

няемым законом интересам лицом, действующим во исполнение обязательного для него приказа или распоряжения, отданных в установленном порядке. Уголовную ответственность за причинение такого вреда несет лицо, отдавшее незаконный приказ или распоряжение (ст. 40 УК).

Представляется, что для повышения эффективности деятельности органов внутренних дел, реализации принципа неотвратимости наказания и обеспечения правовой защищенности деятельности органов внутренних дел необходимо выполнить следующее.

При принятии решения о проведении специальной операции по пресечению противоправной деятельности, задержанию лиц, причастных к ней, руководитель, обладающий всей полнотой данных о тяжести совершенного преступления, личности правонарушителя и обстановки, в условиях которой происходит задержание, устанавливает формально закрепленный порядок применения оружия при задержании лиц, пытающихся скрыться, если иными средствами задержать не представляется возможным.

Профессиональная подготовка сотрудников органов внутренних дел должна включать обучение правилам применения, использования оружия в оперативно сложных ситуациях с целью минимизировать вероятность неправомерного применения, использования оружия и повысить эффективность действий при задержании преступников.

Улучшить техническую оснащенность органов внутренних дел, включая применение современных технологий для оперативного получения информации о личности правонарушителей и их местонахождении, что позволит сократить вероятность использования оружия при задержании.

Важно проводить работу с населением о правилах поведения при задержании органами внутренних дел, чтобы снизить напряженность в отношениях между правоохранительными органами и населением, а также повысить уровень понимания гражданами необходимости пресечения противоправной деятельности в интересах общества.

УДК 343.985

А.А. Чехович

ОПЕРАТИВНО-РОЗЫСКНАЯ ХАРАКТЕРИСТИКА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Информационные технологии являются неотъемлемой составляющей жизни современных людей. В связи с этим уместно отметить, что нередко злоумышленники, руководствуясь корыстными и иными де-

структивными мотивами, применяют информационные технологии с целью совершения преступлений. В настоящее время особую роль для преступников играет сеть Интернет, что объясняется наличием практически безграничных возможностей, включающих простоту и удобство эксплуатации, доступность, минимальные временные затраты при поиске необходимых сведений среди огромного множества информации, относительную анонимность пользователей. Интернет используется злоумышленниками в совершении различных преступлений, наиболее распространенными из которых является несанкционированный доступ к компьютерной информации (НДКИ), ответственность за который предусмотрена ст. 349 Уголовного кодекса Республики Беларусь. По данным информационного центра Министерства внутренних дел Республики Беларусь в 2021 г. было совершено 1 104 таких преступлений, в 2022 – 1 056.

Оперативно-розыскная характеристика (ОРХ) преступлений является основой для формирования и разработки методических рекомендаций по раскрытию отдельных видов преступлений. Она включает в себя описание отличительных качеств, признаков, свойств, присущих конкретному преступлению. По мнению А.М. Абрамова, ОРХ представляет собой систему свойств и информационных признаков определенного вида преступлений, знание которых способствует эффективному решению организационно-тактических задач по их предупреждению и раскрытию, служит теоретической и информационной основой для разработки тактических приемов с целью эффективного раскрытия конкретных преступлений.

Структурными элементами ОРХ могут выступать: уголовно-правовые признаки конкретного преступления; распространенность преступлений, а также сопутствующих им явлений; фазы развития преступления; особенности объекта и предмета преступного посягательства, влияющие на подготовку, совершение и сокрытие преступления; условия криминальной ситуации, предмет преступного посягательства; мотивация криминального поведения; черты личности лица, совершившего преступление, а также потерпевших лиц и др.

Из всего многообразия структурных элементов ОРХ полагаем целесообразным рассмотреть следующие, позволяющие наиболее полно изучить проблемы оперативно-розыскного противодействия НДКИ: особенности объекта и предмета преступного посягательства, место и обстановка совершения НДКИ, следы преступления и их локализация, орудия совершения НДКИ, особенности личности преступника.

Рассматривать ОРХ НДКИ необходимо с особенности предмета преступного посягательства, указанного в ст. 349 «Несанкционированный

доступ к компьютерной информации» Уголовного кодекса Республики Беларусь. Выделение компьютерной информации как самостоятельного предмета обусловлено ее специфическими характеристиками. Она не может существовать в материальном мире, вне компьютера, компьютерной сети либо машинного носителя информации. Компьютерная информация при ее потреблении не исчезает и не подвергается какому-либо износу. Она может быть растиражирована в неограниченном количестве, а также создана и изменена только при помощи компьютерной техники. Помимо простоты создания и обработки, компьютерная информация легко удаляется при помощи компьютерной техники и передается по компьютерным сетям в рекордно короткие сроки на неограниченные расстояния. Кроме того, доступ к ней может быть осуществлен из любой точки мира, без учета географических и административных границ. Указанные свойства компьютерной информации, помимо выделения в качестве самостоятельного предмета, обуславливают и особенности преступного посягательства на нее. Однако наиболее специфическим свойством компьютерной информации является то, что при изъятии, в отличие от материального предмета, она сохраняется в первоисточнике и доступ к ней могут иметь одновременно несколько лиц, например при работе с информацией доступ к файлу, где она содержится, одновременно могут осуществлять несколько пользователей компьютерной сети. При этом изъятая компьютерная информация в виде файла на машинном носителе будет определена компьютером как вновь созданная.

Обстановка совершения НДКИ имеет существенное значение раскрытия преступления, и обычно ее определяют обстоятельства, характеризующие пространственные, временные, вещественные, технические и психологические особенности события рассматриваемого преступления. НДКИ может совершаться как непосредственным физическим воздействием на объект, содержащий компьютерную информацию (персональный компьютер, сервер информационной сети), так и удаленным способом, причем используемая для этого компьютерная техника может располагаться как стационарно, так и в виде перемещающейся точки, например, использование злоумышленником переносного или планшетного компьютера во время движения в транспорте. Указанная особенность НДКИ создает огромные трудности при определении места его совершения.

Третью группу способов совершения НДКИ составляют смешанные, которые могут осуществляться как путем непосредственного, так и удаленного доступа.

Удаленный доступ может осуществляться при помощи сети Интернет или локальной компьютерной сети. По способам удаленного досту-

па можно выделить способы, связанные с преодолением технической защиты с последующим подключением к чужой системе, и способы перехвата информации. Отдельно необходимо выделить использование социальной инженерии, которая имеет специфические особенности: при ее использовании применяются психологические приемы воздействия на лицо, которое имеет доступ к компьютерной информации ограниченного доступа. Такой способ воздействия не оставляет никаких цифровых и материальных следов.

При совершении НДКИ имеет специфический вид и следовая картина, для которой характерно нахождение следов в разных местах одновременно и на большом расстоянии друг от друга. Любые действия с компьютерной информацией оставляют «цифровые следы», которые аналогично ей не могут существовать вне среды ее оборота и подвержены таким способам обработки, как копирование, удаление, удаленный доступ. При этом не ясно, следует ли относить к следам совершения НДКИ «цифровые следы», оставленные на стороннем ресурсе или компьютерной технике при подготовке к совершению несанкционированного доступа, а именно исходные коды и файлы для написания вредоносного программного обеспечения или программы по удаленному доступу к компьютерной технике.

Объектом преступного посягательства при совершении НДКИ может выступать как непосредственно компьютерная информация, так и средства ее обработки и хранения, т. е. компьютерная техника, составляющие компьютерной сети или машинные носители информации.

Стоит отметить, что преступников, способных совершить данного вида преступления, необходимо разделить на две группы: профессионалы, которые обладают специальными знаниями в области программирования, и злоумышленники, обладающие минимальными навыками работы с персональным компьютером.

Как показывает анализ оперативно-розыскной практики, профессионалы редко совершают несанкционированный доступ в одиночку. Они обычно действуют организованной преступной группой, в которой каждому участнику отведена конкретная роль (разведчик, программист и др.). Такие группы заранее подготавливаются к совершению преступления, нередко ведут длительное наблюдение за объектом преступного посягательства. Часто в такой группе присутствуют лица, имеющие в силу своих профессиональных обязанностей доступ к информации, к которой преступники решают совершить несанкционированный доступ. У преступной группы профессионалов зачастую имеются как программные, так и технические средства для его совершения. Такие преступники активно противодействуют раскрытию преступления путем

уничтожения либо маскировки следов противоправной деятельности – «цифровых следов».

Другой вид преступника, совершившего НДКИ, представлен злоумышленником, обладающим минимальными навыками обращения с компьютерной техникой. Как правило, он применяет одинаковые методы при совершении НДКИ различного уровня, приобретая преступную схему в теневой части сети Интернет, так называемом «Даркнете», либо используя методы социальной инженерии. Такие преступники редко обладают навыками противодействия раскрытию совершенного преступления, а потому оставляют «цифровые следы» своей противоправной деятельности. Злоумышленники реализуют свой преступный умысел исключительно с материальной составляющей, когда совершают НДКИ ради получения материальных благ.

Таким образом, оперативно розыскное противодействие несанкционированному доступу к компьютерной информации является одним из приоритетных направлений деятельности правоохранительных органов Республики Беларусь. Как показывает практика, несанкционированный доступ в настоящее время является не только самостоятельным видом преступной деятельности, но и стал инструментом в руках преступников для совершения других всевозможных преступлений. Особое значение при этом имеет знание элементов оперативно-розыскной характеристики данного вида преступлений, которое позволяет выступать информационной основой и эффективно проводить оперативно-розыскные и иные мероприятия, направленные на предупреждение, выявление и пресечение рассматриваемого преступления, а также выявление лиц, их подготавливающих, совершающих или совершивших.

УДК 343.98

А.М. Шинкевич

ПЕРСПЕКТИВЫ РАЗВИТИЯ И ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

Оперативно-розыскная деятельность (ОРД) является негласным государственно-правовым средством защиты общества и государства. В Республике Беларусь на законодательном уровне она совершенствуется с 1992 г. Каждый из органов, которым предоставлено право осуществлять ОРД, решает свои непосредственные задачи с использованием негласных методов. Преимущественно в органах внутренних дел ОРД направлена на борьбу с преступностью. Из всех уполномоченных