Механизм реализации ч. 4 ст. 49 Закона об ОРД раскрывается в постановлении Совета Министров Республики Беларусь от 23 апреля 2021 г. № 241 «О порядке использования сведений, содержащихся в материалах оперативно-розыскной деятельности» (далее – Постановление), где определены субъекты, которые уполномочены направлять сведения, содержащиеся в материалах ОРД, в целях профилактики правонарушений; установлен порядок предоставления вышеуказанных сведений – вынесение постановления о направлении сведений, содержащихся в материалах ОРД, которое помещается в дело оперативного учета либо номенклатурное дело, либо другое дело, а также направления информационных писем в адрес компетентных органов, рассматривающих обстоятельства, причины и условия, способствующие совершению правонарушений, и принимающих по результатам этого решения.

На наш взгляд, особого внимания заслуживает п. 3 Постановления, где указывается, что «сведения, содержащиеся в материалах ОРД, могут использоваться органами, осуществляющими ОРД, в целях профилактики правонарушений после предоставления указанных материалов в порядке, определенном законодательством, в орган уголовного преследования для подготовки и проведения следственных и иных процессуальных действий, доказывания в уголовном процессе, а также в иных случаях…». Более подробно механизм реализации профилактики правонарушений не раскрывается, обосновано вызывая ряд вопросов в практической деятельности, в том числе начала ее осуществления.

Анализ законодательства показывает, что согласно ст. 198 Уголовно-процессуального кодекса Республики Беларусь (УПК) данные предварительного следствия или дознания не подлежат разглашению и могут предаваться гласности лишь с разрешения следователя, лица, производящего дознание. В этой связи, во-первых, сведения, содержащиеся в материалах ОРД, после предоставления их в орган уголовного преследования для подготовки и проведения следственных и иных процессуальных действий, доказывания в уголовном процессе, не могут без разрешения следователя, лица, производящего дознание, предоставляться в целях профилактики правонарушений. Во-вторых, необходимо учитывать ст. 199 УПК, в которой указывается, что, установив при производстве по материалам проверки или уголовному делу нарушения закона, причины и условия, способствовавшие совершению преступления, орган уголовного преследования вправе внести в соответствующие организации или должностному лицу представление о принятии мер по устранению нарушений закона, причин и условий, способствовавших совершению преступления.

Таким образом, речь идет о профилактике правонарушений в порядке, определенном уголовно-процессуальным, а не оперативно-розыскным законодательством, т. е. направляться информационное письмо в адрес компетентных органов, рассматривающих обстоятельства, причины и условия, способствующие совершению правонарушений, в рамках Постановления не должно.

В целях исключения дублирования профилактики правонарушений в оперативно-розыскном и уголовно-процессуальном законодательстве, а также недопущения подмены одних материалов другими, полагаем необходимым с момента начала уголовного процесса реализовывать профилактику правонарушений в соответствии со ст. 199 УПК, т. е. путем направления в компетентные органы предписания, а вышеуказанное информационное письмо направлять на основании материалов ОРД, которые не использовались для принятия решения в порядке ст. 174 УПК или подготовки и проведения следственных и иных процессуальных действий.

Предложенный нами подход позволит четко разграничить профилактику правонарушений при осуществлении ОРД и повысить эффективность оперативно-служебной деятельности соответствующих подразделений в данном направлении, определить дальнейшее развитие мер по выявлению причин и условий, способствующих совершению правонарушений, а также их устранению.

УДК 343.985

А.А. Чехович

СПОСОБЫ СОВЕРШЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Неотъемлемым элементом оперативно-розыскной характеристики преступления любого вида являются данные о наиболее типичных способах его совершения. Под способом совершения преступления в оперативно-розыскной деятельности (ОРД) принято понимать объективно и субъективно обусловленную систему поведения субъекта до, во время и после совершения преступления, оставляющего различного рода характерные следы. Применительно к несанкционированному доступу к компьютерной информации (НДКИ) это будут преимущественно цифровые следы, которые с помощью средств и методов ОРД позволяют получить представление о сути происшедшего на месте совершения преступления, отличительных чертах личности преступника, выдвинуть наиболее вероятную версию совершения такого рода преступления, с последующим определением наиболее оптимальных методов его раскрытия.

Рассматривая способы совершения НДКИ, необходимо отметить, что под таковыми понимается взлом системы защиты компьютерной информации, которая состоит из комплекса правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации, на что указано в Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

К правовым мерам по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, устанавливающие условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

При нарушении организационных средств защиты информации преступники чаще всего, используя служебное положение и имеющиеся у них идентификаторы доступа, осуществляют доступ к конфиденциальной компьютерной информации, либо к машинным носителям информации, после чего копируют, изменяют, либо похищают конфиденциальные сведения целиком, либо идентификационные данные для доступа к таким сведениям.

К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации. Анализ сведений ИЦ МВД Республики Беларусь[1] показывает, что большинство НДКИ преступники совершают, нарушая технические средства защиты информации. Таким образом, классифицируем способы совершения НДКИ как организационные и технические.

НДКИ, сопряженный с нарушением технических мер по защите компьютерной информации, чаще всего преступниками реализовывается посредством социальной инженерии, когда необходимые идентификаторы для доступа в закрытые сети передачи информации, либо к персональным страницам в социальных сетях, они получают непосредственно у потерпевших, путем применения психологических приемов воздействия.

Вторым, не менее распространенным способом совершения НДКИ является использование специально созданного программного обеспечения по подбору паролей для несанкционированного доступа к информационному ресурсу. Программный продукт для подбора паролей имеет определенный алгоритм действия, не сложен в изготовлении при наличии соответствующих навыков. Это программы, способные из заданного пользователем диапазона символов подобрать в максимально короткие сроки пароль доступа к сведениям ограниченного доступа, или сети, где такие сведения циркулируют. Такая технология взлома системы защиты получила название «Брутфорс» (от англ. brute force – грубая сила), когда преступник получает доступ к информации ограниченного доступа или закрытую сеть, путем подбора идентификаторов. При этом установленные программные средства защиты информации не фиксируют НДКИ, так как доступ осуществляется с использованием зарегистрированных в системе идентификаторов.

Встречаются и менее распространенные способы совершения НДКИ, носящие «бытовой» характер. Эти способы представляют собой несанкционированный доступ к личному кабинету пользователя услуги, например, интернет-банкинга, когда его владельцы пренебрегают правилами хранения и использования сеансовых ключей доступа (идентификаторов учетной записи), передавая их третьим лицам.

Таким образом, следует, что НДКИ преимущественно совершается тремя, наиболее распространенными способами: путем использования специального программного средства по подбору идентификаторов по технологии «Брутфорс»; посредством применения приемов социальной инженерии; злоупотреблением доверием владельцев идентификаторов доступа в личные кабинеты информационных систем. Их общей особенностью выступает стремление преступника завладеть идентификационными данными для несанкционированного доступа к компьютерной информации с целью получения материальной и иной выгоды.

УДК 343.9

А.И. Чурносов

ЦИФРОВЫЕ СЛЕДЫ КАК ИСТОЧНИК ПОЛУЧЕНИЯ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ И ОПЕРАТИВНО-РОЗЫСКНОЙ ИНФОРМАЦИИ НА ПРИМЕРЕ ОРГАНОВ ПОГРАНИЧНОЙ СЛУЖБЫ РЕСПУБЛИКИ БЕЛАРУСЬ

В XXI в. произошло преобразование общественной жизни, и в первую очередь это связано с научно-техническим прогрессом. Были созданы объективные условия для роста количества преступлений против информационной безопасности, что является негативной тенденцией, присущей любому современному обществу. Бурное развитие компьютерных технологий и повышение их роли в современной жизни человечества закономерно повлекло к внедрению компьютерных систем практически во все сферы деятельности человека. Такие тенденции, как появление компьютерной техники с огромными производительными возможностями, широкая функциональность ее применения, предопределяют компьютеризацию управленческой и экономической сфер жизни общества и необходимость более тщательного подхода к обеспечению безопасного функционирования компьютерных систем.

На современном этапе для лиц, производящих дознание в органах пограничной службы Республики Беларусь, все более актуальным становится исследование и изъятие цифровых следов при расследовании преступлений, создающих угрозу пограничной безопасности, в первую очередь по уголовным делам, возбуждаемым по признакам преступлений, связанным с организацией незаконной миграции, ст. 371[1] (в 2021 г. органами дознания возбуждено 16 уголовных дел в отношении 17 лиц, а в 2022 г. – 35 уголовных дел в отношении 66 лиц); незаконным перемещением через таможенную границу Евразийского экономического союза и (или) Государственную границу Республики Беларусь наркотических средств, психотропных веществ либо их прекурсоров или аналогов – ст. 328[1] (в 2021 г. органами дознания возбуждено 9 уголовных дел в отношении 7 лиц, а в 2022 г. – 11 уголовных дел в отношении 11 лиц) Уголовного кодекса Республики Беларусь.

[1] Здесь и далее сведения информационного центра Министерства внутренних дел Республики Беларусь за 2017–2022 гг. о зарегистрированных на территории республики преступлениях, предусмотренных ст. 349 Уголовного кодекса Республики Беларусь.