АС может быть проведена по ряду базовых признаков.

1. По природе возникновения:

– естественные угрозы – угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, не зависящих от человека;

– искусственные угрозы – угрозы, вызванные деятельностью человека.

2. По степени преднамеренности проявления:

– угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала. Например: проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных, и т. п.); неправомерное включение оборудования или изменение режимов работы устройств и программ; неумышленная порча носителей информации; пересылка данных по ошибочному адресу

абонента (устройства); ввод ошибочных данных; неумышленное повреждение каналов связи;

– угрозы преднамеренного действия (например, угрозы действий злоумышленника для хищения информации).

3. По непосредственному источнику угроз:

– угрозы, источником которых является человек. Например: внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность); вербовка (путем подкупа, шантажа и т. п.) персонала или отдельных пользователей, имеющих определенные полномочия; угроза несанкционированного копирования секретных данных пользователем АС; разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. п.);

– угрозы, источником которых являются санкционированные программно-аппаратные средства. Например: запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т. п.); возникновение отказа в работе операционной системы;

– угрозы, источником которых являются несанкционированные программно-аппаратные средства. Например: нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях), заражение компьютера вирусами с деструктивными функциями;

– угрозы, непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение и т. п.).

4. По положению источника угроз:

– угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС. Например: перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т. п.); перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоко-

лов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему; дистанционная фото- и видеосъемка;

– угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС. Например: хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.); отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т. д.); применение подслушивающих устройств;

– угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам);

– угрозы, источник которых расположен в АС. Например: проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации; некорректное использование ресурсов АС.

5. По степени зависимости от активности АС:

– угрозы, которые могут проявляться независимо от активности АС. Например: вскрытие шифров криптозащиты информации; хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем);

– угрозы, которые могут проявляться только в процессе автоматизированной обработки данных (например, угрозы выполнения и распространения программных вирусов, снятие передаваемых данных).

6. По степени воздействия на АС:

– пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС (например, угроза копирования секретных данных);

– активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС. Например: внедрение аппаратных вложений, программных «закладок» и «вирусов», т. е. таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы; действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т. п.); угроза умышленной модификации информации.

7. По этапам доступа пользователей или программ к ресурсам АС:

– угрозы на этапе запрета доступа к ресурсам АС;

– угрозы при разрешенном доступе к ресурсам АС.

8. По способу доступа к ресурсам АС:

– угрозы с использованием прямого стандартного пути доступа к ресурсам АС. Например: незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы и т. д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»); несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т. п.;

– угрозы скрытого нестандартного пути доступа к ресурсам АС. Например: вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т. п.); угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС.

9. По месту расположения информации в АС:

– угрозы доступа к информации на внешних запоминающих устройствах (например, угроза несанкционированного копирования секретной информации с жесткого диска);

– угрозы доступа к информации в оперативной памяти. Например: чтение остаточной информации из оперативной памяти; чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных АС и систем программирования; угроза доступа к системной области оперативной памяти со стороны прикладных программ;

– угрозы доступа к информации, циркулирующей в линиях связи. Например: незаконное подключение к линиям связи с целью работы «между строк» с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений; незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных

сообщений; перехват всего потока данных с целью дальнейшего анализа не в реальном масштабе времени;

– угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере (например, угроза записи отображаемой информации на скрытую видеокамеру).

Вне зависимости от конкретных видов угроз АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие свойства информации и систем ее обработки:

1. *Конфиденциальность информации* – субъективно определяемая (приписываемая) характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы и среды сохранять указанную информацию в тайне от субъектов, не имеющих полномочий доступа к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты их законных интересов от других субъектов информационных отношений.

2. *Целостность информации* – существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию или каким-либо требованиям). Субъектов интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т. е. ее неискаженности.

3. *Доступность информации* – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Таким образом, в соответствии с существующими подходами принято считать, что информационная безопасность АС обеспечена в случае, если для любых информационных ресурсов в системе поддерживается определенный уровень конфиденциальности (невозможности несанкционированного получения какой-либо информации), целостности (невозможности несанкционированной или случайной ее модификации) и доступности (возможности за разумное время получить требуемую информацию).

Соответственно, для АС можно рассматривать три основных вида угроз:

1. Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой.

2. Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, это означает, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

3. Угроза отказа служб возникает, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Описанные выше угрозы были сформулированы в 60-х гг. для открытых *UNIX*-подобных систем, где не предпринимались меры по защите информации. На современном этапе информационных технологий подсистемы или функции защиты являются неотъемлемой частью комплексов по обработке информации. Информация не представляется «в чистом виде», на пути к ней имеется хотя бы какая-нибудь система защиты: чтобы угрожать нарушением конфиденциальности, атакующая сторона должна преодолеть эту систему. Однако не существует абсолютной системы защиты, вопрос лишь во времени и средствах, требующихся на ее преодоление.

К основным направлениям (методам) реализации злоумышленником информационных угроз относятся:

– непосредственное обращение к объектам доступа;

– создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

– модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;

– внедрение в технические средства АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС.

К числу основных методов реализации угроз информационной безопасности АС относятся:

– определение злоумышленником типа и параметров носителей информации;

– получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;

– получение злоумышленником детальной информации о функциях, выполняемых АС;

– получение злоумышленником данных о применяемых системах защиты;

– определение способа представления информации;

– определение злоумышленником содержания данных, обрабатываемых в АС, на качественном уровне (применяется для мониторинга АС и для дешифрования сообщений);

– хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные;

– использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН) – конфиденциальные данные перехватываются злоумышленником путем выделения информативных сигналов из электромагнитного излучения и наводок по цепям питания средств вычислительной техники, входящей в АС;

– уничтожение средств вычислительной техники и носителей информации;

– хищение (копирование) носителей информации;

– несанкционированный доступ пользователя к ресурсам АС в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;

– несанкционированное превышение пользователем своих полномочий;

– несанкционированное копирование программного обеспечения;

– перехват данных, передаваемых по каналам связи;

– визуальное наблюдение – конфиденциальные данные считываются с экранов терминалов, распечаток в процессе их печати и т. п.;

– раскрытие представления информации (дешифрование данных);

– уничтожение машинных носителей информации;

– внесение пользователем несанкционированных изменений в программно-аппаратные компоненты АС и обрабатываемые данные;

– установка и использование нештатного аппаратного и/или программного обеспечения;

– заражение программными вирусами;

– внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи;

– внедрение дезинформации;

– выведение из строя машинных носителей информации без уничтожения информации – выведение из строя электронных блоков накопителей на жестких дисках и т. п.;

– проявление ошибок проектирования и разработки аппаратных и программных компонентов АС;

– обход (отключение) механизмов защиты – загрузка злоумышленником нештатной операционной системы с дискеты, использование отладочных режимов программно-аппаратных компонент АС и т. п.;

– искажение соответствия синтаксических и семантических конструкций языка – установление новых значений слов, выражений и т. п.;

– запрет на использование информации – имеющаяся информация по каким-либо причинам не может быть использована.

Система противодействия

В ведущих странах мира сложилась система концептуальных взглядов на проблемы обеспечения информационной безопасности.

Концентрация больших объемов обобщенной и систематизированной информации в организациях (в том числе и в МВД) привела к увеличению возможности утечки секретных и конфиденциальных сведений и к мерам по безопасности информации. Тем не менее злоумышленные действия над информацией не уменьшаются, а имеют устойчивую тенденцию роста. Анализ практики показывает, что предпринимаемые действия не всегда носят системный характер, направлены на ликвидацию только отдельных угроз. Одной из причин такого положения дел является незнание или неумелое использование основных принципов и практических подходов к решению проблем информационной безопасности, незнание терминологического аппарата данной предметной области.

Раскрытие ключевых терминов предметной области – не самоцель, а формирование на этой основе начальных представлений о целях и задачах защиты информации.

Под информационной безопасностью понимается состояние защищенности информационной среды, при котором исключается возможность ознакомления с информацией (конфиденциальность), изменения или уничтожения (целостность) ее лицами, не имеющими на это права, а также сохраняется возможность ее использования (доступность).

Под защитой информации понимаются любые действия, направленные на обеспечение *конфиденциальности*, *целостности и доступности* информации.

Охраняемая зона объекта – ограниченная территория, имеющая обозначенный периметр, на которой принимаются меры по защите информации.

Рубежи защиты – созданные на объекте при помощи организационных и технических мер различные процедуры защиты информации.

Главным критерием в выборе средств защиты информации считают ее ценность (реальную или потенциальную).

Ценность информации определяется возможным ущербом от овладения информацией конкурентами, приносимым доходом, а также компенсацией возможных затрат на ее защиту. Для конкурентов же эта ценность должна компенсировать риск, связанный с ее получением (добыванием).

Для повышения эффективности защиты информации проводят анализ ее уязвимостей – характерных особенностей и недостатков в защите.

Целью защиты информации является сведение к минимуму потерь, вызванных нарушением целостности данных, их конфиденциальности или недоступности информации для потребителей.

Основными задачами системы информационной безопасности являются:

– своевременное выявление и устранение угроз безопасности ресурсам, причин и условий, способствующих финансовому, материальному и моральному ущербу;

– создание механизма и условий оперативного реагирования на угрозы безопасности;

– эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;

– создание условий для минимизации и локализации возможного ущерба, ослабления негативного влияния последствий.

Мероприятия по защите информации должны исключать:

– выход электромагнитного и акустического полей, наводок в сетях питания, кабельных линиях, заземлении, радио- и телефонных сетях за пределы контролируемой зоны;

– доступ в помещение, где осуществляется обработка информации, а также визуальные возможности получения информации;

– работу специальных устройств ведения разведки, которые могут находиться в строительных конструкциях помещений и предметах их интерьера, а также внутри самого помещения или непосредственно в средствах обработки и передачи информации;

– перехват информации из каналов передачи данных;

– несанкционированный доступ к информационным ресурсам;

– воздействие излучений, приводящих к разрушению информации.

Приведенная совокупность определений достаточна для формирования общего, пока еще абстрактного взгляда на построение системы информационной безопасности. Для формирования более детального представления необходимо знание основных принципов организации системы информационной безопасности.

Первым и наиболее важным является принцип непрерывного совершенствования системы информационной безопасности. Суть этого принципа заключается в постоянном выявлении слабых мест системы, которые возникают от изменения характера внутренних и внешних угроз.

Вторым является принцип комплексного использования всех доступных средств защиты во всех структурных элементах организации и на всех этапах работы с информацией. Комплексный характер защиты информации проистекает прежде всего из того, что злоумышленники всегда ищут самое слабое звено в системе безопасности.

Важными условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и организации, профессионализм представителей службы безопасности, подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами.

С позиций системного подхода для реализации приведенных принципов процесс да и сама система защиты информации должны отвечать некоторой совокупности требований. Защита информации должна быть:

– централизованной;

– плановой;

– конкретной и целенаправленной;

– активной;

– надежной и универсальной;

– нестандартной (по сравнению с другими организациями), разнообразной по используемым средствам;

– открытой для изменения и дополнения;

– экономически эффективной: затраты на систему защиты не должны превышать размеры возможного ущерба.

Наряду с основными требованиями, существует ряд устоявшихся рекомендаций, которые будут не бесполезны создателям систем информационной безопасности:

– средства защиты должны быть просты для технического обслуживания и «прозрачны» для пользователей;

– каждый пользователь должен иметь минимальный набор привилегий, необходимых для работы;

– возможность отключения защиты в особых случаях, например, когда механизмы защиты реально мешают выполнению работ;

– независимость системы защиты от субъектов защиты;

– разработчики должны предполагать, что пользователи имеют наихудшие намерения (враждебность окружения), будут совершать серьезные ошибки и искать пути обхода механизмов защиты;

– отсутствие на предприятии излишней информации о существовании механизмов защиты.

Все перечисленные позиции должны лечь в основу формирования системы защиты информации.

При обеспечении информационной безопасности существует два аспекта:

– формальный, связанный с определением критериев, которым должны соответствовать защищаемые информационные технологии;

– практический, характеризующий порядок определения конкретного комплекса мер безопасности применительно к рассматриваемой информационной технологии.

Критерии, которым должны соответствовать защищаемые информационные технологии, являются объектом стандартизации. В настоящее время разработан проект международного стандарта «Общие критерии оценки безопасности информационных технологий». Содержание подобных документов в основном относится к этапу анализа рисков, на котором определяются угрозы безопасности и уязвимости информационных ресурсов, уточняются требования к режиму информационной безопасности.

Изложенные основные концептуальные положения являются основой механизма выработки детальных предложений по формированию политики и построению системы информационной безопасности.

Понятие политики безопасности

Политика безопасности – это формальные правила, по которым должны действовать лица, программы и технические устройства при действиях с информацией. Из практики известно, что правильная политика безопасности даже без выделенных средств защиты дает лучшие результаты, чем средства защиты без политики безопасности.

Политикой безопасности можно назвать и простые правила использования ресурсов (уровень руководителей), и описания всех соединений и их особенностей (уровень инженерно-технического состава). В данном учебном пособии рассмотрена только *зона ответственности руководителя* в формировании политики безопасности, прежде всего планирование защиты информационной системы. Именно участие руководителя, а не только технических специалистов, в разработке политики безопасности позволяет учесть целесообразное и выверенное с точки зрения конкретных функциональных обязанностей распределение информации.

Действия по управлению сложными организационно-техническими системами должны быть спланированы. Планирование информационной безопасности начинается после проведения анализа рисков и выбора средств защиты информации в соответствии с их ранжированием. Планирование – это процесс разработки пакета руководящих документов по реализации избранной политики информационной безопасности.

План защиты включает в себя две группы мероприятий – по построению (формированию) системы защиты и по использованию сформированной системы для защиты информации.

Цель планирования:

– координация деятельности соответствующих подразделений по обеспечению информационной безопасности;

– наилучшее использование всех выделенных ресурсов;

– предотвращение ошибочных действий, способных привести к снижению возможности достижения цели.

Различают два вида планирования: стратегическое или перспективное и тактическое или текущее (рис. 1).

Стратегическое планирование заключается в определении (без детальной проработки) средств и способов достижения конечных целей, в том числе необходимых ресурсов, последовательности и процедуры их использования.

Тактическое планирование заключается в определении промежуточных целей на пути достижения главных. При этом детально прорабатываются средства и способы решения задач, использования ресурсов, необходимые процедуры и технологии.

Рисунок 1. Виды планирования

Точную границу между стратегическим и тактическим планированием провести трудно. Обычно стратегическое планирование охватывает в несколько раз больший промежуток времени, чем тактическое; оно имеет гораздо более отдаленные последствия; шире влияет на функционирование управляемой системы в целом.

С тактическим планированием связано понятие оперативного управления. *Оперативное управление* обеспечивает функционирование системы в соответствии с намеченным планом и заключается в периодическом или непрерывном сравнении фактически полученных результатов с намеченными планами и последующей их корректировкой.

Отклонения системы от намеченных планов могут оказаться такими, что для эффективного достижения цели целесообразно произвести перепланирование либо такой исход должен быть предусмотрен на стадии планирования.

Планирование включает в себя определение, разработку или выбор:

– конечных и промежуточных целей и обоснование задач, решение которых необходимо для их достижения;

– требований к системе защиты информации;

– средств и способов, функциональной схемы защиты информации с учетом стоимости и привлечения других ресурсов;

– совокупности мероприятий защиты, проводимых в различные периоды времени;

– порядка ввода в действие средств защиты;

– ответственности персонала;

– порядка пересмотра плана и модернизации системы защиты;

– совокупности документов, регламентирующих деятельность по защите информации.

Задачи системы защиты объекта могут быть следующими:

– защита конфиденциальной информации от несанкционированного ознакомления и копирования;

– защита данных и программ от несанкционированной (случайной или умышленной) модификации;

– снижение потерь, вызванных разрушением данных и программ, в том числе и в результате воздействий вредоносных программ;

– предотвращение возможности совершения финансовых преступлений при помощи средств вычислительной техники.

Для создания эффективной системы защиты, как правило, необходимо выполнение следующих основных требований:

– комплексность мер защиты, закрытие всего спектра угроз и реализация всех целей стратегии защиты;

– надежность средств, входящих в систему защиты;

– бесконфликтная совместная работа с используемым на объекте программным обеспечением;

– простота эксплуатации и поддержка работы администратора безопасности;

– возможность встраивания средств защиты в программное обеспечение, используемое на объекте;

– приемлемая стоимость.

Политика информационной безопасности определяет облик системы защиты информации – совокупности правовых норм, организационных (правовых) мер, комплекса программно-технических средств и процедурных решений по рациональному использованию вычислительных и коммуникационных ресурсов, направленных на противодействие угрозам с целью исключения (предотвращения) или минимизации возможных последствий проявления информационных воздействий.

Политика безопасности должна гарантировать, что для каждого вида проблем существует ответственный исполнитель. В связи с этим ключевым элементом политики безопасности является доведение до каждого сотрудника его обязанностей по поддержанию режима безопасности.

Требование учета стоимостных ограничений находит отражение в спецификациях средств реализации плана защиты информации. В них определяются общие затраты на обеспечение информа-

ционной безопасности объекта согласно предъявляемым требованиям по защищенности.

Нужно уметь четко ответить на вопросы:

1. Сколько компьютеров (вспомогательного оборудования) установлено в организации? Сколько из них на рабочих местах, в ремонте, в резерве?
2. Можно ли узнать каждый компьютер «в лицо»?
3. Можно ли обнаружить «маскарад» оборудования, когда какой-нибудь компьютер, его часть или программное обеспечение подменены?
4. Какие задачи и с какой целью решаются на каждом компьютере?
5. Есть ли уверенность в необходимости каждой единицы контролируемого оборудования и в том, что среди него нет ничего лишнего, установленного, скажем, для красоты? Ведь если от оборудования нет пользы, с точки зрения безопасности от него можно ожидать только вреда.
6. Каков порядок ремонта и технической профилактики компьютеров?
7. Как проверяется оборудование, возвращаемое из ремонта, перед установкой на рабочее место?
8. Как производится изъятие и передача компьютеров в подразделения и каков порядок приема в работу нового оборудования?

Список вопросов можно продолжить. Аналогичные вопросы можно задать и относительно программного обеспечения и персонала.

Другими словами, защита информации начинается с постановки и решения организационных вопросов. Те, кому уже приходилось на практике заниматься вопросами обеспечения информационной безопасности в автоматизированных системах, отмечают следующую особенность – реальный интерес к проблеме защиты информации, проявляемый менеджерами верхнего уровня, на уровне подразделений, отвечающих за работоспособность автоматизированной системы, сменяется на резкое неприятие.

Как правило, приводятся следующие аргументы против проведения работ и принятия мер по обеспечению информационной безопасности:

– появление дополнительных ограничений для пользователей, затрудняющих использование и эксплуатацию автоматизированной системы организации;

– необходимость дополнительных материальных затрат как на проведение таких работ, так и на расширение штата специалистов, занимающихся проблемой информационной безопасности.

Экономия на информационной безопасности может выражаться в различных формах, крайними из которых являются:

– принятие только организационных мер обеспечения безопасности информации;

– использование только дополнительных технических средств защиты информации.

В первом случае, как правило, разрабатываются многочисленные инструкции, приказы и положения, призванные в критическую минуту переложить ответственность с людей, издающих эти документы, на конкретных исполнителей. Естественно, что требования таких документов (при отсутствии соответствующей технической поддержки) затрудняют повседневную деятельность сотрудников организации и, как правило, не выполняются.

Во втором случае – приобретаются и устанавливаются дополнительные технические средства. Их применение без соответствующей организационной поддержки только усиливает существующий беспорядок.

Рассмотрим комплекс организационных мер, необходимых для реализации защиты информации в компьютерных сетях. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил.

По времени проведения мероприятия, осуществляемые в целях защиты информации в компьютерных сетях, могут быть:

– разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений);

– периодически проводимые (через определенное время);

– проводимые при осуществлении или возникновении определенных условий или изменений в самой защищаемой системе или среде (по необходимости);

– постоянно (непрерывно или дискретно в случайные моменты времени) проводимые.

Разовые мероприятия:

– общесистемные мероприятия по созданию научно-технических и методологических основ защиты (концепции и других руководящих документов);

– мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объек-

тов (исключение тайного проникновения в помещения, установки аппаратуры и т. п.);

– мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и программных средств, документирование и т. п.);

– разработка и утверждение функциональных обязанностей должностных лиц службы компьютерной безопасности;

– внесение необходимых изменений и дополнений в организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, инструкции пользователей системы и т. п.) по вопросам обеспечения безопасности программно-информационных ресурсов и действиям в случае кризисных ситуаций;

– оформление юридических документов (в форме договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе, между участниками информационного обмена и третьей стороной (арбитражем, третейским судом) о правилах разрешения споров, связанных с применением электронной подписи;

– определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;

– разработка правил управления доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями организации с использованием компьютерных средств, а также используемых при их решении режимов доступа к данным; перечня файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну; выявление наиболее вероятных угроз для данной системы, уязвимых мест обработки информации и каналов доступа к ней; оценка возможного ущерба, вызванного нарушением безопасности информации);

– организация пропускного режима;

– определение порядка учета, выдачи, использования и хранения съемных носителей информации, содержащих эталонные и резервные копии программ, архивные данные и т. п.;

– организация учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;

– определение порядка проектирования, разработки, отладки, модификации, приобретения, исследования, приема в эксплуатацию, хранения и контроля целостности программных про-

дуктов, а также порядка обновления версий и установки новых системных и прикладных программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует и что при этом они должны делать);

– создание отделов (служб) компьютерной безопасности или, в случае небольших организаций и подразделений, назначение нештатных ответственных, осуществляющих единое руководство, организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы;

– определение перечня регулярно проводимых мероприятий и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса в критических ситуациях, возникающих из-за несанкционированного доступа, сбоев и отказов техники, ошибок в программах и действиях персонала, стихийных бедствий.

Периодически проводимые мероприятия:

– распределение и смена реквизитов разграничения доступа (паролей, ключей шифрования и т. п.);

– анализ системных журналов и принятие мер по обнаруженным нарушениям правил работы;

– мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации;

– периодически с привлечением сторонних специалистов осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты. На основе полученной в результате анализа информации принимать меры по совершенствованию системы защиты;

– мероприятия по пересмотру состава и построения системы защиты.

Мероприятия, проводимые по необходимости:

– мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;

– мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения;

– мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности, и т. д.).

Постоянно проводимые мероприятия:

– противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности техники и носителей информации и т. п.;

– явный и скрытый контроль за работой персонала системы;

– контроль за применением мер защиты.

Пересмотр Плана защиты рекомендуется производить раз в год. Кроме того, существует ряд случаев, требующих внеочередного пересмотра. К их числу относятся изменения следующих компонентов объекта:

1. Люди. Пересмотр может быть вызван кадровыми изменениями, связанными с реорганизацией организационно-штатной структуры объекта, увольнением служащих, имевших доступ к конфиденциальной информации, и т. д.

2. Техника. Пересмотр Плана защиты может быть вызван подключением других сетей, изменением или модификацией используемых средств вычислительной техники или программного обеспечения.

3. Помещения. Пересмотр Плана защиты может быть вызван изменением территориального расположения компонентов объекта.

Документы, регламентирующие деятельность по защите информации, оформляются в виде различных планов, положений, инструкций, наставлений и других аналогичных документов.

Официальную статистику, свидетельствующую о масштабах преступности в сфере использования информационно-телекоммуникационных технологий, получить на сегодняшний день достаточно сложно. Статистическая отчетность ГИАЦ МВД России (Отчет о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации, – «форма 1-ВТ») не отражает объективную картину ввиду фрагментарности содержащейся в ней информации (в форме, например, нет сведений о количестве зарегистрированных преступлений по ст. 159.3, 159.6, 187 УК РФ). Определенную роль в невозможности отражения реального положения дел сыграло также и отсутствие единообразия при квалификации рассматриваемых деяний с учетом их юридико-экономической природы. Однако, несмотря на объективные недостатки статистической формы, все же можно проследить динамику роста количества зарегистрированных и расследованных преступлений, совершенных в финансовой сфере с использованием информационно-телекоммуникационных технологий. Так, в 2010 г. было выявлено 1 819 случаев совершения мошенничества указанным способом, в 2011 г. – 2 049, 2012 г. – 2 748, 2013 г. – 2 196, 2014 г. – 2 187,

2015 г. – 13 483. При этом в 2014 г. расследовано и направлено в суд только 457 уголовных дел, 1 396 приостановлено за неустановлением лица, совершившего преступление, а в 2015 г. направлено в суд только 1 352 уголовных дела, приостановлено – 9 488. Аналогичная картина наблюдается и с кражей, совершенной с использованием информационно-телекоммуникационных технологий: только каждое 5 преступление расследуется и передается в суд.

Различные коммерческие организации, занимающиеся мониторингом преступности в сфере информационно-телекоммуникационных технологий, наряду с правоохранительными органами и кредитными организациями, предоставляют достаточно разрозненную информацию. Кроме того, в поле зрения официальной статистики попадают лишь сведения о происшествиях, которые в той или иной форме были выявлены и квалифицированы как преступления по существующим на сегодняшний день составам либо как посягательства в сфере компьютерной информации, либо в совокупности с предикатными составами (ст. 158, 159 УК РФ и др.).

По данным Бюро специальных технических мероприятий МВД России, число киберпреступлений в России в 2014 г. увеличилось на 8,6% и составило более 11 тыс. В качественном соотношении киберпреступность выглядит следующим образом: 37% из числа всех совершенных за этот период компьютерных преступлений приходится на мошенничество, 19% – на неправомерный доступ к информации с целью хищения денежных средств, 16% – на распространение детской порнографии и по 8% – на нарушение авторских и смежных прав и распространение вредоносных программ.

Современная криминальная ситуация в сфере телекоммуникаций и компьютерной информации

Понятие «преступления с использованием компьютерных технологий» неразрывно связано с понятием лица, которое его совершает. Изучая личность компьютерного преступника, следует обратить внимание на черты и особенности, присущие именно лицам, использующим высокие технологии при совершении преступлений. Такая специфика касается мировоззрения и особенностей взаимодействия членов преступной среды и накладывает отпечаток на способы и виды совершения лицом противоправных деяний. Трактовка данного понятия неразрывно связана со смыслом, который исследователь в него вкладывает. В связи с этим возможно рассмотрение компьютерного преступника в широком и узком смысле.

Компьютерный преступник в узком смысле – это человек, совершивший хотя бы одно из перечисленных в Уголовном кодексе

преступлений в сфере компьютерной информации. Данное определение существенно ограничивает круг лиц, являющихся компьютерными преступниками. При этом личностные характеристики будут зависеть от того, какое именно противоправное деяние лицо совершило.

Первой в главе 28 УК РФ законодатель установил ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Неправомерный доступ представляет собой приобретение возможности получить компьютерную информацию без разрешения ее владельца.

Совершающий данное деяние преступник практически всегда технически подготовлен и обладает определенным набором программно-аппаратных методов и навыков, позволяющих облегчить совершение преступления. Чаще всего это лицо, имеющее техническое образование. Преступник имеет беспрепятственный доступ к компьютерам и Интернету. В то же время современное развитие информационной сферы привело к тому, что преступнику не обязательно обладать глубокими познаниями компьютерных технологий. Иногда достаточно общих навыков работы с компьютером, подкрепленных подробными инструкциями осуществления доступа, которые можно найти в сети Интернет, и несоблюдением требований безопасности со стороны жертвы.

Границы возраста злоумышленника – от 18 до 45 лет. При этом, как указывает А. И. Долгова, в 1997–1998 гг. преступления в основном совершались лицами старшего возраста. Так, из 20 выявленных преступников 10 совершили преступление в возрасте от 30 до 49 лет, 6 – в возрасте от 25 до 29 лет, 4 выявленных лица совершили преступление в возрасте от 18 до 24 лет. С 1999 г. преступления стали совершаться лицами молодого возраста. В настоящее время соотношение преступников, совершающих неправомерный доступ к охраняемой законом компьютерной информации, распределяется следующим образом:

1. Лица, получившие необходимые для совершения преступлений знания и навыки на начальных этапах компьютеризации общества, составляют 8,9 %.

2. Доля лиц, овладевших опытом противоправной деятельности с появлением первых персональных компьютеров, составляет 30,2 %.

3. Лица, получившие преступные навыки в настоящее время, – 60,9 %.

С учетом изложенного можно произвести классификацию преступников по степени вовлеченности в противоправную деятельность, совершающих предусмотренное ст. 272 УК РФ деяние:

1. «Начинающие». Возраст колеблется от 18 до 30 лет. Преобладают лица мужского пола. Образование – техническое: среднее, среднее специальное или высшее (иногда неоконченное). Лица имеют средний достаток, позволяющий им владеть одним или более компьютерными устройствами. Обладают существенными познаниями в области компьютерных технологий, включая языки программирования, а также программно-аппаратных частей компьютерных устройств. Вместе с тем эти лица не имеют постоянной работы либо их работа связана с компьютерными технологиями (специалисты компьютерных фирм, администраторы баз данных и т. д.). Их личность характеризует увлечение компьютерными технологиями. Противоправную деятельность они, как правило, начинают еще не отдавая себе отчет в том, что их действия являются преступными. Установка на целенаправленное преступное поведение возникает внезапно – в основном под влиянием последовательности удачных взломов средств защиты лицензионных программных продуктов на собственном и принадлежащих другим лицам компьютерных устройствах. Часто их деятельность дополнительно связана с выкладыванием в открытый доступ и незаконным распространением взломанных программных продуктов.

2. «Устойчивые». Средний возраст данной категории преступников составляет 20–25 лет. Сужение возрастной группы объясняется исключением «начинающих», совершивших несколько эпизодов противоправной деятельности и не заинтересовавшихся в дальнейшем.

Преобладает мужской пол, но наблюдается тенденция к проявлению активности женщин: их доля в настоящее время составляет около 5 %.

Преступники данной категории имеют преимущественно высшее либо незаконченное высшее техническое образование. Обладают средним и выше среднего достатком. Могут себе позволить современные компьютерные устройства, а также дополнительные специальные технические приспособления. Владеют глубокими и системными знаниями в сфере компьютерных технологий, языков программирования, а также программно-аппаратной части компьютерных систем. При совершении преступления осмысленно используют комплексы заранее подготовленных программно-аппаратных инструментов, разработанные самостоятельно или найденные в сети Интернет.

Психологический портрет устойчивого компьютерного преступника представляет лицо уравновешенное, со сформи-

ровавшейся системой взглядов и ценностей, но не обладающее высокими амбициями. Устойчивые компьютерные преступники в большинстве случаев имеют постоянную работу в областях, связанных с компьютерными технологиями. Это помогает им в некоторых случаях беспрепятственно получить доступ к компьютеру жертвы и находящейся в нем информации. Могут оставлять в программном обеспечении компьютерных устройств специальные вредоносные программы для возможности использования полученной уязвимости в преступных целях. Преступная установка либо формируется из начинающего типа, либо сразу образуется при целенаправленном внедрении в криминальную среду, содействии и поддержке профессиональных преступников. Основные направления противоправной деятельности – взлом посредством сети Интернет и отдельные действия по получению защищенной информации.

3. «Профессиональные». Преступники данного вида принадлежат к старшей возрастной категории. Их возраст составляет более 25 лет. Доля женщин составляет около 8 %, что еще больше чем в среде «устойчивых» преступников. Происходят из семей выше среднего достатка. Профессиональные компьютерные преступники имеют высшее техническое образование и на высоком уровне обладают знаниями в области компьютеров и компьютерных технологий. Многие из профессиональных компьютерных преступников получают второе высшее образование преимущественно по юридическим или экономическим специальностям. Лица, относящиеся к данной группе, обладают навыками программирования на нескольких языках, глубокими знаниями в области программных средств и устройства аппаратной части компьютерных систем (как персональных компьютеров, так и профессиональных программно-аппаратных комплексов), профессионально работают с различными компьютерными платформами, основными операционными системами и большинством пакетов специализированного программного обеспечения (офисное, пакеты разработки приложений, сетевое программное обеспечение), в совершенстве владеют информацией об основных системах электронных коммуникаций (сотовой связи, сетевых протоколах, методов защиты информации, защищенной связи) и используют эти знания в противоправной деятельности.

Данный тип личности характеризуется устоявшимися взглядами и системой ценностей, а также стойкостью к внешним воздействиям. Это личности довольно амбициозные, но при

этом четко знающие цену своим навыкам. Формирование мотивации преступного поведения происходит обычно на стадии изучения компьютерных технологий и первоначально подкрепляется в основном желанием продемонстрировать свое интеллектуальное превосходство нежели стремлением извлечь прибыль. Часто имеют связи в государственных структурах, которые используют при необходимости. Имеют легальную работу, чаще всего для создания алиби, обычно в отделах информационных технологий в крупных организациях: банках, зарубежных компаниях и государственных органах. При этом основным способом заработка является деятельность в полулегальной и криминальной среде. Постоянно совершенствуются в области методик и средств противоправной деятельности, которые часто разрабатывают сами.

В качестве вывода о преступниках, совершающих предусмотренное ст. 272 УК РФ деяние, можно сказать, что их основная черта – глубокие познания в области компьютерных технологий. Их мотивацией является стремление доказать свое интеллектуальное превосходство.

Криминологическая характеристика преступников, совершающих деяния, попадающие под действие ст. 273 УК РФ, – отсутствие деления на новичков и профессионалов.

Состав предусмотренного ст. 273 УК РФ преступления закрепляет ответственность за создание, распространение и использование вредоносных компьютерных программ. Таким образом, признаки личности преступника ограничиваются самой сутью компьютерной программы. Это программный код, представляющий из себя набор команд, которые выполняются на компьютерном устройстве и результатом которых являются какие-либо вредные для устройства или пользователя этого устройства последствия. А так как это программный код, следовательно, для его написания злоумышленнику необходимо обладать знаниями какого-либо языка программирования и опытом написания компьютерных программ. Из этого можно сделать вывод, что создатель вредоносной компьютерной программы – это квалифицированный компьютерный специалист. При этом в большинстве случаев создатель программы является также и ее распространителем. Как показывает статистика, возраст такого преступника от 23 лет, пол преимущественно мужской. В основном это квалифицированный программист. Часто он также совершает деяния, которые могли бы быть квалифицированы по ст. 272 УК РФ. Он принадлежит ко второй или тре-

тьей группе злоумышленников по ст. 272 УК РФ со всеми присущими им личностными характеристиками.

Объектом охраны, объединяющим преступления, совершенные по экстремистским мотивам, являются общественные отношения в сфере конституционно закрепленного равенства людей независимо от политических, идеологических, расовых, национальных, религиозных или социальных интересов, т. е. общественные отношения в сфере обеспечения основ конституционного строя Российской Федерации.

Данное обстоятельство порождает вопрос о возможности объединения всех преступлений, совершаемых по мотиву политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, в рамках самостоятельного единого видового объекта уголовно-правовой охраны.

Видовым объектом данных посягательств следует считать интересы государственной власти, основы конституционного строя и безопасности государства, поскольку общественное благо обладает большей социальной ценностью, чем личное.

Основным непосредственным объектом посягательств экстремистской направленности следует считать общественные отношения в сфере противодействия экстремизму в Российской Федерации, обеспечения политического, идеологического, расового, национального, социального или религиозного равноправия, стабильность в обществе.

Дополнительным объектом данных преступлений следует считать общественные отношения в сфере охраны жизни, здоровья, имущества, общественного порядка или общественной нравственности.

Проанализировав объективную сторону преступлений экстремистской направленности, можно сделать следующие выводы:

– преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, весьма разнообразны с точки зрении анализа их объективной стороны, в составах этих преступлений используются примерно аналогичная терминология;

– действия известного рода преступлений носят как физический, так и информационный характер, при этом физические действия совершаются, как правило, с особой жестокостью, а информационные характеризуются разнородностью и совершаются публично

или с использованием средств массовой информации. К особенностям преступлений данного вида следует отнести также то, что совершаться они могут не в одном, а в нескольких разных местах. Признаки данного состава преступления могут проявляться: на митингах и собраниях, во время шествий, при продаже или бесплатном распространении литературных и иных печатных произведений в киосках, с лотков, в транспорте.

Общественно опасные последствия законодатель предусмотрел только за преступления, совершаемые с помощью физических действий. Для информационных действий в рамках совершения преступлений по мотиву политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы законодатель последствия не предусмотрел.

Таким образом, конструкции составов преступлений экстремистской направленности могут быть как материальными, так и формальными, что также вызывает некоторые вопросы об однородности группы преступлений экстремистской направленности.

Проанализировав значение предмета преступления, а также потерпевшего в рамках состава преступления как обязательных составляющих объекта преступлений, можно заключить, что преступления экстремистской направленности можно объединить по признакам единства потерпевших, на которых направлено посягательство, – представителей той или иной политической, идеологической, расовой, национальной, религиозной или социальной группы.

При помощи признаков, характеризующих потерпевшего и предмет преступления, в диспозициях норм Особенной части УК РФ может указываться объект уголовно-правовой охраны. Причем признаки предмета преступления и потерпевшего могут определять не только непосредственный, но и видовой объект.

Данное обстоятельство подтверждает систематизация в рамках уголовного закона преступлений против несовершеннолетних, против собственности (хищения), экологических преступлений, преступлений против безопасности движения и эксплуатации транспорта, преступлений в сфере компьютерной информации и др.

Таким образом, предмет преступления (потерпевший) непосредственно связан с объектом – общественными отношениями, в которых он проявляется и защищается в рамках уголовного закона. Предмет (потерпевший) и объект преступления взаимосвязаны и взаимообусловлены, предопределяют друг друга. Предмет пре-

ступления (потерпевший) является частью общественных отношений. А общественные отношения в большинстве своем не могут существовать без предмета преступления (потерпевшего).

Таким образом, мы видим прямую зависимость формирования объекта уголовно-правовой охраны от предмета преступления или потерпевшего.

Однако объект преступления (в том числе преступлений экстремистской направленности) определяется не объективно, т. е. не от фактически причиненного вреда потерпевшему, а от сферы общественных отношений, в определении которой преимущественно играет главенствующую роль потерпевший как участник данных общественных отношений.

В преступлениях экстремистской направленности также признаки потерпевшего определяются не характером причиняемого ему вреда, а отношением к какой-либо политической, идеологической, расовой, национальной, религиозной или социальной группе. Представителям данных социальных групп вред может причиняться как непосредственно, так и опосредованно путем ущемления конституционного равноправия.

Именно отношение к данным группам является конститутивным признаком в определении преступлений экстремистской направленности, что также может быть признаком, объединяющим данные преступления в рамках единого объекта уголовно-правовой охраны.

Потерпевшим как участником общественных отношений, формирующим объект уголовно-правовой охраны при совершении преступлений экстремистской направленности, могут быть как отдельные физические лица, так и политические, идеологические, расовые, национальные, религиозные либо социальные общности, группы, представители общества, которым непосредственно или опосредованно причиняется физический, моральный или материальный вред либо создается реальная угроза причинения такого вреда в связи с принадлежностью к данной общности или группе.

Именно такие социальные свойства потерпевшего, как обладание определенными национальными, религиозными, политическими, идеологическими, расовыми или социальными интересами и причинение вреда данным интересам, предопределяют объект уголовно-правовой охраны, сущность и содержание охраняемых уголовным правом общественных отношений в сфере защиты основ конституционного строя и безопасности государства, которые закреплены в ст. 13, 19 и 29 Конституции Российской Федерации.

Таким образом, определение системы общественных отношений в сфере защиты основ конституционного строя и безопасности государства по общим признакам потерпевших будет способствовать повышению эффективности защиты прав этих потерпевших.

Стратегия противодействия преступлениям, совершенным с использованием информационно-коммуникационных технологий и в сфере компьютерной информации, и система ее субъектов

Проблема противодействия преступлениям, совершаемым в сфере использования информационно-телекоммуникационных технологий, продолжает оставаться одной из наиболее злободневных.

В последнее время большая часть изменений в Уголовный кодекс носит блоковый характер: законодатель реформирует какую-то одну норму или несколько взаимосвязанных норм, но не согласует их со смежными нормами, что нарушает принцип системности закона и его внутреннюю цельность. Законодательные изменения бессистемны и не соответствуют социально-экономической действительности государства. В научном мире разразилась бурная полемика по поводу целесообразности отнесения деяния, предусмотренного ст. 159.6 УК РФ, к мошенничеству. Так, В. В. Хилюта, И. А. Клепицкий отмечают сомнительность наличия такого неотъемлемого признака мошенничества как «обман». Обман возможен только в отношении физического лица, которое вследствие введения его в заблуждение передает добровольно свое имущество преступнику.

В свою очередь, мы считаем, что мошенничество в сфере компьютерной информации относится к новому виду хищений, когда завладение имуществом или приобретение права на имущество сопряжено с проникновением в информационную среду, в которой осуществляются различного рода информационные операции, юридическое значение и последствия которых состоит в приобретении участниками оборота имущества в виде наличных денег, безналичных денежных средств, иных имущественных прав. Следует подчеркнуть, что наличие таких неотъемлемых признаков «традиционного мошенничества», как обман или злоупотребление доверием для деяний, квалифицируемых по ст. 159.6 УК РФ, не требуется.

Обращает на себя внимание непоследовательный подход законодателя и к криминализации деяний, совершаемых с использованием информационно-телекоммуникационных технологий. Исключением не стал и Федеральный закон от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»,

которым введена ответственность за специальные виды мошенничества, среди которых и преступления, совершаемые с использованием информационно-телекоммуникационных технологий, ст. 159.3 «Мошенничество с использованием платежных карт» и ст. 159.6 «Мошенничество в сфере компьютерной информации».

Инициатором изменений выступил Верховный Суд Российской Федерации. Позиция судебного органа объясняется тем, что конкретизация в УК РФ составов мошенничества, в зависимости от сферы правоотношений, в которой они совершаются, должна уменьшить число ошибок и злоупотреблений при возбуждении уголовных дел о мошенничестве, способствовать повышению качества работы по выявлению и расследованию таких преступлений.

Вместе с тем необходимо отметить, что анкетирование сотрудников правоприменительных органов свидетельствует не об уменьшении ошибок, а, наоборот, об их увеличении.

Отсутствие системности в действиях законодателя привело к тому, что ст. 159.6 УК РФ, являющаяся специальной по отношению к ст. 159 УК РФ, частично конкурирует по основному составу (ч. 1 ст. 159.6) с основными составами ч. 1 ст. 272 и ч. 1 ст. 273 УК РФ. Указанное обстоятельство вызвано тем, что перечень альтернативных действий по совершению мошенничества в сфере компьютерной информации гораздо шире перечня последствий, возможных при неправомерном доступе.

В заключение следует отметить, что наиболее совершенным в вопросе уголовно-правового противодействия посягательствам в указанной сфере является законодательство США. В нем криминализирован широкий спектр деяний, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий: мошенничество, совершаемое с использованием «электронных средств платежа, новых методов и услуг», а также создание, распространение и иные манипуляции с электронными средствами доступа, и преступления, связанные с «кражей личности». Конструкция юридических норм американского законодательства позволяет привлекать к ответственности за противоправные деяния в финансовой сфере с использованием новых, еще не получивших широкого распространения информационно-телекоммуникационных технологий.

В большинстве стран наблюдается тенденция по ужесточению ответственности за противоправные посягательства в IT-сфере и непрерывная реформация норм уголовного законодательства как реагирование на возникающие угрозы. Ужесточение ответственности за посягательства с использованием информационно-теле-

коммуникационных технологий, учитывая неограниченность круга потенциальных жертв от преступных действий и размеры причиняемого ущерба, должно быть реализовано и в отечественном законодательстве.

Интересным для имплементации в отечественное уголовное законодательство представляются реализованные в законодательстве Франции и Литвы нормы, предусматривающие ответственность лиц, принимающих поддельную платежную карту к оплате.

§ 4. Предупреждение преступлений, совершаемых с использованием информационно-коммуникационных технологий и в сфере компьютерной информации

Использование современных информационных технологий в промышленной, торговой, банковской, научной, культурной, образовательной и других сферах общественной жизни детерминировало динамический рост и качественное обновление компьютерной преступности в России, что создает новые угрозы для развития общества и государства. При этом обеспечение своевременности и эффективности предупредительной деятельности в сфере информационно-телекоммуникационных технологий представляет собой определенную проблему для органов внутренних дел, решение которой во многом зависит от комплексного подхода к разрешению организационных, правовых и методических аспектов специального предупреждения данного вида преступлений.

Развитие информационно-телекоммуникационных технологий позволяет совершать киберпреступления в большинстве случаев безнаказанно, поскольку уголовное законодательство слабо адаптировано к новым видам преступлений в сфере информационных технологий, хотя онлайн-торговля и банковские операции, услуги скоростной передачи данных, современные форматы связи, электронное образование, игровые и развлекательные порталы прочно вошли в жизнь общества и государства.

Повышение роли информационно-телекоммуникационных технологий отразилось и на современных тенденциях киберпреступности:

1. Нарастает, усиливается организованность, расширяются сферы криминальных интересов, усложняются применяемые преступные схемы.

2. Киберпреступления нередко совершаются в совокупности с иными общественно опасными деяниями и имеют факультативный характер. Это обусловлено тем, что, используя компьютерную информацию в качестве средства совершения преступления, пре-

ступники «превращают» ее в предмет другого общественно опасного деяния (хищение персональных данных с целью последующего вымогательства). Смещение корыстных интересов преступников в киберпространство произошло вследствие того, что данная криминальная деятельность сверхдоходна и относительно безопасна.

3. Наблюдается переход на транснациональный организованный уровень. Информационно-коммуникационные технологии на современном этапе превратились в удобное для многих преступников средство и орудие совершения любого рода преступлений. При этом постоянно расширяющиеся возможности глобальных сетей обусловили повышенный интерес к ним со стороны организованной преступности, в том числе экстремистских и террористических организаций, так как существующие правила эксплуатации киберпространства позволяют обеспечивать анонимность действий в сети и существенно осложняют идентификацию пользовательского оборудования.

По оценкам специалистов, свыше 80% киберпреступлений совершаются в той или иной организационных формах, включая формирование единого «теневого рынка» киберпреступности, основанного на постоянной разработке вредоносного программного обеспечения, заражения пользовательских компьютеров, управления бот-сетями, сбора данных личного и финансового характера, продажи похищенных данных. В связи с существованием указанного преступного сегмента подсчитать точное количество преступных кибердеяний, а тем более количество пострадавших от них, невозможно. Так, отметим, что пострадавшими лишь только от некоторых преступных деяний могу быть сотни или тысячи человек (ст. 273 УК РФ – создание, использование и распространение вредоносных компьютерных программ), что говорит об определенной условности представленной классификации.

В реальной действительности предупреждение преступлений представляет собой сложную систему, состоящую из отдельных элементов деятельности разнообразного характера, целью которой служит оказание воздействия на причины и условия, способствующие совершению преступлений, а также на лиц, их совершающих. Деятельность по предупреждению преступлений носит многоуровневый характер, поскольку, помимо масштабных, долговременных, перспективных мер, таких как постановка стратегических задач борьбы с преступностью, нормативного, организационного и ресурсного обеспечения, необходимым является разработка и принятие мер более узкого, конкретного характера, имеющих прикладное значение и рассчитанных на достижение менее крупных, но не менее значимых целей.

Предупреждение преступлений, совершаемых с использованием высоких технологий, является одним из приоритетных направлений деятельности органов внутренних дел.

В криминологии традиционно выделяют три уровня предупреждения: общесоциальный, специально-криминологический и индивидуальный.

Содержанием первого уровня предупреждения преступлений – общесоциального – являются меры, направленные прежде всего на решение комплексных социальных проблем, но оказывающие положительный эффект на процессы детерминации преступности. Их особенностями, в отличие от специально-криминологического и индивидуального уровня, является отсутствие непосредственной цели воздействия на криминогенные процессы в обществе, однако решение общесоциальных проблем оказывает косвенное воздействие и на условия (а в определенных случаях – и на причины) совершения конкретных видов преступлений. Применительно к системе предупреждения высокотехнологичной преступности можно выделить несколько направлений общесоциального воздействия.

В частности, к общеэкономическим предупредительным мерам следует отнести создание условий для экономического роста и повышения конкурентоспособности национальной экономики, условием достижения которых является развитие национальных инновационных систем, таких как цифровая экономика, ликвидация бюрократических барьеров и снижение уровня коррупции, повышение производительности труда и т. д.

Социальные меры предусматривают противодействие процессам социального и имущественного расслоения в обществе, устойчивую социальную политику, направленную на своевременное и качественное решение социальных вопросов; функционирование системы личной безопасности граждан, а также решение отдельных остросоциальных вопросов, таких как достойная оплата активной трудовой деятельности, наличие безопасных и высококачественных товаров и услуг и др.

Научно-технические меры общесоциального предупреждения преступлений включают формирование и государственную поддержку системы целевых фундаментальных и прикладных исследований как необходимого элемента научного обеспечения национальной безопасности государства; расширение сети научно-исследовательских и образовательных учреждений, обеспечивающих разработку научных исследований в сфере высоких технологий и подготовку соответствующих специалистов; разработку современ-

ных цифровых технологий и перспективных образцов наукоемкой продукции; модернизацию производственного цикла и др.

К общекультурным мерам можно отнести укрепление духовного единства многонационального народа Российской Федерации и повышение международного культурного имиджа России; повышение роли культуры для возрождения и сохранения культурно-нравственных ценностей, организацию патриотического и духовного воспитания граждан России.

Отдельно следует остановиться на законодательных мерах общесоциального предупреждения преступлений в сфере высоких технологий. К ним относятся: повышение качества принимаемых законов как на федеральном, так и региональном уровнях; устранение правовых коллизий, препятствующих деятельности правоприменителей в борьбе с преступностью; функционирование системы анализа применения действующего законодательства и своевременного реагирования на процессы, происходящие в обществе; создание механизма криминологической экспертизы законопроектов; координация законотворчества и правоприменения на международном уровне в рамках соответствия международным стандартам борьбы с преступностью, а также двусторонним и многосторонним межгосударственным соглашениям и договорам.

Так, согласно Доктрине информационной безопасности Российской Федерации среди национальных интересов Российской Федерации в информационной сфере отдельным пунктом выделена защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем как уже развернутых, так и создаваемых на территории России.

Утвержденная в 2017 г. Президентом Российской Федерации Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы к числу приоритетных задач относит обеспечение комплексной защиты информационной инфраструктуры Российской Федерации, в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и системы критической информационной инфраструктуры.

Одной из наиболее актуальных проблем совершенствования законодательного регулирования общественных отношений в сфере высоких технологий является закрепление статуса криптовалюты и сделок с ее использованием. Существующая в настоящее время нормативная неопределенность криптовалютных операций способствует совершению преступлений с их использованием.

Согласно ст. 27 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О центральном банке Российской Федерации» введение на территории Российской Федерации других денежных единиц и выпуск денежных суррогатов запрещаются. В письме от 27 января 2014 г. Банк России указал: «в связи с анонимным характером деятельности по выпуску «виртуальных валют» неограниченным кругом субъектов и по их использованию для совершения операций граждане и юридические лица могут быть, в том числе непреднамеренно, вовлечены в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма» и предостерег граждан и финансовые организации от использования Биткоин в качестве валюты или платежного средства. 4 сентября 2017 г. Банк России в новом письме уточнил, что криптовалюты не гарантируются и не обеспечиваются Центральным банком. Операции с криптовалютами несут в себе высокие риски при проведении обменных операций, в том числе из-за резких колебаний обменного курса.

Следует отметить, что Биткоин, как и любая иная криптовалюта, представляет собой реализацию перспективного направления для развития финансовой и экономической системы страны. Однако в современных условиях на фоне громоздкости и противоречивости действующей правотворческой системы вместо попыток создания механизма регулирования оборота криптовалюты мы наблюдаем уже привычную схему нагромождения запретительных мер, эффективность которых в сфере высоких технологий весьма условна. Пример безуспешных попыток блокирования мессенджера Telegram наглядное тому подтверждение.

Ввиду того что принцип функционирования криптовалют основан на системе распределенного реестра и сама система имеет наднациональный характер, любые действия в виде запрета со стороны одного государства вызовут значительные затруднения в реализации и не будут иметь должного эффекта. Для реализации законодательного запрета оборота криптовалюты как платежного средства необходимо объединение действия многих государств в рамках международного сотрудничества. Поводом для этого может явиться широкое использование криптовалют со стороны транснациональной преступности, в том числе в процессе легализации (отмывания) денежных средств.

С другой стороны, для государства значительно эффективнее было бы не отвергать перспективные технологии, а обеспечить создание необходимых условий для их внедрения в жизнь с учетом требований безопасности и эффективности. На сегодняшний день

проблемы анонимности лиц, пользующихся криптовалютами, а также децентрализованный характер используемой технологии Блокчейн, остаются основными препятствиями для легализации криптовалют. Разрешить данные противоречия возможно путем законодательного закрепления необходимости регистрации субъектов криптовалютного обмена, а также лицензирования деятельности юридических лиц, оказывающих услуги по финансовым операциям с криптовалютами.

Реализация мероприятий по предложенному направлению представляет собой процедуру предоставления необходимых прав на работу с криптовалютой по принципам личной регистрации и однократности предоставления идентификационного ключа на использование электронного кошелька. Для организаций, осуществляющих финансовые операции с криптовалютами, в качестве дополнительных условий целесообразно определить обязанности направлять сообщения о подозрительных операциях, осуществлять сбор и хранение информации о клиентах (на основе действующего законодательства о персональных данных), а также выполнять при необходимости посреднические функции при заключении сделок с платежом в виде криптовалюты, обеспечивающие равные права обеих сторон и возможность приостановки транзакции при нарушении условий сделки.

Меры специально-криминологического предупреждения

Криминологические меры предупреждения преступлений подразумевают деятельность, направленную непосредственно на причины и условия совершения преступлений.

В системе противодействия преступлениям, совершаемым с использованием высоких технологий, целесообразно сосредоточить внимание на разработке нижеперечисленных мер.

1. Повышение эффективности научного обеспечения деятельности по противодействию преступности в сфере высоких технологий.

В частности, анализ основных направлений научных исследований проблем высокотехнологичной преступности показывает, что вопросам информационной безопасности, защиты компьютерной информации, предупреждения компьютерной преступности в Российской Федерации уделяется пристальное внимание как стороны государства, так и со стороны научного сообщества. В то же время в научном сообществе преобладает точка зрения, что основной целью предупреждения данного вида преступлений является создание определенных условий использования информации, максимально ограничивающих возможности неправомерного

воздействия на нее. В то же время в качестве окончательной цели предупреждения рассматриваемых преступлений следует считать создание системы международных и государственных гарантий информационной безопасности, обеспечивающих должный уровень защищенности личности, общества и государства в сфере создания, передачи, хранения, обработки и использования информации, а также функционирования соответствующих электронных средств и информационно-телекоммуникационных систем.

Реализация предлагаемых целей и задач по предупреждению преступлений, совершаемых с использованием высоких технологий, предполагает разработку системы предупредительных мер на основе качественного научного анализа всех аспектов криминологического воздействия на причины и условия совершения данного вида преступлений. Однако в настоящее время у научного сообщества отсутствует единый подход к организации данной работы и содержанию профилактических мер, направленных как на преступность в сфере высоких технологий в целом, так и на отдельные ее проявления в частности.

Основным результатом научно-исследовательской работы должен являться адаптированный перенос ее результатов в правоприменительную практику. Координация усилий правоохранительных органов должна осуществляться уже на этапе сбора криминологической информации (начиная с этапа регистрации заявлений и сообщений о преступлениях) и в дальнейшем представлять собой единую информационную систему, позволяющую беспрепятственно обмениваться информацией, в том числе научными разработками и методиками, в процессе предупреждения, раскрытия и расследования высокотехнологичных преступлений.

2. Совершенствование системы правоприменения и разработка новых форм и методов борьбы с преступлениями, совершаемыми с использованием высоких технологий (методическое обеспечение).

Реализация мер по предупреждению высокотехнологичной преступности на данном направлении представляет собой совершенствование подзаконных актов и различного рода инструктивно-регламентирующей документации, которые в силу своей специфики способны оказать оперативное воздействие на ситуацию в случаях, когда законодательное решение проблемы затруднено в силу разных причин. Кроме того, качественное методическое обеспечение способствует эффективному применению законодательных норм в практической деятельности.

В силу разнородности нормативной базы (правоохранительных органов и иных государственных учреждений, общественных

организаций, коммерческих структур и т. п.) неизбежно возникают проблемы взаимодействия в процессе правоприменения, которые не позволяют эффективно противодействовать преступности. Несогласованность субъектов предупреждения преступлений в этой сфере зачастую предоставляет дополнительные возможности для преступных комбинаций.

В частности, целесообразно рассмотреть вопрос о законодательном закреплении обязанности производителей и продавцов компьютерной техники, средств связи и т. д. предустанавливать в свою продукцию системы антивирусной защиты в целях предотвращения несанкционированного доступа к компьютерной информации. С другой стороны, меры профилактики могут быть направлены не только на потенциального преступника, но и на органы (организации), представляющие интерес для злоумышленников в сфере информационно-телекоммуникационных технологий. В частности, такой мерой могла бы стать система страхования информационных рисков, которая предусматривает страхование средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования от неправомерного блокирования, уничтожения, модификации либо несанкционированного копирования электронной информации. При этом перед заключением страхового договора собственник (владелец) информационного ресурса либо информационно-телекоммуникационной сети и соответствующего оборудования обязан провести ряд установленных мер по защите информации и оборудования (установка сертифицированного программного обеспечения, антивирусная защита и т. д.). Данная мера направлена на уменьшение наносимого материального ущерба и снижение количества несанкционированных проникновений в компьютерные системы, происходящих по их вине.

К мерам предупреждения преступлений, совершаемых с использованием высоких технологий, также относится разработка новых методик противодействия данному виду преступлений, в том числе в процессе оперативно-розыскной деятельности. Так, представляется необходимым законодательно закрепить полномочия правоохранительных органов на осуществление мониторинга опубликованных в социальных сетях или иных ресурсах материалов противоправного характера, а в некоторых случаях обеспечить проведение соответствующих надзорных, оперативно-розыскных, следственных мероприятий с возможностью получения необходимой информации от провайдеров или Роскомнадзора напрямую без судебного разрешения.

3. Принятие организационно-управленческих мер предупреждения преступлений, совершаемых с использованием высоких технологий.

Данное направление характеризуется комплексом мер, направленных на совершенствование деятельности субъектов предупреждения данного вида преступлений. К ним следует отнести:

– создание системы подготовки сотрудников правоохранительных органов по специальностям «Защита информации и информационно-телекоммуникационных сетей», «Информационная безопасность» в образовательных учреждениях МВД, ФСБ, МО, ФТС России и др. Данная мера позволит обеспечить комплектование правоохранительных органов компетентными и профессиональными сотрудниками. Частью данной системы являются проводимые на регулярной основе курсы повышения квалификации, стажировки в практических органах, обмен опытом, семинары и круглые столы для сотрудников и профессорско-преподавательского состава вузов в государственных образовательных учреждениях, а также российских компаниях, занимающихся информационной безопасностью. Для гражданских специалистов (сотрудников служб безопасности предприятий, учреждений, банков и т. п.) целесообразно организовать аналогичные курсы обучения и повышения квалификации при технических образовательных учреждениях, занимающихся подготовкой специалистов по информационной безопасности;

– переход от преимущественно территориального принципа работы правоохранительных органов в сфере предупреждения высокотехнологичной преступности к функциональному. Существующая структура правоохранительных органов и принципы организации работы отдельных подразделений вызывают проблемы координации как внутри этих ведомств, так и в рамках межведомственного взаимодействия. Одной из главных особенностей высокотехнологичной преступности является ее многоэпизодность и трансграничный характер. По этой причине на практике зачастую возникают сложности с определением места совершения преступления, а значит, и территориального органа, который должен заниматься его раскрытием и расследованием. В виртуальном мире понятие территориальности достаточно условно, поэтому существовавшая долгие годы практика проведения разбирательства «по месту совершения преступления» в сочетании с забюрократизированностью уголовно-процессуальной системы не способствует принятию своевременных мер по изобличению преступников и документированию их деятельности. Данная ситуация ставит вопрос о целесообразности специализации сотрудников оперативных и следственных подразделений по преступлениям, совершаемым в сфере высоких технологий,

не только на региональном, но и районном уровне. Данное обстоятельство следует учитывать при решении вопросов о повышении квалификации или переподготовке сотрудников территориальных правоохранительных органов на различных уровнях;

– совершенствование информационно-аналитического обеспечения деятельности по противодействию преступлениям, совершаемым с использованием высоких технологий. Данная работа связана с решением целого ряда задач, включающих сбор и систематизацию криминологически значимой информации, ее анализ и классификацию, определение на этой основе реальной картины состояния дел и перспективное прогнозирование развития ситуации. Эта работа имеет смысл лишь при четкой интеграции ее результатов в законодательную деятельность и правоохранительную практику;

– перевод на новый уровень организации взаимодействия правоохранительных органов со средствами массовой информации. Использование средств массовой информации в системе противодействия высокотехнологичной преступности должно сочетать несколько направлений, таких как отчет перед населением о результатах борьбы с данными преступлениями; проведение правовой пропаганды, направленной на формирование правосознания и нетерпимости к преступным проявлениям; информирование населения о средствах и методах защиты от мошеннических посягательств, о новых формах его осуществления. В силу специфики преступлений, совершаемых с использованием высоких технологий, профилактический эффект от своевременного доведения данной информации чрезвычайно высок, особенно если предаваемая в СМИ информация отвечает требованиям систематичности, наступательности, наглядности и своевременности. К работе со СМИ необходимо привлекать и общественные организации, такие как союз потребителей, союз обманутых соинвесторов (вкладчиков) и т. д. Общественно-корпоративные сообщества (Ассоциация российских банков, союзы предпринимателей и т. д.) также могут сыграть большую роль в противодействии высокотехнологичной преступности.

4. Проведение комплекса целенаправленных мероприятий по устранению причин и условий, способствующих совершению компьютерных преступлений в отношении государственных и иных учреждений, предприятий и организаций.

Объектом данной деятельности являются учреждения, предприятия, организации разных форм собственности, пострадавшие или которые могут пострадать в результате преступных посягательств. Особое внимание должно быть уделено проведению разъяснительной работы с целью формирования понимания всеми

руководителями и сотрудниками данных учреждений важности обеспечения безопасности информационных систем, включая информационно-телекоммуникационные сети и оборудование. Организация бухгалтерского учета, документооборот и делопроизводство, логистика и складское движение товаров, сбор и обработка информации, особенно касающейся персональных данных граждан, другие сферы возможных преступных посягательств должны обладать системами и механизмами защиты от воздействия со стороны злоумышленников. Степень защищенности данных ресурсов может быть различной: от минимальной в сферах, наименее подверженных риску совершения высокотехнологичных преступлений, до максимальной – в кредитно-банковских организациях, страховых компаниях и т. д. При этом необходимо учитывать постоянное совершенствование и высокую изощренность преступных схем, поэтому ни одна корпоративная структура не должна считать себя полностью защищенной от преступных посягательств.

Эффективной мерой повышения компьютерной безопасности является возложение на руководителей или иных уполномоченных лиц персональной обязанности осуществлять контроль за установкой и постоянным обновлением антивирусного программного обеспечения, а также иных систем комплексной защиты с целью совершенствования систем безопасности компьютерной информации в государственных и муниципальных организациях. В свою очередь, в трудовых договорах (контрактах) лиц, работающих в корпоративной компьютерной сети или имеющих доступ к информационным ресурсам, предусмотреть положение об их персональной ответственности за разглашение или передачу посторонним лицам конфиденциальных сведений, касающихся системы защиты информации, служебных паролей или иных средств идентификации.

Отдельно следует остановиться ***на виктомологическом аспекте противодействия преступлениям, совершаемым с использованием высоких технологий.***

Поведение жертвы является составным элементом механизма преступления, поэтому одним из необходимых условий повышения эффективности предупреждения мошенничества в рассматриваемой сфере являются меры виктимологической профилактики, направленной на потенциальных жертв данного вида преступлений.

Основой данной деятельности является воздействие на виктимологические факторы, влияющие на совершение преступлений в сфере высоких технологий. При этом следует учитывать как факт виктимности самих пользователей, так и компьютерных технологий и компьютеров – хранилищ информации. Поэтому к разработке

мер виктимологической профилактики преступлений, совершаемых с использованием высоких технологий, должны привлекаться не только криминологи, но и технические специалисты.

Содержание виктимологической профилактики обусловлено несколькими аспектами. В организационном отношении виктимологическая профилактика имеет особенности, связанные со специальной подготовкой сотрудников правоохранительных органов. Недостаточность профессиональных знаний и практических умений не позволяют им своевременно осуществлять предупредительные мероприятия. Это обусловлено отсутствием в настоящее время приемлемых методических рекомендаций по организации и тактике виктимологической профилактики высокотехнологичных преступлений, конкретных методик работы с жертвами подобных преступлений.

В частности, определенные трудности вызывает проблема информационного обеспечения виктимологической профилактики преступлений, совершаемых с использованием высоких технологий. Поэтому совместная работа правоохранительных органов со службами компьютерной безопасности, изготовителями антивирусных программных продуктов является залогом успеха виктимологической профилактики.

В качестве субъектов осуществления виктимологической профилактики высокотехнологичных преступлений выступают как государство в лице правоохранительных органов, так и общественные формирования и иные негосударственные структуры. По своему объему виктимологическая профилактика данного вида преступлений охватывает различные формы поведения, являющиеся закономерным результатом разных вариантов виктимности: легкомысленность поведения, излишнее любопытство, пользовательская небрежность, незнание элементарных мер защиты, возрастные и интеллектуальные особенности и др. В качестве механизма регулирования виктимологической защиты выступают не только нормы права, но и морали, корпоративные и этические правила поведения. В целом виктимологическая профилактика должна быть ориентирована на широкую социальную превенцию в целях минимизации высокотехнологичной преступности как общественно опасного явления.

Одним из существенных факторов активного использования мошеннических схем в информационно-телекоммуникационных сетях является недостаточное правовое регулирование деловых отношений в глобальной сети Интернет, в том числе вопросов электронной формы сделки по гражданскому законодательству, дея-

тельности с использованием электронных платежных средств, проведения интернет-аукционов, участия в дистанционной торговле.

В частности, в условиях неопределенности правового статуса участников электронной торговли основное значение приобретает ряд профилактических рекомендаций для пользователей:

1. Визуальная оценка. В данном случае рекомендации интернет-покупателям могут состоять в следующем: необходимо особое внимание уделять внешнему оформлению интернет-магазина. Имеется в виду прежде всего дизайн сайта. Не стоит принимать в качестве достоверных отзывы пользователей, размещенные на этом же сайте. Правильным решением в данном случае является поиск отзывов на других сайтах. Необходимо обращать внимание на то, какую площадь веб-страницы занимает баннерная реклама. Положительную оценку получают сайты, не имеющие ни одной рекламной площадки или имеющие рекламу своих дочерних или, наоборот, головных предприятий. Отсутствие рекламы – дополнительные удобства для пользователя. Присутствие рекламы означает, что магазин зарабатывает прибыль не на продаже товаров, а на рекламе.

2. Ценовая политика. Пользователям необходимо понимать, что цена товара определяется конъюнктурой рынка и не может резко отличаться от средней. В Интернете достаточно сервисов, предоставляющих возможность поиска того или иного товара. Они помогут определить среднюю стоимость товара среди множества предложений.

3. Условия и права. Обратившись в новый интернет-магазин, особое внимание следует обратить на следующие разделы сайта: «О магазине», «Об оплате» и «О доставке». Действующие легально интернет-магазины всегда размещают о себе полную информацию: адрес, телефон, реквизиты юридического лица и расчетного счета. Такие магазины обычно работают по системе «оплата товара после доставки». Во многих случаях мошенники просят сделать предоплату за доставку причем с использованием электронных платежных систем. Отсутствие информации, запутанная система получения товара, предложение совершить предоплату являются признаками мошеннической схемы.

Для противодействия фишингу сегодня используются различные способы совершенствования программно-технических средств защиты информации: постоянная модернизация анти-фишинговых и анти-спам фильтров почтовыми службами – с одной стороны, и использование клиентами для хранения конфиденциальной информации и обмена ею достаточно защищенных почтовых служб и ящиков – с другой.

В целях виктимологической профилактики целесообразно рекомендовать пользователям использовать наиболее подходящий, защищенный и правильно настроенный веб-браузер, который незамедлительно предупреждает пользователя о возможной опасности. Это касается не только браузеров, но и других используемых программ, например, электронных кошельков WebMoney. Кроме того, антивирусные пакеты многих производителей этого программного обеспечения пополнились модулями, защищающими пользователя от фишинга.

Однако, как показывает практика, основная проблема связана с небрежностью в вопросах защиты персональной информации самими пользователями. Поэтому важной задачей правоохранительных органов является информационно-просветительская деятельность среди населения по предотвращению высокотехнологичной преступности. При этом не следует увлекаться доведением до населения конкретных мошеннических схем, используемых преступниками, поскольку вариативность данных схем очень высокая, новые способы обмана жертв появляются регулярно и с завидным постоянством, при этом огромная территория нашей страны способствует возникновению «очаговых» схем, имеющих ограниченное распространение. Поэтому простое информирование населения о новых способах совершения мошенничества может иметь противоположный эффект: наиболее виктимные слои населения (пожилые люди, доверчивые и легкомысленные пользователи и т. д.) подобной информацией, скорее всего, не заинтересуются, а преступники могут взять на вооружение сообразительность своих «коллег».

Основная работа сотрудников правоохранительных органов должна заключаться прежде всего в доведении до граждан элементарных правил безопасности, таких как недопустимость:

– загрузки из сети Интернет программных продуктов из непроверенных источников; перехода по рекламным ссылкам в Интернете, сулящим бесплатные услуги, различные призы или существенные скидки; просмотра корреспонденции от неизвестных адресатов;

– общения в социальных сетях с незнакомыми пользователями, за которыми могут скрываться мошенники, сектанты, вербовщики в террористические организации;

– покупки SIM-карт с рук или оставления своих паспортных данных сомнительным конторам;

– отправки денежных переводов лицам, предлагающим посреднические услуги в разрешении проблем с родственниками, знакомыми, якобы попавшими в беду;

– передачи данных с кредитных или дебетовых карт, пользовательских паролей и кодовых слов, запрашиваемых по телефону или через социальные сети от лица друзей, знакомых, кредитных или иных организаций под различными предлогами;

– указания в своем профиле социальной сети личной информации, в том числе о своем образе жизни, планируемых отъездах и т. п.;

– проведения операций в интернет-банкинге без проверки истинности адреса личного кабинета или при наличии дополнительных не предусмотренных стандартной процедурой запросов (защита от «фишинга»);

– непринятия срочных мер по блокированию кредитных или дебетовых карт при получении SMS о несанкционированном списании или переводе средств третьим лицам;

– регистрации в личных кабинетах, на интернет-ресурсах или онлайн-магазинах с простыми паролями, состоящими из нескольких цифр, коротких слов, соседних клавиш на клавиатуре, личных памятных дат, адресов или номеров телефонов;

– записей личных паролей на стикерах, приклеенных к монитору, или в других легкодоступных местах.

Таким образом, виктимологическая профилактика преступлений, совершаемых с использованием высоких технологий, должна быть организована с учетом виктимности различных групп населения; учитывать различные аспекты обеспечения данного вида деятельности; иметь конкретную направленность на осознание необходимости соблюдения мер предосторожности в информационно-телекоммуникационном пространстве; основываться на доступных для населения или работников – неспециалистов рекомендациях по совершенствованию своей защищенности от киберугроз.

Глава II. Организационно-методическое обеспечение расследования преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации

§ 1. Электронные носители информации в уголовном судопроизводстве

Понятие, виды и свойства электронных носителей информации как источников криминалистически значимой информации. Общие положения порядка их изъятия

Несмотря на происходящие изменения в качественных характеристиках современной преступности, связанных с использованием при совершении преступлений информационных и коммуникационных технологий, уголовно-процессуальное законодательство Российской Федерации долгое время оставалось не восприимчивым к данной очевидной тенденции. Первое упоминание об электронных носителях в уголовно-процессуальном законе состоялось в 2012 г. с принятием Федерального закона от 28 июля 2012 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации», который установил некоторые особенности порядка проведения следственных действий, в ходе которых производится изъятие электронных носителей информации.

При этом до настоящего времени на законодательном уровне не разрешен вопрос о понятии электронных носителей информации. При таких обстоятельствах большинство авторов, исследующих данный вопрос[1], используют определение, содержащееся в п. 3.1.9. ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения», согласно которому под электронным носителем понимается «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники». При этом не трудно заметить, что под данное определение попадает абсолютно любое микропроцессорное устройство.

[1] *Васюков В. Ф., Булыжкин А. В.* Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Рос. следователь. 2016. № 6. С. 3–8; *Рыжаков А. П.* Обыск и выемка: основания и порядок производства [Электронный ресурс]. Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 01.08.2017).

По образному выражению Б. В. Вехова, отсутствие законодательного определения понятия «электронный носитель информации» позволяет отнести к этой категории стиральную или кофемашину, микроволновую печь, телевизор, паспорт гражданина Российской Федерации, электронный полис обязательного медицинского страхования, электронный ключ от домофона или системы зажигания автомобиля и др.[1].

Очевидно, что для целей уголовного судопроизводства является обоснованным отнесение к электронным носителям информации не только съемных носителей информации (например, карт памяти, флэш-накопителей, съемных жестких дисков, оптических дисков и др.), но и самих персональных компьютеров и серверов, а также иных микропроцессорных устройств, конструктивно предназначенных для постоянного или временного хранения компьютерной информации.

Вместе с тем распространение данного правового режима на любую микропроцессорную технику, в том числе и на устройства, конструктивно не предназначенные для хранения компьютерной информации, является необоснованным.

Представляется целесообразным *электронный носитель информации определить как устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.*

Ключевой характеристикой электронных носителей информации, определяющей их криминалистически значимые признаки, является то, что они предназначены для хранения определенных фактических данных в цифровой форме, иными словами, для хранения компьютерной информации. Последняя в соответствии с примечанием 1 к ст. 272 УК РФ представляет собой сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Общее же понятие информации содержится в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», определяющей ее как сведения (сообщения, данные) независимо от формы их представления.

---

[1] *Вехов Б. В.* Характеристика электронных доказательств в российском уголовном судопроизводстве // Электронные носители информации в криминалистике: монография / под ред. О. С. Кучина. М., 2017. С. 139.

Для компьютерной информации характерны следующие криминалистически значимые признаки, предопределяющие специфические особенности работы с электронными носителями информации[1]:

– значительный объем при малых размерах носителя, способность к сжатию и последующему восстановлению;

– быстрота обработки, простота уничтожения, способность к преобразованию в доступный для восприятия вид;

– способность к передаче по каналам связи, доступность одновременно нескольким пользователям;

– возможность нахождения исключительно на электронном носителе (включая отдельные компьютеры и разветвленные информационные системы) в машиночитаемом виде;

– создание, изменение, копирование и использование компьютерной информации осуществляется посредством микропроцессорных устройств, обладающих возможностью чтения / записи соответствующих носителей;

– наличие индивидуализирующих признаков – метаданных, включая дату и время создания файла, внесение в него изменений, использованное программное обеспечение, в отдельных случаях – применявшееся оборудование и др.;

– способность к дублированию, т. е. переносу с одного электронного носителя на другой, при котором копия полностью эквивалентна (тождественна) оригиналу, включая как саму информацию, так и метаданные.

Основными видами компьютерной информации, представляющими интерес с точки зрения расследования, являются:

– системная информация, предназначенная для функционирования отдельных микропроцессорных устройств, информационных систем, информационных сетей;

– индивидуализирующая информация – имена пользователя, пароли, коды доступа, учетные записи, электронная подпись, иная информация и программы, позволяющие идентифицировать пользователя, воспользоваться программным продуктом, получить доступ к информационным ресурсам, электронным кошелькам и пр.;

– персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

---

[1] См.: *Гаврилин Ю. В.* Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: монография. Тула, 2009.

– медиафайлы – фото-, видео- и аудиозаписи, текстовые файлы, графическая информация;

– файлы истории – данные о событиях, произошедших в информационной системе за определенный период времени, включая запущенные программы, посещенные сетевые адреса, поисковые запросы и пр.;

– программа для ЭВМ – представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ и порождаемые ею аудиовизуальные отображения;

– база данных – представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ);

– электронный документ – документированная информация, представленная в электронной форме, т. е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

– электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

– интернет-страница – часть сайта в сети Интернет, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети Интернет;

– сетевой адрес – идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему;

– электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

– криминальная информация – вредоносные программы (заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, переписка соучастников), запрещенная информация (экстремистские материалы, сведения, составляющие тайну) и пр.;

– охраняемая компьютерная информация, содержащаяся в критической информационной инфраструктуре Российской Федерации – информация, включенная в реестр учета значимых объектов критической информационной инфраструктуры в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Следует отметить, что приведенный перечень является ориентировочным, составлен в учебных целях, а также не претендует на полноту и всеобъемлющий характер.

Криминалистическую классификацию электронных носителей информации целесообразно производить по различным основаниям.

По отношению к расследуемому событию электронные носители подразделяются на первичные и вторичные. К первичным относятся оригинальные экземпляры электронных носителей информации, связанной с событием преступления, запись которой была произведена в процессе подготовки, совершения или сокрытия преступления. Вторичные электронные носители содержат полученную в установленном уголовно-процессуальным законом порядке копию информации, содержащейся на первичных электронных носителях. Так, сервер, на котором находится база данных программы автоматизации бухгалтерского учета, относится к первичным носителям информации, а съемный жесткий диск, на который было выполнено копирование этой базы данных в ходе выемки, следует относить ко вторичным.

По возможности перемещения в пространстве электронные носители информации подразделяются на стационарные, перемещение которых невозможно без демонтажа технических средств создания, хранения и обработки информации либо конструктивно не предназначенные для переноса информации с одного стационарного носителя на другой, и портативные, конструктивно предназначенные для переноса информации с одного носителя на другой или хранения данных. К первым относятся внутренний накопитель на жестком магнитном или магнитооптическом диске (синоним – жесткий диск, HDD), ко вторым – USB флэш-накопитель (USB-диск, флэш-накопитель), оптический диск (лазерный диск, компакт-диск), карта памяти (флэш-карта) и пр.

По месту нахождения электронные носители подразделяются на локальные, сетевые (удаленные) и облачные. Локальные электронные носители – это все портативные носители, а также жесткие диски компьютеров, доступ к которым возможен только с данного компьютера. Соответственно, к сетевым носителям относятся

жесткие диски серверов, а также иных компьютеров, объединенных в локальную сеть и предоставляющих доступ к своим информационным ресурсам. Облачные носители информации представляют собой хранилища данных, предоставляющие независимым друг от друга пользователям услуги по хранению информации на единой технологической платформе.

По отношению к выполнению функции хранения информации электронные носители подразделяются на носители, выполняющие функцию хранения информации как свою основную и единственную функцию (флеш-накопители, карты памяти, компакт-диски и др.), а также на носители, способные выполнять иные функции. Примером последних является современный смартфон, способный, помимо хранения значительного объема информации (некоторые «флагманские» модели смартфонов компании Apple способны хранить свыше 256 Мб информации), выполнять и иные функции: совершать звонки, определять свое местоположение в пространстве по сигналам ГЛОНАСС, GPS и др.

По содержанию электронные носители информации весьма подробно классифицирует профессор Б. В. Вехов, выделяя[1]: машинные носители информации (ферромагнитная полимерная лента (полоса) или металлическая нить, гибкий полимерный или жесткий магнитный диск, жесткий оптический или магнитооптический диск и др.), интегральные микросхемы (идентификационные карты на интегральных микросхемах типа Sim-карт и др.), микроконтроллеры (устройства на технологии PayPass, USB-устройства, Flash-карты и др.), электронные вычислительные машины (компьютеры, активное серверное оборудование, банкоматы, терминалы, контрольно-кассовые машины, сотовые радиотелефоны, ресиверы, видеорегистраторы и др.), комбинированные носители информации (платежная карта с магнитной полосой и интегральной микросхемой и т. п.), комбинированные носители информации (платежная карта с магнитной полосой и интегральной микросхемой и т. п.), информационные системы, в том числе поисковые, информационно-телекоммуникационные сети, например, сеть Интернет.

Основные положения действующего уголовно-процессуального законодательства, регламентирующие правовое положение электронных носителей информации, специфику их изъятия, хранения

[1] *Вехов Б. В.* Характеристика электронных доказательств в российском уголовном судопроизводстве // Электронные носители информации в криминалистике: монография / под ред. О. С. Кучина. М., 2017. С. 142–143.

и в определенных случаях возврата законным владельцам, можно свести к следующим тезисам[1].

1. Электронные носители информации признаются вещественными доказательствами и приобщаются к уголовному делу в случаях, если они:

– служили орудиями, оборудованием или иными средствами совершения преступления;

– сохранили на себе следы преступления;

– являлись предметом преступного посягательства;

– могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела.

2. О признании электронных носителей информации вещественными доказательствами выносится соответствующее постановление. При этом по уголовным делам о преступлениях в сфере экономики данное постановление выносится в срок не позднее 10 суток с момента их изъятия, в иных случаях – с учетом требований разумного срока уголовного судопроизводства (ч. 4 ст. 81 УПК РФ). В случае если для осмотра изъятых электронных носителей информации ввиду их большого количества или по другим объективным причинам требуется больше времени, по мотивированному ходатайству следователя или дознавателя этот срок может быть продлен еще на 30 суток руководителем следственного органа или начальником органа дознания. В случае если для признания электронных носителей информации вещественными доказательствами требуется назначение судебной экспертизы, срок вынесения постановления о признании их вещественными доказательствами не может превышать 3 суток с момента получения следователем или дознавателем заключения эксперта.

3. Электронные носители информации, не признанные вещественными доказательствами, подлежат возврату лицам, у которых они были изъяты, с учетом требований разумного срока уголовного судопроизводства (ч. 4 ст. 81 УПК РФ), а по уголовным делам о преступлениях в сфере экономики – не позднее 5 суток по истечении установленных сроков вынесения постановления о признании изъятых предметов и документов вещественными доказательствами (по общему правилу – 10 суток, при большом объеме –

---

[1] См.: Федеральный закон от 28 июля 2012 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» и Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

еще 30 суток, при проведении экспертизы для решения вопроса о признании вещественным доказательством – 3 суток с момента получения заключения эксперта) – ч. 4 ст. 81.1 УПК РФ.

4. Устанавливаются специальные требования к хранению электронных носителей (пп. «а» п. 5 ч. 2 ст. 82 УПК РФ):

– в опечатанном виде;

– в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией;

– в условиях, обеспечивающих сохранность как самих электронных носителей, так и содержащейся на них информации.

5. По общему правилу (пп. «б» п. 5 ч. 2 ст. 82 УПК РФ) после осмотра и производства других необходимых следственных действий электронные носители возвращаются их законному владельцу, за исключением случаев, когда подобный возврат может негативно сказаться на процессе доказывания и расследования по уголовному делу.

6. В случае невозможности возврата изъятых электронных носителей информации их законный владелец или обладатель содержащейся на них информации вправе после производства неотложных следственных действий ходатайствовать о копировании содержащейся на них информации при одновременном соблюдении следующих условий:

– электронные носители, предназначенные для копирования, предоставляются законным владельцем изъятых электронных носителей или обладателем содержащейся на них информации;

– копирование осуществляется с участием законного владельца изъятых электронных носителей или обладателя содержащейся на них информации и (или) их представителей;

– копирование осуществляется с участием специалиста в присутствии понятых в подразделении органа предварительного расследования или в суде;

– должны обеспечиваться условия, исключающие возможность утраты или изменения копируемой информации;

– копирование информации не может воспрепятствовать расследованию преступления.

7. Об осуществлении копирования информации и о передаче электронных носителей, содержащих скопированную информацию, законному владельцу изъятых электронных носителей или обладателю содержащейся на них информации составляется протокол (ч. 2.1 ст. 82 УПК РФ).

8. Допускается возможность копирования информации с других электронных носителей в ходе производства любого след-

ственного действия с приложением электронных носителей, содержащих скопированную информацию, к протоколу следственного действия (ч. 8 ст. 166 УПК РФ).

9. Устанавливается особая (специальная) процедура изъятия электронных носителей информации в ходе производства обыска или выемки, содержащая следующие требования:

– обязательное участие специалиста;

– обязательное копирование информации с изымаемых электронных носителей при одновременном наличии следующих условий: соответствующее ходатайство законного владельца изъятых электронных носителей или обладателя содержащейся на них информации; выполнение копирования специалистом, участвующим в обыске (выемке); присутствие понятых; предназначенные для копирования другие электронные носители предоставляются законным владельцем изъятых носителей или обладателем содержащейся на них информации; копирование информации не может воспрепятствовать расследованию преступления или повлечь за собой утрату или изменение информации;

– об осуществлении копирования информации и о передаче электронных носителей, содержащих скопированную информацию, законному владельцу изъятых электронных носителей информации или обладателю содержащейся на них информации делается запись в протоколе обыска (выемки) (ч. 9.1 ст. 182, ч. 3.1. ст. 183 УПК РФ).

10. Установлено право на подачу в суд ходатайства, заявления, жалобы, представления в форме электронного документа, подписанного лицом, направившим такой документ, электронной подписью.

11. Электронный документ, содержащийся на электронном носителе, является иным документом, если он отвечает требованиям относимости и допустимости, заверен электронной подписью, обладает реквизитами и не содержит признаков вещественного доказательства (ответы на запросы, справки, официальная переписка и пр.).

Появление в уголовном деле такого источника доказательственной информации, как электронный носитель, возможно в ходе производства таких следственных действий, как: осмотр места происшествия, выемка, обыск и личный обыск. Кроме того, электронные носители информации могут прилагаться к рапорту об обнаружении признаков преступления, представляемому для решения вопроса о возбуждении уголовного дела в порядке, установленном Инструкцией о порядке представления результатов оперативно-

розыскной деятельности органу дознания, следователю или в суд[1]. При этом уголовно-процессуальный закон непосредственно регламентирует процедуру изъятия электронных носителей лишь в ходе обыска или выемки (ч. 9.1 ст. 182, ч. 3.1. ст. 183 УПК РФ), предъявляя следующие два обязательных требования к этой процедуре:

1) участие специалиста;

2) выполнение копирования информации с изымаемых электронных носителей (при определенных условиях) с фиксацией данного факта в протоколе следственного действия.

Говоря об участии специалистов в следственных действиях, связанных с изъятием электронных носителей информации, необходимо отметить следующее.

В литературе содержится рекомендация, что для подтверждения своей квалификации специалисты, привлекаемые к изъятию, должны представить информацию о наличии:

– диплома о высшем техническом образовании (с указанием учебных дисциплин, направленных на получение знаний, умений, навыков в исследовании, разработке, внедрении и сопровождении информационных технологий и систем);

– опыта работы в должности не менее одного года. При этом в соответствии с должностными обязанностями такого сотрудника он должен наделяться функциями по обеспечению правильной технической эксплуатации, бесперебойной работы компьютерного оборудования организации на профессиональном уровне[2].

Данные рекомендации не в полной мере основаны на требованиях действующего законодательства. Так, профессиональным стандартом «Специалист по безопасности компьютерных систем и сетей», утвержденным приказом Минтруда России от 1 ноября 2016 г. № 598н, предусматривается, что в него входят трудовые функции: обслуживание, администрирование средств защиты информации в компьютерных системах и сетях, оценивание их уровня безопасности, разработка программно-аппаратных средств защиты информации, проведение инструментального мониторинга защищенности компьютерных систем и сетей, проведение эксперти-

---

[1] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68.

[2] *Васюков В. Ф., Булыжкин А. В.* Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Рос. следователь. 2016. № 6. С. 5.

зы при расследовании компьютерных преступлений, правонарушений и инцидентов.

Стандартом предъявляются следующие требования к образованию и обучению: высшее образование – специалитет или магистратура в области информационной безопасности, наличие допуска к государственной тайне (при необходимости), рекомендуется дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности. Таким образом, в качестве специалистов следует привлекать лиц, соответствующих указанным квалификационным требованиям.

Несмотря на то что вышеназванный профессиональный стандарт требования к опыту практической работы не предъявляет, представляется, что рекомендация относительно наличия у специалиста как минимум годичного стажа работы по специальности является обоснованной.

Задачами специалиста при изъятии электронных носителей являются:

– оказание консультативной помощи при выработке тактики проведения следственного действия;

– обнаружение средств экстренного уничтожения информации;

– определение способов нейтрализации средств экстренного уничтожения информации;

– выявление признаков применения «облачных» технологий хранения данных;

– обнаружение средств шифрования данных и криптографических контейнеров, фиксация их содержания;

– обнаружение систем дублирования и резервного хранения информации;

– оказание помощи следователю при составлении протокола в описании объектов;

– копирование данных, поиск и извлечение конкретной значимой информации;

– фиксация информации с удаленных сетевых ресурсов, выявление идентификационных данных;

– определение криминалистически значимых сведений об используемой операционной системе и программном обеспечении;

– обнаружение сведений о подключенных ранее к компьютеру электронных носителях.

Вместе с тем законодательное требование об обязательном участии специалиста при проведении каждого без исключения обыска или выемки, в ходе которых осуществляется изъятие электронных носителей, выглядит чрезмерным и неоправданным. С одной сто-

роны, практического значения в привлечении профильных специалистов для изъятия флеш-карты фотоаппарата или ноутбука у подозреваемого не усматривается. С другой стороны, существующего количества профильных специалистов, состоящих в штате правоохранительных органов, явно недостаточно[1]. Несмотря на то что законодатель не ограничивает органы предварительного расследования в части приглашения специалиста исключительно из правоохранительной системы, представляется, что вышеназванное требование содержит предпосылки для признания соответствующих протоколов следственных действий недопустимыми доказательствами, а также создает «питательную среду» для злоупотребления стороной защиты своими процессуальными правами.

В этой связи представляется целесообразным внесение изменений в действующее уголовно-процессуальное законодательство, закрепив положение о том, что если в ходе следственного действия не проводится непосредственное восприятие и исследование информации, содержащейся на электронных носителях информации (как, например, в случае его осмотра), или копирование информации в порядке ч. 8 ст. 166, ч. 9.1 ст. 182, ч. 3.1. ст. 183 УПК РФ, то решение вопроса об участии специалиста должно осуществляться следователем (дознавателем) самостоятельно в порядке ст. 168 УПК РФ.

Еще одной процессуальной особенностью изъятия электронных носителей информации является то, что по ходатайству законного владельца изымаемых электронных носителей или обладателя содержащейся на них информации специалистом, участвующим в обыске или выемке, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. При этом не допускается копирование информации, если это может воспрепятствовать расследованию преступления либо по заявлению специалиста повлечь за собой утрату или изменение информации. Электронные носители, содержащие скопированную информацию, передаются законному владельцу или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей

[1] По данным ЭКЦ МВД России, в настоящее время во всех государственных судебных экспертных учреждениях (МВД России, Минюста России, ФСКН России, ФСБ России и СК России) работает не более 450 специалистов (экспертов) в области компьютерной информации. Из них в ЭКЦ территориальных органов МВД России – 255 человек.

информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе делается запись.

Соответственно, условиями правомерности копирования в ходе обыска или выемки информации, находящейся на электронных носителях, являются:

– поступление соответствующего ходатайства законного владельца изъятых электронных носителей или обладателя содержащейся на них информации;

– предоставление предназначенных для копирования электронных носителей законным владельцем изъятых носителей или обладателем содержащейся на них информации;

– разрешение поступившего ходатайства о производстве копирования информации с изымаемых носителей осуществляется следователем (дознавателем);

– выполнение копирования производится специалистом, участвующим в обыске (выемке);

– копирование не сможет воспрепятствовать расследованию преступления или повлечь за собой утрату или изменение информации (в 50 % изученных уголовных дел в копировании информации отказывалось в связи с наличием вероятности воспрепятствования расследованию);

– обязательное участие понятых при копировании.

На практике при реализации данного положения действующего законодательства могут возникать определенные процессуальные препятствия, а именно:

– в ходе осмотра места происшествия, обыска или выемки чаще всего не представляется возможным определить в полном объеме содержание и характер всей информации, находящейся на изымаемых электронных носителях. Поскольку основанием для их изъятия служит лишь вероятностные данные о наличии на них криминалистически значимой информации, сделать однозначный вывод в момент изъятия электронных носителей о том, что использование скопированной информации не может воспрепятствовать расследованию преступления, не всегда представляется возможным. К тому же данная информация может использоваться для продолжения преступной деятельности (например, данные реквизитов банковских карт), для перевода денежных средств, добытых преступным путем, в оффшорные юрисдикции, иного распоряжения денежными средствами в системах дистанционного банковского обслуживания, включая перевод на пластиковые карты физических лиц,

счета подконтрольных фирм-однодневок, индивидуальных предпринимателей, приобретения криптовалют (например, Биткоин) и пр. При таких обстоятельствах основания для удовлетворения ходатайства о копировании информации с изымаемых электронных носителей на момент проведения следственного действия могут не усматриваться. Ситуацию осложняет и то обстоятельство, что в момент производства следственного действия зачастую отсутствует возможность определения вероятности утраты информации при ее копировании;

– при изъятии электронных носителей большого объема, измеряемого сотнями гигабайт или терабайтами информации, например, стационарных персональных компьютеров, серверов и т. п., предоставление другого электронного носителя для копирования информации во время производства следственного действия не всегда представляется возможным. К тому же время копирования информации может составлять несколько часов. Так, для копирования 1 терабайта информации при средней скорости копирования 40 МБ/с может потребоваться свыше 7 часов;

– на стадии производства неотложных следственных действий, включая обыск и выемку, в ходе которых изымаются электронные носители информации, не всегда имеется возможность достоверно определить отношение заявителя ходатайства о копировании информации к изымаемым электронным носителям, а также его права на изымаемую информацию и ее носители.

Подобные «несостыковки» способны породить сложности правоприменения, вызвать определенные конфликтные ситуации и обжалование незаконных по мнению стороны защиты действий следователя (дознавателя).

Учитывая изложенное, вызывает сомнение обоснованность предусмотренного ч. 9.1 ст. 182, ч. 3.1 ст. 183 УПК РФ права законного владельца изымаемых электронных носителей или обладателя содержащейся на них информации на получение копии изымаемой информации непосредственно в процессе следственного действия (обыска или выемки). Представляется целесообразным исключить из текста ч. 9.1 ст. 182, ч. 3.1 ст. 183 УПК РФ положения о копировании. Учитывая, что положения ч. 2.1 ст. 82 УПК РФ уже предусматривают право на копирование (после производства неотложных следственных действий в подразделении органа предварительного расследования или в суде), данное изменение не приведет к ущемлению прав названных лиц и сокращению объема процессуальных гарантий.

Кроме того, копирование информации с изымаемых электронных носителей непосредственно в ходе следственного действия предусматривается только при их изъятии в ходе обыска или выемки. Однако если электронные носители изымаются в ходе осмотра места происшествия, то требование о копировании находящейся на них информации может быть заявлено лишь по окончании производства неотложных следственных действия (ч. 2.1 ст. 82 УПК РФ). В данном случае усматривается некоторая непоследовательность законодателя.

В контексте рассмотрения процедуры копирования информации с изымаемых электронных носителей нельзя не остановиться на еще одном аспекте данного вопроса: что предпочтительнее – изымать электронный носитель вместе с содержащейся на ней информацией или произвести ее копирование, не изымая при этом сам носитель.

Ответ на данный вопрос зависит от того, в рамках какого следственного действия производится изъятие информации, имеющей доказательственное значение, и (или) ее носителя: следственного осмотра (осмотра места происшествия), обыска или выемки. Отметим, что применительно к обыску и выемке законодатель императивно указывает единственный вариант действий в подобной ситуации – это изъятие электронного носителя в соответствии с вышеописанными процедурами.

Применительно же к следственному осмотру ситуация интереснее, поскольку императивных требований относительно способа изъятия доказательственной компьютерной информации УПК РФ в отношении данного следственного действия не содержит. Соответственно, изъятие информации возможно как вместе с электронным носителем, на котором эта информация находится, так и путем ее копирования на иной электронный носитель. Заметим, что последний способ не получил широкого распространения в практике. По нашим данным, к нему прибегали не более чем в 5 % изученных уголовных дел.

При этом и тот и другой способ имеют свои достоинства и недостатки. В пользу копирования информации в ходе осмотра места происшествия говорит тот факт, что данный способ позволяет минимизировать издержки владельцев электронных носителей, в том числе свидетелей, и снижает вероятность обжалования действий следователя. При этом значительно увеличивается время производства следственного действия, а также возникают риски утраты криминалистически значимой информации. Неслучайно в криминалистике «золотым» стандартом считается изъятие следа вместе со

следоносителем. Соответственно, изъятие компьютерной информации путем ее копирования (изготовления образа электронных носителей) оправдано при изъятии следов преступления в информационной системе потерпевшего, поскольку снижает его издержки.

Изъятие же электронных носителей также имеет как плюсы, так и минусы. Достоинствами подобного способа являются: ускорение и упрощение хода следственного действия, снижение психологической нагрузки на участников, уровня требований к квалификации специалиста, рисков невосполнимой утраты криминалистически значимой компьютерной информации. Недостатками же подобного способа изъятия компьютерной информации являются: возникающие сложности при изъятии компонентов распределенной компьютерной системы, элементы которой могут находиться в разных помещениях, городах и даже государствах; существующие риски потери компьютерной информации, находящейся в оперативной памяти, при отключении компьютерной системы от электропитания; громоздкость изымаемого оборудования; вероятность нарушения работы организации и создание предпосылок к ее банкротству. Кроме того, применительно к данной процедуре возникает риск изъятия компьютерной информации, относящейся к охраняемой законом тайне, для которой требуется судебное решение.

Таким образом, принятие тактического решения о способе изъятия компьютерной информации в ходе следственного осмотра принадлежит лицу, проводящему следственное действие исходя из вышеперечисленных факторов.

Процессуальный порядок изъятия электронных сообщений (включая электронную почту, сообщения социальных сетей и сервисов мгновенных сообщений) и иной информации, содержащейся в информационно-коммуникационных сетях

Развитие информационных технологий, средств связи и коммуникации обусловило существенные изменения способов совершения значительного числа преступлений, совершаемых дистанционно (т. е. без непосредственного контакта с потерпевшим)[1]. Дистанционный способ совершения преступления предполагает, что взаимодействие преступника с потерпевшим или третьими лицами осуществляется опосредованно, используя информационные ресурсы сети Интернет в первую очередь такие, как социальные сети

[1] См.: *Гаврилин Ю. В.* Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: монография. Тула, 2009.

(например, ВКонткате, Одноклассники, Facebook и др.), электронная почта (например, gmail.com, mail.ru, yandex.ru и др.), сервисы мгновенных сообщений (например, WhatsApp, Viber, Telegram и др.) и пр.

Использование при совершении преступлений вышеназванного общераспространенного программного обеспечения влечет возникновение обширной следовой картины, обнаружение, фиксация и изъятие которой требует использования как особых криминалистических технологий[1], так и неукоснительного соблюдения уголовно-процессуальных требований.

Прежде чем приступить к рассмотрению указанных требований, необходимо определиться с терминологией и понятийным аппаратом, а также механизмом правовой охраны электронных сообщений.

Понятие электронного сообщения содержится в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», определяющей его как информацию, переданную или полученную пользователем информационно-телекоммуникационной сети – технологической системы, предназначенной для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

К электронным сообщениям относятся письма, пересылаемые по электронной почте (e-mail), личные сообщения в социальных сетях (ВКонтакте и др.), переписка посредством сервисов мгновенных сообщений (мессенджеров), текстовые сообщения, передаваемые посредством мобильной связи (SMS, MMC).

Следует обратить внимание, что до 2005 г. в законодательстве Российской Федерации присутствовало такое понятие, как «электронная почта». Оно определялось Правилами оказания услуг почтовой связи[2] как сообщение, принимаемое от отправителя на бумажном или магнитном носителе, передаваемое электронным путем на расстояние, определяемое структурой и возможностями технических и сетевых средств, и доставляемое

---

[1] См.: *Гаврилин Ю. В., Лыткин Н. Н.* Использование компьютерно-технических следов при установлении события преступления // Известия Тульского государственного университета. Тула, 2006. Вып. 15. С. 44–50; *Гаврилин Ю. В.* Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Рос. следователь. 2013. № 23. С. 2–5 и др.

[2] Утверждены постановлением Правительства Рос. Федерации от 26 сентября 2000 г. № 725. Утратили силу с 1 мая 2005 г. в связи с изданием постановления Правительства Рос. Федерации от 15 апреля 2005 г. № 221.

адресату воспроизведенным в физической или электронной форме. В нестоящее время данный нормативный акт утратил силу, соответственно, понятие «электронная почта» как правовая категория не подлежит применению, а используется исключительно как название соответствующей интернет-технологии телематической передачи данных.

В общем виде электронная почта (*email, e-mail*, от англ. *electronic mail*) представляет собой сервис обмена цифровыми (электронными) сообщениями любого содержания (текстовые документы, медиафайлы, программы, архивы и т. д.) между пользователями компьютерной сети. Их передача, даже на значительные расстояния, осуществляется в течение нескольких секунд (в зависимости от загруженности почтовых серверов и каналов связи).

Создание сообщений для пересылки по электронной почте начинается с запуска специальной программы (почтового клиента). К наиболее распространенным программам электронной почты относятся: Gmail, Hotmail, Yahoo!Lavabit, FastMail, Яндекс.Почта, Рамблер, Mail.Ru. Сформировав сообщение, пользователь дает команду на его отправление, после чего сообщение через сервер провайдера отправителя поступает на сервер программы – почтового клиента отправителя, который пересылает данное сообщение через определенную последовательность узлов сети Интернет на сервер программы – почтового клиента получателя. При запуске программы почтового клиента получателя пользователь видит поступление к нему нового сообщения. Если он решает открыть это сообщение, оно поступает с сервера почтового клиента в папку «Входящие» на компьютере получателя.

Социальная сеть – интерактивный многопользовательский сайт, контент (содержание) которого наполняется его посетителями, с возможностью указания какой-либо информации об отдельном человеке, по которой аккаунт (страницу) пользователя смогут найти другие участники сети[1].

Значительный импульс развитию социальных сетей придало широкое распространение мобильной связи, технологий беспроводной высокоскоростной передачи данных для мобильных устройств, а также снижение стоимости подобных услуг. В итоге аудитория социальных сетей ежегодно демонстрирует высокие значения процентов прироста. Так, по данным, которые приводит Российский Бизнес-Журнал, аудитория самой популярной социальной сети

[1] *Чернец В., Базлова Т., Иванова Э.* Влияние через социальные сети / под общ. ред. Е. Г. Алексеевой. М., 2010. С. 29.

в мире Facebook на апрель 2017 г. составила 1 968 млн пользователей. На втором месте находится сервис обмена мгновенными сообщениями WhatsApp – 1 200 млн пользователей, на третьей позиции – видеохостинг YouTube – 1 000 млн пользователей[1]. Наиболее популярными социальными сетями в Российской Федерации, по данным фонда «Общественное мнение», являются ВКонтакте (61 %), Одноклассники (57 %), Facebook (16 %)[2].

Отличительные свойства социальных сетей:

– представляют собой сложную социальную структуру, состоящую из отдельных групп лиц, объединенных общим интересом, и индивидов, объединенных с другими индивидами («друзьями», подписчиками) на основе личной симпатии;

– направлены на удовлетворение потребности в общении пользователей между собой, расширении круга контактов, а также стимулирование достижения определенных целей посещения данного интернет-ресурса (поиск знакомых, ведение сетевого дневника (блога), получение и распространение информации, ее подтверждение или опровержение и пр.);

– содержат персональный профиль пользователя, который может включать подлинные или вымышленные анкетные данные, фотоизображение, круг увлечений;

– наличие возможности для осуществления поиска нужных пользователей со схожими интересами или по иным критериям (образование, место жительства, профессия и др.);

– предоставляют возможность взаимодействия участников путем просмотра профилей, размещения комментариев, иного контента (текстовых, графических, фото-, видеофайлов), отправки личных сообщений;

– предоставляют возможности редактирования и удаления профиля, а также изменения настройки видимости для определенного круга пользователей;

– служат индикатором персонального статуса пользователя в социальной сети (количество просмотров страницы, одобрений размещенного сообщения или иного контента, число друзей, подписчиков и пр.);

---

[1] Какие социальные сети самые популярные в 2017 году [Электронный ресурс] // Рос. Бизнес-Журнал. URL: http:rosbj.ru/2017/05/13/1250-samye-populyarnye-socialnye-seti-2017 (дата обращения: 23.08.2017).

[2] Онлайн-практики россиян: социальные сети [Электронный ресурс] // ФОМ: социологические исследования и коммуникационные решения. URL: http:fom.ru/SMI-i-internet/12495 (дата обращения: 24.08.2017).

– позволяют получить практическую выгоду от участия в социальной сети (повышение личной самооценки, трудоустройство, получение социально-полезных связей, положительной оценки со стороны иных лиц, создание семьи и пр.)[1].

Система мгновенного обмена сообщениями, так называемый мессенджер, (от англ. *messenger* – курьер) – программа для обмена текстовыми, звуковыми, фото- и видеосообщениями в реальном времени через сеть Интернет, а также организации групповых текстовых чатов или видеоконференций. В отличие от электронной почты, обмен сообщениями между пользователями происходит в реальном времени, при этом у пользователя существует возможность видеть, подключены ли к сети в данный момент абоненты, занесенные в список его контактов. Наиболее популярными в настоящее время в России программами мгновенного обмена сообщениями являются WhatsApp,Viber, Telegram, Skype.

Особенностью современных мессенджеров, обуславливающих их высокую популярность, в том числе и в криминальной среде, является использование ими криптографических алгоритмов защиты информации, обеспечивающих сквозное шифрование передаваемых пользователями сообщений. При этом ключи для расшифровки сообщений хранятся на устройствах пользователей, а не на внешних серверах. Соответственно, по информации разработчиков мессенджеров, никто, кроме пользователей, не может получить доступ к переписке.

Еще одной особенностью данных программ является то, что за их использование не взимается плата (за исключением расходов на интернет-трафик), что делает их фактически альтернативой телефонной связи.

Под услугами телефонной связи понимаются отношения между абонентом и (или) пользователем услуг телефонной связи и оператором связи при оказании услуг местной, внутризоновой, междугородной и международной телефонной связи в сети связи общего пользования, а также при оказании услуг подвижной радиосвязи, услуг подвижной радиотелефонной связи и услуг подвижной спутниковой радиосвязи в сети связи общего пользования[2].

Оказание услуг телефонной связи может сопровождаться предоставлением оператором связи иных услуг, технологически нераз-

---

[1] *Соловьев В. С.* Криминогенный потенциал социального сегмента Интернета: методика оценки и меры нейтрализации: монография. Краснодар, 2016. С. 8–9.

[2] См. п. 1 Правил оказания услуг телефонной связи, утв. постановлением Правительства Рос. Федерации от 9 декабря 2014 г. № 1342 «О порядке оказания услуг телефонной связи».

рывно связанных с услугами телефонной связи и направленных на повышение их потребительской ценности. К числу таких услуг относится и передача так называемых коротких текстовых сообщений (SMS), состоящих из букв и (или) символов и предназначенных для передачи по сети телефонной связи.

Для уяснения правовой природы информации, содержащейся в сообщениях, передаваемых посредством электронной почты, социальных сетей, сервисов мгновенных сообщений и мобильной связи, следует отметить, что согласно ч. 2 ст. 23 Конституции Российской Федерации каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Применительно к отношениям, связанным с реализацией права на тайну телефонных переговоров, Конституционный Суд Российской Федерации сформулировал правовую позицию, согласно которой информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на ее территории законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям необходимо получение судебного решения[1].

В другом Постановлении Конституционный Суд указывает, что вышеприведенная правовая позиция определяет правовые стандарты передачи любых сообщений – независимо от того, какими средствами осуществляется такая передача, – имеет общее значение и распространяется на правовое регулирование отношений, связанных с реализацией как права на тайну телефонных переговоров, так и права на тайну переписки, почтовых, телеграфных и иных сообщений, которое закреплено этими конституционными положениями,

[1] Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 г. «О связи»: определение Конституционного Суда Рос. Федерации от 2 октября 2003 г. № 345-О // Рос. газ. 2013. № 250; Об отказе в принятии к рассмотрению жалоб гражданина Муллина Александра Анатольевича на нарушение его конституционных прав положениями статьи 9 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьи 53 Федерального закона «О связи»: определение Конституционного Суда Рос. Федерации от 21 октября 2008 г. № 528-О-О. Документ опубликован не был. Доступ из справ.-правовой системы «Консультант Плюс».

допускающими возможность его ограничения только на основании судебного решения[1].

Приведенные Конституционные положения находят свое отражение в действующем законодательстве. Так, согласно ст. 63 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» на территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами. Операторы связи обязаны обеспечить соблюдение тайны связи. Ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляется только на основании решения суда, за исключением случаев, установленных федеральными законами.

Согласно ч. 1 ст. 13 УПК РФ ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения.

На основании изложенного, следует констатировать, что информация, содержащаяся в сообщениях, передаваемых посредством электронной почты, социальных сетей, сервисов мгновенных сообщений и мобильной связи, относится к охраняемой законом тайне переговоров, получение которой возможно в рамках особых юридических процедур.

Однако прежде чем приступить к детальному анализу данных процедур, следует проследить эволюцию действующего законодательства, регламентирующего данные правоотношения.

Как уже отмечалось, важнейшей вехой в развитии отечественного законодательства, регламентирующего процессуальный порядок изъятия электронных сообщений, являлось принятие Федерального закона от 28 июля 2012 г. № 143-ФЗ, определяющего порядок изъятия электронных носителей. С указанной

[1] По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А. И. Сушкова: Постановление Конституционного Суда Рос. Федерации от 26 октября 2017 г. № 25-П // Собр. законодательства Рос. Федерации. – 2017. – № 45, ст. 6735.

целью ст. 182 УПК РФ дополнена ч. 91, определяющей порядок их изъятия в ходе обыска, а ст. 183 – ч. 31, регламентирующей порядок их изъятия в ходе выемки.

Федеральным законом от 28 июля 2012 г. № 139-ФЗ в целях ограничения доступа к сайтам в сети Интернет, содержащим информацию, распространение которой в Российской Федерации запрещено, создан единый реестр доменных имен, указателей страниц сайтов в сети Интернет, содержащих информацию, распространение которой запрещено. Создание, формирование и ведение реестра осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в порядке, определенном постановлением Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено». Данным постановлением определено, что Министерством внутренних дел Российской Федерации принимаются решения в отношении распространяемой посредством сети Интернет информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, а также о способах и местах культивирования наркосодержащих растений.

Приказом МВД России от 12 декабря 2016 г. № 827 функции по подготовке и принятию соответствующих решений возложены на Главное управление по контролю за оборотом наркотиков МВД России. Одновременно приказом утвержден и порядок действий начальников территориальных органов МВД России в случае выявления информации о возможном наличии на страницах сайтов сети Интернет сведений о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прокуроров, местах их потребления, а также способах и местах культивирования наркосодержащих растений. Взаимодействие с Роскомнадзором при этом происходит посредством заполнения размещенной на его сайте электронной формы для приема обращения.

Критериями оценки материалов для включения в данную систему являются[1]:

любое изображение ребенка, совершающего реальные или смоделированные сексуальные действия, или любое изображение половых органов ребенка в сексуальных целях;

информация[2]:

– о производстве, распределении, распространении, продаже, приобретении или хранении детской порнографии;

– о привлечении несовершеннолетних в качестве исполнителей в зрелищных мероприятиях порнографического характера, о местах проведения таких мероприятий либо контактная информация;

– направленная на возбуждение сексуальных чувств по отношению к несовершеннолетним либо оправдывающая сексуальное поведение в отношении несовершеннолетних;

– о порядке действий по изготовлению, разработке и использованию наркотических средств и психотропных веществ (в том числе описание процессов и (или) инструкций (схем) их разработки, изготовления и использования), а также способах использования прекурсоров для их изготовления;

– описывающая либо дающая представление о создании специальных условий для посева и выращивания растений, содержащих наркотические средства, психотропные вещества и их прекурсоры, совершенствовании технологии выращивания, выведении новых сортов, повышении урожайности и устойчивости к неблагоприятным метеорологическим условиям;

---

[1] Об утверждении Критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено: приказ Роскомнадзора, МВД России, Роспотребнадзора, ФНС России от 18 мая 2017 г. № 84/292/351/ММВ-7-2/461@.

[2] Здесь и далее имеется в виду фото-, видео-, аудио- и (или) текстовая информация.

– описывающая либо дающая представление о местах культивирования растений, содержащих наркотические средства, психотропные вещества и их прекурсоры, а также местах их дикого произрастания, в том числе содержащая описание маршрутов (схем) проезда (прохода) к таким местам;

– о способах ухода от уголовной и административной ответственности за правонарушения, связанные с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров;

– о местах приобретения, ценах и способах получения тех или иных видов наркотических средств, психотропных веществ и их прекурсоров;

– направленная на формирование положительного образа лиц, осуществляющих изготовление, разработку и использование наркотических средств, психотропных веществ и их прекурсоров, предоставляющих услуги по их приобретению, либо культивирование растений, содержащих наркотические средства, психотропные вещества и их прекурсоры;

– содержащая предложения, просьбы, приказ совершить самоубийство;

– содержащая указание на самоубийство как на способ решения проблемы;

– выражающая одобрение: совершения самоубийства либо действий, направленных на самоубийство, или намерений реального (воображаемого) собеседника или третьего лица совершить самоубийство, а также призыва, побуждающего совершить самоубийство;

– направленная на популяризацию конкретных действий других людей, которые уже совершили самоубийство, и (или) утверждения (суждения) о преимуществах, которые получили лица, совершившие самоубийство, в том числе представление самоубийства как обыденного явления (приемлемого, логичного и закономерного в современном обществе поступка);

– содержащая осуждения, высмеивания неудавшейся попытки совершить самоубийство, включая описание отношения, чувств и обсуждения темы лицами, имеющими опыт попытки самоубийства;

– содержащая наличие любого объявления, в том числе о знакомстве, с целью совершения самоубийства, в том числе группового и (или) ассистированного, осуществленного с чьей-либо помощью, либо в чьем-то присутствии, либо под чьим-то наблюдением, а также в целях попытки совершения самоубийства, наличие опроса (голосования), теста, рейтинга на предмет выбора самоубийства как способа решения проблемы, равно как на предмет выбора наиболее

безболезненного, надежного, доступного, эстетичного способа самоубийства;

– о способах совершения самоубийства; описании (демонстрации) процессов, изображающих (воспроизводящих) любую последовательность действий, и (или) возможных результатов (последствий) совершения самоубийства, средств и (или) мест для их совершения;

– о необходимых для самоубийства условиях (выбор места, времени, способа, иные подготовительные действия, которые необходимо совершить для достижения цели самоубийства).

Федеральным законом от 5 мая 2014 г. № 110-ФЗ усилен контроль за платежами, проходящими онлайн, в том числе введены ограничения для анонимных платежей. Установлена процедура упрощенной идентификации клиента – физического лица (в том числе по данным государственных информационных систем). По общему правилу идентификация не проводится при совершении платежей до 15 000 руб.

Федеральным законом от 5 мая 2014 г. № 97-ФЗ вводится понятие организатора распространения информации в сети Интернет, устанавливается уведомительный порядок начала его деятельности, а также на него возлагается обязанность хранить информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение шести месяцев с момента окончания осуществления таких действий, предоставлять указанную информацию уполномоченным государственным органам, оказывать им содействие в реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий. Кроме того, на оператора связи возложена обязанность идентификации пользователей услугами связи по передаче данных и предоставлению доступа к сети Интернет и используемого ими оконечного оборудования.

Федеральным законом от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» на операторов связи возложена обязанность хранить на территории Российской Федерации и при необходимости предоставлять уполномоченным государственным органам, осуществляющим опе-

ративно-розыскную деятельность или обеспечение безопасности Российской Федерации:

– информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий;

– текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

На организатора распространения информации в сети Интернет возложены аналогичные обязанности в отношении сообщений пользователей сети Интернет. Кроме того, при использовании для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети Интернет возможности дополнительного кодирования электронных сообщений организатор распространения информации в сети Интернет обязан представлять в уполномоченный орган информацию, необходимую для декодирования данных сообщений.

Федеральным законом от 6 июля 2016 г. № 375-ФЗ регламентирована процессуальная форма изъятия электронных сообщений и иных сообщений, передаваемых по сетям электросвязи. Ст. 185 УПК РФ дополнена ч. 7 следующего содержания: «при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка».

Федеральным законом от 29 июля 2017 г. № 276-ФЗ установлены ограничения на использование информационных ресурсов (сайтов, программ), посредством которых обеспечивается доступ к заблокированным сайтам, доступ к которым ограничен на территории Российской Федерации. Наиболее популярные технологии для захода на заблокированные интернет-ресурсы – это использование анонимайзеров и VPN-сервисов. Анонимайзеры – программы, позволяющие скрывать реквизиты пользователя интернет-ресурсов; VPN-сервисы – программы, устанавливающие между пользователем и этим сервисом шифрованный канал для обмена данными, не позволяющий установить третьим лицам содержание трафика. На владельцев интернет-ресурсов, позволяющих обеспечить доступ на заблокированные сайты, возложены обязанности сервисов

в течение 30 дней подключиться к Федеральной государственной информационной системе, содержащей перечень информационных ресурсов, доступ к которым ограничен на территории Российской Федерации, и закрыть доступ к таким ресурсам. В противном случае доступ к этим ресурсам подлежит блокированию. Операторы связи, оказывающие услуги по предоставлению доступа к сети Интернет, должны отключить показ ссылок на заблокированные ресурсы.

Федеральный закон от 29 июля 2017 г. № 241-ФЗ обязывает организатора обмена мгновенными сообщениями обеспечивать передачу электронных сообщений только тех пользователей сети Интернет, которые прошли соответствующую процедуру идентификации (с использованием абонентского номера, на основании соответствующего договора). Кроме того, мессенджеры должны: в течение суток с момента получения соответствующего требования уполномоченного органа ограничить возможность осуществления пользователем сервиса обмена сообщениями; обеспечивать техническую возможность отказа пользователей сервиса обмена мгновенными сообщениями от получения электронных сообщений от других пользователей; хранить идентификационные сведения об абонентском номере только на территории Российской Федерации.

Процессуальный порядок изъятия электронных сообщений регламентируется ч. 7 ст. 185 УПК РФ, согласно которой при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка.

Упоминаемое же законодателем в тексте приведенной уголовно-процессуальной нормы понятие «электросвязь» раскрывается в п. 35 ст. 2 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»: это любые излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам.

Учитывая, что наиболее распространенным способом передачи электронных сообщений является электронная почта, следует отметить, что, исходя из технологических особенностей функционирования данного сервиса сети Интернет, передаваемые по ней электронные сообщения сохраняются как минимум на электронных носителях следующих информационных систем:

– компьютере (смартфоне) лица, отправляющего почту;
– сервере провайдера отправителя;

– сервере исходящих сообщений программы – почтового клиента отправителя сообщений;

– сервере входящих сообщений программы – почтового клиента получателя сообщений;

– сервере провайдера получателя сообщений;

– компьютере (смартфоне) лица, получающего почту.

Время нахождения электронных сообщений на вышеперечисленных носителях определяется индивидуальными параметрами (настройками, выбранными информационными политиками) информационной системы с учетом требований действующего законодательства о хранении передаваемого контента и сведений о фактах получения/отправки электронных сообщений.

Несмотря на широкое многообразие программ – почтовых клиентов, организация расположения информации в них, как правило, включает в себя:

а) папку «Входящие» – для хранения поступающих почтовых сообщений. Когда конкретный компьютер подключается к серверу провайдера и программа работы с электронной почтой забирает оттуда всю почту, она помещается в указанную папку и в ней хранится до момента удаления ее пользователем (следует иметь в виду, что специалисты могут ее восстановить и после удаления);

б) папку «Исходящие» – для хранения сообщений, созданных пользователем и подготовленных к отправлению. Обычно сообщения электронной почты создаются в автоматическом режиме, т. е. до подключения компьютера к Интернету, а потом при подключении отправляются. Отправленные сообщения удаляются из папки «Исходящие» и перемещаются в папку «Отправленные»;

в) папку «Отправленные» – для хранения копий переданных с данного компьютера сообщений электронной почты (оттуда они могут быть удалены);

г) папку «Корзина» – для хранения удаленных сообщений. Из данной папки удаленные сообщения могут быть восстановлены.

Следует иметь в виду, что пользователем могут создаваться и другие папки под любыми именами.

Основания для выемки электронных сообщений подразделяются на фактические и юридические.

Фактическим основанием для выемки является наличие данных, указывающих на то, что в электронной переписке могут содержаться сведения, имеющие значение для уголовного дела.

Юридическим основанием служит судебное решение, полученное в порядке ст. 165 УПК РФ. В соответствии со ст. 165 УПК РФ следователь с согласия руководителя следственного органа, а дозна-

ватель с согласия прокурора возбуждает перед судом ходатайство о производстве выемки, о чем выносится постановление. Ходатайство о производстве выемки подлежит рассмотрению судьей районного суда или военного суда соответствующего уровня по месту производства предварительного следствия или производства следственного действия не позднее 24 часов с момента поступления указанного ходатайства. Рассмотрев указанное ходатайство, судья выносит постановление о разрешении производства следственного действия или об отказе в его производстве с указанием мотивов отказа. В исключительных случаях, когда производство выемки в жилище не терпит отлагательства, выемка может производиться на основании постановления следователя или дознавателя без получения судебного решения. В этом случае следователь или дознаватель в течение 24 часов с момента начала производства следственного действия уведомляет судью и прокурора о производстве выемки. К уведомлению прилагаются копии постановления о производстве выемки и протокол следственного действия для проверки законности решения о его производстве. Получив указанное уведомление, судья в срок, предусмотренный ч. 2 ст. 165 УПК РФ, проверяет законность производства выемки и выносит постановление о его законности или незаконности. В случае если судья признает произведенную выемку незаконной, все доказательства, полученные в ходе ее производства, признаются недопустимыми в соответствии со ст. 75 УПК РФ.

Говоря о процессуальном порядке изъятия электронных сообщений, нельзя не сказать и о процессуальных особенностях их изъятия из смартфонов – средств подвижной радиотелефонной (мобильной) связи с доступом в сеть Интернет и иных информационно-коммуникационных устройств, включая планшетные компьютеры (далее – информационно-коммуникационные устройства). Сегодня активно развиваются криминалистические средства извлечения криминалистически значимой информации из устройств мобильной связи, в частности «Cellebrite UFED», «Мобильный криминалист», «Belkasoft Evidence Center Ultimate», «Elcomsoft Mobile Forensic Bundle». Функциональные возможности данных систем более подробно мы рассмотрим далее, однако можно констатировать, что данные устройства позволяют извлекать данные из большинства моделей мобильных устройств на iOS, Android, BlackBerry, Windows Phone и др. При этом в числе потенциально извлекаемых данных находятся любые факты использования мобильного устройства (входящие и исходящие звонки, SMS и MMS-сообщения, переписка в социальных сетях, сервисах мгновенных сообщений, электронная почта и др.). В этой связи актуальным является вопрос относитель-

но правомерности использования указанных выше средств криминалистической техники при извлечении информации, относящейся к охраняемой законом тайне. Данный вопрос имеет важное практическое значение, поскольку без четкого понимания ответа на него существенно повышаются правовые риски признания полученных доказательств недопустимыми.

Прежде всего следует отметить, что Конституция Российской Федерации в ч. 2 ст. 23 закрепляет право каждого на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Процессуальными формами получения вышеназванной информации являются:

1. Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка (ч. 7 ст. 185 УПК РФ).

2. Получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186 УПК РФ).

3. Получение информации в ходе следственного осмотра мобильного устройства (ст. 176 УПК РФ).

4. Получение информации в ходе производства экспертизы (ст. 195 УПК РФ).

Если первая и вторая из обозначенных процессуальных форм не вызывает сомнений с точки зрения порядка соблюдения конституционно-правовой гарантии тайны переписки, почтовых и иных сообщений, то в отношении третьей и четвертой формы таковые сомнения присутствуют. При этом следует отметить, что в подобных случаях применению средств криминалистической техники исследования информационно-коммуникационных устройств в целях извлечения контента, включающего сведения, составляющие тайну переписки, почтовых и иных сообщений, как правило, не предшествует получение соответствующего судебного решения. Данное обстоятельство влечет риски признания полученных таким образом доказательств недопустимыми.

Вместе с тем представляется, что если электронные носители информации (информационно-коммуникационные устройства) получены в ходе следственных действий на основании судебного решения (осмотр жилища при отсутствии согласия проживающих в нем лиц, обыск, выемка), то их последующее исследование с применением средств криминалистической техники дополнительного судебного решения не требует.

Свои процессуальные особенности имеет и порядок изъятия информации, содержащейся в информационно-коммуникацион-

ных сетях. Действующее уголовно-процессуальное законодательство не предусматривает самостоятельной правовой процедуры (отдельного следственного действия), направленной на решение данной задачи. Обобщение правоприменительной практики свидетельствует, что основное средство фиксации и изъятия доказательственной информации в сетях общего пользования (включая сеть Интернет) представляет собой следственный осмотр (осмотр места происшествия).

В общем виде алгоритм его проведения можно представить следующим образом.

На подготовительном этапе приглашаются специалист, требования к квалификации которого были уже рассмотрены, и понятые, способные понимать характер и содержание действий следователя и специалиста по обнаружению, фиксации и изъятию следов преступления. Несмотря на то что следственный осмотр не относится к числу следственных действий, при проведении которых участие понятых является обязательным, их приглашение все же целесообразно, поскольку в случае вероятного последующего удаления информации (сайта, страницы, сообщения в социальной сети) заинтересованными лицами именно допрос понятых может свидетельствовать о нахождении в определенное время конкретной информации на определенном сетевом ресурсе.

На рабочем этапе, после инструктажа участников осмотра и разъяснения им их процессуальных прав и обязанностей, необходимо зафиксировать, с помощью какой компьютерной техники осуществляется доступ в сеть. Затем производится запись адреса, подлежащего осмотру сайта в сети Интернет, запись в протоколе информации, отображенной на экране, делается копия изображения (скриншот) экрана (нажатием клавиши PrtSc с последующей вставкой скопированного таким образом изображения в файл, созданный в офисном приложении, и его распечатка). Далее специалист производит сохранение страницы на неперезаписываемый носитель информации (например, CD-R диск), после чего производится словесное описание осматриваемой интернет-страницы в протоколе осмотра с приведением дословного содержания отображаемой информации.

На заключительном этапе производится опечатывание диска со скопированной информацией и скриншотами, подписание понятыми распечаток и протокола осмотра.

Разумеется, здесь приведены лишь ключевые элементы технологии осмотра сайта в сети Интернет для фиксации и изъятия доказательственной информации. Более подробно тактика осмотра места происшествия при расследовании уголовных дел о пре-

ступлениях, совершенных с использованием информационно-коммуникационных технологий, будет рассмотрена далее при анализе криминалистических методов и средств изъятия доказательственной информации.

Отметим, что в практической деятельности правоохранительных органов нередко изъятие сообщений из переписки по электронной почте осуществляется путем изъятия всей компьютерной техники в ходе обыска (выемки) и назначения впоследствии компьютерной экспертизы. Полученные таким образом доказательства могут быть признаны недопустимыми по причине нарушения рассмотренных выше требований ч. 7 ст. 185 УПК РФ к порядку изъятия электронных сообщений или иных передаваемых по сетям электросвязи сообщений путем проведения их осмотра и выемки. К тому же подобные действия приводят к неоправданному возрастанию нагрузки на экспертные подразделения, как следствие – увеличение сроков производства экспертизы и расследования по уголовному делу.

§ 2. Криминалистические особенности обнаружения, фиксации, изъятия и исследования электронных следов преступления

Понятие и свойства электронных следов преступления

Механизм совершения преступлений с использованием информационно-коммуникационных технологий характеризуется спецификой образующих его элементов. Эта специфика обусловлена в первую очередь особенностями способов подготовки, совершения и сокрытия таких преступлений, в основе которых лежат технологии дистанционной передачи данных с использованием информационно-коммуникационных сетей. В свою очередь, данное обстоятельство закономерно обуславливает специфику и иных элементов в структуре механизма преступления: орудий и средств его совершения, которыми выступают программное обеспечение, компьютерная техника (включая как микропроцессорные устройства, так и устройства приема, передачи и хранения данных, включая электронные носители информации), сеть Интернет (включая находящиеся в ней информационные ресурсы и сервисы, электронные сообщения) и др. Компьютерная информация в механизме рассмвтриваемых преступлений может выступать либо как предмет преступного посягательства (при ее неправомерном уничтожении, копировании, блокировании или модификации), либо в качестве средства совершения преступления (например, при совершении вымогательства, преступления против личности дистанционным способом и т. п.).

Все приведенные выше особенности механизма совершения преступлений с использованием информационно-коммуникационных технологий закономерно влекут и исключительное своеобразие следовой картины данных преступлений.

Следовая картина названных преступлений весьма специфична и требует разработки принципиально иных методов и средств по сравнению с традиционными. Следы совершения указанных преступлений, в силу их специфики, редко остаются в виде изменений внешней среды. Соответственно, они не рассматриваются в рамках трасологии, поскольку в большинстве случаев носят информационный характер, т. е. представляют собой те или иные изменения в охраняемой законом информации в результате ее уничтожения, модификации, копирования, блокирования[1]. В этой связи обнаружение, фиксация и изъятие таких следов требуют использования особых криминалистических технологий[2], разработка и совершенствование которых на протяжении уже ряда лет представляет исключительно актуальное направление криминалистики.

Все это предопределяет появление самостоятельного раздела криминалистической техники – криминалистического исследования электронных носителей информации, направленного на обеспечение единообразного подхода к работе с данными объектами, к числу которых относятся любые устройства, конструктивно предназначенные для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

К числу объектов криминалистического исследования электронных носителей информации относятся и средства подвижной радиотелефонной (мобильной) связи с доступом в сеть Интернет (смартфоны) и иные информационно-коммуникационные устройства, включая планшетные компьютеры. В связи с наличием в абсолютном большинстве современных смартфонов модуля получения геопространственной информации, использующего сигналы систем ГЛОНАСС и (или) GPS-навигации, перспективным направлением

---

[1] *Гаврилин Ю. В.* Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Рос. следователь. 2013. № 23. С. 3.

[2] *См.: Гаврилин Ю. В., Лыткин Н. Н.* Использование компьютерно-технических следов при установлении события преступления // Известия Тульского государственного университета. Тула, 2006. Вып. 15. С. 44–50; *Гаврилин Ю. В.* Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Рос. следователь. 2013. № 23. С. 2–5 и др.

развития вышеназванного раздела криминалистической техники является исследование данных средств навигации[1].

Помимо перечисленного, к числу объектов криминалистического исследования электронных носителей относятся: системы обработки информации или отдельные функциональные устройства таких систем; системные блоки персональных компьютеров, ноутбуков, нетбуков и т. п; машинные носители (накопители на жестких и гибких магнитных дисках, флеш-накопители, карты памяти, оптические диски и т. п.); уже упомянутые навигаторы, трекеры; мобильные телефоны и SIM-карты к ним; радиоэлектронные устройства; платежные пластиковые карты и скимминговые устройства; платы игровых автоматов; видеорегистраторы и пр.

Электронные носители информации как источники доказательственной информации и объекты криминалистических исследований были рассмотрены в предыдущем параграфе. Как уже отмечалось, их ключевой характеристикой является то, что они предназначены для хранения определенных фактических данных в цифровой форме, иными словами, для хранения компьютерной информации. Соответственно, именно электронные носители информации отражают результаты ее создания, уничтожения, копирования, блокирования, модификации или иного преобразования, т. е. следовую картину совершенного противоправного деяния. Как и любые иные объекты материального мира, электронные носители информации характеризуются конкретными морфологическими признаками: тип, вид, марка, модель, цвет, емкость, форм-фактор, серийный номер и пр.

Уточним, что при совершении преступлений с использованием информационно-коммуникационных технологий остаются и традиционные (трасологические) следы – предметы, вещества, отображения. Это и следы пальцев рук на клавиатуре иных аппаратных компонентов информационной системы; микрочастицы (например, волокна одежды на мебели, волосы, перхоть, попавшие на клавиатуру); следы обуви; следы орудий взлома и инструментов в помещениях, где происходил непосредственный физический контакт с компьютерной техникой, а также сами электронные носители как объекты материального мира и пр. За десятки лет развития крими-

[1] *См.: Гаврилин Ю. В.* Использование возможностей средств навигации в установлении обстоятельств совершения преступлений // Актуальные проблемы борьбы с преступностью: материалы межвузовской науч.-практ. конф. (Тула, 15 марта 2017 г.). Тула, 2017.

налистики накоплен колоссальный опыт работы с подобного рода следами[1].

Однако в ходе расследования преступлений, совершенных с использованием информационно-коммуникационных технологий, наибольшей спецификой обладают, разумеется, электронные следы преступления. Они представляют собой результаты создания или преобразования компьютерной информации в форме уничтожения, копирования, блокирования или модификации, а также соответствующие им изменения физических характеристик ее носителя, причинно связанные с событием преступления.

Заметим, что в языке криминалистике нет единообразного подхода к наименованию и классификации вышеназванных следов. Они рассматривались в работах Ю. М. Батурина и А. М. Жодзишского[2], Н. С. Полевого[3], В. В. Крылова[4], В. Б. Вехова[5], А. В. Сорокина[6], Б. В. Андреева, П. Н. Пака, В. П. Хорста[7], А. Г. Волеводза[8], В. А. Мещерякова[9], Ю. В. Гаврилина и Н. Н. Лыткина[10] и др. В различных источниках данные следы именуются и как компьютерные, и как компьютерно-технические, и как цифровые, и как информационные, и как бинарные, и пр.

Вместе с тем сущность данных следов состоит в том, что они, оставаясь на электронных носителях информации, отражают изменения в хранящейся в них информации по сравнению с исходным состоянием.

---

[1] *Грановскнй Г. Л.* Основы трасологии. М., 1965; *Сорокин В. С.* Обнаружение и фиксация следов на месте происшествия. М., 1966; *Крылов И. Ф.* Следы на месте преступления. Л., 1961; *Крылов И. Ф.* Криминалистическое учение о следах. Л., 1976.

[2] *Батурин Ю. М., Жодзишский А. М.* Компьютерная преступность и компьютерная безопасность. М., 1991.

[3] Компьютерные технологии в юридической деятельности / под ред. Н. С. Полевого. М., 1994.

[4] *Крылов В. В.* Информационные компьютерные преступления. М., 1997; *Крылов В. В.* Расследование преступлений в сфере информации. М., 1998.

[5] *Вехов Б. В.* Компьютерные преступления. Способы совершения. Методики расследования. М., 1996.

[6] *Сорокин А. В.* Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. Курган, 1999.

[7] *Андреев Б. В., Пак П. Н., Хорст В. П.* Расследование преступлений в сфере компьютерной информации. М., 2001.

[8] *Волеводз А. Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002.

[9] *Мещеряков В. А.* Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2002.

[10] *Гаврилин Ю. В., Лыткин Н. Н.* Использование компьютерно-технических следов в раскрытии и расследовании преступлений: монография. М., 2006.

На логическом уровне происходит модификация информации (т. е. внесение изменений в информацию баз данных, программ, текстовых файлов, файлов-отчетов и протоколов работы, системного реестра, учетных записей пользователей сети Интернет и др.), уничтожение информации (удаление из каталогов имен файлов, стирание или добавление отдельных записей), копирование информации (т. е. ее дублирование на том же самом или ином электронном носителе), блокирование информации (т. е. лишение возможности доступа к ней) либо создание новой информации.

На физическом уровне происходит размагничивание или намагничивание определенных секторов (кластеров) рабочих поверхностей носителей или изменение электрического заряда в изолированной области полупроводниковой структуры.

Электронные следы преступления как специфическая форма преобразования компьютерной информации являются[1]:

1. Отражением события преступления в информационном поле.

2. Материальными по своей природе, но не отражающими пространственную форму следообразующего объекта.

3. Результатом преобразования компьютерной информации.

4. Способными к дублированию, т. е. переносу (копированию) на другие носители информации без какого-либо изменения их характеристик.

Базовые принципы работы с электронными следами преступления:

1. Любые действия по обнаружению, фиксации и изъятию электронных следов не должны приводить к изменениям информации на электронных носителях, признанных вещественными доказательствами.

2. Работа с носителями информации, содержащими электронные следы преступления, должна вестись только с участием профильного специалиста надлежащей квалификации.

3. Все действия по обнаружению, фиксации, изъятию, исследованию электронных следов и последующему хранению электронных носителей информации должны быть надлежаще процессуально оформлены.

4. Четкое разделение ответственности субъектов уголовно-процессуальной деятельности, в распоряжении которых находятся электронные носители информации, содержащие электронные следы преступления, за их сохранность в неизменном состоянии.

---

[1] *Гаврилин Ю. В., Лыткин Н. Н.* Использование компьютерно-технических следов в раскрытии и расследовании преступлений: монография. М., 2006. С. 35.

Все электронные следы можно разделить на две большие группы: локальные (находящиеся на индивидуально определенных электронных носителях, доступ к информации на которых осуществляется непосредственно на месте их нахождения) и сетевые (доступ к которым осуществляется опосредованно, с использованием сетевого оборудования).

Локальные следы подразделяются, в свою очередь, также на две группы: мета-данные и искомые данные. К мета-данным относятся признаки, идентифицирующие компьютерную информацию: имя, размер и формат файла, автор файла, дата и время создания, изменения, связи файла, его категория. К искомым данным относится информация, имеющая отношение к расследуемому событию (входящая в предмет доказывания), и иная информация (не относящаяся к расследуемому событию).

Криминалистически значимую информацию о работе пользователя в сети Интернет в операционной системе MicrosoftWindows XP содержат:

файлы реестра и системных событий, расположенные в каталоге %Windir%\System32\Config\;

файл, содержащий перечень и настройки активных подключений;

Documents and Settings\All Users\Application;

data\Microsoft\Network\Connections\Pbk\rasphone.pbk;

файлы, содержащие протоколы работы модемов %Windir%\ Modem Log_%Modemname%.txt;

файлы Index.dat, содержащие сведения об интернет-ресурсах, посещаемых пользователем;

файлы, расположенные в каталогах: Documents and Settings\%username%\Local Setings\Temporary Internet Files\ Content.IE5\;

файлы, расположенные в каталогах: Documents and Settings\%username%\cookies\;

файлы, содержащие настройки и протоколы работы программ, предназначенных для работы пользователя в сети Интернет.

Локальными электронными следами являются также результаты работы антивирусных и тестовых программ, а также вредоносное программное обеспечение на компьютере или ином устройстве, например, смартфоне потерпевшего.

Сетевые следы представляют собой сведения о прохождении информации по каналам связи между отдельными компьютерами, объединенными в локальную сеть или подключенными к Интернету. Данные сведения сохраняются в специальных файлах регистрации (log-файлах), ведение которых осуществляется информационными

системами в автоматическом режиме. Какое бы событие или действие ни произошло в информационной системе, сведения о нем (кто инициировал его, когда и в какое время оно произошло; если при этом были затронуты файлы, то какие) регистрируются в log-файлах. Log-файлы фиксируют дату сеанса связи, информацию о времени связи (времени начала, окончания и продолжительности сеанса связи), статические или динамические IP-адреса, телефонные номера, скорость передачи сообщения, характеристики сеанса связи, включая тип использованных протоколов, сами протоколы, MAC-адрес использованного сетевого оборудования, системное время и др.

IP-адрес (айпи-адрес, от англ. *Internet Protocol Address*) – уникальный сетевой адрес компьютера (сервера, сетевого оборудования) в сети, построенный на основе протокола адресации IP в виде четырех десятичных чисел значением от 0 до 255, разделенных точками, например, 192.168.0.1.

MAC-адрес (от англ. *Media Access Control* – управление доступом к среде, также *Hardware Address*) – это уникальный идентификатор, присваиваемый производителем каждой единице сетевого адаптера используемого оборудования (ноутбука, нетбука, планшетного ПК, смартфона). Он имеет, примерно, следующий вид: 00-04-5F-B2-FC-9F или 00:04:5F:B2:FC:9F.

Следует иметь в виду, что MAC-адрес передается оператору связи только при непосредственном подключении к его оборудованию. Если для подключения используется промежуточное оборудование (например, ADSL-модем, WiFi-маршрутизатор или USB-модем), то MAC-адрес оператору связи не передается. Кроме того, значение MAC-адреса может принудительно изменяться на произвольное самим пользователем, что предусмотрено настройкой соответствующих параметров в операционной системе. Значение MAC-адреса фиксируется не каждым оператором связи. Некоторые производители присваивают одинаковый MAC-адрес всей партии сетевых адаптеров.

Используя бесплатные и общедоступные интернет-сервисы Whois, существует возможность установления сведений о собственнике доменного имени сайта в сети Интернет, а также об организации, осуществившей регистрацию доменного имени и заключившей соответствующий договор с собственником доменного имени, дате регистрации, сроке действия права на это имя, иные данные, на основании которых нетрудно установить лицо, создавшее тот или иной сайт в сети Интернет.

Возможность установления названной информации зависит от того, является ли данный IP-адрес маршрутизируемым («белым»)

в сети Интернет (к такому IP-адресу можно обратиться из любого сегмента сети Интернет) или он относится к частным («серым») IP-адресам (к таким IP-адресам нельзя обратиться из какого-либо другого сегмента сети Интернет напрямую)[1]. Информацию о частных IP-адресах получить с использованием интернет-сервиса Whois нельзя. Технологии получения подобной информации имеют свои особенности исходя из диапазона IP-адресов и носят индивидуальный характер.

При получении доступа в сеть Интерент посредством точек публичного подключения (в организациях общественного питания, транспорта, образования, гостиницах, общественных местах и пр.) электронный журнал (log-файл) сервера организации, предоставляющей услуги по доступу в сеть Интернет, будет содержать следующие данные: IP-адрес, предоставленный лицу в конкретный момент времени, данные о сетевых адресах, к которым был получен доступ с использованием данного IP-адреса, дату, место, время начала и окончания доступа, MAC-адрес сетевой карты устройства, с которого был произведен выход в сеть, номер SIM-карты, через которую произошла авторизация пользователя при подключении к Интернету, операционную систему и браузер его устройства.

В конечном счете сетевые следы позволяют установить лицо, совершившее преступление дистанционным способом. Технология решения данной тактической задачи будет рассмотрена в следующих параграфах, посвященных частным методикам расследования отдельных видов преступлений, совершенных с использованием информационно-коммуникационных технологий.

Следами, позволяющими установить лицо, совершившее неправомерный доступ к охраняемой законом компьютерной информации (путем уничтожения, блокирования, копирования или модификации), находящейся на интернет-сайте, являются:

– сведения об IP-адресах, с которых производится администрирование интернет-сайта, доменного имени и/или IP-адреса, выявление сторонних заходов;

– сведения о запросах, посылаемых при обращениях к интернет-сайту, и поиск среди них тех, что могли использоваться для поиска уязвимостей при обработке запросов на сервере и выдачи закрытой информации, а также при удаленном управлении сервером посредством «шеллов»;

---

[1] IP-адреса относятся к частным, если они принадлежат следующим диапазонам: 10.0.0.1–10.255.255.254, 127.0.0.1–127.255.255.254, 169.254.0.1–169.254.255.254, 172.16.0.1–172.31.255.254, 192.168.0.1–192.168.255.254.

– сведения об ошибках, возникающих в интересующий промежуток времени;

– следы подбора пароля для аутентификации на сервере, на котором настроена работа интернет-сайта;

– программы для удаленного администрирования;

– программы / файлы, которые позволяют получать несанкционированный доступ к сведениям на сервер / копировать информацию на сервере;

– вредоносные программы;

– сведения о загрузке / выгрузке файлов на / с сервера.

Следами, позволяющими установить, откуда была предпринята DoS/DDoS-атака, направленная на блокирование интернет-ресурса, являются:

– период прекращения штатного функционирования сетевого ресурса;

– запросы, которые посылались сетевому ресурсу до прекращения его штатного функционирования, а именно: их количество, промежуток между отправками, содержание запроса;

– IP-адреса, с которых произведена отправка обнаруженных запросов;

– сведения об ошибках, возникающих на сетевом ресурсе, в интересующий период времени;

– сведения о прекращении штатного функционирования сетевого ресурса.

Следами создания, использования и распространения вредоносных программ для ЭВМ являются:

– переписка (в том числе в социальных сетях, на интернет-ресурсах, в программах для мгновенного обмена сообщениями, почтовых клиентах);

– история сетевых соединений;

– вредоносные программы, в том числе эксплойты;

– программы для повышения привилегий в системе;

– командные центры (серверы управления) обнаруженных программ.

Большое количество ценной криминалистически значимой информации содержат социальные сети. Речь при этом идет не только о контенте, который выкладывают пользователи на свои страницы, анализ которого позволяет определить и круг общения пользователя, его образ жизни, увлечения, способы проведения досуга, род занятий, уровень доходов, географию перемещений, семейное положение и состав семьи, используемый автотранспорт, а также иные данные. Каждый пользователь социальной сети имеет персональный иденти-

фикатор (указывается в адресной строке браузера, после доменного имени сайта социальной сети), для получения которого пользователю необходимо пройти процедуру регистрации. Соответственно, в организации, владеющей соответствующей социальной сетью, можно получить данные учетной записи пользователя: указанные им при регистрации анкетные данные, дату и время регистрации, IP-адрес доступа к сети Интернет при регистрации, адрес электронной почты, абонентский номер сотовой связи (для SMS-подтверждения), а также продолжительность использования учетной записи и иные сведения. Заметим, что если указываемый при регистрации адрес электронной почты может быть вымышленным, то номер мобильного телефона, вероятнее всего, будет реальным (хотя, возможно, и зарегистрированным на подставное лицо), поскольку для регистрации в социальной сети требуется SMS-подтверждение путем введения специального кода, направляемого на телефонный номер, указанный при регистрации. Таким образом, для установления лица, фактически использующего SIM-карту, соответствующую номеру мобильного телефона, указанного при регистрации в социальной сети, следует запросить у оператора сотовой связи детализацию звонков, а также данные о способах пополнения финансового баланса SIM-карты. При этом если для пополнения баланса данной SIM-карты использовались электронные кошельки или банковские карты, то информацию о лицах, на которые они открыты, можно получить в соответствующей кредитно-финансовой организации на основании ст. 26 Закона РФ от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности».

Полный перечень информации, подлежащей хранению организатором распространения информации в сети Интернет, к числу которых относятся и социальные сети, предусмотрен п. 3 Правил хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации[1].

[1] О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста,

Кроме того, можно получить сведения о произведенных в социальной сети платежных операциях, а на основании судебного решения – переписку пользователя. Правовую основу получения этой информации составляют приведенные выше Правила.

В организациях, осуществляющих администрирование соответствующей социальной сетью, ведутся электронные журналы регистрации событий в информационной системе – log-файлы, в которых фиксируются следующие действия пользователя: какой IP-адрес у компьютера, с которого пользователь осуществил доступ к странице социальной сети, когда и сколько времени он провел на сайте, что смотрел и скачивал, какой у него браузер.

Отправления электронной почты и соответствующие интернет-сервисы по предоставлению подобных услуг несут значительный массив ценной криминалистически значимой информации. Это не только информация, содержащаяся в тексте самого почтового отправления, но и информация о маршруте его следования в процессе отправки-получения (RFC-заголовок, служебный заголовок, свойства письма, для ознакомления с которыми необходимо открыть электронное письмо и в командной панели выбрать команду отображения свойств письма). Данная информация содержит сведения об IP-адресе, с которого письмо было отправлено, и реальный электронный почтовый ящик[1]. Как правило, IP-адрес отправителя содержится в строках «X-Originating-IP» или «Received: from» свойств электронного почтового отправления.

Криминалистически значимой информацией, которую возможно получить в организациях, являющихся собственниками интернет-сервисов электронной почты, являются: сведения, содержащиеся в учетной записи (аналогично социальным сетям), сеансы доступа к электронному почтовому ящику, произведенные изменения в учетной записи (смена пароля, изменение телефона, контрольного вопроса и пр.), переписка пользователя (по судебному решению).

Правовую основу получения указанной информации составляют: п. 4 ч. 1 ст. 13 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции»; п. 2 ч. 1 ст. 6 и ст. 7 Федерального закона

изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации: постановление Правительства Рос. Федерации от 31 июля 2014 г. № 759 // Собр. законодательства Рос. Федерации. – 2014. – № 32, ст. 4526.

[1] Зачастую при получении письма в поле «От кого» может быть указан произвольный, в том числе не принадлежащий отправителю электронный почтовый ящик.

от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»; п. 7 ст. 185 УПК РФ.

Заметим, что данные сведения можно получить не только от российских организаций – собственников сервисов электронной почты, но и от организаций, зарегистрированных вне юрисдикции Российской Федерации. С 1 июля 2018 г. вступил в силу пп. 2 п. 3 ст. 10.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», согласно которому организатор распространения информации в сети Интернет обязан хранить на территории Российской Федерации:

– информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;

– текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети Интернет до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

Постановлением Правительства Российской Федерации от 31 июля 2014 г. № 759 определен состав информации, подлежащей хранению в соответствии названными требованиями, место и правила ее хранения, порядок ее предоставления уполномоченным государственным органам.

В числе электронных следов, содержащихся в социальных сетях, приложениях электронной почты и сервисах мгновенных сообщений, являются сведения о контактах пользователя информационного ресурса с иными лицами (друзья и подписчики в социальных сетях, абонентские номера из телефонной книги и пр.). Их исследование позволяет наглядно продемонстрировать структуру связей внутри группы; выявить частоту соединений между владельцами мобильных устройств и их контактами с построением диаграммы коммуникативной активности; осуществлять установление общих контактов нескольких лиц; определять наиболее используемые в тот или иной момент времени контакты; осуществлять сортировки контактов по определенным признакам; получать информацию о каждом отображаемом контакте (предпочитаемый тип связи, первую и последнюю дату связи, общее время разговоров и количество принятых и отправленных сообщений). Решение обозначенных задач осуществляется с использованием приведенных выше средств извлечения криминалистически значимой информации из устройств мобильной связи.

В настоящее время широкое распространение получили *системы перевода электронных денежных средств*. Электронные денежные средства – денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность и (или) деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций (п. 18 ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»). Наиболее распространенными сервисами перевода электронных денежных средств в настоящее время являются: Яндекс.Деньги, QIWI-кошелек, WebMoney и др. Функциональные возможности данных систем зависят от того, согласен ли клиент пройти процедуру идентификации в соответствии с требованиями Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Так, без осуществления процедур идентификации клиента предельно допустимый остаток на балансе не может превышать 15 000 руб., ограничения на платежи составляют 40 000 руб. в месяц, снятие наличных не может превышать 5 000 руб. в день и 20 000 руб. в месяц. При осуществлении упрощенной идентификации предельно допустимый остаток на балансе повышается до 60 000 руб., ограничения на платежи и переводы составляют 200 000 руб. в месяц, снятие наличных не может превышать 5 000 руб. в день и 40 000 руб. в месяц. При осуществлении стандартной идентификации предельно допустимый остаток на балансе повышается до 600 000 руб., отсутствуют ограничения на платежи и переводы, ограничения на снятие наличных составляют до 100 000 руб. в день и до 200 000 руб. в месяц.

В зависимости от того, в каком объеме прошел клиент процедуру идентификации, зависит и объем информации, содержащей-

ся в его учетной записи в системе. Приложения 1 к Положениям Банка России от 12 декабря 2014 г. № 444-П «Об идентификации некредитными финансовыми организациями клиентов, представителей клиента, выгодоприобретателей, бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и от 15 октября 2015 г. № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию)доходов, полученных преступным путем, и финансированию терроризма» содержат во многом схожий перечень сведений, получаемых при идентификации (упрощенной идентификации). К таким сведениям относятся: фамилия, имя и отчество (при наличии последнего); дата и место рождения; гражданство; реквизиты документа, удостоверяющего личность; адрес места жительства (регистрации) или места пребывания; идентификационный номер налогоплательщика (при наличии); номера телефонов и факсов (при наличии); иная контактная информация (при наличии); место работы и должность клиента, адрес его работодателя; сведения о целях установления и предполагаемом характере деловых отношений с некредитной финансовой организацией, сведения о целях финансово-хозяйственной деятельности; сведения о финансовом положении; сведения о деловой репутации; сведения об источниках происхождения денежных средств и (или) иного имущества клиента и др. Указанные сведения на основании п. 4 ч. 1 ст. 13 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» и п. 2 ч. 1 ст. 6 и ст. 7 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» могут быть запрошены в организации, оказывающей услуги по осуществлению перевода электронных денежных средств. В ходе расследования по уголовному делу данные сведения можно получить во время выемки.

Кроме того, в организациях, оказывающих услуги по переводу электронных денежных средств по приведенным выше основаниям, возможно получение информации о сеансах доступа к учетной записи (электронному кошельку) за определенный период времени. Значительной ценностью обладают также данные систем видеорегистрации терминалов оплаты.

В соответствии со ст. 26 Закона РФ от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» справки по счетам и вкладам физических лиц, а также справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредит-

ной организацией органам предварительного следствия по делам, находящимся в их производстве, при наличии согласия руководителя следственного органа.

Операторы связи, оказывающие услуги подвижной радиотелефонной (сотовой) связи, на основании ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи», Правил оказания услуг телефонной связи[1], располагают следующей криминалистически значимой информацией:

– о лице, на которое зарегистрирована SIM-карта;

– о входящих и исходящих соединениях;

– о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий;

– о движении денежных средств по счету;

– об индивидуальном номере устройства (IMEI);

– о точном местонахождении устройства в момент соединения (привязка к базовым станциям);

– о других SIM-картах, которые использовались в этом же устройстве;

– о текстовых сообщениях пользователей услугами связи, голосовой информации, изображениях, звуках, видео-, иных сообщениях пользователей услугами связи – до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки[2].

Абонентские устройства мобильной телефонной связи могут содержать следы преступления в виде информации: о IMEI – номере (номерах) устройства; о набранных / полученных звонках; о полученных / отправленных SMS-сообщениях; о переписке и звонках с использованием таких приложений, как Skype, WhatsApp, Viber, Telegram и т. д.; о переписке по электронной почте; о посещенных интернет-ресурсах; о наличии программного обеспечения, следах его установки и работы.

Еще одним ценным источником криминалистически значимой информации, относящимся к числу электронных следов, являют-

---

[1] О порядке оказания услуг телефонной связи: постановление Правительства Рос. Федерации от 9 декабря 2014 г. № 1342 // Собр. законодательства Рос. Федерации. – 2014. – № 51, ст. 7431.

[2] Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи: постановление Правительства Рос. Федерации от 12 апреля 2018 г. № 445 // Собр. законодательства Рос. Федерации. – 2018. – № 17, ст. 2489.

ся данные геопространственной информации. Получившие широкое распространение навигационные приложения, присутствующие в стандартном наборе приложений большинства смартфонов (например, GoogleMaps, Яндекс.Карты и т. п.), используют геоданные мобильных устройств (сведения о их местоположении в определенный момент времени), чтобы показывать более точные результаты поиска на карте, строить более удобные для пользователя маршруты и формировать персональные подсказки. Данные о перемещениях мобильного устройства (смартфона с функцией геолокации) постоянно отправляются на серверы компании – поставщика услуг геолокации и (или) сохраняются непосредственно во встроенной памяти смартфона (в зависимости от настроек приложения геолокации).

В основе работы программ геолокации лежит использование сигналов ГЛОНАСС или GPS передатчиков, которыми оснащаются подавляющее большинство современных мобильных устройств (смартфонов). При невозможности приема сигнала ГЛОНАСС или GPS геолокационные приложения могут использовать информацию базовых станций мобильной связи для приблизительного определения местоположения абонента.

К числу тактических задач расследования, решению которых может способствовать использование геопространственной информации, относятся: установление фигурантов и возможных свидетелей преступления; розыск лиц; установление места и обстоятельств совершения преступления; установление средств совершения преступления; установление алиби лица; розыск похищенного имущества; установление факта и времени нахождения лица в определенном месте; проверка показаний о месте и времени определенного события; установление длительности нахождения лица в определенном месте; проверка факта совместного нахождения разных лиц[1]. Решение указанных задач возможно посредством анализа данных контента картографических приложений с помощью в частности аппаратно-программного комплекса UFED (производство компании Cellebrite, Израиль). Данная программа извлекает географические координаты из различных источников: мобильных устройств и их карт памяти, а также облачных сервисов, на которых хранятся данные программ геолокации. Геолокация представляет собой определение реального географического местоположения электронного

[1] *Гаврилин Ю. В.* Использование возможностей средств навигации в установлении обстоятельств совершения преступлений // Актуальные проблемы борьбы с преступностью: материалы межвузовской науч.-практ. конф. (Тула, 15 марта 2017 г.). Тула, 2017.

устройства, например, радиопередатчика, сотового телефона или компьютера, подключенного к Интернету.

Важно отметить, что, используя данное программное обеспечение, возможно успешное решение вышеназванных тактических задач только при условии использования владельцем мобильного устройства программ геолокации.

Повышению эффективности работы по выдвижению и проверке следственных версий способствуют такие аналитические возможности комплекса UFED, как:

– совместное отображение маршрутов передвижения разных лиц в определенный промежуток времени на единой картографической основе;

– восстановление хронологии событий по имеющимся данным геолокации;

– установление точного времени и даты посещения лицом определенного объекта (места);

– систематизация данных геолокации для их аналитической обработки за счет группировки массивов данных по месту, времени, типам месторасположения, расстоянию и другим критериям.

Тактические основы обнаружения, фиксации и изъятия электронных следов преступления

В соответствии со ст. 85 УПК РФ доказывание состоит в собирании, проверке и оценке доказательств в целях установления обстоятельств, входящих в предмет доказывания. Криминалистическое содержание собирания доказательств состоит в обнаружении, фиксации и изъятии доказательственной информации[1].

Обнаружение доказательственной информации – деятельность по поиску доказательственной информации, базирующаяся на знании закономерностей возникновения следов преступления, приемов и средств их выявления.

Фиксация и изъятие доказательственной информации – деятельность, направленная на запечатление с использованием криминалистических средств и методов выявленной доказательственной информации в установленном законом порядке и приобщение выявленных доказательств (носителей доказательственной информации) к материалам уголовного дела в целях ее сохранения для дальнейших исследования, оценки и использования.

---

[1] *Гаврилин Ю. В., Головин А. Ю., Тишутина И. В.* Криминалистика в понятиях и терминах: учеб. пособие. М., 2006.

Обнаружение доказательственной информации как разновидность поисковой деятельности, осуществляется в рамках производства следственных действий, т. е. регламентированных УПК РФ действий, специально направленных на собирание доказательств (ч. 1 ст. 86 УПК РФ), таких как следственный осмотр, обыск, выемка и др., и иных процессуальных действий, таких как направление требований, поручней и запросов (ч. 4 ст. 21 УПК РФ), а также приобщение в качестве доказательств (ч. 2 ст. 86 УПК РФ) по решению ведущего производство по делу лица материалов, представленных на основании ходатайств участвующих в уголовном процессе частных лиц (обвиняемый, потерпевший и др.) и лиц, оказывающих последним юридическую помощь (защитник, представитель потерпевшего и др.)[1].

Информационная сущность фиксации доказательственной информации[2] в процессе расследования преступлений, совершенных с использованием информационно-коммуникационных технологий состоит в том, что:

1) производится перекодировка компьютерной информации, содержащейся на электронном носителе, в доступную для восприятия человеком форму;

2) компьютерная информация изымается вместе с электронным носителем, на котором она находится, либо копируется на иной носитель, когда изъятие оригинального носителя невозможно или нецелесообразно;

3) обеспечивается сохранение компьютерной информации для неоднократного ее использования в процессе доказывания: при назначении экспертиз, предъявлении в ходе допроса и пр.;

4) устанавливаются обстоятельства, входящие в предмет доказывания (дата и время совершения преступления, электронный адрес, абонентский номер устройства в сети оператора связи, физический адрес места нахождения устройства и пр.);

5) решается вопрос об относимости компьютерной информации;

6) закрепляются сведения о процессуальных способах получения компьютерной информации для решения вопроса о ее допустимости.

При проведении следственных действий, направленных на фиксацию компьютерной информации, имеющей доказательственное значение, необходимо учитывать ряд факторов, влияющих на тактику их производства, а именно:

---

[1] Курс уголовного процесса / А. А. Арутюнян [и др.]; под ред. Л. В. Головко. М., 2016.

[2] См.: Криминалистика: учебник для вузов / Т. В. Аверьянова [и др.]; под ред. Р. С. Белкина. М., 1999. С. 148.

1. Состав и конфигурация информационной системы, количество компьютеров (рабочих станций), находящихся в помещении, в котором планируется производство следственного действия. Важное значение имеет расположение серверов, дислокация рабочих станций, а также информация об использовании собственниками информационной системы облачных хранилищ компьютерной информации. Зачастую при изъятии компьютерной информации в крупных организациях объектом осмотра может являться несколько десятков компьютеров (как серверов, так и рабочих станций), расположенных в различных помещениях, на разных этажах одного здания, в разных зданиях, различных городах и странах. Искомая информация может быть расположена в хорошо охраняемом помещении или облачном хранилище, физически расположенном вне территории Российской Федерации. Следы данной деятельности могут быть оставлены в средствах вычислительной техники, расположенной по всему миру.

2. Использование средств защиты компьютерной информации от несанкционированного доступа, в том числе дистанционно управляемых автономных устройств, предназначенных для экстренного уничтожения информации, и аппаратных, программных, программно-аппаратных средств криптографической защиты информации.

3. Используемые методы размещения информации на электронных носителях, способы ее обработки и форматы представления. Информация, имеющая доказательственное значение, может храниться не только в отдельных текстовых, графических, мультимедийных файлах, но и в базах данных (в том числе распределенных), файлах, имеющих специфическую структуру, для интерпретации которых необходимы специализированное оборудование и программное обеспечение. Компьютерная информация может преобразовываться как с помощью общераспространенных прикладных программ, так и узкоспециализированного программного обеспечения, а также уникальных (созданных под конкретную задачу) программ. Требуемая информация может находиться на одном или нескольких компьютерах, серверах, высокоскоростных RAID-массивах. Устройства, предназначенные для хранения компьютерной информации, становятся все более миниатюрными, расширяются возможности их маскировки.

Как уже отмечалось, основными следственными действиями, направленными на обнаружение, фиксацию и изъятие электронных следов преступления и имеющими существенную специфику, явились следственный осмотр (включая осмотр места происшествия,

предметов, документов), обыск (в жилище, ином помещении, личный), выемка (электронных носителей информации, электронных сообщений), назначение экспертизы.

Рассмотрим тактические особенности производства перечисленных следственных действий. При этом следует отметить, что все они (за исключением назначения экспертизы) имеют единые тактические основы, включающие в себя деятельность на подготовительном, рабочем и заключительном этапах их производства. Подготовительный этап включает в себя две последовательные стадии: до выезда на место производства следственного действия и по прибытии на него. Рабочий этап также включает в себя обзорную и детальную стадии.

Эффективность проведения следственного действия, направленного на обнаружение, фиксацию и изъятие электронных следов преступления, определяется тщательностью подготовки к нему. В число подготовительных мероприятий, проводимых до выезда на место его проведения, входит:

– изучение материалов уголовного дела, обобщение и систематизация ориентирующей информации о предмете поиска, месте производства следственного действия и личности подозреваемого;

– определение круга и обеспечение явки необходимых участников (включая необходимых специалистов и понятых, обладающих знаниями в сфере информационно-коммуникационных технологий, способных осознавать содержание следственного действия, поисковых операций и их результатов, а также сотрудников оперативных подразделений и подразделений силовой поддержки, призванных обеспечить внезапность проникновения следственной группы в помещение, в котором будет проводиться следственное действие, и блокирование элементов управления информационной системой);

– определение состава и конфигурации информационной системы, предположительно содержащей электронные следы, решение вопроса о целесообразности проведения предварительных оперативно-розыскных (оперативно-технических) мероприятий по установлению местонахождения, состава и функционального назначения средств вычислительной техники, наличия на них специальных аппаратных и (или) программных средств защиты информации и возможностей доступа к защищаемой информации, используемых операционных систем и программного обеспечения, мест хранения общих файлов данных и резервных копий, паролей администраторов системы, зарегистрированных имен и паролей пользователей;

– мысленное моделирование возможностей обстановки следственного действия, последовательности поисковых действий, место-

нахождения лиц, осуществляющих администрирование и эксплуатацию информационной системы, способов и технологии изъятия компьютерной информации, ее носителей и иного оборудования с учетом возможности размещения криминалистически значимой компьютерной информации на сетевых ресурсах третьих лиц, в том числе в облачных хранилищах данных;

– прогнозирование возможности оказания противодействия расследованию и производству следственного действия, учет возможностей маскировки объектов поиска (брелок, интерактивная фоторамка, детская игрушка, сувенир и пр.).

Решение указанных задач осуществляется следователем по согласованию со специалистом, привлекаемым к участию в следственном действии.

Подготовка к проведению следственного действия, направленного на обнаружение и изъятие электронных следов, продолжается и по прибытии на место его проведения. На данной стадии ключевыми задачами являются:

– фиксация времени начала производства следственного действия;

– обеспечение внезапности при проникновении (входе) в помещение, в котором будет проводиться следственное действие;

– взятие под физический контроль всех помещений, где могут находиться элементы информационной системы (серверы, сетевое оборудование, рабочие станции, электронные носители информации или иная компьютерная техника), а также узлы электроснабжения с целью недопущения к указанным объектам доступа кого-либо из числа лиц, эксплуатирующих или администрирующих информационную систему;

– отключение сетевых подключений, включая Wi-Fi-соединения;

– установление запрета кому бы то ни было, за исключением специалиста, производить любые манипуляции с электронными носителями информации и сетевым оборудованием, а также электроснабжением;

– выяснение у системного администратора информационной системы: когда и каким образом последний раз производилось резервное копирование компьютерной информации, структуры информационной системы, местонахождения носителей этой информации, паролей, электронных ключей доступа к информационным ресурсам, паролей для входа в BIOS и выхода из режима гибернации, а также перечня лиц, имеющих права доступа к тем или иным элементам информационной системы, и их прав;

– определение алгоритма выполнения действий каждым участником следственного действия, разъяснение им их прав и обязанно-

стей, инструктаж о мерах предосторожности при работе с электронными носителями информации.

Обзорная стадия рабочего этапа проведения следственных действий, направленных на обнаружение и изъятие электронных следов, начинается с описания общей конфигурации и состава информационной системы. Осуществляется фиксация входящих в нее объектов (элементов), их морфологических признаков и технических характеристик (тип, название, комплектация, индивидуализирующая объект информация – маркировочные обозначения, серийные номера и пр.), а также местонахождения и взаимного расположения. Производится диагностика наличия средств моментального уничтожения информации (генераторов магнитных полей, электромагнитных пушек и пр.)[1]. Составляется схема расположения компонентов информационной системы, средств компьютерной техники, находящихся в помещениях, в которых проводится следственное действие, производится ориентирующая и обзорная фотосъемка. Затем осуществляется фиксация (с использованием узловой фотосъемки) выполняющихся на момент начала следственного действия программ (приложений) и изображения на мониторах отдельных компьютеров, входящих в состав информационной системы, а также проверка соответствия показаний даты и времени, установленных в настройках компьютерной техники, текущим значениям. Последнее – обязательно при изъятии данных систем видеорегистрации. Завершается стадия принятием следователем решения на основании информации, полученной от специалиста, о порядке и последовательности производства детальной стадии.

На детальной стадии рабочего этапа проведения следственных действий, направленных на обнаружение и изъятие электронных следов преступления, необходимо с участием специалиста:

– осмотреть и скопировать информацию на включенных компьютерах, снять образ оперативной памяти работающих устройств. При этом рекомендуется следующая последовательность сохранения так называемой короткоживущей информации

[1] Устройства, предназначенные для безвозвратного стирания информации с жестких магнитных дисков под действием внешнего магнитного поля, делают повторное использование жесткого диска невозможным. Для уничтожения данных с жесткого диска (срабатывания системы) нередко достаточно нажать скрытую кнопку с помощью шариковой ручки или карандаша. Существуют энергонезависимые устройства уничтожения информации, выполненные в виде отдельного модуля (в виде сейфа), или устанавливается в 3,5 дюймовый отсек компьютера и использующие его электропитание. Управление такими устройствами может вестись по радиоканалу либо автоматически (срабатывает при попытке поднять системный блок с поверхности стола), либо от сигнала датчика движения.

из энергозависимых носителей: о текущей сетевой конфигурации; о текущих пользовательских сессиях; о содержимом оперативного запоминающего устройства (исполняемые программы (задачи, процессы), о списке процессов, открытых файлах (в том числе временных), образцах трафика, введенных ключах и паролях, сетевой конфигурации (динамически присвоенный IP-адрес, маска подсети, счетчики сетевых интерфейсов, таблица маршрутизации), текущем времени;

– извлечь энергонезависимые электронные носители информации (например, карты памяти, флеш-накопители и т. п.), используя корректные программные средства и процедуры;

– произвести осмотр электронных носителей неразрушающими методами с целью определения тех из них, которые будут подлежать изъятию;

– по ходатайству владельца электронного носителя информации или собственника информационной системы может быть произведено копирование информации с подлежащих изъятию носителей с соблюдением юридических процедур, подробно рассмотренных выше.

Для повышения эффективности решения последней задачи с 2011 г. в экспертно-криминалистических подразделениях МВД России используется программно-аппаратный комплекс «Оттиск», предназначенный для создания копий содержимого, а также восстановления информации, хранящейся (хранившейся) в микросхемах памяти SD, SM, MMC, USB Flash, MemoryStick, CompactFlash и др., в том числе с неисправным контроллером доступа. Комплекс позволяет осуществлять доступ к информации, хранящейся на электронных носителях, производить автоматизированный сбор информации о накопителях на жестких дисках, копирование данных без внесения изменений на исходный носитель, созданий копии накопителя на жестких дисках[1]; взаимодействовать со всеми современными носителями информации; создавать две копии информации одновременно; осуществлять контроль целостности копии, а также выполнять иные функции.

В настоящее время существует довольно широкий спектр средств криминалистической техники, позволяющей производить посекторное (побайтовое) копирование информации с электронных носителей, включая блокираторы записи, производящие запись на свой внутренний диск, тем самым обеспечивая неизменность информации на исследуемом компьютере;

[1] Создание образа жесткого диска объемом 1 Тб производится менее чем за 4 часа, что от 3 до 10 раз быстрее аналогичных средств копирования.

портативные криминалистические накопители позволяют хранить десятки терабайт компьютерной информации; дубликаторы информации обеспечивают быстрое копирование на скорости более чем 7 Гб/мин, адаптированы для использования в «полевых» условиях и обеспечивающих 100 % защиту от записи исследуемого диска.

Широко используются специальные аппаратно-программные комплексы для обнаружения и извлечения криминалистически значимой информации. Так, программный комплекс «Мобильный криминалист» позволяет извлекать данные из большинства моделей мобильных устройств (на платформе iOS, Android, BlackBerry, WindowsPhone и др.); импортировать резервные копии устройств, а также их физические образы (JTAG, Chip-off); получать данные из облачных хранилищ по логину/паролю или токену: iCloud, Google, Microsoft, Email и из др. облачных сервисов; загружать и анализировать биллинги операторов сотовой связи; извлекать контакты, сообщения, звонки, файловую систему, местоположения и удаленную информацию; находить общие места пребывания нескольких лиц и строить маршруты их передвижения на карте; выявлять общие связи между несколькими устройствами и устанавливать круг общения пользователя; просматривать все события в хронологическом порядке и выявлять периоды активности пользователя; анализировать контент по ключевым словам, регулярным выражениям и др., использовать поисковые фильтры для быстрого обнаружения необходимой информации. Кроме того, комплекс позволяет производить исследование структуры файловой системы (включая удаленные данные и таблицы баз данных), извлекать имена пользователя, пароли, файлы истории, временные файлы, создаваемые в процессе работы отдельных приложений, анализировать геопространственную информацию о предыдущих местоположениях подозреваемого.

Заключительный этап проведения следственных действий, направленных на обнаружение и изъятие электронных следов преступления, включает в себя следующие основные мероприятия:

– изъятие протоколов работы сетевых устройств, систем авторизации пользователей, сетевого трафика и т. п.;

– выключение работающих средств компьютерной техники с использованием штатных процедур корректного завершения работы;

– упаковка и опечатывание изымаемых электронных носителей информации;

– копирование файла с видеозаписью следственного действия на неперезаписываемый электронный носитель (оптический диск),

который помещается в конверт, клапан которого опечатывается и скрепляется подписями участников;

– отражение перечня изъятого в протоколе, его процессуальное оформление в соответствии с требованиями ст. 166, 167 и 180 УПК РФ.

Упаковка изымаемых электронных носителей информации должна отвечать следующим требованиям: исключение возможности непроцессуальной работы с электронными носителями; недопущение физического повреждения, разукомплектования носителя, повреждения находящейся на нем информации. С указанной целью производится опечатывание клапанов упаковки таким образом, чтобы вскрытие было невозможно без повреждения опечатывающих наклеек. Сам электронный носитель целесообразно помещать в экранирующую тару («мешок Фарадея»).

При изъятии мобильных устройств (планшетных компьютеров, смартфонов) в протоколе осмотра указывается тип, марка изъятого электронного носителя информации, что в процессе изъятия клавиши устройства не нажимались, касания сенсорного экрана не производились, аккумулятор и съемные накопители не извлекались. Устройство в состоянии гибернации (засыпания) упаковывается так, чтобы исключить всякий доступ к органам его управления (экрану, клавишам) и разъемам без повреждения упаковки.

Определенной спецификой обладает рабочий этап осмотра ранее изъятого электронного носителя информации, включая мобильное устройство (планшетный компьютер, смартфон). При этом производится изучение внешней упаковки на предмет повреждений, соответствия надписей на упаковке ее содержимому, определения типа, вида, параметров устройства, описания технического состояния (внешний вид, размеры, целостность корпуса, признаки), разъемов, а также проверка на наличие вредоносных программ, поиск скрытых файлов, непосредственное изучение контента.

При осмотре содержимого интернет-страниц или сайтов может быть решено значительное число тактических задач, в частности установление события, способа, времени, последствий и обстоятельств совершения преступления, данных о личности подозреваемых, состояния средств защиты информации, сведений о количестве посещений ресурса и др. Решению данных задач может способствовать анализ содержания контента интернет-страницы и баз данных сайта, определение времени размещения соответствующей информации, выявление нарушений в работе сайта или изменений в размещенной информации, порядок аутентификации пользователей информации, данные систем учета посетителей сайта и т. д.

При проведении осмотра необходимо использовать лицензионное программное обеспечение с указанием в протоколе номера лицензии. Все действия, производимые начиная с момента входа в интернет-браузер, включая процесс изготовления снимков изображения экрана, подлежат отражению в протоколе. Полученные в ходе осмотра распечатки содержимого экрана прилагаются к протоколу и подписываются всеми участниками следственного действия. Для получения снимков изображения экрана необходимо нажать клавишу PrtSc, открыть программу редактирования текстов или изображений, вставить полученное изображение, распечатать страницы и сохранить полученные данные на неперезаписываемом электронном носителе (или носителе с включенной функцией защиты от записи).

Следует отметить, что нередко допускаются следующие ошибки при изъятии компьютеров, объединенных в локальную вычислительную сеть:

– рабочие станции, при последующем осмотре которых выясняется, что искомая информация хранилась на сервере;

– серверы, но искомая информация находилась на компьютерах конкретных работников и изъята не была;

– бездисковые рабочие станции;

– все средства вычислительной техники организации (персональные компьютеры, серверы, машинные носители информации, видеорегистраторы, мобильные телефоны и т. д.);

– базы данных, копии баз данных без средств их интерпретации, сведений об особенностях их конфигурационных настроек и т. п.

Надлежащим же порядком действий следует признать предварительное установление местонахождения искомой информации и общей конфигурации сети:

– составление схемы расположения средств вычислительной техники в помещениях, в которых проводится следственное действие, фотофиксация обстановки в помещении, а также самих средств вычислительной техники по правилам обзорной и узловой фотосъемки;

– осуществление поиска сведений об именах пользователей и паролях доступа к различным информационным ресурсам (путем индивидуального опроса персонала, при осмотре рабочих мест и записей сотрудников, используя оперативно-розыскные методы и средства);

– производство осмотра и копирования информации на включенных компьютерах в случаях наличия на них криптоконтейнеров,

необходимости проведения в дальнейшем исследования распределенных баз данных, возможности доступа к облачным хранилищам и т. п.

– изъятие исключительно необходимых электронных носителей информации.

Допускаются тактические ошибки и в процессе изъятия компьютерной информации в условиях активного противодействия расследованию. Основным недостатком при этом является то, что с момента начала следственного действия до момента изъятия компьютерной информации проходит время, достаточное для уничтожения искомой информации и/или содержащих ее объектов. В целях недопущения указанных негативных последствий необходимо обеспечить максимально эффективное использование фактора внезапности при производстве следственного действия, а именно: использование возможностей оперативно-розыскной деятельности для предварительного установления состава и конфигурации информационной системы, расположения ее основных элементов и узлов; обеспечение достаточного количества привлеченных сил и средств, обеспечивающих блокирование ключевых элементов информационной системы; неожиданное вхождение в обыскиваемое помещение; исключение доступа кого бы то ни было к основным элементам информационной системы.

§ 3. Экспертно-криминалистическое обеспечение расследования преступлений, совершенных с использованием информационно-коммуникационных технологий

Расследование практически любого преступления, совершенного с использованием информационных и коммуникационных технологий, не обходится без назначения и производства экспертиз. Подготовка настоящего параграфа осуществлена на основе материалов, предоставленных ЭКЦ МВД России.

Согласно ст. 9 Федерального закона от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» судебная экспертиза – процессуальное действие, состоящее из проведения исследований и дачи заключения экспертом по вопросам, разрешение которых требует специальных знаний в области науки, техники, искусства или ремесла и которые поставлены перед экспертом судом, судьей, органом дознания, лицом, производящим дознание, следователем, в целях установления обстоятельств, подлежащих доказыванию по конкретному делу.

Приложение № 2 к приказу МВД России от 29 июня 2005 г. № 511 содержит перечень родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, в число которых входит и компьютерная экспертиза. Последняя представляет собой *род криминалистической экспертизы, проводимой в целях получения доказательств на основе изучения закономерностей функционирования информации в средствах вычислительной техники*[1].

Основными задачами компьютерной экспертизы являются:

– поиск на электронном носителе (в средствах вычислительной техники) информации, обладающей определенными характеристиками (содержание, свойства);

– поиск на электронном носителе следовопределенных манипуляций с компьютерной информацией в процессе ее создания, обработки, изменения, копирования, уничтожения и пр.;

– определение свойств и функциональных возможностей программного обеспечения для средств вычислительной техники и его классификация;

– определение свойств и функциональных возможностей средств вычислительной техники и их периферийных устройств;

– установление определенных обстоятельств, имеющих значение для дела, по компьютерной информации.

Объектами компьютерной экспертизы являются:

– компьютерная информация, находящаяся на электронных носителях;

– информационные системы и их отдельные компоненты;

– микропроцессорные устройства, не являющиеся компьютерной техникой в традиционном понимании.

Следует отметить, что в связи с широким распространением бесконтактных способов совершения преступлений номенклатура объектов исследования компьютерных экспертиз претерпевает существенные изменения. Так, все больший удельный вес в числе объектов исследования занимают средства мобильной связи (до 90 % по уголовным делам, связанным с незаконным сбытом наркотических средств, совершенным дистанционным способом).

Кроме того, практика производства компьютерных экспертиз свидетельствует, что решение экспертных задач исключительно инструментальными методами не всегда представляется возмож-

[1] Порядок назначения судебных экспертиз, исследований и использования экспертно-криминалистических учетов в органах внутренних дел Российской Федерации: справ. пособие / под ред. П. Л. Гришина. М., 2016. С. 137.

ным. В частности, для расшифровки криптоконтейнеров, получения доступа к заблокированным мобильным устройствам, расшифровки физического образа мобильного устройства, а также решения иных экспертных задач существенную помощь эксперту способны оказать сведения о паролях, кодах, ключах, которые можно получить в ходе производства оперативно-розыскных мероприятий и (или) следственных действий.

Определенной спецификой обладает исследование информации, находящейся в облачных хранилищах данных. Последние в автоматическом режиме осуществляют сохранение резервных копий информации, находящейся в мобильных телефонах, планшетных компьютерах, иных устройствах, в зависимости от настроек операционной системы. Поскольку интернет-ресурсы, включая облачные хранилища, непосредственно не могут быть представлены для исследования эксперту, подлежащая исследованию информация должна быть предварительно извлечена из такого хранилища в рамках производства соответствующих следственных действий, например, осмотра предметов и документов.

Весьма специфичным объектом исследования выступает информация, находящаяся в оперативной памяти изъятого устройства. В целях сохранения и фиксации и последующего исследования информации возможно использование фотографирования экрана устройства либо отключение устройства от сети связи путем перевода его в авиарежим. Учитывая, что доступ к данной информации после перезагрузки устройства станет невозможным либо она буде автоматически удалена, объектом исследования в таких случаях, исходя из сроков производства экспертизы, может выступать либо само устройство (упакованное таким образом, чтобы исключить манипуляции с ним без повреждения упаковочного материала), либо протоколы следственных действий, содержащие описание и снимки экрана.

В процессе производства компьютерной экспертизы используются **специальные знания** в области информатики и вычислительной техники, информационных систем и технологий, программной инженерии, информационной безопасности, электроники, радиотехники и систем связи, инфокоммуникационных технологий.

Вопросы, выносимые на разрешение компьютерной экспертизы, должны удовлетворять следующим требованиям.

1. При постановке вопроса необходимо использовать нормативно определенный понятийный аппарат, исключающий сленговые, жаргонные термины («винт» – накопитель на жестких магнитных дисках, «логи» – протоколы, «логин» – имя пользователя и т. п.).

При этом целесообразно использовать терминологию, определенную ГОСТ 15971-90 «Системы обработки информации. Термины и определения», ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», ГОСТ Р 52292-2004 «Информационная технология. Электронный обмен информацией. Термины и определения», иными нормативными актами.

2. В случае отсутствия нормативного определения того или иного термина необходимо использовать терминологию, применяемую разработчиками аппаратных средств и программных продуктов в технической документации.

3. Вопрос должен быть четко сформулирован и не допускать неоднозначного толкования.

4. Вопрос должен быть направлен на установление конкретного обстоятельства расследуемого события. При этом действующее уголовно-процессуальное законодательство предоставляет эксперту право расширить объем исследования, в том числе предоставить заключение по вопросам, хотя и не обозначенным в постановлении о назначении судебной экспертизы, но имеющим отношение к предмету экспертного исследования.

5. Формулировка вопроса не должна касаться содержания отдельных этапов исследования информации. Так, описание характеристик носителей информации и особенностей размещения информации на них, восстановление и исследование информации среди удаленных файлов являются обязательным этапом исследования информации[1].

6. Вопросы не должны быть направлены на получение информации справочного характера (разъяснение значения используемой терминологии, предоставление информации относительно общих принципов функционирования техники определенного типа, высказывание суждения, мнения и пр.), для ответа на которые не требуется производство исследования объектов.

7. Вопросы не должны носить правового характера, т. е. быть направленными на правовую оценку деяния, а также выходить за пределы компетенции эксперта, т. е. его специальных знаний. Данное обстоятельство прямо отмечено в п. 4 Постановления Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам».

---

[1] *См.: Саенко Г. В., Тушканова О. В.* Исследование компьютерной информации: типовая экспертная методика // Типовые экспертные методики исследования вещественных доказательств / под ред. Ю. М. Дильдина; общ. ред. В. В. Мартынова. М., 2010. Ч. 1.

8. Вопросы должны соответствовать существующей методической и технической базе, уровню подготовки и инструментальному оснащению экспертов того экспертного учреждения, которому назначается экспертиза.

9. Вопросы должны соответствовать представляемым на исследование объектам.

Наиболее распространенными при назначении компьютерной экспертизы являются *информационно-поисковые задачи* по исследованию компьютерной информации, содержащейся на электронных носителях, соответствующей определенным критериям. При этом перед экспертом ставятся следующие вопросы:

1. Имеется ли на представленных на исследование машинных носителях (дать перечень) информация, содержащая следующие ключевые слова: (дать перечень ключевых слов)?

2. Имеется ли на представленных на исследование машинных носителях (дать перечень) информация о (указать, о чем именно)?

Исследование начинается с экспертного осмотра, в процессе которого описывается и фотографируется упаковка объектов, представленных на экспертизу, извлекаются и фотографируются сами объекты исследования с указанием их габаритных размеров, цвета, расположения органов управления, кнопок, индикаторов, разъемов, наклеек, описанием индивидуализирующих особенностей (в том числе повреждений, числовых и буквенных обозначений и пр). При наличии на устройстве энергонезависимой памяти фиксируются настройки даты и времени и сопоставляются с текущими значениями.

В начале исследования используемое стендовое оборудование приводится в режим защиты от записи, производится его подключение к исследуемому объекту и устанавливается структура расположенной на нем информации: количество, наименование и размер разделов; наличие неразмеченного пространства и его размер; наименование файловой системы в каждом разделе; размер занятого в разделе пространства; значение хеш-функции для машинного носителя (опционально).

Затем производится посекторное копирование информации с исследуемых объектов (электронных носителей носителей) на дополнительные носители. Дальнейшее исследование информации производится по полученным копиям. При этом, в зависимости от поставленных на разрешение эксперта вопросов, может осуществляться восстановление удаленной информации, проверка информации антивирусным программным обеспечением, определение области поиска представляющей интерес информации с учетом наличия на объекте исследования зашифрованных обла-

стей, файлов – криптоконтейнеров, файлов-архивов, областей дискового пространства, закрытых паролем. Решается вопрос о возможности расшифровки / доступа к скрытым (зашифрованным) данным.

Ключевым элементом экспертного исследования является просмотр либо экспериментальный запуск программного обеспечения, имеющегося на объекте исследования, в целях установления его функциональных характеристик. Экспериментальный запуск производится исключительно на аппаратно-программном комплексе эксперта. Следует отметить, что такие исследования проводятся не только сотрудниками правоохранительных органов (экспертами в области компьютерной экспертизы), но и работниками сторонних организаций (вирусными аналитиками), использующими в своей работе специализированные базы данных вирусных кодов, антивирусные энциклопедии, методы статического и динамического анализов, иной специфический инструментарий, методологию и программное обеспечение.

Обнаруженная информация по возможности приводится к формату, пригодному для поиска и просмотра, и добавляется к области поиска. Просмотр информации можно осуществлять как с помощью программного обеспечения, имеющегося на аппаратно-программном комплексе эксперта, так и с помощью программного обеспечения, имеющегося на объектах исследования.

Если объем искомой информации значительный и позволяет сформировать приложение к заключению эксперта на бумажном носителе, то информация может быть распечатана частично. После чего производится копирование информации на CD- и DVD-диски однократной записи, о чем указывается в заключении эксперта. Запись информации на диск должна производиться без изменения формата, свойств и метаданных, после чего на нерабочей поверхности CD- или DVD-диска с помощью специального маркера выполняется пояснительная надпись, заверенная подписью эксперта, с указанием номера и даты экспертизы, номера приложения.

Определенной спецификой обладает *технология поиска информации, содержащейся в абонентских устройствах подвижной телефонной связи (сотовых телефонах)*.

Перед экспертом могут быть поставлены вопросы:

1. Имеется ли в представленном на экспертизу абонентском устройстве, установленных в нем SIM-карте и карте памяти созданная в процессе его эксплуатации информация: список контактов определенных лиц или абонентских номеров, отправленные и при-

нятые SMS-сообщения определенного содержания, аудио-, видео- и графические файлы, последние исходящие и входящие вызовы, данные программ геолокации, свидетельствующие о нахождении абонентского устройства в определенном месте в определенное время, и др.

2. Каково значение IMEI, представленного на исследование абонентского устройства?

3. Имеется ли в памяти абонентского устройства программное обеспечение, позволяющее производить определенные действия (дать перечень), например, получать скрытно от пользователя SMS-сообщения, скрытно от пользователя отправлять SMS-сообщения на определенный абонентский номер, получать и передавать сведения об абонентском устройстве без уведомления пользователя?

4. Производился ли запуск на абонентском устройстве программного обеспечения, способного выполнять скрытно от пользователя не запланированные им функции?

5. Имеется ли у абонентского устройства функция выхода в сеть Интернет? Если да, то имеются ли данные об обращении к определенным интернет-ресурсам?

Поиск и исследование информации в процессе экспертного исследования проводятся в следующей последовательности:

1. Получение физического дампа памяти абонентского устройства с использованием таких средств криминалистический техники, как «XRY», «UFED», «Мобильный криминалист», а также специального программного обеспечения.

2. В зависимости от стоящих перед экспертом задач может осуществляться с использованием специализированных программ (R-studio, UFS Explorer, Belkasoft, AccessData, EnCase и др.) восстановление удаленной информации.

3. Анализ установленного, а также не установленного, но имеющегося на устройстве программного обеспечения и приложений.

4. Проверка всей имеющейся информации антивирусным программным обеспечением.

5. Поиск интересующей информации, исходя их обстоятельств дела и вопросов, поставленных перед экспертом. При этом из выборки исключается штатное программное обеспечение, стандартные приложения, информация, созданная ранее определенной даты.

6. Файлы, представляющие интерес, исследуются с отражением в заключении эксперта их функциональных возможностей, активированных функций (например, разрешение на доступ в сеть Интернет, отправление, прием и удаление SMS-сообщений, полу-

чение информации о номере телефона, серийном номере, информации о вызовах, доступе к данным контактов, медиа-файлам, камере, микрофону, фотографиям, разрешение на демонстрацию сообщений поверх окон и пр.).

7. Для углубленного изучения программный файл может быть преобразован в код, доступный для восприятия на соответствующем языке программирования, например, Java. Для этого можно воспользоваться программой Dex2Jar либо Android SDK.

8. В зависимости от обстоятельств дела может производиться статический и динамический анализ программного обеспечения. В последнем случае оно запускается на аппаратно-программном комплексе эксперта. При этом фиксируются его возможности отправления и получения данных о сборе и отправке пользовательских данных, производимых криптографических операциях, создаваемых и удаляемых файлах и пр.

9. На основании оценки результатов статического и динамического исследования делается вывод о соответствии выявленной информации о программе обстоятельствам дела, а также наличии (отсутствии) на устройстве искомой информации, в частности:

– в каталоге (наименование) мобильного устройства имеется программное обеспечение (наименование), позволяющее производить следующие действия (перечень действий: получать SMS-сообщения, отправлять SMS-сообщения на номер..., управлять сетевыми соединениями, организовывать соединение с ... адресом, получать и передавать сведения о мобильном устройстве и т. д.) без уведомления пользователя. В памяти мобильного устройства имеются следующие сведения о его загрузке (дать перечень сведений) и работе (дать перечень сведений);

– в памяти мобильного устройства имеются сведения о (дать перечень сведений: о получении SMS-сообщений с номера..., с текстом... и т. п.; об отправлении SMS-сообщений с номера..., с текстом...; об обращении к интернет-ресурсам... и т. д.);

– в памяти мобильного устройства программное обеспечение, позволяющее производить следующие действия (дать перечень действий) без уведомления пользователя, не обнаружено;

– в памяти мобильного устройства сведения о ... (дать перечень) не обнаружены.

При *исследовании информации, содержащейся на магнитной полосе платежных пластиковых карт,* перед экспертом могут быть поставлены следующие вопросы:

1. Какая информация имеется на магнитной полосе пластиковой карты, представленной на исследование?

2. Соответствует ли информация, записанная на магнитную полосу пластиковой карты, информации, имеющейся в элементах внешнего оформления данной карты?

3. Может ли представленная на исследование пластиковая карта быть воспринята в технологии функционирования платежной системы в качестве платежной (при условии использования информации, записанной на магнитную полосу карты)? (на определенную дату или период времени).

При *исследовании информации, содержащейся на платах игровых автоматов,* эксперт, как правило, отвечает на следующие вопросы:

1. Как атрибутируют (именуют) себя программы, имеющиеся на представленных электронных платах?

2. Каковы настройки и статистика работы устройств, из которых изъяты представленные электронные платы?

3. Соответствуют ли показания даты и времени, имеющиеся на представленных электронных платах, текущим показаниям даты и времени?

Для ответа на вопросы эксперт может применять систему манипуляции с ключами (механическими или магнитными) и клавишами игрового автомата или использовать специализированное оборудование, позволяющее физически подключать к компьютеру наиболее распространенные типы плат игровых автоматов с последующим документированием системных настроек игрового автомата, денежной и игровой статистики.

В рамках судебной компьютерной экспертизы *информации, содержащейся в системах видеорегистрации,* эксперт может помочь следователю получить доступ к видеоинформации (мультимедиа информации), а также восстановить удаленную или поврежденную информацию.

Задача *определения принадлежности программ и данных к конкретным классам,* как правило, решается в контексте расследования нарушения авторских и смежных прав на программы и базы данных. При этом эксперт может ответить на следующие вопросы:

1. Имеются ли на (дать перечень объектов) произведения (дать перечень произведений)? (при наличии образцов для сравнительного исследования).

2. Имеются ли на (дать перечень объектов) произведения, атрибутирующие себя как (дать перечень наименований)? (при отсутствии образцов для сравнительного исследования).

3. Имеются ли на (дать перечень объектов) произведения, у которых в качестве правообладателя указаны (дать перечень наи-

менований)? Если да, то какие сведения о наименовании / правообладателях имеются в данных произведениях? Если да, то какие сведения о дате и времени установки программных продуктов (для установленного программного обеспечения) / создания и последнего сохранения произведений имеются в представленных объектах? Если да, то какие сведения о пользователях программных продуктов, ключах установки и т. п. имеются в представленных объектах? (для установленного программного обеспечения).

4. Появляются ли при воспроизведении произведения сообщения об ограничении его функциональных возможностей?

5. Имеются ли на (дать перечень объектов) программные продукты, с помощью которых можно совершать следующие действия (дать перечень действий)?

6. Имеются ли на (дать перечень объектов) сведения о (дать перечень сведений)? (формулировка вопроса зависит от обстоятельств дела, объектов, представляемых на экспертизу, и должна быть предварительно согласована с экспертом).

Задача определения возможности совершения каких-либо действий с помощью средств компьютерной техники решается путем проведения соответствующих экспертных экспериментов. Объем и порядок проведения экспериментов зависят от предварительного изучения материалов дела, документации на объекты, представленные на исследование (при наличии), сведений, полученных от специалистов в конкретной предметной области.

В настоящее время *идентификационная задача установления материальных объектов* по компьютерной информации проводится только в комплексе с другими видами экспертиз (используются файлы, информация в которых получена в результате конформного преобразования идентификационных свойств объекта).

Решение задачи *установления фактических обстоятельств совершения преступления* (имел ли место факт выхода в сеть Интернет, факт передачи денежных средств с помощью конкретного программного обеспечения и т. п.) также может иметь комплексный характер.

В последнее время становится востребованным исследование так называемых *больших данных* (Bigdata), в ходе которого анализируются и сопоставляются между собой массивы информации, получаемые из различных источников (от операторов сотовой связи, центров управления дорожным движением, органов, регистрирующих сведения о населении и его имуществе, из социальных сетей, компьютеров и мобильных телефонов и т. д.). В процессе исследования такой информации можно получить сведения, которые помогут ограничить

круг лиц, подозреваемых в совершении преступления, установить связи преступника, его имущественное положение и многое другое.

Одной из проблем организационного характера, возникающих при назначении компьютерной экспертизы, является недостаточное количество экспертов, имеющих соответствующий допуск, длительность их производства, а также существенная стоимость при проведении экспертизы в иных учреждениях (от 15 до 300 тыс. руб. за одну экспертизу). В отдельных субъектах Российской Федерации (например, в МВД по Республике Тыва) специалисты данной экспертной специальности вообще отсутствуют, а в ряде подразделений штатная численность составляет от 1 до 3 единиц.

Длительность проведения экспертиз является одной из основных причин продления процессуальных сроков по уголовным делам указанной категории. Из-за нехватки экспертов, имеющих допуск к их производству, очередь составляет от 3 до 6 месяцев. Так, по уголовному делу, возбужденному СО ОМВД России по Камызякскому району Астраханской области по факту несанкционированного снятия денежных средств с банковской карты М., компьютерная экспертиза ввиду очередности была исполнена лишь спустя 5 месяцев. При этом, согласно заключению эксперта, ответить на поставленные вопросы следователя о наличии вредоносных программ не представилось возможным, так как планшетный компьютер находился в заблокированном состоянии.

Загруженность экспертов обусловлена также привлечением их в качестве специалистов при изъятии и осмотрах следователями электронных носителей в соответствии с ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ.

Однако данные требования уголовно-процессуального закона направлены на сокращение сроков проведения судебных экспертиз и исследований путем максимального использования знаний специалистов для оптимизации количества изымаемых объектов, непосредственно имеющих значение для расследования уголовного дела.

Разрешение данной проблемы возможно с привлечением к участию в процессуальных действий специалистов сторонних организаций.

Так, раскрытию преступления по уголовному делу, возбужденному СУ УМВД России по г. Саранску по признакам преступления, предусмотренного ч. 1 ст. 272 УК РФ, в отношении И. и его скорейшему направлению в суд, способствовало привлечение специалистов интернет-провайдера ЗАО «Контакт ТВ», которые оказали помощь в установлении IP-адреса и места, с которого обвиняемый путем подбора пароля осуществил несанкционированный доступ и временно заблокировал электронный почтовый ящик потерпевшего.

В январе 2016 г. уголовное дело было направлено в суд. И. приговорен к 1 году 6 месяцам лишения свободы.

Недостаточное количество экспертов, имеющих допуск к производству компьютерной экспертизы, приводит к проблеме, возникающей при рассмотрении сообщений и проведении проверок в порядке ст. 144–145 УПК РФ. Так, на сегодняшний день в ряде субъектов Российской Федерации сложилась практика возбуждения уголовных дел по фактам несанкционированного снятия денежных средств с банковских карт по ст. 158 УК РФ как кража, а не как мошенничество, предусмотренное ст. 159.6 УК РФ, в связи с тем, что на момент возбуждения уголовного дела следствие не располагает достоверными сведениями (заключением эксперта) об использовании преступниками вредоносного программного обеспечения.

§ 4. Особенности родовой методики расследования преступлений, совершенных с использованием информационно-коммуникационных технологий

Информационные и коммуникационные технологии все более активно используются в целях совершения противоправных действий. При этом значительное число «традиционных» преступлений, таких как кража, мошенничество, присвоение и растрата, вымогательство, причинение имущественного путем обмана или злоупотребления доверием и другие, совершаются в совокупности с неправомерным доступом к компьютерной информации, созданием, использованием и распространением вредоносных компьютерных программ, нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей[1].

В настоящем параграфе будут рассмотрены основные закономерности расследования преступлений, совершенных с использованием информационно-коммуникационных технологий, которые в соответствии с положениями ст. 150, 151 УПК РФ расследуются следователями (дознавателями) органов внутренних дел. Данные закономерности позволяют утверждать о наличии родовой криминалистической методики их расследования. При этом ограниченный объем настоящего пособия, а также специфика способов совершения преступлений, обусловил произведенную автором группиров-

[1] *Гаврилин Ю. В.* Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы. автореф. дис. ... д-ра юрид. наук. М., 2010. С. 4–5.

ку обозначенных преступлений на неравные по объему категории: 1) нарушение авторских и смежных прав; 2) хищения; 3) вымогательство; 4) неправомерный сбыт объектов, изъятых из гражданского оборота. Применительно к данной классификации рассмотрим способы совершения преступлений. Иные же особенности родовой криминалистической характеристики, а также особенности разрешения отдельных следственных ситуаций и решения тактических задач (установление события преступления, лица, совершившего преступление, обстоятельств его совершения и др.) приведены применительно ко всей группе преступлений, совершенных с использованием информационно-коммуникационных технологий в целом.

Особенности криминалистической характеристики преступлений, совершенных с использованием информационно-коммуникационных технологий

При определении криминалистической характеристики преступления наблюдается относительное единство во взглядах ученых[1]. Одно из наиболее удачных, на наш взгляд, определений криминалистической характеристики преступления предложил профессор Н. Г. Шурухнов, который определил ее как отражение системы криминалистических черт, свойств, признаков преступления, отобразившихся в объективной действительности[2]. Роль данных, образующих криминалистическую характеристику преступления, состоит в том, что они позволяют увидеть связи между различными обстоятельствами совершения преступления и в условиях недостатка исходной информации выдвинуть обоснованные версии, выбрать оптимальный путь по установлению лиц, совершивших преступление[3]. Как правильно отмечает В. П. Лавров, что знание криминалистической характеристики позволяет делать выводы об оптимальных путях раскрытия и расследования преступления.

К криминалистической характеристике принято относить информацию о материальных следах, времени и месте совершения преступлений, субъектах преступлений, типичных способах совершения и сокрытия преступлений, предметах преступного посяга-

---

[1] *См.: Пантелеев И. Ф.* Методика расследования преступлений. М., 1975. С. 9–10; *Сергеев Л. А.* Расследование и предупреждение хищений, совершаемых при производстве строительных работ: автореф. дис. ... канд. юрид. наук. М., 1966. С. 4–5; *Танасевич В. Г.* Теоретические основы методики расследования преступлений // Сов. гос-во и право. 1977. № 6. С. 92 и др.

[2] *Зуев Е. И., Шурухнов Н. Г.* Криминалистическая характеристика преступлений // Криминалистика (актуальные проблемы). М., 1988. С. 119.

[3] *Шурухнов Н. Г.* Расследование краж. М., 1999. С. 21.

тельства, лицах, совершающих противоправные деяния, и других существенных обстоятельствах преступлений, способствующих ретроспективному познанию события.

Рассмотрим наиболее существенные элементы криминалистической характеристики преступлений, совершенных с использованием информационно-коммуникационных технологий.

1. Данные о способах совершения преступлений

Способ совершения преступления общепризнанно является одним из главных элементов криминалистической характеристики преступления. В широком понимании способ преступления представляет собой объединенную единым замыслом систему действий по его подготовке, совершению и сокрытию, детерминированную объективными и субъективными факторами и сопряженную с использованием соответствующих орудий и средств[1]. Из этого определения очевидны три его составляющие. В случае наличия всех трех из них принято говорить о полноструктурном способе преступления. Однако отдельные составляющие могут отсутствовать, в том числе и при совершении преступлений, посягающих на информационную безопасность в сфере экономики. Так, при совершении преступлений с внезапно возникшим умыслом отсутствует подготовка. Иногда отсутствует и сокрытие преступления. В таких случаях можно говорить о неполноструктурном способе преступления.

В узком понимании способ совершения преступления представляет собой систему действий по выполнению объективной стороны состава преступления.

1.1. Способы нарушения авторских и смежных прав

1. Приобретение электронного носителя информации, содержащего контрафактный экземпляр программы для ЭВМ, и его незаконное использование с причинением ущерба правообладателю. Так, сотрудниками ГУ МВД России по Воронежской области в ходе проведения оперативно-розыскного мероприятия «Обследование помещений, зданий, сооружений, участков местности и транспортных средств» в офисе ООО «Д» были изъяты 14 накопителей информации, содержащих программные продукты, правообладате-

[1] *Зуйков Г. Г.* Криминалистическое понятие и значение способа совершения преступления // Труды ВШ МОПП СССР. М., 1967. Вып. 15. С. 53; *Зуйков Г. Г.* Криминалистическое учение о способе совершения преступления // Соц. законность. 1971. № 11. С. 14.

лями которых согласно справки об исследовании являются Корпорация «Microsoft», ООО «1С», Корпорация «Corel». В результате нарушения авторских прав правообладателей работников ООО «Д», выразившегося в незаконном использовании объектов авторского права корпорации «Corel», причинен материальный ущерб на общую сумму свыше 700 тыс. руб., что является крупным ущербом.

2. Незаконное копирование нелицензионного экземпляра программы для ЭВМ в сети Интернет, а также программы для ЭВМ, позволяющей нейтрализовать средства защиты программного продукта, в целях дальнейшего беспрепятственного его использования. Так, в производстве СЧ СУ УМВД России по Владимирской области находилось уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 146 УК РФ, по факту незаконного использования объектов авторского права А. начальником отдела информационных технологий ООО «Н». Из материалов уголовного дела следует, что А. в ходе осуществления профессиональной деятельности, связанной с подготовкой документации для проектирования элементов интерьеров подвижных составов (электропоездов), использовал нелицензионное программное обеспечение «SolidWorks Premium 2016», которое установил на рабочий компьютер самостоятельно.

В ходе предварительного следствия выявлен дополнительный эпизод преступной деятельности А. по признакам преступления, предусмотренного ч. 1 ст. 273 УК РФ, по факту использования компьютерной программы, заведомо предназначенной для несанкционированной нейтрализации средств защиты компьютерной информации, предоставляющей возможность работать с программным продуктом «SolidWorks Premium 2016» в полнофункциональном режиме способом, не предусмотренным правообладателем.

1.2. Способы совершения хищений

Хищения, совершенные посредством информационно-коммуникационных технологий, можно разделить на три основные группы.

Первая группа – это мошенничества, при которых потерпевшее лицо добровольно передает принадлежащие ему денежные средства лицу, совершающему преступление, в счет приобретения какого-либо товара, оказания услуг или выполнения работ. При этом потерпевший вводится преступником в заблуждение относительно своих истинных намерений и теряет принадлежащие ему средства. Основными площадками для совершения такого рода хищений являются различные интернет-магазины, интернет-аукционы, интернет-казино, сайты по обмену электронных платежных средств и т. д. Как правило, такие деяния квалифицируются по ст. 159 УК РФ.

Вторая группа – это хищения электронных денежных средств, находящихся на принадлежащих потерпевшему электронных кошельках, совершенные путем их взлома, осуществляемого посредством использования вирусного программного обеспечения, взломщиков электронных кошельков, фишинговых сайтов, сайтов-клонов и др. Такие деяния, в зависимости от конкретного способа их совершения, квалифицируются по ст. 158 УК РФ либо по ст. 159.6 УК РФ.

Третья группа хищений основана на том, что преступник путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей фактически выдает себя за собственника денежных средств, находящихся на счету потерпевшего, и без его ведома и согласия обращает данные средства в свою пользу. При этом непосредственного контакта потерпевшего с субъектом преступления не происходит.

Указанный перечень хищений не является исчерпывающим, встречаются все новые и более изощренные их способы, которые можно дифференцировать на способы, совершенные в отношении физических и юридических лиц.

1.2.1. Способы совершения хищений в отношении физических лиц

1. Перевод через систему ДБО на карточный счет потерпевшего значительной суммы денежных средств и последующее обращение к потерпевшему с просьбой вернуть якобы ошибочно переведенные денежные средства. При этом возможно предложение оставить потерпевшему определенную «комиссию» от возвращенной суммы. Потерпевший соглашается и переводит мошеннику полученные деньги с удержанием оговоренной комиссии. Однако мошенник обращается в банк с заявлением о производстве ошибочного перевода, и банк повторно списывает со счета потерпевшего ранее переведенную ему сумму и зачисляет ее на счет мошенника.

2. Использование методов социальной инженерии для выяснения данных платежных карт. С указанной целью мошенники звонят гражданам, представляясь сотрудниками банков, и просят сообщить данные платежных карт (номер, CVV, PIN-коды и пр.) под предлогом того, что карта якобы заблокирована, либо предлагают набрать комбинацию цифрового кода на мобильном телефоне, к которому привязана карта, или на клавиатуре банкомата. При этом могут программироваться интерактивные голосовые ответы для звонков клиентам. Полученная информация может использоваться для

совершения неправомерных транзакций от имени законного держателя банковской карты. Разновидностью названного способа является получение информации об SMS-сообщениях, подтверждающих совершение операции в системе ДБО. Например, лицу, продающему свой автомобиль на том или ином интернет-ресурсе, поступает звонок от потенциального покупателя, выражающего явную заинтересованность в сделке. После выяснения состояния автомобиля и небольшого формального торга «покупатель» соглашается приобрести автомобиль на согласованных условиях и предлагает сразу внести задаток за автомобиль на банковскую карту продавца. При переводе он просит владельца сообщить код авторизации транзакции, полученный на телефон посредством SMS-сообщения. Получив данный код, мошенники не переводят денежные обещанные средства, а, напротив, производят списание денежных средств со счета потерпевшего.

3. Использование вредоносных программ для получения доступа к счету потерпевшего в системе ДБО. Задачей такого программного обеспечения является сбор и передача информации о реквизитах входа (имя, пароль) в систему ДБО либо выполнение иных несанкционированных законным пользователем функций как в тайне от последнего, так и в явном виде. В некоторых случаях подобное вредоносное программное обеспечение затрудняет работу ранее установленного программного обеспечения, может выводить поверх интерфейса собственное диалоговое окно, требующее ввода определенной конфиденциальной информации (логина и пароля, номера телефона или сведений о кредитной карте). С 2016 г. получило широкое распространение вредоносное программное обеспечение, целью которого являются мобильные устройства, работающие на платформе Android. После попадания в устройство вредоносная программа запрашивала баланс привязанной к номеру банковской карты, скрывала поступающие уведомления и начинала переводить денежные средства с банковского счета потерпевшего на счета, подконтрольные злоумышленникам. Как правило, это специально созданные карточные счета мошенников, к которым привязана одна или несколько платежных карт. Спустя небольшой промежуток времени (несколько минут) лицо, на имя которого оформлена карта («дроп», который может быть и не осведомлен о преступном умысле мошенников), снимает денежные средства, поступившие на его карту, в банкомате. Затем эти деньги передаются организатору мошеннической схемы, а «дроп» может оставить себе комиссионное вознаграждение. Деньги со счета потерпевшего могут переводиться и на счет подставного юридического лица, которое имеет договор банков-

ского обслуживания с оказанием услуг «зарплатного проекта» и подключением десятков платежных карт, оформленных по фиктивным данным. Списанная со счета потерпевшего сумма распределяется по «зарплатным» картам, после чего «дропы» снимают деньги через банкоматы и отдают организатору мошеннической схемы.

4. Разновидностью данного способа является использование вредоносного программного обеспечения для операционных систем современных смартфонов, в частности операционной системы Android, на которой функционирует большая часть используемых в Российской Федерации мобильных устройств. Учитывая объем и содержание конфиденциальной информации, находящейся в большинстве смартфонов (сведения о привязанной к номеру телефона банковской карте, имя и пароль входа в систему ДБО, SMS-сообщения, подтверждающие совершение транзакций и др.), данные способы приобретают все большую опасность. Используя вредоносное программное обеспечение «троянского» типа, у злоумышленников появляется возможность получить практически полный контроль над мобильным устройством: осуществлять перехват входящих или исходящих SMS-сообщений, производить USSD-запросы, вносить в черный список определенный номер, сообщения с которого будут скрываться от пользователя, отображать диалоговое окно или сообщение в соответствии с полученными с управляющего сервера параметрами.

5. Списание небольших сумм со счетов клиентов. На начальных этапах развития и внедрения систем дистанционного банковского обслуживания относительно немногие их клиенты точно знали остатки по своим счетам и то, какие операции они проводили. Однако в связи с широким распространением услуги SMS-информирования о проведенных операциях и величине остатка на счете распространенность данного способа резко сократилась. В качестве примера расследования уголовных дел указанной категории следует привести уголовное дело № 42379, возбужденное СО ОМВД России по Суздальскому району 13 сентября 2015 г. по признакам преступления, предусмотренного п. «в» ч. 2 ст. 158 УК РФ, по факту хищения денежных средств с банковских счетов граждан, открытых в ПАО «***банк». В ходе предварительного расследования установлена причастность к совершению указанного преступления менеджера по продажам дополнительного офиса ПАО «***банк» А. Из материалов уголовного дела следует, что А. в ходе исполнения служебных обязанностей обладала правом доступа к документам и отчетам из автоматизированных электронных систем, в том числе к автоматизированной системе «Филиал», в которых в электронной

форме содержатся конфиденциальные сведения о клиентах ПАО «***банк», их идентификационных и контактных данных, а также о счетах и номерах банковских карт. Далее А. незаконно, вопреки законным интересам клиентов ПАО «***банк», используя их персональные данные, неоднократно проводила расходные операции по их банковским счетам на пластиковые карты, открытые от имени данных клиентов. Впоследствии перечисленные денежные средства обналичивались А. без ведома клиентов. Тем самым А. с целью хищения денежных средств клиентов незаконно использовала полученные в ходе служебной деятельности сведения, составляющие банковскую тайну, без согласия их владельца.

6. Оформление кредитов или кредитных карт на клиентов банков в тайне от последних с последующим снятием с них наличных денежных средств или оплатой ими товаров, работ, услуг. Совершение подобного рода хищений происходит, как правило, при пособничестве со стороны недобросовестных банковских работников, не осуществляющих надлежащей идентификации заемщика, либо использовании паспортных данных третьих лиц, не осведомленных о таких действиях, для оформления на их имя кредита, введения недостоверных сведений в информационную систему банковского обслуживания и подписания необходимых документов: заявления, анкеты заемщика, кредитного договора и др. В результате в обоих случаях лицу, на чье имя оформлена кредитная карта, причиняется материальный ущерб в виде обязательств по кредиту, которое оно не получало. При этом потерпевшие некоторое время (обычно до наступления времени просрочки первого платежа и получения претензии от банка-кредитора) остаются в неведении, что на их имя получен кредит. Учитывая, что некоторые банки предоставляют значительный по времени (до нескольких месяцев) льготный период, когда проценты на предоставленные заемные средства не начисляются и погашение «тела кредита» не производится, время совершения преступления и время начала производства расследования может значительно отличаться.

7. Разновидностью вышеназванного способа является неправомерное использование кредитной карты, выданной или направленной посредством почтовой связи определенному лицу другим лицом в тайне от первого.

8. Хищения с использованием поддельных банковских платежных карт. Таковые могут осуществляться как через сеть Интернет путем оплаты покупок либо перечислением денежных средств на другие счета, так и через POS-терминалы за приобретение товаров и услуг, либо имитируя их легальную оплату.

9. Хищения денежных средств держателей банковской карты, которая была ранее похищена вместе с ПИН-кодом, а ее законный держатель не произвел своевременного блокирования.

10. Скимминг представляет собой способ тайного получения конфиденциальной информации законных держателей банковских карт (прежде всего номера карт и иной информации, записанной на магнитную полосу банковской карты, а также ПИН-кодов) с использованием специального оборудования (скиммера), представляющего собой специальную накладку на стандартные органы управления банкомата (картоприемник, клавиатуру), а также средство видеофиксации ввода ПИН-кода. Некоторые скиммеры осуществляют трансляцию полученной информации по радиоканалу. Большинство же из них фиксируют данные на встроенный электронный носитель. В дальнейшем информация, записанная на магнитную полосу банковской карты посредством использования специального устройства – энкодера, переносится на магнитные полосы заготовок банковских карт, что позволяет осуществлять операции с продублированной банковской картой: снимать наличные в банкомате, осуществлять переводы денежных средств и пр.

11. Разновидностью скимминга является установка поддельных терминалов оплаты или банкоматов, осуществляющих копирование данных банковских карт и их пресылку для последующего воспроизведения с помощью энкодера на продублированной банковской карте.

12. Введение вредоносного программного обеспечения в информационную систему «банк-банкомат», позволяющего осуществлять копирование и последующую пересылку данных банковской карты законного держателя для их последующего воспроизведения.

13. Размещения на электронных торговых площадках (таких как Avito.ru, Molotok.ru, Youla.ru, Irr.ru и пр.) заведомо подложных объявлений о продаже товаров либо предоставлении услуг с условием обязательной предоплаты. После чего введенные в заблуждение потерпевшие перечисляют сумму первоначального взноса на указанные реквизиты банковских карт, как правило, оформленных на подставных лиц, ведущих асоциальный образ жизни. Так, в первом полугодии 2017 г. в Энгельский районный суд Саратовской области направлено уголовное дело по обвинению местного жителя в совершении 9 преступлений, предусмотренных ч. 2–3 ст. 159 УК РФ. Обвиняемый размещал на сайте Avito.ru объявление о продаже автомобильных колес на литых дисках в сборе на автомобиль марки «Мерседес» по низкой цене, но со 100 % предоплатой. После перечисления денежных средств на банковскую карту преступника последний прекращал отвечать на телефонные звонки. Совершенные преступления раскрыты по резуль-

татам анализа MAC-адресов, IP-адресов, детализаций телефонных переговоров потерпевших с привязкой к приемопередающим базовым станциям, а также выемки электронных сообщений с электронных почтовых ящиков.

14. Создание в сети Интернет сайтов, визуально похожих на существующие сайты организаций, осуществляющих интернет-торговлю или оказание финансовых услуг. Разновидностью данного способа является распространение мобильных приложений для смартфонов, обладающих описанными выше характеристиками. Внешне дизайн и функциональные возможности таких сайтов-подделок или мобильных приложений схож до степени смешения с дизайном официальных сайтов широко известных авиакомпаний, банков, интернет-магазинов, платежных систем и т. п. На таких сайтах-клонах могут предлагаться товары или услуги по цене, значительно ниже рыночной, требуется перечисление предоплаты. Так, ГСУ ГУ МВД России по Краснодарскому краю в феврале 2017 г. окончено производством уголовное дело в отношении Р., М., Н., а также иных соучастников за совершение преступлений, предусмотренных ч. 1 и 2 ст. 210, ч. 4 ст. 159 УК РФ. Установлено, что указанные лица в 2013–2014 гг., действуя от якобы от имени Форекс-брокера, организовали деятельность по привлечению вкладов граждан в высокодоходные сферы мировой экономики, фондовых и финансовых рынков. Участниками преступного сообщества был создан интернет-сайт, а также использован специальный программный продукт – «HYIP Manager Script», предназначенный для автоматического вычисления процентов по вкладам на основании заданных администратором параметров и демонстрации в личном кабинете потерпевшим процесса фиктивного начисления процентов по вкладам. Фактически инвестирование денежных средств не осуществлялось, а деятельность преступного сообщества представляла собой финансовую пирамиду. В результате совершения указанных действий 533 гражданам, проживающим на территории Краснодарского края и Республики Адыгеи, причинен ущерб на общую сумму 137,5 млн руб.

15. Несанкционированное использование реквизитов законного пользователя, используемых им для входа в систему ДБО, иными лицами, которым эти данные стали известны в силу недостаточной осмотрительности потерпевшего и заботы об обеспечении конфиденциальности указанной информации. Получение имени и пароля, принадлежащих определенному лицу, для входа под его именем в его «Личный кабинет» в системе ДБО возможно в процессе совместного использования одного персонального компью-

тера сотрудниками организации или членами семьи потерпевшего. После первого входа в систему ДБО с введением имени и пароля система предлагает сохранить введенные реквизиты для последующего упрощенного входа. В этом случае последующий пользователь получает беспрепятственный доступ в личный кабинет неосмотрительного владельца карточного счета. Разновидностью способа является получение злоумышленником доступа к мобильному телефону, к абонентскому номеру которого привязана банковская карта. Пользуясь тем, что за действиями злоумышленника никто не следит, он осуществляет перевод денежных средств от имени законного пользователя на свой карточный счет или счет иного подставного лица. Так, по уголовному делу, находившемуся в производстве СУ УМВД России по г. Казани, по обвинению В. и Ж. в совершении нескольких эпизодов кражи с причинением значительного ущерба гражданину, а также в особо крупном размере, установлено, что указанные лица осуществляли хищение денежных средств граждан с банковских карт и лицевых счетов абонентских номеров оператора сотовой связи ООО «Т2 Мобайл». Хищение осуществлялось путем восстановления абонентского номера потерпевшего, подключенного к услуге «мобильный банк», предоставляющей держателю абонентского номера возможность управления счетом собственника и распоряжения денежными средствами, находящимися на нем. В ходе проведения обысков по месту жительства указанных лиц удалось обнаружить и изъять многочисленные доказательства причастности к совершенному преступлению, в том числе сотовые телефоны, которые использовались при хищении денежных средств, SIM-карты, банковские карты, оформленные на подставных лиц, другие предметы и документы. По делу было назначено свыше 30 экспертиз, в том числе и специалистам сторонних организаций. Приговор в отношении названных лиц вступил в законную силу.

16. Распространения в сети Интернет и среди абонентов сотовой связи ложных сведений относительно возможности наступления негативных последствий как для получателя сообщения, так и для его близких в связи, например, с якобы имеющем место фактом привлечения близкого лица к уголовной или административной ответственности, госпитализацией в медицинское учреждение и т. п., сопряженных с предложением о перечислении денежных средств на указанный мошенниками счет. Так, в мае 2017 г. вступил в силу приговор Балаковского районного суда Саратовской области в отношении организованной преступной группы, участники которой посредством телефонных звонков сообщали потерпевшим, что они являются их родственниками, попавшими в беду, и для «решения вопроса»

потерпевшие передавали деньги курьеру. Преступление раскрыто по результатам анализа детализаций телефонных переговоров потерпевших с привязкой к приемопередающим базовым станциям с установленными IMEI-номерами, используемыми преступниками. Все участники преступной группы осуждены: организатор – к 10 годам, соучастники – к 1 году 6 месяцам и 2 годам лишения свободы.

1.2.2. Способы хищений в отношении юридических лиц

1. Фишинг. Использование вредоносного программного обеспечения, позволяющего удаленно управлять банковскими счетами юридических лиц. Для распространения «троянских» программ используются различные методы: создается сеть «фишинговых» сайтов, осуществляются массовые рассылки сотрудникам организации писем по электронной почте, содержащих вредоносные эксплойты (компьютерные программы или фрагменты программного кода, выполняющие скрытно от пользователя незапланированные им функции), использование методов «социальной инженерии» (когда мошенники стимулируют пользователей самостоятельно устанавливать вредоносное программное обеспечение, например, в тексте письма, отправленного в бухгалтерию организации якобы от имени Федеральной налоговой службы, содержащего требования срочной обработки сообщения, при этом могут приводиться контактные данные реальных сотрудников налоговой службы). Направив на корпоративную электронную почту сотрудника организации письмо, содержащее вредоносный программный код, путем обмана или злоупотребления доверием злоумышленники побуждают пользователя открыть вредоносный файл, после чего вредоносное программное обеспечение активируется. Получив доступ в информационную систему потерпевшего, преступники получают возможность перехватывать данные, осуществлять переводы денежных средств на подконтрольные им банковские счета. С указанной целью на подконтрольном компьютере с использованием вредоносного программного обеспечения запускалось программное обеспечение «Клиент-Банк», с помощью которого формировались и отправлялись на исполнение платежные поручения.

2. Непосредственный доступ к охраняемой законом информации юридического лица, относящейся к коммерческой тайне, с целью ее модификации и блокирования. Такая информация может касаться, например, размера остатков денежных средств на лицевых счетах абонентов данной организации. Так, в производстве СЧ по РОПД СУ УМВД России по Тульской области находилось уголовное дело по обвинению Г. в совершении 8 преступлений, пред-

усмотренных ч. 2 ст. 159.6 УК РФ. Расследованием установлено, что в период с апреля по июль 2014 г. Г., Г1., Р. и А. распределили между собой преступные роли. Г1., имеющий доступ к компьютерной программе «Clarify», предназначенной для осуществления полного цикла операций по обслуживанию абонентов оператора сотовой связи «Билайн», осуществлял поиск в сети Интернет абонентских номеров оператора сотовой связи «Билайн», в том числе заблокированных по причине «Suspension-Мошенничество», на лицевых счетах которых находились денежные средства, принадлежащие ОАО «ВымпелКом», после чего производил незаконную, без соответствующих заявлений абонентов оператора сотовой связи «Билайн», разблокировку заблокированных абонентских номеров и замену на новые имеющиеся в его пользовании SIM-карты, модифицируя компьютерную информацию. Иные соучастники осуществляли активацию замененных SIM-карт, производили переводы денежных средств, находящихся на лицевых счетах абонентов оператора сотовой связи «Билайн», на подконтрольные им банковские карты и телефонные номера, а также обналичивали денежные средства в банкоматах. В результате хищения ОАО «ВымпелКом» был причинен ущерб на общую сумму 1 722 809 руб. 47 коп.

3. Несанкционированный доступ к криптографическим возможностям смарт-карты.

4. Подмена документа при передаче его на подпись в смарт-карту. Пользователь видит на экране монитора одну информацию, а в смарт-карту на подпись отправляется другая. Параллельно могут быть подменены данные об остатках на счете, выполненных транзакциях и т. д.

1.3. Способы совершения вымогательства

1. Получение информации о частной жизни путем внедрения в смартфон потерпевшего вредоносного программного обеспечения, позволяющего: осуществлять запись, блокирование или перенаправление телефонных звонков; копировать данные из адресной книги; отправлять данные о местоположении; копировать фотографии; использовать микрофон для подслушивания; отправлять и получать SMS; отключать антивирусное программное обеспечение; получать доступ к истории чатов (Skype, Viber, WhatsApp); просматривать историю браузера и выполнять иные функции. Получив сведения, позорящие потерпевшего или его близких, либо иные сведения, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких, вымогатели предъявляют требования передачи

им чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой распространения названных сведений.

2. Организация распределенных сетевых атак (Distributed Denial of Service, или DDoS), направленных на блокирование доступа к серверу потерпевшего внешними пользователями. В основе таких атак лежит технологическое ограничение пропускной способности сетевой инфраструктуры, поддерживающей интернет-сайт потерпевшего. Во время DDoS-атаки в адрес интернет-ресурса отправляется большое количество запросов с целью исчерпать его возможности обработки данных и нарушить его нормальное функционирование. Если число запросов превышает предельные возможности какого-либо компонента информационной инфраструктуры, могут возникнуть значительные задержки при формировании ответа на запросы либо полный отказ в обслуживании запроса. Для отправки на интернет-ресурс потерпевшего сверхбольшого количества запросов вымогатели могут создать компьютерную сеть (ботнет), все элементы которой выполняют соответствующий вредоносный программный код и удаленно управляются вымогателями. Элементами такой сети могут являться и компьютеры законных пользователей, не осведомленных о противоправных действиях вымогателей. Требования последних при этом могут касаться прекращения DDoS-атаки и восстановления работоспособности интернет-сайта потерпевшего.

3. Распространение программ по типу «троянский конь», выполняющих в тайне от законного пользователя незапланированные им функции: блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Целью действий программ-вымогателей является блокирование доступа пользователя к данным на компьютере или ограничение возможностей работы на компьютере и требование денежных средств за возврат к исходному состоянию системы. Перевод денежных средств может осуществляться путем отправки платного SMS-сообщения на определенный абонентский номер, предлагаемый программой, либо на электронный кошелек на имя подставного лица. Так, приговором Хорошевского районного суда г. Москвы от 1 декабря 2014 г. К. был признан виновным в совершении вымогательства и распространении вредоносных программ для ЭВМ – преступлений, предусмотренных ч. 1 ст. 163, ч. 1 ст. 273, ч. 2 ст. 273 УК РФ. Под угрозой уничтожения и повреждения компьютерных систем, используя вредоносную компьютерную программу, заведомо предназначенную для несанкционированного блокирования компьютерной информации, хранящей-

ся на ресурсах сайтов ЗАО Банк «Тинькофф Кредитные системы», ЗАО «Лаборатория Касперского», ОАО «Промсвязьбанк» и ЗАО «ИД «Комсомольская правда», К. выдвинул требование о передаче ему денежных средств на сумму свыше 11 млн руб.

1.4. Способы незаконного распространения объектов, изъятых из гражданского оборота

На основании общепризнанных актов международного права, таких как Единая конвенция о наркотических средствах (заключена в г. Нью-Йорке 30 марта 1961 г.), Конвенция о мерах, направленных на запрещение и предупреждение незаконного ввоза, вывоза и передачи права собственности на культурные ценности (заключена в г. Париже 14 ноября 1970 г.), Конвенция о психотропных веществах (заключена в г. Вене 21 февраля 1971 г.), Конвенция о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении (заключена 16 декабря 1971 г.), Конвенция о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении (заключена в г. Париже 13 января 1993 г.) и других законодательство абсолютного большинства государств запрещает или ограничивает оборот наркотических средств, психотропных веществ, оружия, похищенных культурных ценностей и других объектов, запрещенных к свободному обороту (далее – предметов, изъятых из оборота).

Российская Федерация – не исключение. Уголовная ответственность установлена за незаконный сбыт или пересылку наркотических средств, психотропных веществ и их аналогов с использованием электронных или информационно-телекоммуникационных сетей (включая Интернет) – п. «б» ч. 2 ст. 228.1 УК РФ, распространение, публичную демонстрацию или рекламирование порнографических материалов или предметов, материалов или предметов с порнографическими изображениями несовершеннолетних с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) – п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1 УК РФ.

Однако развитие информационных и коммуникационных технологий дало новый импульс развитию криминального бизнеса в указанных сферах, в основе которого находится возможность совершения данных преступлений дистанционным способом (т. е. без непосредственного контакта покупателя и продавца). Дистанционный способ совершения преступления предполагает, что взаимодействие участников преступной деятельности осуществляется опосредованно, используя информационные ресурсы сети Интернет

в первую очередь такие, как социальные сети, электронная почта, сервисы мгновенных сообщений и пр.

Рассматриваемый способ реализации предметов, изъятых из оборота, может осуществляться на основе различных интернет-технологий, в частности:

– создания специализированных сайтов на серверах вне юрисдикции государства, на целевую аудиторию которых они ориентированы, предлагающих запрещенные к обороту объекты. Наличие подобных сайтов легко выявляется путем указания в поисковой строке любого интернет-браузера (Google, Yahoo, Aol, Яндекс и др.) наименования того или иного предмета, изъятого из оборота. Данные сайты представляют собой нелегальные интернет-магазины, через которые можно не только приобрести предметы, изъятые из оборота, но и получить подробные инструкции о порядке их применения, способах оплаты и получения, а также иную связанную с данными объектами информацию. Для повышения привлекательности реализуемого товара на таких сайтах используются даже такие маркетинговые инструменты, как скидки, акции «три предмета по цене двух» и пр. Активная блокировка подобных сайтов на основании ст. 15.1 и 15.3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» приводит к росту популярности нелегальных сайтов, доступ к которым осуществляется через Tor-браузер;

– использования возможностей социальных сетей для незаконного сбыта изъятых из оборота предметов.

Использование той или иной интерент-технологии при совершении дистанционного сбыта предметов, изъятых из оборота, может осуществляться по следующим направлениям:

– распространение информации о наличии возможности приобретения определенных предметов, изъятых из оборота, их свойствах (характеристиках). Такое распространение может осуществляться для неопределенного круга лиц (например, при создании интернет-сайтов) или определенной (целевой) аудитории (например, при создании группы в социальной сети);

– установление непосредственного контакта сбытчика и приобретателя предметов, изъятых из оборота, согласование цены и наименования, а в отдельных случаях и ассортимента приобретаемых объектов посредством переписки или телефонных переговоров;

– информирование покупателя о способах и порядке расчетов (использование электронных кошельков, криптовалют, перечисление денежных средств на счет мобильного телефона с терминала

самообслуживания, иные способы оплаты, при которых не производится идентификация плательщика);

– информирование покупателя о месте и времени получения заранее подготовленной «закладки» – тайного помещения предмета, изъятого из оборота, в определенное место, которое сообщается покупателю после поступления от него платежа путем направления ему метки геолокации, фотоизображения, а также словесного описания тайника;

– обеспечение обмена информацией между участниками преступной группы, осуществляющей незаконный сбыт предметов, изъятых из оборота, в соответствии с их ролью в преступной иерархии и криминальной специализацией.

2. Способы сокрытия преступлений

1. Использование для обналичивания похищенных денежных средств электронных кошельков и электронных платежных систем, открытых на подставных лиц.

2. Использование криптовалют в криминальных взаиморасчетах, выпуск и обращение которых не зависит от денежно-кредитной политики какого-либо государства, не требует ведения специальной отчетной документации, при этом обеспечивает относительную анонимность пользователей. Несмотря на то что каждая транзакция подлежит регистрации с присвоением уникального номера, эта регистрация привязывается к электронному кошельку, который может быть открыт на вымышленных лиц, а не к личности его владельца. При этом криптовалюты на специализированных сайтах подлежат обмену на реальные деньги, подлежащие переводу на электронные кошельки, а также могут бесконтрольно переводиться и за пределы юрисдикции Российской Федерации, что обуславливает их использование в схемах, направленных на легализацию (отмывание) доходов, полученных преступным путем.

3. Сокрытие подлинных персональных данных от провайдера при подключении к сети Интерент. По-прежнему операторы мобильной связи осуществляют распространение SIM-карт (в переходах метро, возле крупных торговых точек, в иных многолюдных местах) без процедуры идентификации пользователя.

4. Использование для входа в Интернет зарубежных IP-адресов, находящихся вне юрисдикции Российской Федерации.

5. Использование ремейлеров – серверов, получающих почтовые сообщения и переправляющих их по адресам, указанным отправителем. В процессе переадресовки вся информация об отправителе уничтожается.

6. Использование анонимайзеров – средств, позволяющих изменять данные об обратном адресе и службе электронной почты отправителя. При этом остается возможность установить IP-адрес компьютера отправителя.

7. Использование второго электронного почтового ящика, с помощью которого отправляется электронная почта под любыми вымышленными исходными данными.

8. Сокрытие присутствия в операционной системе (*Rootkit*). Это программный код или техника, направленная на сокрытие присутствия в системе заданных объектов (процессов, файлов, ключей реестра и т. д.).

9. Использование сети Tor (*The Onion Router* – луковая маршрутизация) – бесплатного и открытого программного обеспечения, позволяющего получать анонимный удаленный доступ и защищать передаваемые данные от анализа трафика. После запуска программы Tor Browser все данные проходят через три различных прокси-сервера, которые выбираются случайным образом. Каждый раз данные шифруются разными ключами для каждого прокси-сервера. Дойдя до конечного узла сети Tor, данные вновь попадают в сеть Интернет, и сервер, которому субъектом направлено сообщение, видит лишь IP-адрес компьютера с модемом (роутером) – точкой выхода сообщения из сети Tor. IP-адрес компьютера субъекта остается сокрытым.

10. Использование VPN (*Virtual Private Network* (*VPN*) – виртуальная частная сеть) – технологии, позволяющей обеспечивать сетевые соединения (логическую сеть) поверх другой сети (например, сеть Интернет).

3. Способы подготовки к совершению преступлений

1. Сбор сведений об информационной системе, средствах ее защиты и информационных процессах путем распространения вредоносного программного обеспечения, внешне не проявляющегося и до определенного момента никак не сказывающегося на ее функциональных возможностях. Так, 15 февраля 2015 г. в результате целевой атаки на торговый терминал с использованием вредоносной программы Corkow (aka Metel) курс доллара к рублю внутри торгового дня поднялся на 15 %. Сама атака длилась 14 минут, но подготовка к ней заняла полгода. Попав на компьютер с торговой системой в сентябре 2014 г., программа постоянно обновлялась, избегая обнаружения средствами антивирусной защиты, которые были установлены и корректно работали в банке. Все это время злоумышленники получали информацию о пользователях устройства,

процессах, запущенных на нем, и другие данные, необходимые для планирования атаки.

2. Хищение ключей электронной подписи (ЭП) клиентов систем дистанционного банковского обслуживания с незащищенных электронных носителей информации (флеш-накопителей, жесткого диска и пр.) или из оперативной памяти компьютера.

3. Сбор информации о типичных платежных операциях клиентов систем дистанционного банковского обслуживания, типичных маршрутах передвижения и иного стандартного поведения (места снятия наличности, наиболее частых покупок с использованием банковских карт и пр.) с целью последующей маскировки хищения и обхода алгоритма антифрод-защиты банка[1].

4. **Типичные следы** преступлений, совершенных с использованием информационно-коммуникационных технологий, были рассмотрены в предыдущем параграфе.

5. **Данные о личности преступника.** Для целей раскрытия и расследования преступлений, совершенных с использованием информационно-коммуникационных технологий важное значение имеет типовой набор личностных характеристик, которыми обладает подозреваемый, что, в свою очередь, во многом формирует характер и содержание складывающейся следственной ситуации. При этом такой набор существенных личностных характеристик находится в зависимости как от избранного способа совершения преступления, так и от роли подозреваемого в составе преступной группы. Построить универсальную модель типичного субъекта рассматриваемых преступлений можно, лишь прибегая к высокой абстракции, что снижает практическую значимость такой обобщенной модели ввиду невозможности на ее основе проведения узкой выборки, поскольку под ее признаки попадает весьма широкий круг лиц.

Кроме того, важное значение имеет и линия поведения, избираемая подозреваемым на различных этапах расследования, которая может существенно различаться исходя из содержания и качества полученной в процессе расследования доказательственной базы.

Вместе с тем исследование следственной практики за 20-летний период позволяет сформировать типовой набор личностных характеристик, предопределяющий линию поведения организа-

[1] Антифрод-система – специальное программное обеспечение, предназначенное для выявления и пресечения хищений денежных средств при совершении интернет-транзакций, на основе политики управления рисками кредитной организации или платежной системы, через которые осуществляется платеж.

торов совершения преступления, который в большинстве своем включает в себя:

– обладание широким кругозором, коммуникабельность, расчетливость, высокие интеллектуальные способности, четкое понимание собственной выгоды;

– обладание специальными знаниями в банковской сфере, наличие профильного образования и опыта работы по специальности;

– наличие глубоких познаний в области компьютерных технологий, включая особенности функционирования программного обеспечения систем дистанционного банковского обслуживания;

– обладание хорошими психологическими способностями, умение моделировать ситуацию такими образом, чтобы получить желаемый результат, создавать у окружающих мотивацию на желательную для данного лица линию поведения;

– преобладание после задержания защитной доминанты в линии поведения, включая и попытки вступить в коррупционные отношения с сотрудниками правоохранительных органов с целью избежания уголовной ответственности: введение следствия в заблуждение относительно механизма преступления, своей роли в составе преступной группы и перекладывание ответственности на иных лиц;

– высокая адаптивность к изменяющейся ситуации и гибкость в принятии решений, продуманность своих действий и решений, сочетающиеся при этом с авантюризмом и дерзостью;

– высокая осторожность и конспирация, проявляющаяся в использовании широкого спектра способов сокрытия данных о своей личности, включая частые смены номеров телефонов и телефонных аппаратов, отсутствие при себе и в своем жилище предметов, которые могут стать доказательством совершения противоправных действий, заранее разработанная линия поведения в случае задержания, наличие адвоката, специализирующегося по делам о преступлениях, совершенных с использованием информационных технологий.

От описанного выше набора свойств и качеств, присущих личности организатора преступления, существенным образом отличаются характеристики лиц, используемых для совершения отдельных элементов механизма преступления. К ним относятся специалисты-программисты; лица, обеспечивающие распространение вредоносных программ и их эксплуатацию с целью последующего перевода денежных средств на подконтрольные счета физических или юридических лиц; а также лица, осуществляющие снятие наличных денежных средств в банкоматах – так называемые «дропы», их кураторы – «дроповоды» и др.

Задача «дропа» – снять деньги с банковской карты, рискуя при этом попасть на запись видеокамеры банкомата. Среди них можно выделить как дилетантов, не осведомленных о противоправных действиях организатора преступления, не осознающих правовые последствия своих действий и не предпринимающих мер защиты и конспирации. Как правило, такие лица совершают однократные операции по снятию денежных средств. Ими могут быть знакомые, родственники участников преступной группы, т. е. лица, не имеющие криминальных навыков, обладающие в некоторой степени правовым инфантилизмом.

Другая категория «дропов» – профессионалы, осознающие противоправный характер своей деятельности и предпринимающие меры конспирации. На них могут быть зарегистрированы юридические лица, не осуществляющие фактической предпринимательской деятельности или ведущие ее лишь для создания видимости, либо они могут обладать статусом индивидуального предпринимателя. Денежные средства снимаются или в банках под видом заработной платы или дивидендов учредителя. Внешне они себя позиционируют как предприниматели. При этом имеют лишь самое общее поверхностное представление о правовых основах предпринимательской деятельности, сообщая банковским работникам заранее подготовленные фразы, стараясь при этом не вызывать подозрение. Они осознают, что период времени, в течение которого подобная деятельность не будет вызывать подозрений, весьма незначителен и составляет несколько месяцев. Некоторым «дропам» за это время удается подняться выше в криминальной иерархии и стать «дроповодом» – лицом, которое самостоятельно не производит операции по снятию наличных, но при этом имеет налаженную сеть «дропов», которым он передает заранее подготовленные документы, банковские карты, иную необходимую информацию, производит получение снятых ими со счета наличных денежных средств, а также предоставляет им вознаграждение в виде определенного процента от снятой со счета суммы.

Есть и другая более многочисленная категория лиц, относящихся к «дропам» – лицам без определенного источника дохода и предыдущего криминального опыта. Информацию о простом и быстром заработке они получают либо через социальные сети, либо через специализированные сайты по поиску работы. Информация на последних, разумеется, не содержит всей полноты сведений о предлагаемой «вакансии». Более подробно будущий «дроп» инструктируется уже после нескольких собеседований, когда координатор «дропов» – «дроповод» убедится в благонадежности новобранца.

Заметим, что легализация и обналичивание денежных средств, добытых преступным путем, возможна и путем их перевода за рубеж.

Совершение рассматриваемых преступлений невозможно без *технических специалистов* – лиц, обладающих специальными познаниями, умениями и навыками создания программного обеспечения, системного администрирования информационных систем, используемых при совершении противоправного деяния, детально владеющих алгоритмами работы программного обеспечения систем дистанционного банковского обслуживания. В число задач технических специалистов могут входить следующие:

– разработка и техническая поддержка специализированных интерент-сайтов для онлайн-продажи предметов, изъятых из гражданского оборота, или совершения мошенничества;

– защита информационных ресурсов, их перенос на серверы с нескомпрометированными IP и MAC адресами (при необходимости);

– обеспечение анонимности доступа к сайту и безопасности информации на нем;

– обучение членов преступной группы навыкам работы с программным обеспечением и др.

Если использование информационно-коммуникационных технологий применяется для обеспечения анонимности дистанционного сбыта изъятых из гражданского оборота объектов (наркотиков, оружия, порнографической продукции и др.), то структура преступной организации дополняется *подразделением по сбыту*, в состав которого входят оптовые региональные распространители, операторы интернет-магазина, а также закладчики (кладмены). Последние осуществляют помещение криминального товара в определенное место, о котором посредством месенжджера Telegram информируют покупателя. В отдельных случаях иерархия закладчиков может включать в себя несколько уровней (крупный опт – склад, мелкий опт – мастер-клад, розница –клад).

Тактика проверки сообщения о преступлении. Особенности организации взаимодействия участников расследования в стадии возбуждения уголовного дела

В соответствии с ч. 2 ст. 140 УПК РФ основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления. Процессуальными средствами их установления являются действия, предусмотренные ч. 4 ст. 21, ч. 1, 3 ст. 144 УПК РФ. Перечень конкретных обстоятельств, подлежащих установлению в стадии возбужде-

ния уголовного дела, зависит от содержания диспозиции уголовно-правовой нормы, по признакам которой возбуждается уголовное дело.

Так, при решении вопроса о возбуждении уголовного дела по факту хищения денежных средств, принадлежавших потерпевшему и находившихся на его счете в кредитной организации, должны быть установлены факты:

– списания денежных средств со счета их собственника без согласия последнего;

– зачисления указанных денежных средств на счета иных лиц, не состоящих в договорных отношениях с пострадавшим;

– характеристики несанкционированной транзакции: дата и время ее совершения, номер счета списания / зачисления, сумма, идентификационные данные отправителя / получателя платежа.

В стадии возбуждения уголовного дела в зависимости от источника исходной информации возможны две типичные проверочные ситуации:

1) информация о преступлении поступила от лица, которому причинен вред вследствие совершения преступления;

2) признаки преступления выявил орган дознания в процессе реализации им оперативно-розыскной деятельности.

В первой следственной ситуации процессуальными средствами установления перечисленных фактов являются:

1. Получение письменного объяснения заявителя с указанием характера и размера вреда, обстоятельства его причинения, вероятного круга подозреваемых лиц.

Так, при поступлении заявления о хищении денежных средств с электронного средства платежа, принадлежащего потерпевшему, устанавливаются: наименование банковского учреждения и реквизиты счета, с которого произошло неправомерное списание денежных средств, дата, время и обстоятельства обнаружения такого списания, сумма материального ущерба (с учетом возможного неоднократного списания), используемый заявителем сервис дистанционного банковского обслуживания, поступавшие от него уведомления, дата и время их получения, способ входа в систему ДБО, используемое при этом оборудование (персональный компьютер, смартфон, планшетный компьютер, банкомт, банковский терминал самообслуживания и пр.), местонахождение данных устройств, производил ли пользователь спорные транзакции, подключена ли услуга SMS-информирования, а также отправлял ли пользователь SMS-сообщение с кодом подтверждения транзакции, известны ли пользователю получатели списанных с его счета

денежных средств и в каких отношениях он с ними состоит (ответ на данный вопрос возможен при условии получения заявителем в банке расширенной выписки по своему счету, содержащей номера банковских счетов, лицевые счета мобильных телефонов, ФИО получателей).

2. Осмотр места происшествия, в рамках которого осматривается непосредственно микропроцессорное устройство (стационарный компьютер, ноутбук, планшетный компьютер, смартфон), с использованием которого заявитель установил факт совершения преступления, например, факт списания с банковского счета денежных средств. В последнем случае фиксируются наличие на устройстве программного обеспечения системы ДБО, а также сообщения, поступившие на устройство в связи со спорной транзакцией (уведомления и запросы системы ДБО). По результатам осмотра устройство подлежит изъятию для последующего назначения и производства судебно-компьютерной экспертизы. Телефон и компьютер должны быть изъяты с участием специалиста. Телефон необходимо перевести в авиарежим, компьютер – в режим гибернации.

3. Направление поручения в орган дознания на получение в кредитной организации справки по счету заявителя. В соответствии со ст. 26 Закона РФ от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, а при наличии согласия руководителя следственного органа – органам предварительного следствия по делам, находящимся в их производстве. Соответственно, на данной стадии орган дознания может получить названные сведения исключительно на основании судебного решения. Указанное обстоятельство, наряду с нормативно незакрепленным сроком на подготовку кредитной организацией ответа на запрос, порождает значительные сложности в оперативном получении информации о движении денежных средств по лицевым счетам абонентских номеров (банковских карт), сведений о владельцах абонентских номеров (банковских карт) и иных сведений, имеющих значение для решения вопроса о возбуждении уголовного дела.

4. Назначение судебной компьютерной экспертизы в отношении изъятых в ходе осмотра предметов.

Во второй проверочной ситуации, с учетом требований Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания,

следователю или в суд[1] оперативные подразделения органов дознания по результатам оперативно-розыскных мероприятий предоставляют должностным лицам органов предварительного расследования следующие материалы и сведения:

1. Рапорт об обнаружении признаков преступления с отражением информации о времени, месте и обстоятельствах его совершения, содержании проведенных оперативно-розыскных мероприятий, документов и иных объектов, полученных в ходе их проведения (аудио-, видеозаписи, фотоснимки, электронные носители информации и т. п.).

2. Постановление о предоставлении материалов оперативно-розыскной деятельности органу предварительного следствия, подписанное руководителем органа (подразделения), осуществляющего оперативно-разыскную деятельность с указанием перечня предоставляемых документов (например, справки о результатах проведения оперативно-розыскных мероприятий, копии рассекреченных документов).

3. Копия судебного решения о проведении оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища.

4. Постановление о проведении оперативно-розыскных мероприятий руководителя органа, осуществляющего оперативно-разыскную деятельность (начальника или его заместителя), в случае проведения оперативного эксперимента или оперативного внедрения.

5. Постановление о рассекречивании сведений, составляющих государственную тайну, их носителей, к которым относятся в том числе сведения об организации и тактике проведения оперативно-поисковых и оперативно-технических мероприятий, используемых при их проведении технических средствах, о штатных негласных сотрудниках, с указанием конкретного перечня документов, подлежащих рассекречиванию.

6. Документы, фиксирующие содержание и результаты проведения оперативно-розыскных мероприятий, в том числе протоколы

[1] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68.

изъятия электронных носителей, оперативного наблюдения, перехвата компьютерной информации и т. п.

7. Справки кредитных организаций, документы и видеозаписи, включая записи камер видеонаблюдения, банкоматов и пр.

8. Заключение специалиста о результатах исследования электронных носителей информации, а также иных объектов, изъятых в ходе оперативно-розыскных мероприятий.

9. Копии запроса, направляемого в НЦБ Интерпола, по форме, определенной в приложении 9 к Инструкции по линии Интерпола.

Справочно:

Инструкцией по организации информационного обеспечения сотрудничества по линии Интерпола[1] установлено, что в ходе проведения оперативно-розыскных мероприятий, дознания или предварительного следствия по преступлениям экономической направленности через НЦБ Интерпола может быть получена следующая информация:

а) официальные наименования юридических лиц, зарегистрированных за рубежом;

б) их юридический адрес, номер, дата регистрации;

в) фамилии и имена физических лиц – руководителей (в отдельных случаях – учредителей, акционеров);

г) направление деятельности;

д) размеры уставного капитала;

е) сведения криминального характера о деятельности юридических и физических лиц.

В отдельных случаях через НЦБ Интерпола возможно получение сведений о наличии недвижимости и иной собственности за рубежом у лиц, являющихся фигурантами дел оперативного учета, а также подозреваемых или обвиняемых в совершении тяжкого преступления, при условии, если известно предполагаемое местонахождение (регистрация) объектов собственности (страна, штат, регион, город, компания), а также получение ограниченной информации по некоторым вопросам финансово-хозяйственной деятельности юридических лиц (выполнение контрактов, финансовое положение), если запрашиваемая информация не относится к коммерческой тайне. Получение указанных сведений и истребование копий финансово-хозяйственных и других коммерческих документов по каналам

[1] Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола: приказ МВД России, Минюста России, ФСБ России, ФСО России, ФСКН России, ФТС России от 6 октября 2006 г. № 786/310/470/454/333/971.

Интерпола зависит от добровольного согласия проверяемых лиц на предоставление документов и дачу объяснений.

Сведения, составляющие банковскую тайну, в том числе об открытии физическими и юридическими лицами счетов в банках и о движении денежных средств по ним, могут быть получены от правоохранительных органов иностранных государств – членов Интерпола только после рассмотрения соответствующим органом юстиции, прокуратуры или судом иностранного государства официального обращения (международного следственного поручения по уголовному делу) Генеральной прокуратуры Российской Федерации, копия которого может быть передана по каналам Интерпола.

10. Иные материалы, в том числе объяснения лиц, располагающих информацией, имеющей значение для дела, а также иные объекты, полученные в ходе оперативно-розыскных мероприятий.

Органом, осуществляющим оперативно-разыскную деятельность, при подготовке и оформлении для передачи уполномоченным должностным лицам (органам) материалов, документов и иных объектов, полученных при проведении оперативно-розыскных мероприятий, должны быть приняты необходимые меры по их сохранности и целостности (защита от деформации, размагничивания, обесцвечивания, стирания и др.). При представлении фонограммы к ней прилагается бумажный носитель записи переговоров.

Допускается представление материалов, документов и иных объектов, полученных при проведении оперативно-розыскных мероприятий, в копиях (выписках), в том числе с переносом наиболее важных частей (разговоров, сюжетов) на единый носитель, о чем обязательно указывается в сообщении (рапорте), на бумажном носителе записи переговоров. В этом случае оригиналы материалов, документов и иных объектов, полученных при проведении оперативно-розыскных мероприятий, если они не были в дальнейшем истребованы уполномоченным должностным лицом (органом), хранятся в органе, осуществившем оперативно-розыскные мероприятия, до завершения судебного разбирательства и вступления приговора в законную силу либо до прекращения уголовного дела (уголовного преследования).

Результаты оперативно-разыскной деятельности, представляемые для решения вопроса о возбуждении уголовного дела, должны содержать достаточные данные, указывающие на признаки преступления, а именно сведения: о том, где, когда, какие признаки и какого именно преступления обнаружены; при каких обстоятельствах имело место их обнаружение; о лице (лицах), его совершившем (если они известны), и очевидцах преступления (если они извест-

ны); о местонахождении предметов и документов, которые могут быть признаны вещественными доказательствами по уголовному делу; о любых других фактах и обстоятельствах, имеющих значение для решения вопроса о возбуждении уголовного дела.

Так, например, результатом такого оперативно-розыскного мероприятия, как прослушивание телефонных переговоров является соответствующая аудиозапись телефонных переговоров, общий объем которых в оцифрованном виде может превышать десятки гигабайт. При этом, наряду со сведениями, имеющими значение для дела, такие аудиозаписи содержат в большом количестве нейтральные сведения. В этом случае в орган предварительного расследования предоставляются аудиозаписи и распечатки наиболее значимых переговоров, содержащих информацию, имеющую отношение к расследуемому событию, в том числе информацию об осознании членами преступной группы преступного характера совершаемых ими действий.

Также большой объем информации может содержаться по результатам снятия информации с технических каналов связи. В этом случае в орган предварительного расследования представляется справка, включающая распечатку наиболее значимых электронных писем, сведения об онлайн-платежах и пр.

С учетом данных, полученных в результате предварительной проверки сообщения о преступлении, совершенном с использованием информационно-коммуникационных технологий, принимается решение о возбуждении уголовного дела, об отказе в возбуждении уголовного дела или передаче сообщения о преступлении по подследственности в соответствии с положениями ст. 151 УПК РФ.

В следственной практике зачастую возникает неопределенность, связанная с установлением места совершения преступления и, соответственно, местом производства предварительного расследования. Это обстоятельство обусловлено тем, что в механизме преступлений, совершенных с использованием информационно-коммуникационных технологий, присутствует несколько мест локализации следов: место жительства субъекта преступления, место его подключения к сети Интернет, местонахождение потерпевшего, адреса открытия и обслуживания его банковских счетов, адреса открытия и обслуживания банковских счетов, на которые переведены похищенные денежные средства, и т. д.

Следственным департаментом МВД России в органы предварительного следствия направлены директивные указания от 20 июня 2014 г. № 17/3-16230 об исключении фактов необоснованного перенаправления в порядке ст. 152 УПК РФ материалов доследственной

проверки о преступлениях рассматриваемой категории, влекущих увеличение сроков ее проведения и утрату следов преступления, необходимости при наличии достаточных оснований принимать процессуальное решение о возбуждении уголовного дела по месту поступления заявления о совершенном преступлении.

Кроме того, заместитель Генерального прокурора Российской Федерации В. Я. Гринь в информационном письме от 3 ноября 2015 г. № 36-11-2015 предлагает при осуществлении прокурорского надзора при передаче материалов проверок и уголовных дел учитывать следующую позицию: «...правомерным является признание территориальной подследственности в субъекте Российской Федерации, где непосредственно выполнялись действия, входящие в объективную сторону преступления, вне зависимости от того, что последствия наступили на другой территории, а также по месту наступления общественно опасных последствий ...».

Следует подчеркнуть, что независимо от источника исходной информации о преступлении его эффективное расследование возможно при условии оперативного сопровождения со стороны органа дознания. При этом в соответствии с п. 6.7 Решения совещания у заместителя Министра внутренних дел Российской Федерации – начальника Следственного департамента МВД России от 29 июля 2016 г. № 3 в целях устранения недостатков работы, повышения эффективности деятельности органов предварительного следствия введено в практику принятие процессуальных решений по сообщениям о преступлениях, предусмотренных ст. 159–159.6, 160, 165, 171, 172, 174, 174.1, 193, 193.1, 195–197, 200.1, 200.2, 200.3, 201, 272–274, 285, 286 УК РФ, если они совершены в кредитно-финансовой сфере, оборонно-промышленном, жилищно-коммунальном, топливно-энергетическом, агропромышленном комплексах, в сфере государственного оборонного заказа, информационных технологий (за исключением мошенничеств с использованием мобильных телефонных средств связи), долевого строительства многоквартирных домов, а также связаны с деятельностью «финансовых пирамид», и повлекли причинение ущерба либо извлечение незаконного дохода в сумме, превышающей 6 млн руб., только следователями. При этом в соответствии с указанием Следственного департамента МВД России от 20 июня 2014 г. № 17/3-16230 в органах предварительного следствия МВД России регионального и городского (окружного) уровня с 1 июля 2014 г. организовано закрепление следователей, специализирующихся на расследовании преступлений в сфере информационных технологий, с учетом достаточного опыта работы в органах предварительного следствия и наличия специальных познаний

в указанной области. Аналогичное требование содержится и в указании Следственного департамента МВД России от 15 августа 2014 г. № 17/2-21427 с тем лишь уточнением, что количество закрепленных за данным направлением следователей должно быть не менее двух, а также в иных организационно-управленческих документах[1].

Указанием Следственного департамента МВД России от 26 декабря 2017 г. исх. № 17/3-4125 «Об организации расследования преступлений, совершенных с использованием современных информационно-коммуникационных технологий» начальникам следственных органов регионального уровня и приравненных к ним следственных органов МВД России поручено обеспечить заблаговременное обсуждение материалов доследственных проверок в аппаратах следственных органов МВД России по субъектам Российской Федерации, уделяя особое внимание их полноте и качеству, проведению необходимых исследований, результатам оперативно-розыскных мероприятий по изобличению лиц, совершивших преступления, организовать результативное взаимодействие с оперативными подразделениями.

Особенности организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий

В современных условиях деятельность органов внутренних дел по установлению обстоятельств, подлежащих доказыванию в ходе досудебного производства, в силу особенностей механизма совершения рассматриваемых преступлений приобрела сложный и многоаспектный характер. Множественность источников информации о преступлении и лицах, его совершивших, потерпевших и свидетелях, комплексность методов и средств ее поиска и получения, проверки и оценки объективно предполагают участие в этом процессе нескольких субъектов, каждый из которых в пределах своей компетенции вносит свой вклад в реализацию задач уголовного судопроизводства.

В этой связи без эффективной совместной оперативно-служебной деятельности подразделений органов внутренних дел при раскрытии и расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий, невозможно выполнение ключевой задачи уголовного судопроизводства – защи-

[1] См.: п. 4 указания Следственного департамента МВД России от 26 декабря 2017 г. исх. № 17/3-4125 «Об организации расследования преступлений, совершенных с использованием современных информационно-коммуникационных технологий».

ты прав и законных интересов лиц и организаций, потерпевших от преступлений.

В целом взаимодействие при расследовании преступлений организуется следователями и начальниками органов предварительного следствия (каждый на своем уровне) в соответствии с положениями УПК РФ, Закона об ОРД, ведомственными нормативными правовыми актами, в том числе Инструкцией по организации совместной оперативно-служебной деятельности подразделений органов внутренних дел Российской Федерации при раскрытии преступлений и расследовании уголовных дел, утвержденной приказом МВД России от 29 апреля 2015 г. № 495дсп, а также локальными правовыми актами территориальных органов МВД России на окружном, межрегиональном, региональном и районном уровнях.

По данным обзора о состоянии организации совместной работы подразделений МВД России при раскрытии преступлений и расследовании уголовных дел[1], более чем в 40 территориальных органах МВД России на региональном уровне практикуется создание специализированных следственных подразделений, постоянно действующих следственно-оперативных групп по раскрытию и расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий, в частности по раскрытию и расследованию мошенничества с использованием мобильных средств связи и сети Интернет.

Так, в структуре УУР ГУ МВД России по Краснодарскому краю создан отдел организации раскрытия мошенничества общеуголовной направленности штатной численностью 8 единиц. В территориальных подразделениях УР Краснодарского края за линией мошенничества, совершенного с использованием средств связи, закреплены конкретные сотрудники, что позволило повысить качество оперативно-служебной деятельности при раскрытии и оперативном сопровождении уголовных дел, возбужденных по фактам совершения мошенничеств, совершенных дистанционно. Взаимодействие УУР, БСТМ и следственных органов осуществляется в рамках специализированной следственно-оперативной группы[2], деятельность которой позволила оперативно решать вопросы, возникающие при проведении оперативно-розыскных, технических мероприятий и следственных действий при расследовании мошенничества, совершенного дистанционно.

---

[1] Указание Следственного департамента МВД России от 31 октября 2017 г. № 17/2-33775.

[2] Приказ ГУ МВД России по Краснодарскому краю от 24 июня 2016 г. № 704.

В соответствии с положениями ст. 38 УПК РФ и ведомственными нормативными правовыми актами МВД России следователь обеспечивает организацию совместной работы по расследованию в рамках уголовного дела, обладая полномочиями давать органу дознания обязательные для исполнения письменные поручения о проведении оперативно-розыскных мероприятий, производстве отдельных следственных действий, исполнении постановлений о задержании, приводе, аресте, производстве иных процессуальных действий, а также получать содействие при их осуществлении.

Однако до настоящего времени не искоренена практика формального отношения к исполнению поручений, данных органу дознания. Ответы на поручения по уголовным делам о неочевидных преступлениях зачастую однотипны, содержат информацию об отработке одних и тех же лиц по разным преступлениям, причастность которых не установлена, или без указания проведенных мероприятий по установлению виновных лиц, похищенного имущества. Имеются факты несвоевременного исполнения поручений либо не в полном объеме.

Практика показывает, что оперативное сопровождение расследования уголовных дел осуществляется лишь на первоначальном этапе – «по горячим следам» до установления лица, подлежащего привлечению в качестве обвиняемого. В дальнейшем активность участия оперативных подразделений по установлению похищенного имущества, дополнительных свидетелей и иных обстоятельств, подлежащих доказыванию, снижается. Оперативное сопровождение, вплоть до окончания расследования и направления уголовного дела в суд, осуществляется лишь по резонансным преступлениям, а по остальному массиву уголовных дел – в единичных случаях, в виде сбора дополнительной информации или обеспечения привода потерпевших, свидетелей, обвиняемых.

Еще одним направлением повышения эффективности внешнего взаимодействия участников расследования является использование территориальными органами внутренних дел систем электронного документооборота, а также заключение соглашений об информационном обмене с кредитно-финансовыми организациями и организациями связи. Во исполнение п. 1.1. Решения Коллегии МВД России от 24 октября 2017 г. № 3км «О мерах по совершенствованию организации раскрытия и расследования мошенничеств» в Следственном департаменте МВД России проанализирована организация деятельности территориальных органов МВД России на окружном, межрегиональном и региональном уровнях по заключению соглашений с подразделениями ПАО «Сбербанк России», другими

кредитно-финансовыми организациями, в том числе не имеющими собственной филиальной сети в регионах, территориальными органами ФНС России и Росреестра, уполномоченными многофункциональными центрами (далее – МФЦ), органами социальной защиты населения, расположенными на территориях субъектов Российской Федерации, об электронном обмене документами и информацией, а также эффективность взаимодействия с данными организациями при раскрытии и расследовании мошенничеств.

Результаты анализа показали востребованность систем электронного документооборота с ведущими кредитными учреждениями и операторами сотовой связи с возможностью получения информации по всей территории Российской Федерации.

По состоянию на март 2018 г. на основе соглашения между МВД России и ПАО «Сбербанк России» от 23 октября 2017 г. об обмене информацией в электронном виде 24 территориальными органами внутренних дел заключены договоры с региональными представительствами указанной кредитной организации, еще в ряде субъектов Российской Федерации данный вопрос находится в стадии согласования. В соответствии с вышеназванным соглашением электронный документооборот между сторонами осуществляется на принципах конфиденциальности, согласованности действий, взаимопомощи и безвозмездности при соблюдении требований федеральных законов, в частности от 27 июля 2006 г. № 147-ФЗ «Об информации, информационных технологиях и о защите информации», от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» и иных нормативных правовых актов.

Отдельными территориальными органами внутренних дел дополнительно заключены соглашения об электронном обмене информацией с КИВИ Банк (АО), которые позволяют получить в срок до 3 суток необходимые сведения о владельце «QIWI-кошелька» и произведенных им транзакциях за интересующий период.

Кроме того, существует положительная практика заключения соглашений об электронном документообороте с организациями связи, в частности с ПАО «Мегафон», в рамках которых в срок до 10 дней становится возможным получение сведений об анкетных данных абонента по номерам телефона и SIM-карты, ИНН юридического лица, а также подключенных услугах и платежах.

Так, МВД по Республике Марий Эл с января 2016 г. в рамках заключенного с территориальным отделением ПАО «Сбербанк России» соглашения используется система удаленного доступа «SBERSIGN», предоставленная кредитной организацией, позволяю-

щая посредством электронного документооборота в срок до 7 дней получать информацию об открытых расчетных счетах клиента, движении денежных средств, а также данные о подключении услуг дистанционного банковского обслуживания «Мобильный банк» и соответствующих номерах телефонов.

Сведения о производимых по банковским картам транзакциях предоставляются на основании ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» без получения судебного решения, что позволяет существенно уменьшить временные затраты на получение необходимой информации и сократить срок предварительного следствия.

Помимо этого, в указанном подразделении функционируют системы по электронному обмену документами и информацией с ПАО «Мегафон» и ПАО «Вымпелком».

В ГУ МВД России по Пермскому краю успешно используется система электронного документооборота в рамках заключенного в 2015 г. соглашения с ПАО «Сбербанк России». Соглашение предусматривает возможность осуществления блокировки лицевых счетов абонентов на стадии регистрации заявления о преступлении. Кроме того, подписаны соответствующие соглашения с КИВИ Банк (АО), ПАО «Почта Банк», ПАО «Мегафон», а также Федеральной службой по государственной регистрации кадастра и картографии по Пермскому краю.

Восточно-Сибирским ЛУ МВД России на транспорте с июля 2017 г. действует соглашение о сотрудничестве с КИВИ Банк (АО) в области обмена оперативной и иной информацией по уголовным делам и делам оперативной проверки, предусматривающее возможность предоставления посредством электронного документооборота в течение 1–2 суток необходимых сведений о владельце «QIWI-кошелька» и произведенных им транзакциях за интересующий период.

С сентября 2016 г. Главным следственным управлением ГУ МВД России по г. Москве в рамках соглашения конкретный сотрудник имеет возможность доступа к автоматизированной системе обработки запросов ОАО «Мегафон».

Указанная система предоставляет возможность направления электронных запросов (с приложением соответствующих разрешительных документов) по находящимся в производстве следователей ГСУ уголовным делам о предоставлении различных сведений об абонентах сети и получения ответов на них. Ответ на запрос инициатора поступает в виде сопроводительного письма в формате «pdf», подписанного электронной подписью уполномоченного сотрудника ОАО «Мегафон»,

с приложением запрашиваемых данных в формате «xls» с указанием имени, точного размера и отпечатка файла. При этом имеется возможность обработки следующих следственных запросов:

1. Предоставление сведений об анкетных данных абонента по номеру телефона.

2. Предоставление сведений об анкетных данных абонента и номере телефона по номеру SIM-карты.

3. Предоставление сведений о номере телефона и данных абонента по ФИО и иным анкетным данным.

4. Предоставление сведений о номере телефона и данных абонента по ИНН юридического лица.

5. Предоставление сведений о подключенных абонентом услугах, а также платежах.

Предполагается дальнейшее наращивание функционала системы за счет обеспечения возможности направления запросов с обязательным приложением соответствующих постановлений суда, с последующим получением на электронном носителе в офисе ПАО «Мегафон» информации:

– о телефонных соединениях абонента (детализации) с указанием базовых станций по номеру телефона;

– обо всех телефонных соединениях абонентов оператора связи, находившихся в конкретном месте (биллинга);

– о телефонных соединениях абонента (детализации) с указанием базовых станций по номеру IMEI телефона.

Наличие у правоохранительных органов подобных каналов информационного взаимодействия позволяет повысить эффективность деятельности по выявлению, раскрытию и расследованию преступлений, а также усилить защищенность граждан от противоправных посягательств.

Особенности организации первоначального этапа расследования преступлений против собственности, совершенных с использованием информационно-коммуникационных технологий

Эффективное расследование преступлений, совершенных с использованием информационно-коммуникационных технологий, возможно при выполнении определенного алгоритма действий.

1. Выполнить комплекс процессуальных действий с заявителем:

– незамедлительно после принятия решения о возбуждении уголовного дела уведомить о принятом решении заявителя. Если уголовное дело возбуждается в отношении конкретного лица, то ему вручается копия постановления о возбуждении против него уголовного дела (п. 1. ч. 4 ст. 46 УПК РФ);

– вынести постановление о признании заявителя потерпевшим;

– допросить потерпевшего об обстоятельствах совершения преступления. Если совершено хищение принадлежащих ему денежных средств, в протоколе допроса подлежит отражению обстоятельства обнаружения хищения: какие именно действия были выполнены потерпевшим лично до и после совершения преступления; с какой целью, предпринимались ли им какие-либо действия по установлению лица, совершившего преступление, самостоятельно; если да, то с использованием какой техники и программного обеспечения; предоставлялись ли потерпевшим кому-либо сведения о себе, с какими лицами, по каким адресам в сети Интернет он обращался; имеются ли скриншоты переписки; на какие именно электронные кошельки, расчетные счета производил перечисления денежных средств; с использованием каких сервисов осуществлялась коммуникация с лицом, совершившим преступление; какова точная сумма причиненного преступлением ущерба (с учетом имущественного положения физического лица, размера его личных доходов, доходов семьи, наличия иждивенцев, кредитных или иных имущественных обязательств); каков круг лиц, которым могло быть известно о наличии денежных средств на банковских счетах, а также кто из них имел возможность доступа к управлению счетами потерпевшего, в том числе к его мобильному телефону; поступали ли потерпевшему в период, предшествующий хищению денежных средств, SMS-сообщения или электронные письма с указанием попыток осуществления транзакций, которые он не совершал; не было ли сбоев в работе аккаунтов в социальных сетях; сообщал ли данные своих счетов кому-либо в ходе телефонных разговоров, в том числе с сотрудниками банков. Если будут установлены подобные факты, у потерпевшего нужно выяснить всю информацию, касающуюся передачи сведений о своих счетах и режима доступа к ним, принять меры по сохранности поступивших потерпевшему сообщений и иной информации;

– получить исковое заявление, вынести постановление о признании гражданским истцом;

– в случаях наличия у потерпевшего документов, подтверждающих факт совершения хищения (платежных поручений, приходных кассовых ордеров, скриншотов, фиксирующих перевод денежных средств в платежных системах, претензионных требований со стороны третьих лиц), и / или документов, отражающих переписку потерпевшего с лицом, совершившим преступление (чаще всего скриншоты экрана с перепиской в социальных сетях

или посредством электронной почты), – вынести постановление о производстве их выемки и произвести их изъятие в установленном порядке;

– провести осмотр компьютерной техники потерпевшего, в ходе которого фиксировать сведения, имеющие доказательственное значение (переписка с лицом, совершившим преступление, сведения о переводе средств в электронных платежных системах). Целесообразно оформлять приложения к протоколу следственного действия в виде скриншотов экрана компьютера (с целью обеспечения наглядности);

– принять решение о признании и приобщении к материалам уголовного дела в качестве вещественных доказательств изъятых предметов и документов.

Важнейшей задачей данного этапа является установление способа совершения преступления.

2. Одним из ключевых элементов в расследовании по уголовным делам о преступлениях, совершенных с использованием информационно-коммуникационных технологий, является установление лица, совершившего преступление.

В большинстве случаев на данное лицо указывает местонахождение электронно-вычислительной техники, которая использовалась в качестве орудия преступления.

При совершении хищений денежных средств с использованием систем дистанционного банковского обслуживания осуществляется управление электронными счетами и (или) ведется переписка с потерпевшими. В данной ситуации с целью установления лица, совершившего хищение денежных средств, необходимо:

– получить сведения о движении денежных средств потерпевшего в кредитной организации или у оператора платежной системы на основании запроса следователя, согласованного с руководителем следственного органа (в соответствии с требованиями ст. 26 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» и ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»);

– на основании запросов в обозначенные организации необходимо также получить сведения, указанные владельцем счета при его регистрации, а также сведения об IP-адресах, с которых осуществлялась регистрация в системе дистанционного банковского обслуживания и доступ к счету при совершении сомнительной транзакции;

– в случаях перемещения похищенных денежных средств с использованием платежных систем, операторами которых явля-

ются юридические лица, зарегистрированные за пределами Российской Федерации, следует в установленном порядке направить запрос об оказании международно-правовой помощи;

– полученную на основании вышеуказанных запросов информацию об IP-адресах проверить посредством открытого интернет-сервиса, расположенного по адресу https://www.ripe.net/, или любого другого схожего с ним по функциональности сервиса, позволяющего установить принадлежность IP-адреса к конкретному провайдеру. Дальнейшие действия будут зависеть от того, каков этот IP-адрес: статический или динамический;

– в случае совершения спорных транзакций со статического IP-адреса на основании судебного решения необходимо произвести выемку сведений об абонентах в организации-провайдере, которой принадлежат интересующие следствие IP-адреса, либо в порядке п. 4. ч. 2 ст. 38 УПК РФ дать поручение органам дознания на получение данной информации[1]. В соответствии с положениями ст. 53 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» к сведениям об абонентах относятся фамилия, имя, отчество или псевдоним абонента-гражданина, наименование (фирменное наименование) абонента – юридического лица, фамилия, имя, отчество руководителя и работников этого юридического лица, а также адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента. Данные сведения укажут, что именно с компьютерной техники конкретного абонента или организации, находящейся по конкретному адресу, осуществлялись спорные онлайн-транзакции, велась определенная переписка и т. д.

При установлении конкретного лица, совершившего противоправные действия с использованием статического IP-адреса, следует принять во внимание, что такими адресами пользуются, как правило, крупные организации или государственные органы. В таких организациях нередко предоставляется публичный (сво-

[1] В соответствии с п. 1.1. ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, указанную информацию, информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами.

бодный) доступ в сеть Интернет всем желающим (на основании процедуры регистрации) либо имена и пароли для своих сотрудников и посетителей. В обоих случаях конкретному пользователю выделяется IP-адрес, под которым он получает доступ в Интернет. Сведения, содержащиеся в этом журнале (IP-адрес, предоставленный конкретному пользователю, сведения об интернет-адресах, к которым осуществлялось подключение с данного IP-адреса, дата, место, время начала и окончания доступа, MAC-адрес сетевой карты, номере SIM-карты, через которую произошла авторизация пользователя при подключении к Интернету, используемая им операционная система и браузер), также подлежат изъятию посредством выемки;

– если доступ в сеть Интернет осуществлялся с динамического IP-адреса и с использованием SIM-карты оператора сотовой связи, то для идентификации соответствующего лица необходимо запросить у оператора сотовой связи детализацию звонков, а также данные о способах пополнения финансового баланса SIM-карты. Если для пополнения баланса использовался электронный кошелек отечественной платежной системы (Яндекс.Деньги) или банковские карты, эмитированные отечественными банками, то последующие запросы необходимо направить этим субъектам для предоставления сведений о том, кто является владельцем электронного кошелька либо кто является клиентом (держателем) счета банковской карты.

Для установления лица, разместившего в социальной сети какую-либо противозаконную информацию, необходимо:

– направить запрос администратору социальной сети с постановкой следующих вопросов: когда и во сколько была создана группа (указывается название соответствующей группы в социальной сети) или размещено фото-, видеоматериал (указывается название файла в конкретной группе) по адресу (приводятся данные из адресной строки); каков логин пользователя социальной сети, создавшего группу или разместившего фото-, видеоматериал; во сколько зашел и во сколько вышел пользователь с сайта социальной сети при создании группы (размещении фото-, видеоматериала); какие идентификационные данные сообщил при регистрации пользователь (фамилия, имя, отчество, номер мобильного телефона, адрес электронной почты и т. д.); каков IP-адрес пользователя, создавшего группу или разместившего фото-, видеоматериал в указанные дату и время доступа; какие операционная система и браузер используются на компьютере указанного пользователя.

Адреса для направления запросов

Социальная сеть	Организация	Адрес
Mail.ru (Мой мир)	ООО «Мэйл.ру»	Ленинградский проспект, д. 79, стр. 39, г. Москва, 125167
Odnoklassniki.ru	ООО «Мэйл.ру»	Ленинградский проспект, д. 79, стр. 39, г. Москва, 125167
Vkontakte.ru (vk.com)	ООО «В контакте»	ул. Херсонская д. 12-14, литер А, помещение 1-Н, г. Санкт-Петербург, 191024
Mamba.ru	ЗАО «Мамба»	ул. 2я Звенигородская, д. 3, стр. 42, г. Москва, 123022
vkrugudruzei.ru	ООО «КМ онлайн»	ул. Пришвина, д.8, корп. 1, г. Москва, 127549
Loveplanet.ru	Группа компаний «РосБизнесКонсалтинг»	ул. Профсоюзная, д. 78, стр.1, г. Москва, 117393

– определить провайдера, за которым закреплен IP-адрес, выделенный искомому пользователю, разместившему противоправный контент. Это можно сделать, используя сервис **www.whois-service.ru**, в поисковую строку которого вводится интересующий IP-адрес, после чего система представит ответ о данных провайдера, который выдал соответствующий адрес[1];

– направить запрос провайдеру с постановкой следующих вопросов: кому из пользователей выделен указанный IP-адрес (указывается дата, время доступа на сайт социальной сети и время выхода из нее, когда была создана группа или размещено видео); к какому виду относится этот IP-адрес – статический или динамический? Использовался ли NAT[2] при предоставлении доступа этому клиенту к сети Интернет; если использовался статический IP-адрес, то необходимо потребовать предоставить имеющиеся данные о физическом лице, заключившим договор с провайдером, а также MAC-адрес

[1] Для европейской части сети действует поисковая система по адресу: www.ripe.net.

[2] NAT – это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

компьютерного устройства, через который предоставлен доступ к сети Интернет, физический адрес подключения, номер SIM-карты, через которую произошла авторизация пользователя при подключении к Интернету (если использовалась), операционная система и браузер указанного компьютерного устройства; регистрировался ли с кем-либо из пользователей договор по доступу в сеть Интернет, MAC-адрес компьютерного устройства которого установлен провайдером по предыдущему пункту запроса, если да, то с кем; выделялся ли IP-адрес для пользователя, MAC-адрес компьютерного устройства которого был установлен провайдером по предыдущему пункту запроса, если да, то когда, во сколько, по какому адресу был осуществлен доступ в Интернет и какие ресурсы сети Интернет посещал пользователь; если использовался механизм NAT, то необходимо потребовать предоставить адрес местонахождения источника Wi-Fi, через который пользователь получил доступ в Интернет, и количество пользователей, получивших доступ в Интернет через этот источник и находившихся одновременно на сайте социальной сети (название) с (время) по (время).

– направить запросы другим провайдерам в населенном пункте по месту проверки сообщения (расследования уголовного дела) с постановкой следующих вопросов: регистрировался ли с кем-либо из пользователей договор по доступу в сеть Интернет, MAC-адрес компьютерного устройства (указывается номер, предоставленный провайдером по предыдущему запросу), если да, то с кем; выделялся ли IP-адрес для пользователя, MAC-адрес компьютерного устройства (указывается номер, предоставленный провайдером по предыдущему запросу), если да, то когда, во сколько, по какому адресу был осуществлен доступ в сеть Интернет и какие ресурсы сети Интернет посещал пользователь;

– направить запрос и судебное решение российскому оператору сотовой связи, номер SIM-карты которого использовался для авторизации пользователя при подключении к сети Интернет (может быть предоставлен провайдером исходя из вышеуказанного запроса) или номер SIM-карты которого указан при регистрации пользователя в социальной сети. В запросе ставятся следующие вопросы: на кого зарегистрирована SIM-карта (указывается предоставленный провайдером или администратором социальной сети номер); пополнялся ли баланс указанной SIM-карты способами, позволяющими идентифицировать плательщика (банковская карта, электронный кошелек отечественных платежных систем и т. п.), если да, то указать соответствующие идентификационные данные;

– направить запросы и судебные решения в банки (субъектам отечественных платежных систем и т. п.) с требованием предоставить пер-

сональные данные лиц, карты (электронные кошельки и т. п.) которых использовались для пополнения баланса номера SIM-карты (указывается соответствующий установленный номер);

– направить запрос и судебное решение в организацию, являющуюся администратором сервиса электронной почты, почтовый ящик которой указан при регистрации пользователя в социальной сети.

Сведения о наиболее распространенных в России сервисах электронной почты и организациях, осуществляющих их администрирование

E-mail	Компания	Адрес, телефон
@mail.ru, @inbox.ru, @list.ru, @bk.ru	ООО «Мэйл.Ру»	125167, Россия, Москва, Ленинградский проспект, д. 39, стр. 79 тел. +7 495 725-63-57
@yandex.ru	ООО «Яндекс»	119021, Москва, ул. Льва Толстого, 16, тел: +7 495 739-70-00
@rambler.ru, @lenta.ru, @myrambler.ru, @autorambler.ru, @ro.ru, @r0.ru	ООО «Рамблер Интернет Холдинг»	117105, Москва, Варшавское ш., 9, стр. 1, БЦ «Даниловская мануфактура», корпус «Ряды Солдатенкова» тел: +7 495 785-17-00
@qip.ru, @pochta.ru, @fromru.com, @front.ru, @hotbox.ru, @Hotmail.ru, @krovatka.su, @land.ru, @mail15.com, @mail333c.com, @newmail.ru, @nightmail.ru, @5ballov.ru, @aeterna.ru, @ziza.ru, @memori.ru, @photofile.ru, @fotoplenka.ru, @pochta.com, @nm.ru	ООО «Медиа Мир»	117485, Москва, Профсоюзная 84/32, тел: +7 495 363-11-11

Электронные почтовые ящики вида @gmail.com, @hotmail.com, @yahoo.com принадлежат сервисам электронной почты, находящимся в США.

В запросе необходимо поставить вопрос о предоставлении данных пользователя, указанных им при регистрации почтового ящика, сведений о его активности, IP-адреса и MAC-адреса компьютерного устройства, с которого осуществлена регистрация почтового ящика и с которого осуществлен доступ к указанному почтовому ящику за интересующий период времени, а также абонентском номере активации и восстановлении пароля владельца электронного почтового ящика.

Если предоставленные IP-адреса отличаются от уже полученных, то необходимо вновь направить запрос провайдеру с целью получения данных, которые могут идентифицировать владельца почтового ящика.

Если преступление совершено с *использованием интернет-сайта* (например, интерент-магазина, сайта-клона и т. п.), то порядок установления его владельца следующий:

– используя интернет-сервис Whois, в процессе следственного осмотра с участием специалиста получаем открытую информацию о лице, на которое зарегистрировано доменное имя (регистрант), и организации, на ресурсах которой размещается интернет-сайт с интересующим доменным именем;

– если в качестве владельца сайта указано Private Person (частное лицо), то необходимо направить запрос в компанию-регистратор домена. При этом следует иметь в виду, что в большинстве случаев регистрационные данные, которые предоставляет владелец домена, администрацией не проверяются и могут не соответствовать действительности. Кроме того, сервисом Whois предоставляется информация только для доменов второго уровня вида xxx.ru, информацию для доменов вида yyy.xxx.ru необходимо получать у владельцев домена второго уровня;

– в полученной информации в поле nserver, как правило, указан владелец веб-хостинга (технической площадки) сайта, который может предоставить регистрационные данные (могут быть недостоверными), а также IP-адреса авторизации, достоверные контактные данные, платежные реквизиты;

– при установлении адреса электронной почты – выполнить действия по установлению владельца электронного почтового ящика, описанные выше.

Если преступление совершено с *использованием электронного кошелька электронной платежной системы*, то порядок действий по установлению его владельца следующий:

– направить администратору платежной системы запрос о предоставлении регистрационных данных участника, зарегистриро-

вавшего электронный кошелек с идентификационным номером ..., информации о всех кошельках, зарегистрированных вышеуказанным участником, и истории операций по ним за весь имеющийся период с указанием IP-адресов, с которых происходила авторизация участника, а также в случае перечисления средств с кошельков, зарегистрированных данным участником, – аналогичной информации по другим участникам электронной платежной системы (за исключением сервисов обмена электронных денег) – получателям денежных средств;

Адреса для направления запросов

Платежная система	Организация	Адрес
«Webmoney»	ООО «ВебМани.Ру»	ул. Коровий вал, д.7, г. Москва, 119049
«Яндекс.Деньги»	ООО «ПС Яндекс. Деньги»	а/я 57, г. Москва, 119021
«QIWI»	ЗАО «QIWI банк»	мкр. Чертаново Северное, д. 1А, корп. 1, г. Москва, 117648.
Деньги@Mail.Ru	ООО «Деньги.Мэйл. Ру»	Ленинградский проспект, д. 39, стр. 79, г. Москва, 125167

– в полученных ответах будет содержаться информация, с каких IP-адресов осуществлялось управление данными кошельками (счетами) и куда переведены (где обналичены) деньги. Далее устанавливается местонахождение владельца запросами соответствующим интернет-провайдерам, которым принадлежат IP-адреса;

– при установлении адреса электронной почты – выполнить действия по установлению владельца электронного почтового ящика, описанные выше.

Если при совершении преступления использовалось сетевое оборудование, то его *местонахождение можно установить по MAC-адресу*.

С указанной целью необходимо:

– направить запрос интернет-провайдеру, через которого осуществлялся выход в Интернет, о предоставлении MAC-адреса оборудования соответствующего абонента, подключенного по IP-адресу...;

– направить запросы операторам связи для поиска оборудования с определенным MAC-адресом в их сети и предоставления регистрационных данных абонента, его использующего.

3. Получить в органах Росреестра информацию о собственниках объекта недвижимости, где находится электронно-вычислительная техника – орудие преступления.

4. В установленном законом порядке произвести обыск в жилище с участием специалиста в области компьютерных технологий (сотрудников ЭКЦ, специализирующихся на производстве компьютерных экспертиз или сотрудников Центра информационных технологий, связи и защиты информации (ЦИТСиЗИ) ГУ(У) МВД России по субъектам Российской Федерации). В ходе обыска обязательному изъятию подлежат следующие предметы и документы:

– компьютерная техника, электронные носители информации;

– документы, отражающие факты выдачи денежных средств;

– средства, предназначенные для защиты информации;

– свободные образцы почерка и подписи, содержащиеся в письмах, личных дневника, записных книжках и т. д.;

– машинописные тексты;

– литература, содержащая сведения, которые относятся к этапам подготовки, совершения и сокрытия хищений денежных средств с использованием сети Интернет;

– фотографии, видеозаписи (особенно важно их изъятие при расследовании преступлений, совершенных организованными группами в целях доказывания наличия устойчивых межличностных связей между их участниками);

– иные предметы и документы, имеющие доказательственное значение.

При проведении обыска по месту жительства лица, разместившего противоправный контент в социальной сети, либо у лиц, которые могут причастны к этому, на компьютерных устройствах этих лиц могут быть видеоролики, фотографии и переписка по e-mail, соответствующая характеру деяния, а в электронном журнале (log-файле) его компьютера могут быть данные о ресурсе, к которым осуществлялся доступ (социальная сеть), дата, время начала и окончания доступа. При изъятии компьютера и электронных носителей информации необходимо руководствоваться требованиями к их изъятию, предусмотренными ст.182, 183 УПК РФ.

5. Допросить в качестве подозреваемого лицо, совершившее преступление, выяснив у него:

– насколько он хорошо владеет компьютерной техникой и программным обеспечением;

– имеется ли компьютерная техника по месту проживания и по месту работы, кто имеет доступ к пользованию ей, уточнив ее технические характеристики;

– перечень конкретных операций с компьютерной информацией, которые подозреваемый выполняет на своем рабочем месте;

– как часто осуществляет выход в Интернет, наиболее часто посещаемые ресурсы;

– каким интернет-браузером пользуется при осуществлении выхода в Интернет, каковы его настройки (сохраняются ли история посещений, cache-память, cookie-файлы и т. п.);

– установлены ли на компьютере антивирусные или защитные программы, если да, узнать их наименование;

– имеются ли у него электронная почта, сайты, домашние страницы, каковы их реквизиты;

– каким образом настроен удаленный доступ к сети для выхода в Интернет (кто и когда производил настройку);

– каким образом взломана информационная защита компьютера потерпевшего: подбор или хищение ключей и паролей; отключение средств защиты; разрушение средств защиты; использование несовершенства защиты;

– знаком ли он с потерпевшим, если да, то с какого времени, в каких отношениях состоит;

– имеет ли он источник дохода, если да, уточнить его размер;

– имеются ли у него, его родственников, друзей счета в банках, электронные кошельки в платежных системах, как давно открыты, как часто пользуется этими счетами;

– поступали ли на указанные счета денежные средства, если да, то когда именно, от каких лиц, за какие услуги;

– осуществлял ли за конкретный период времени денежные переводы, в случае если осуществлял, то указать реквизиты денежного перевода;

– осуществлял ли за последнее время крупные покупки, если да, то когда именно, в какой период времени, каким способом производил оплату, имеются ли документы, подтверждающие факт покупки;

– имели ли место встречи с потерпевшим лично либо посредством видеосвязи (видеозвонки по мобильным устройствам, Skype и т. д.), если да, выяснить дату, время, место, цель встречи.

6. С учетом материалов уголовного дела избрать меру пресечения в отношении подозреваемого.

7. Произвести сбор материала, характеризующего личность подозреваемого.

8. Назначить по изъятой компьютерной технике и электронным носителям информации судебную экспертизу с целью выяснения следующих основных вопросов:

– какие операционные системы и браузеры установлены на представленном на исследование компьютере;

– соответствует ли дата и время, установленные на представленном на исследование компьютере, реальным, если нет, то как они отличаются от реальных;

– имеются ли на предоставленном на исследование устройстве сведения о сетевых соединениях в сети Интернет за период времени с (дата) по (дата) включительно;

– какова история посещений ресурсов сети Интернет на представленном компьютере с указанием даты и времени посещений;

– какой IP-адрес присваивался при посещении ресурсов сети Интернет с представленного на исследование компьютера;

– имеются ли на предоставленном на исследование устройстве (носителе информации) программы, которые определяются антивирусным программным обеспечением как «вредоносные», если да, то какие у них функциональные возможности, сетевые взаимодействия, способ проникновения и следы работы в системе;

– какие программы установлены в автозагрузку в оперативной системе на предоставленном на исследование устройстве;

– имеются ли на предоставленном на исследование носителе информации компьютерные программы или другая компьютерная информация, которые имеют функциональные возможности скрытно от пользователя копировать информацию, необходимую для аутентификации в операционной системе, но при этом не являются компонентом операционной системы, если да, то какие у них функциональные возможности, сетевые взаимодействия, способ проникновения в систему и следы работы в системе;

– имеются ли на предоставленном на исследование носителе информации средства удаленного администрирования и управления компьютером;

– имеются ли на предоставленном на исследование носителе информации сведения о логинах и паролях доступа к интернет-ресурсам, установленным программам, интернет-кошелькам, системам дистанционного банковского обслуживания и т. д., если да, то какие;

– имеются ли на предоставленном на исследование носителе информации сведения о человеке с ФИО (доступ к социальным сетям, переписка, паспортные данные и т. д.), если да, то каковы атрибуты соответствующих файлов их содержащих;

– имеются ли в дампе оперативной памяти сведения о запущенных процессах, сетевых соединениях, если да, то какие;

– имеются ли в дампе сетевого трафика сетевые соединения от / к следующим IP-адресам (перечисление IP-адресов);

– имеются ли на машинных носителях информации представленные на исследование объекты программного обеспечения, позволяющие пользоваться услугами электронной почты, если да, то какое программное обеспечение (название, версии);

– имеются ли на машинных носителях информации файлы, содержащие электронные почтовые сообщения, о каких электронных почтовых ящиках имеются сведения на представленных на исследование системном блоке;

– имеется ли на машинных носителях информации представленные на исследование объекты программного обеспечения, позволяющие пользоваться услугами мгновенного обмена сообщениями в сети Интернет, если да, то какое программное обеспечение (название, версии);

– имеются ли на машинных носителях информации представленные на исследование объекты в обнаруженных программах для мгновенного обмена сообщениями следы переписки в сети Интернет с другими абонентами, если да, то какие именно;

– какие MAC-адреса имеет сетевое оборудование представленных на экспертизу объектов;

– каким образом организован доступ (общий или ограниченный) к данным на представленном на исследование компьютере;

– имеются ли на представленном на исследование компьютере файлы (указываются интересующие по содержанию файлы с антисоциальной информацией);

– имеется ли на представленном на исследование компьютере удаленная информация, если да, то ее следует копировать на представленный носитель.

В случаях когда в ходе производства экспертизы необходимо устанавливать наличие переписки, содержащейся в файлах различных мессенджеров или электронной почты, а также ее содержание, рекомендуется перед ее началом получить постановление суда о разрешении производства осмотра корреспонденции. Получение указанного судебного решения будет в полной мере соответствовать уголовно-процессуальному принципу тайны переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений и гарантирует соблюдение соответствующего конституционного права.

В отношении log-файлов, полученных с сервера социальной сети, могут быть поставлены следующие вопросы:

– имеются ли данные указывающие на возможные случайные ошибки в представленных log-файлах, если да, то можно ли установить причину этих ошибок (неисправность работы ЭВМ, системы ЭВМ, сбои программного обеспечения и т. п.);

– имеются ли данные, указывающие на модификацию или удаление log-файлов, не вызванные случайными ошибками, если да, то каких именно и можно ли восстановить первоначальное содержание файлов.

В отношении log-файлов, полученных с сервера социальной сети, судебная компьютерная экспертиза может и не назначаться, а достоверность содержащейся в них информации может быть установлена иными более экономичными следственными действиями. Так, задачи первого и второго вопросов могут быть достигнуты осмотром носителя с log-файлами при участии специалиста, который может дать соответствующие необходимые разъяснения.

Современные мобильные устройства используются очень интенсивно в противоправной деятельности и содержат в себе большой объем криминалистически значимой информации, поэтому необходимо тщательно подходить к постановке вопросов перед экспертом, учитывая, что он устанавливает не факт, а обстоятельства совершения преступления. Помимо мобильного устройства для производства экспертизы, эксперту необходимо предоставить следующую информацию о преступном деянии:

1) от потерпевшего:

– о системах ДБО (наименование кредитной организации или сервиса, а также программного обеспечения; перечень устройств и услуг, для которых они использовались; велось ли протоколирование и т. д.);

– наблюдались ли отклонения от стандартного функционирования устройства в процессе ДБО;

– как и когда обнаружено происшествие (несанкционированная транзакция, факт мошенничества и т. д.);

– чем подтверждается (банковской выпиской, SMS-сообщением, записью телефонного разговора, протоколом работы программы, протоколами работы интернет-обозревателя и т. д.);

– использовались ли средства защиты информации (антивирусное программное обеспечение, защищенные каналы связи, криптографические средства защиты информации и т. д.);

– для каких еще целей использовалось мобильное устройство (звонки, SMS, работа с интернет-ресурсами, скачивание и просмотр фото-, видео- и мультимедиа файлов, игры и т. д.);

– источники получения системного (прошивки) и прикладного программного обеспечения (официальные и неофициальные ресурсы);

– источник получения устройства (приобретение у официального продавца, на рынке, подарок и т. д.);

2) из кредитной организации / банка:

– как и когда установлен факт кражи / мошенничества (заявление клиента, фиксация инцидента службой безопасности организации, сообщение от правоохранительных органов и т. д.);

– об операциях, произведенных потерпевшим (сумма, точное время, способ оплаты, номера реквизитов отправителя и получателя, номера платежных карт, номера телефонов, IP-адреса, IMEI-номера и т. д.);

– особенности организации ДБО с потерпевшим (привязка к абонентскому номеру, номеру аппарата, наличие ограничений на совершаемые действия и т. д.);

3) от оператора сотовой связи:

– о принятых и переданных SMS-сообщениях (биллинговая информация, в том числе номер телефона, IMEI);

– о телефонных соединениях (биллинговая информация, в том числе номер телефона, IMEI);

– о сетевом трафике;

4) от обвиняемого:

– всю информацию, которую он сообщит о преступлении.

9. Принять меры к установлению имущества подозреваемого, принадлежащих ему денежных средств, в том числе находящихся на расчетных счетах и электронных кошельках, на которые для возмещения ущерба и обеспечения гражданского иска необходимо наложить арест на основании судебного решения в порядке ст. 115 УПК РФ.

Дальнейшее планирование и производство предварительного расследования по уголовным делам о хищениях, совершенных с использованием сети Интернет, должно осуществляться исходя из доказательственной базы, собранной в рамках выполнения изложенного выше алгоритма.

Дополнительно укажем, что в случаях когда для совершения преступления использовались сайты-однодневки или фишинговые сайты, то следователю необходимо:

– направить поручение в подразделения «К» БСТМ регионального органа внутренних дел с целью установления организации – хостинга провайдера, а также регистратора доменных имен;

– направить запрос в установленные компании с целью установления сведений о лице, зарегистрировавшем сайт (обратившегося за предоставлением услуг хостинга), с указанием IP-адресов обращения, администрирования, сведений о способах оплаты услуг с указанием номеров счетов или электронных кошельков;

– в последующем необходимо выполнить действия, указанные в основном алгоритме расследования.

Отметим проблему, встречающуюся при расследовании рассматриваемой категории уголовных дел, даже с учетом выполнения рассмотренного выше алгоритма – использование преступниками прокси-серверов. Сущность этой проблемы заключается в следующем: лица, совершающие преступления, производят все операции с подконтрольными им счетами и аккаунтами с использованием специализированного программного обеспечения, позволяющего производить обращение к ресурсам через сервера, расположенные за территорией Российской Федерации. В таком случае операторы ресурса в сети Интернет фиксируют IP-адрес прокси-сервера, а не лица, отправившего конкретную команду. Выходом из подобной ситуации является направление запроса об оказании правовой помощи в страну, в которой зарегистрирован провайдер, с IP-адреса которого передана команда на проведение операции, с целью выяснения сведений об IP-адресе обращения к серверу, который может быть истинным адресом преступника.

Расследуя уголовные дела о преступлениях, совершенных с использованием информационных и коммуникационных технологий, необходимо учитывать возможную причастность к их совершению сотрудников кредитных организаций и в обязательном порядке, при наличии оснований, давать процессуальную оценку действиям этих лиц.

В марте 2016 г. СО СП № 7 СУ УМВД России по г. Тюмени в суд было направлено уголовное дело по обвинению Ч. в совершении двух преступлений, предусмотренных ч. 1 ст. 158 УК РФ, который, являясь сотрудником ПАО «Сбербанк России», оказал содействие К. и З. в подключении через банкомат услуги «Сбербанк Онлайн». Завладев выданными банкоматами чеками, содержащими логин и пароль к картам указанных лиц, Ч. похитил денежные средства ПАО «Сбербанк России» в сумме 54 тыс. руб. В мае 2016 г. приговором мирового судьи Калининского района г. Тюмени Ч. признан виновным и осужден к наказанию в виде штрафа в размере 10 тыс. руб.

В качестве еще одного примера можно отметить уголовное дело, находившееся в 2017 г. в производстве СО ОМВД России по Суздальскому району Владимирской области. Установлено, что менеджер по продажам дополнительного офиса ПАО «Сбербанк России» А. в ходе исполнения служебных обязанностей обладала правом доступа к автоматизированной системе «Филиал-Сбербанк», содержащей конфиденциальные сведения о клиентах кредитной организации, используя которые неоднократно проводила расходные операции по их банковским счетам, открыв от имени данных клиентов дополнительные пластиковые карты. Впоследствии перечисленные денежные средства обналичивались А. В апреле 2017 г. А. приговором

Суздальского районного суда Владимирской области признана виновной в совершении преступлений, предусмотренных п. «в» ч. 2 ст. 158, ч. 3 ст. 183, п. «в» ч. 2 ст. 158, ч. 3 ст. 183, п. «в» ч. 2 ст. 158, ч. 3 ст. 183 УК РФ. Ей назначено наказание в виде лишения свободы на срок 3 года 6 месяцев условно.

При совершении рассматриваемых преступлений в действиях виновных лиц могут содержаться признаки иных преступлений, чему должна даваться надлежащая правовая оценка.

Так, в сентябре 2016 г. СУ УМВД России по Тюменской области в суд направлено уголовное дело в отношении С. и М. по обвинению в совершении преступлений, предусмотренных ч. 4 ст. 159.6 и 174.1 УК РФ. Обвиняемые с 4 июня по 2 сентября 2015 г. путем ввода и блокирования компьютерной информации совершили хищение с расчетных счетов граждан денежных средств в сумме 400 тыс. руб., которые С. через терминал самообслуживания ПАО «Сбербанк России» без предоставления своих персональных данных ввел в законный наличный денежный оборот. С. и М. приговорены к 5 и 4 годам лишения свободы условно соответственно со штрафом 200 тыс. руб.

ГСУ ГУ МВД России по Свердловской области 21 марта 2015 г. возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 272 и ч. 1 ст. 159.6 УК РФ, в отношении Ш., который, используя персональный компьютер, подключенный к сети Интернет, запустил скопированную им в память устройства самообслуживания вредоносную программу, заблокировавшую системы кредитной организации и нарушившую правила эксплуатации. В результате совершения противоправных действий обвиняемый похитил денежные средства кредитной организации. 5 августа 2016 г. Кировградским районным судом Свердловской области Ш. признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 273, ч. 2 ст. 272, ч. 2 ст. 159.6 и ч. 1 ст. 274 УК РФ, и приговорен к 2 годам 6 месяцам лишения свободы.

Профилактическая деятельность по уголовным делам о преступлениях, совершенных с использованием информационных и коммуникационных технологий

Согласно ч. 2 ст. 158 УПК РФ, установив в ходе досудебного производства по уголовному делу обстоятельства, способствовавшие совершению преступления, дознаватель, руководитель следственного органа, следователь вправе внести в соответствующую организацию или должностному лицу представление о принятии мер по устранению указанных обстоятельств или других нарушений закона. Данное представление подлежит рассмотрению с обязательным уведомлением о принятых мерах не позднее одного месяца со дня его вынесения.

Указанием Следственного департамента МВД России от 26 декабря г. 2017 исх. № 17/3-4125 «Об организации расследования преступлений, совершенных с использованием современных информационно-коммуникационных технологий» начальникам органов предварительного следствия регионального уровня и приравненных к ним органов предписано обратить особое внимание на установление и устранение обстоятельств, способствующих совершению указанных преступлений, исключив формальный подход к выполнению данных полномочий.

В соответствии с ч. 1 ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» в целях ограничения доступа к сайтам в сети Интернет, содержащим информацию, распространение которой в Российской Федерации запрещено, создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено».

Ч. 3 ст. 15.1 вышеуказанного Федерального закона, п. 5.1.7 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228, на Роскомнадзор возложены функции по созданию, формированию и ведению Единого реестра.

В соответствии с ч. 5 ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ основанием для включения в Единый реестр сведений о сайте в сети Интернет является вступившее в законную силу решение суда о признании информации, распространяемой посредством сети Интернет, информацией, распространение которой в Российской Федерации запрещено, либо решение уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятое в отношении распространяемых посредством сети Интернет:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11 ноября 2003 г. № 138-ФЗ «О лотереях» о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи;

е) информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции;

ж) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети Интернет, информацией, распространение которой в Российской Федерации запрещено.

Постановлением Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» утверждены Правила создания, формирования и ведения Единого реестра, а также правила принятия уполномоченными органами решений в отношении отдельных видов информации и материалов, распространение которых в Российской Федерации запрещено.

Компетенция Министерства внутренних дел Российской Федерации о принятии решений о включении в Единый реестр информации, распространение которой запрещено, рассмотрена выше.

Роспотребнадзор принимает решения в отношении распространяемой посредством сети Интернет информации о способах совершения самоубийства, а также призывов к совершению самоубийства.

Роскомнадзор принимает решения в отношении:

– материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера, распространяемых посредством сети Интернет;

– информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, о способах и местах культивирования наркосодержащих растений и о способах совершения самоубийства и призывов к совершению самоубийства, размещенной в продукции средств массовой информации, распространяемой посредством сети Интернет;

– информации, распространяемой посредством сети Интернет, решение о запрете к распространению которой на территории Российской Федерации принято уполномоченными органами или судом.

Федеральная налоговая служба – в отношении распространяемой посредством сети Интернет информации, нарушающей требования Федерального закона от 29 декабря 2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11 ноября 2003 г. № 138-ФЗ «О лотереях» о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи.

Таким образом, полномочиями по самостоятельному принятию решений в отношении запрещенной информации Роскомнадзор обладает только в отношении указанной выше информации. Кроме того, Роскомнадзор не обладает полномочиями по обращению в суд с целью признания информации запрещенной к распространению в порядке, предусмотренном ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ. Представления, вносимые территориальным органам Роскомнадзора, должны содержать требования об ограничении доступа к информационному ресурсу, в отношении которого имеется либо соответствующее решение уполномоченного органа, либо судебное решение. Правом на обращение в суд с целью признания информации запрещенной к распространению обладают органы прокуратуры, что вытекает из положений ч. 1 ст. 45 ГПК РФ и ч. 1 ст. 39 КАС РФ.

Глоссарий

База данных – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимая от прикладных программ[1].

Блокирование информации – действие, искусственно затрудняющее доступ пользователей к компьютерной информации, не связанное с ее уничтожением, а также создание условий (в том числе и с помощью специальных программ), исключающих пользование компьютерной информацией ее законным владельцем.

Внешнее запоминающее устройство (ВЗУ) – запоминающее устройство, подключаемое к центральной части вычислительной системы и предназначенное для хранения большого объема данных[2].

Вычислительная сеть – взаимосвязанная совокупность территориально рассредоточенных систем обработки данных, средств и (или) систем связи и передачи данных, обеспечивающая пользователям дистанционный доступ к ее ресурсам и коллективное использование этих ресурсов[3].

Данные – информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека[4].

Доступ к информации – возможность получения информации и ее использования[5].

---

[1] Организация данных в системах обработки данных. Термины и определения [Электронный ресурс]: ГОСТ 20886-85. – Взамен ГОСТ 20886-75; введ. 1986-07-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015708.

[2] Оборудование периферийное систем обработки информации. Термины и определения [Электронный ресурс]: ГОСТ 25868-91. – Взамен ГОСТ 25868-83; введ. 1993-01-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015782.

[3] Телеобработка данных и вычислительные сети. Термины и определения [Электронный ресурс]: ГОСТ 24402-88. – Взамен ГОСТ 24402-80; введ. 1989-07-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015767.

[4] Системы обработки информации. Термины и определения [Электронный ресурс]: ГОСТ 15971-90. – Взамен ГОСТ 15971-84; введ. 1992-01-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015664.

[5] Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31 (ч. 1), ст. 3448.

Защита данных – организационные, программные и технические методы и средства, направленные на удовлетворение ограничений, установленных для типов данных или экземпляров типов данных в системе обработки данных[1].

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[2].

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[3].

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[4].

Информационный накопитель – устройство записи, воспроизведения и хранения информации.

И*нформационный носитель (носитель данных)* – материальный объект, предназначенный для записи и хранения данных[5] (диск, лента, твердотельный носитель).

Информация – сведения (сообщения, данные) независимо от формы их представления[6].

Компьютер – (англ. *computer* – «вычислитель») – устройство или система устройств, способная выполнять заданную (четко определенную или изменяемую) последовательность операций на основе различных свойств (механических, электронных, биологических, оптических, квантовых и других физических явлений) компонентов ее функциональных узлов; совокупность технических средств, создающая возможность проведения обработки информации и получение результата в необходимой форме[7].

---

[1] Организация данных в системах обработки данных. Термины и определения [Электронный ресурс]: ГОСТ 20886-85. – Взамен ГОСТ 20886-75; введ. 1986-07-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015708.

[2] *Там же.*

[3] *Там же.*

[4] *Там же.*

[5] Системы обработки информации. Термины и определения [Электронный ресурс]: ГОСТ 15971-90. – Взамен ГОСТ 15971-84; введ. 1992-01-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015664.

[6] *Там же.*

[7] *Там же.*

Компьютерная информация – 1) информация, находящаяся в памяти компьютера, на машинных или иных носителях, информационных системах, передающаяся по информационно-телекоммуникационным сетям и доступная для восприятия средствам вычислительной техники; 2) сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[1].

Компьютерная система – любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных[2].

Компьютерные данные – любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию[3].

Локальная вычислительная сеть (ЛВС) – вычислительная сеть, охватывающая небольшую территорию и использующая ориентированные на эту территорию средства и методы передачи данных[4].

Машинный носитель (данных) – сменный носитель данных, предназначенный для записи и считывания данных, представленных в стандартных кодах[5].

Несанкционированный доступ к информации – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

Оперативно-розыскное мероприятие – определенная в Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-

---

[1] Примечание 1 ч. 1 ст. 272. УК РФ.

[2] Конвенция о преступности в сфере компьютерной информации (ETS № 185) [Электронный ресурс]: заключена в г. Будапеште 23 ноября 2001 г. Конвенция на англ. языке опубликована не была. Пер. на рус. язык предоставлен Аппаратом Гос. Думы Федер. Соб. Рос. Федерации. Доступ из справ.-правовой системы «Консультант Плюс».

[3] *Там же.*

[4] Телеобработка данных и вычислительные сети. Термины и определения [Электронный ресурс]: ГОСТ 24402-88. – Взамен ГОСТ 24402-80; введ. 1989-07-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015767.

[5] Оборудование периферийное систем обработки информации. Термины и определения [Электронный ресурс]: ГОСТ 25868-91. – Взамен ГОСТ 25868-83; введ. 1993-01-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015782.

розыскной деятельности» и проводимая специально уполномоченными на то субъектами совокупность организационно-тактических действий по применению гласных и негласных сил, средств и методов, направленных на выявление фактических данных, необходимых для решения задач оперативно-розыскной деятельности.

Операционная система – совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг[1].

Периферийное оборудование – совокупность технических средств и программного обеспечения, предназначенная для взаимодействия центрального процессора с внешней средой и для хранения информации[2].

Получение компьютерной информации – это оперативно-розыскное мероприятие, которое заключается в применении технических средств и информационных технологий по обнаружению и фиксации информации, находящейся в компьютерах, информационных системах или на отдельных информационных накопителях (носителях), а также передаваемой по информационно-телекоммуникационным сетям, в целях ее дальнейшего получения, изъятия, использования и / или блокирования для решения задач оперативно-розыскной деятельности.

Программа – данные, предназначенные для управления конкретными компонентами системы обработки информации в целях реализации определенного алгоритма[3]; последовательность инструкций, определяющих решение конкретной задачи вычислительной системой[4].

---

[1] Системы обработки информации. Термины и определения [Электронный ресурс]: ГОСТ 15971-90. – Взамен ГОСТ 15971-84; введ. 1992-01-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015664.

[2] Оборудование периферийное систем обработки информации. Термины и определения [Электронный ресурс]: ГОСТ 25868-91. – Взамен ГОСТ 25868-83; введ. 1993-01-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015782.

[3] Обеспечение систем обработки информации программное. Термины и определения [Электронный ресурс]: ГОСТ 19781-90. – Взамен ГОСТ 19781-83 и ГОСТ 19.004-80; введ. 1992-01-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/gost-19781-90.

[4] Судебная компьютерно-техническая экспертиза. Термины и определения [Электронный ресурс]: ГОСТ Р 57429-2017 / введ. впервые 2017-09-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200144960.

Программа для электронно-вычислительных машин – представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения[1].

Средство вычислительной техники (СВТ) – совокупность технических устройств и программ, обеспечивающих их функционирование, способных функционировать самостоятельно или в составе других систем[2].

Технические средства системы обработки информации – все оборудование, включая носители данных, предназначенное для автоматизированной обработки информации[3].

Технический канал связи – одна из составляющих частей телекоммуникационной сети, состоящая из технических средств и устройств, обеспечивающих проводную и беспроводную связь по передаче и обмену информации во времени и в пространстве.

Техническое средство – совокупность технических устройств средств вычислительной техники либо их частей[4].

Технология TDM (цифровой канал E1) – мультиплексирование с временным разделением каналов. Технология передачи голосового сигнала в цифровом качестве, как правило, по волоконно-оптическому кабелю. Оптический передатчик преобразует входной электрический сигнал в модулированный световой поток для его дальнейшей передачи по оптоволокну к оптическому приемнику, который на выходе производит его обратную декодировку в электрический сигнал. Технология TDM применяется в цифровых системах связи для передачи нескольких каналов по одной линии связи. В России в качестве стандартной принята схема объединения нескольких каналов в один первичный цифровой канал, известный как канал E1. Этот стандарт получил большое распространение для

---

[1] Ст. 1261 ч. 4 Гражданского кодекса Рос. Федерации.

[2] Судебная компьютерно-техническая экспертиза. Термины и определения [Электронный ресурс]: ГОСТ Р 57429-2017 / введ. впервые 2017-09-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200144960.

[3] Системы обработки информации. Термины и определения [Электронный ресурс]: ГОСТ 15971-90. – Взамен ГОСТ 15971-84; введ. 1992-01-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015664.

[4] *Там же.*

подключения корпоративных телефонных систем и систем передачи данных к сетям операторов связи.

Удаленная атака – сканирование системы на предмет открытых портов с последующим захватом контроля над компьютером, что грозит финансовыми потерями или в лучшем случае приводит в негодность операционную систему.

Утилита – сервисная (вспомогательная) компьютерная программа в составе общего программного обеспечения для выполнения специализированных типовых задач, связанных с работой оборудования и операционной системы.

Электронная вычислительная машина (ЭВМ) – вычислительная машина, основные функциональные устройства которой выполнены на электронных компонентах[1].

Файл – идентифицированная совокупность экземпляров полностью описанного в конкретной программе типа данных, находящихся вне программы во внешней памяти и доступных программе посредством специальных операций[2].

Электронная почта – корреспонденция в виде сообщений, передаваемая между пользователями через вычислительную сеть[3].

Электронное устройство, предназначенное для негласного получения информации – специально изготовленное изделие, содержащее электронные компоненты, скрытно внедряемое (закладываемое или вносимое) в места возможного съема защищаемой акустической речевой, визуальной или обрабатываемой информации (в том числе в ограждения помещений, их конструкции, оборудование, предметы интерьера, а также в салоны транспортных средств, в технические средства и системы обработки информации)[4].

---

[1] Системы обработки информации. Термины и определения [Электронный ресурс]: ГОСТ 15971-90. – Взамен ГОСТ 15971-84; введ. 1992-01-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015664.

[2] Организация данных в системах обработки данных. Термины и определения [Электронный ресурс]: ГОСТ 20886-85. – Взамен ГОСТ 20886-75; введ. 1986-07-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015708.

[3] Судебная компьютерно-техническая экспертиза. Термины и определения [Электронный ресурс]: ГОСТ Р 57429-2017 / введ. впервые 2017-09-01 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200144960.

[4] Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя): постановление

IP-адрес (ай-пи адрес, сокращение от англ. *Internet Protocol Address*) – сетевой адрес узла в компьютерной сети, построенный по протоколу IP. При связи через сеть Интернет требуется глобальная уникальность адреса, в случае работы в локальной сети требуется уникальность адреса в пределах сети.

MAC-адрес (от англ. *Media Access Control* – управление доступом к среде) – это уникальный идентификатор, сопоставляемый с различными типами оборудования для компьютерных сетей.

Правительства Рос. Федерации от 16 апреля 2012 г. № 314 // Собр. законодательства Рос. Федерации. – 2012. – № 17, ст. 1988.

Список использованной литературы

Нормативные правовые акты

Конституция Российской Федерации : офиц. текст // Собр. законодательства Рос. Федерации. – 2014. – № 15. – Ст. 1691.

Уголовный кодекс Российской Федерации [Электронный ресурс] : федер. закон : [принят Гос. Думой 24 мая 1996 г. : по состоянию на 18 февраля 2019 г.] // Справ.-правовая система «Консультант Плюс». – М., 1997. – Режим доступа: http://www.consultant.ru.

Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс] : федер. закон : [принят Гос. Думой 22 ноября 2001 г. : по состоянию на 18 февраля 2019 г.] // Справ.-правовая система «Консультант Плюс». – М., 1997. – Режим доступа: http://www.consultant.ru.

О банках и банковской деятельности : федер. закон от 2 декабря 1990 г. № 395-1 // Собр. законодательства Рос. Федерации. – 1996. – № 6. – Ст. 492.

О связи : федер. закон от 7 июля 2003 г. № 126-ФЗ // Собр. законодательства Рос. Федерации. – 2003. – № 28. – Ст. 2895.

Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31 (Ч. 1). – Ст. 3448.

О полиции : федер. закон от 7 февраля 2011 г. № 3-ФЗ // Собр. законодательства Рос. Федерации. – 2011. – № 7. – Ст. 900.

Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации : постановление Правительства Рос. Федерации от 31 июля 2014 г. № 743 // Собр. законодательства Рос. Федерации. – 2014. – № 32. – Ст. 4516.

Об утверждении Правил уведомления организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций о начале осуществления деятельности по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, предназначенных и (или) используемых для приема, передачи, доставки и (или) обработки электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет», а также ведения реестра указанных организаторов : постановле-

ние Правительства Рос. Федерации от 31 июля 2014 № 746 // Собр. законодательства Рос. Федерации. – 2014. – № 32. – Ст. 4519.

Об утверждении Правил хранения организатором распространения информации в информационно-телекоммуникационной сети «Интернет» текстовых сообщений пользователей информационно-телекоммуникационной сети «Интернет», голосовой информации, изображений, звуков, видео-, иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет»: постановление Правительства Рос. Федерации от 26 июня 2018 г. № 728 // Собр. законодательства Рос. Федерации. – 2018. – № 27. – Ст. 4081.

Об основах организации ведомственного контроля за деятельностью органов внутренних дел Российской Федерации : приказ МВД России от 3 февраля 2012 г. № 77.

Об организации рассмотрения сообщений об отдельных видах преступлений экономической направленности : приказ МВД России от 1 декабря 2016 г. № 785.

Об утверждении Требований к оборудованию и программно-техническим средствам, используемым организатором распространения информации в сети «Интернет» в эксплуатируемых им информационных системах, для проведения уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, мероприятий в целях реализации возложенных на них задач [Электронный ресурс] : приказ Минкомсвязи России от 29 октября 2018 г. № 571 // Справ.-правовая система «Консультант Плюс». – М., 1997. – Режим доступа: http://www.consultant.ru.

Учебники, учебные пособия, монографии, статьи

Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникативных технологий / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2018. – № 4. – С. 145–150.

Гаврилин Ю. В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы / Ю. В. Гаврилин, А. В. Победкин // Труды Академии управления МВД России. – 2018. – № 3. – С. 106–114.

Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2017. – № 4. – С. 45–50.

Грибунов О. П. Расследование преступлений в сфере компьютерной информации и высоких технологий : учеб. пособие / О. П. Грибунов, М. В. Старчиков. – М. : ДГСК МВД России, 2017. – 159 с.

Климов Д. В. Расследование хищений, связанных с использованием сети «Интернет» : учеб. пособие / Д. В. Климов. – Н. Новгород : Нижегородская академия МВД России, 2017. – 24 с.

Основы теории электронных доказательств : монография / под ред. С. В. Зуева. – М. : Юрлитинформ, 2019. – 400 с.

Петров В. А. Выявление, квалификация и организация расследования преступлений, совершенных с использованием криптовалюты : учеб.-метод. пособие / В. А. Петрова. – М. : Юрлитинформ, 2017. – 200 с.

Расследование мошенничества в сфере компьютерной информации : учеб. пособие / авт.-сост. П. А. Капустюк [и др.]. – Иркутск : Восточно-Сибирский ин-т МВД России, 2018. – 47 с.

Тактика следственных действий, направленных на отыскание, обнаружение, изъятие и исследование электронных носителей и информации на них : учеб. пособие / А. А. Кузнецов [и др.]. – Омск : Омская академия МВД России, 2015. – 115 с.

Электронные носители информации в криминалистике : монография / под ред. О. С. Кучина. – М. : Юрлитинформ, 2017. – 304 с.

ДЛЯ ЗАМЕТОК

Учебное издание

Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий

Учебное пособие

Часть 1

Редактор *К. В. Громова*
Верстка *С. Х. Аминов*

Подписано в печать 16.10.2019. Формат $60 \times 84\ ^{1}/_{16}$.
Усл. печ. л. 12,09. Уч.-изд. л. 11,69. Тираж 151 экз. Заказ № ____
Отделение полиграфической и оперативной печати РИО
Академии управления МВД России.
125993, Москва, ул. Зои и Александра Космодемьянских, д. 8

ISBN 978-5-906942-87-6