должен уметь рефлексивно проникать в рассуждения и намерения допрашиваемого, уметь влиять на ход его мыслей. Также следователь должен в совершенстве применять коммуникативные навыки для умения доходчиво излагать свои мысли, менять тон изложения, свободно и непринужденно менять темы. Следователь должен обладать артистическими навыками для того, чтобы скрывать свои намерения, имитировать уверенность.

Таким образом, не существует универсальных методов преодоления противодействия. Поставленные следователем цели достигаются лишь тогда, когда он применяет все указанные методы в совокупности. Можно лишь добавить к сказанному, что для комплексного применения методов необходимо руководствоваться целесообразностью, законностью, своевременностью и логикой.

Попова Д.Д.

Санкт-Петербургский университет МВД России
Научный руководитель Е.В. Горкина, кандидат юридических наук, доцент

Киберпреступность в Российской Федерации: тактика расследования, вопросы противодействия и пути предупреждения

Киберпреступность – феномен, сформировавшийся в процессе научно-технического и технологического прогресса. Мы живем в век высоких технологий, становления виртуального мира – это так или иначе влияет на экономическую и социальную сферы жизни людей всего мира.

Чем более развито государство, тем быстрее идет процесс цифровизации, растет уровень технологий, инновационных достижений. Однако цифровизация создает дополнительные риски – многие цифровые сервисы заменяют некоторые государственные услуги (медицинские, образовательные), а стоимость электронных услуг дешевеет. Помимо этого создаются риски и угрозы криминогенного характера.

Преступники осваивают новые технологии быстрее легитимных структур. Они адаптируют их для использования в преступных целях и идут на шаг впереди правоохранительной системы, а высокий темп развития технологий в наше время еще больше усложняет процесс противодействия преступности.

Несомненно, такие преступления требуют немедленного реагирования правоохранительных органов. Почти все киберпреступления расследуются Управлением «К» МВД России, региональными структурными подразделениями, а также ФСБ России.

Поводом для возбуждения уголовного дела является, как правило, заявление о хищении денежных средств, какой-либо личной, интимной информа-

ции, о несанкционированном доступе. Такие заявления чаще всего поступают от организаций и реже от граждан. Эту ситуацию можно объяснить тем, что граждане боятся разглашения в ходе следствия той информации, которая была у них похищена и которая может содержать какие-либо тайны жизни. Поэтому следователь должен наладить психологический контакт, уметь объяснить гражданину, что изъятая информация не будет разглашена и имеет значение для расследования совершенного преступления.

В уголовном законодательстве России регулирование преступлений в сфере компьютерной информации осуществляет глава 28 УК РФ «Преступления в сфере компьютерной информации», которая включает в себя: ст. 272 (Неправомерный доступ к компьютерной информации); ст. 273 (Создание, использование и распространение вредоносных компьютерных программ); ст. 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей); ст. 274.1 (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации). То есть Российское законодательство определяет киберпреступность посредством кодификации деяний в данной главе, а также объединяет данные преступления по предмету и средству совершения.

Для начала расследования киберпреступления необходимо провести неотложные следственные действия. В частности, нужно провести осмотр места происшествия, в данном случае осмотр носителя информации, который имеет непосредственную связь с похищенной информацией. Следователь должен собрать вещественные доказательства, но надо иметь в виду, что данные носители могут быть утеряны, поэтому существует необходимость изъятия для последующего исследования в лабораторных условиях в рамках компьютерной технической экспертизы. Это имеет огромное значение для сбора доказательств.

В ходе компьютерной технической экспертизы будут исследованы системные и программные файлы на наличие несанкционированного доступа, аномальной активности, определены тип и характеристика атак. Самыми важными сайтами при исследовании будут являться файлы расширения log. Лог-файлы содержат в себе информацию о последних действиях компьютера, хранят историю всех интернет-соединений.

К дальнейшей работе подключаются сотрудники оперативных подразделений, которые должны провести ряд оперативно-розыскных мероприятий по установлению принадлежности найденных в лог-файлах IP-адресов к конкретным лицам.

Говоря о расследовании киберпреступлений, нельзя забывать о проблемах современного общества, которые иногда являются причинами быстрого роста таких преступлений.

Актуальной проблемой нашей цифровой жизни на данный момент является утечка персональных данных, а также их продажа на различных хакерских форумах и Telegram-каналах. По статистике исследования KPOK и EveryTag наиболее популярный канал утечки информации и персональных данных – фотографирование или скриншоты экранов – 35%, и только 30% приходится на различные мессенджеры, почту и социальные сети. Поэтому Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры) предложена единая платформа для мониторинга фишинговых сайтов, которая поможет в противодействии мошенничеству[1].

Рост киберпреступности в 2021 г. говорит о низкой цифровой грамотности населения. С этой проблемой уже пытается разобраться Минцифры России. Министерство опубликовало на своем официальном сайте проект правил предоставления субсидии на разработку программ повышения цифровой грамотности населения[2]. Данные правила были утверждены постановлением Правительства Российской Федерации от 3 февраля 2022 г. № 94[3], подписанным Председателем Правительства Российской Федерации М.В. Мишустиным. Новые образовательные сервисы будут направлены на разные слои населения, в том числе на студентов, пенсионеров и детей.

Говоря о введении специальной нормативной базы для регулирования киберотношений, важно отметить, что Государственной Думой Российской Федерации было предложено ввести ответственность за использование персональных данных, которые были похищены[4]. То есть ввести ответственность не только для тех, кто их украл, но и для тех, кто ими пользуется, зная нелегальный характер их получения.

Подводя итоги, можно сказать, что киберпреступность является одной из самых актуальных угроз нашего века. Решение проблем невозможно найти на уровне отдельных государств, так как в большинстве случаев члены преступных группировок располагаются на разных континентах и подпадают под юрисдикцию большого количества государств. Нельзя не сказать о

[1] Трофимова Д.Н. Киберпреступность в Российской Федерации: пути предупреждения // Молодой ученый. 2020. № 15 (305). С. 259-261. URL: https://moluch.ru/archive/305/68693/ (дата обращения: 16.03.2022).

[2] Чернышенко Д. Личная цифровая грамотность – важное условие работы в онлайн-среде // Правительство России. URL: http://government.ru/news/43803/ (дата обращения: 17.03.2022).

[3] Правительство поддержит разработку программы для повышения цифровой грамотности // Правительство России. URL: http://government.ru/news/44479/ (дата обращения: 17.03.2022).

[4] В ГД предложили ввести ответственность за использование краденых персональных данных // ДумаТВ. URL: https://dumatv.ru/news/v-gd-predlozhili-vvesti-otvetstvennost-za-ispolzovanie-kradenih-personalnih-dannih (дата обращения: 17.03.2022).

необходимости формирования и совершенствовании организации деятельности российских правоохранительных структур.

Шмырева Е.А.

Уфимский юридический институт МВД России
Научный руководитель С.Р. Низаева, кандидат юридических наук

Тактика использования мобильных технических средств при производстве осмотра места происшествия

Согласно положению ФЗ № 3 «О полиции» одной из обязанностей органов внутренних дел является использование в своей служебной деятельности достижений научно-технического прогресса, а также информационно-коммуникационных систем. Как нам известно, в настоящее время существует огромный, неисчерпываемый перечень гаджетов, виджетов и иных различных технологичных разработок, позволяющих улучшить и усовершенствовать работу многих организаций, служб и сотрудников, в том числе и правоохранительных органов. Но не каждое устройство можно использовать при выполнении оперативно-служебных задач, так как до внедрения их рабочую деятельность должны пройти процедуры тестирования, лицензирования и соответствующая стадия утверждения.

В эпоху тотальной модернизации во всех областях жизни устанавливаются достаточно прочные связи между человеком и актуальными разработками в научно-технической сфере. Современные проблемы требуют современных решений, в том числе и внедрение новаций в уголовно-процессуальную и криминалистическую деятельность.

Если мы рассмотрим такое процессуальное действие, как осмотр места происшествия, то столкнемся с рядом проблем, которые возможно решить путем внедрения современных технологий.

Нужно отметить, что не всегда место происшествия является местом, где было совершено противоправное деяние, так как, например, чтобы помешать следствию, следы преступления могут быть частично или полностью уничтожены либо перемещены на другое место. Из этого следует, что в некоторых делах место происшествия представляет собой обширную территорию, которую зачастую невозможно исследовать в полном и всестороннем объеме.

Начнем с того, что, как правило, осмотр места происшествия представляет собой следственное действие, регламентированное уголовно-процессуальным законодательством, которое по всем параметрам подходит под определение «неотложности». В частности, это связано и с основной целью его проведения – своевременным установлением, изучением, подробным