Программа состоит из множества мер защиты и социальной помощи, к числу которых относятся:

помещение в безопасное место – основная мера защиты, применяемая практически в 100 % случаев, при этом следует отметить, что в рамках Евросоюза не существует проблем с перемещением защищаемого лица в любое из европейских государств;

замена личных документов (может применяться одновременно с помещением в безопасное место) – замена всех документов, которые оформляются на новую фамилию (удостоверение личности, водительское удостоверение, код налогоплательщика, медицинская карта, карта занятости и прочие идентификационные документы), осуществляется согласно разработанной легенде, которой защищаемое лицо и члены его семьи должны безоговорочно придерживаться, любое отступление от установленных правил поведения и избранной легенды влечет за собой прекращение мероприятий по обеспечению безопасности и сворачивание мер по обеспечению защиты;

замена персональных данных в информационных базах данных;

обеспечение возможности свидетельствовать в суде по видеосвязи;

оказание финансовой поддержки (ежемесячное пособие и оплата аренды жилья), социальной и правовой помощи, содействие в обеспечении медицинского обслуживания.

Осуществление государственной защиты свидетелей и осведомителей не ограничено какими-либо сроками, все мероприятия, предусмотренные программой защиты, осуществляются до полной нейтрализации угрозы. Решение о прекращении применения мер по обеспечению безопасности и защиты принимает Центральная комиссия.

По приведенной схеме действуют системы обеспечения безопасности во всех европейских государствах, где существуют программы защиты свидетелей и иных лиц. Различие составляет только структура подразделений полиции и их нормативное регулирование.

Опыт осуществления государственной защиты свидетелей и иных лиц в Германии представляет интерес в части включения защищаемого лица в общественные отношения и применения такой меры по обеспечению безопасности, как замена персональных данных в информационных банках данных. Самые крупные базы данных государства – базы регистрационной и федеральной налоговых служб. Человек, меняя место жительства внутри Германии или даже прибыв из другого государства, в первую очередь сообщает свои данные в местную регистрационную службу. После заполнения бланка в электронном виде часть данных автоматически направляется более чем в 25 других баз данных.

В частности, существуют базы данных по датам рождения, домашним животным, обследованию граждан в целях профилактики рака и других заболеваний, лицам, признанным инвалидами, утилизации отходов и даже по невыплате арендной платы. Раз в год имеющаяся в базах данных информация обновляется.

Правовое регулирование защиты свидетелей и иных лиц в Германии осуществляется на парламентском уровне. Научные службы Бундестага в 2018 г. подготовили и опубликовали разъяснительную статью по вопросам, которые необходимо учитывать при обеспечении защиты свидетелей в уголовном процессе, в разрезе правовой ситуация в Германии.

Зарубежный опыт правовой регламентации и деятельности правоохранительных органов в указанной сфере интересен не только своей новизной для Республики Беларусь, но и конкретностью государственных программ в сфере обеспечения безопасности свидетелей и иных лиц. На наш взгляд, вполне очевидна необходимость имплементации в национальное законодательство отдельных положений, в частности, заслуживает внимания социальная направленность защиты, а также наличие комплексной государственной программы по защите свидетелей и иных лиц.

УДК 343.985

Н.В. Яджин

О СПОСОБАХ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ПОМОЩЬЮ ВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, РАЗМЕЩЕННОГО НА МОБИЛЬНОМ ТЕЛЕФОНЕ ПОТЕРПЕВШЕГО

С развитием, совершенствованием и внедрением в повседневную жизнедеятельность информационных технологий как в Российской Федерации, так и в ряде зарубежных государств, где активно развиваются информационные технологии, участились случаи совершения мошенничества, связанного как с вредоносным вмешательством через компьютерные сети в работу различных систем, так и с распространением вирусного программного обеспечения, размещенного на мобильном телефоне потерпевшего.

Президент Российской Федерации В.В. Путин на расширенном заседании коллегии МВД Российской Федерации, состоявшемся 3 марта 2021 г., обратил внимание, что, несмотря на то что «за прошедший период увеличилось число раскрытых тяжких и особо тяжких преступлений... динамика не столь позитивная... по преступлениям в сфере ин-

формационных технологий: за последние шесть лет их число выросло в 10 раз». Кроме того, им поставлена задача перед органами внутренних дел – «эффективно ответить на этот криминальный вызов, защитить граждан и добросовестный бизнес, который активно осваивает цифровое пространство. Для этого важно своевременно информировать людей о способах защиты от мошенников, повышать профессиональную подготовку и техническое оснащение органов внутренних дел. И, конечно, нужно наладить более четкое взаимодействие с банковским сообществом, интернет-провайдерами, операторами сотовой связи».

Проведенный нами анализ практики раскрытия и расследования мошенничества, совершаемого с помощью вирусного программного обеспечения, размещенного на мобильном телефоне потерпевшего, показал, что для хищения денежных средств мошенники используют вредоносную программу, следуя определенному алгоритму:

приобретение или разработка вредоносного программного обеспечения, предназначенного для объединения с каким-либо приложением к мобильному устройству;

размещение вирусной программы в сети Интернет, на сайтах или в интернет-магазинах;

активизация в результате скачивания или установки пользователем на своем мобильном устройстве вирусной программы, действующей по своему назначению (вирусное программное обеспечение может быть предназначено как для сканирования физической памяти мобильного устройства, так и для поиска установленного программного обеспечения);

копирование вирусной программой информации о счете потерпевшего, логинов, паролей доступа, а также иной информации, необходимой для хищения денежных средств, при обнаружении на мобильном устройстве программного обеспечения дистанционного банкинга;

перенаправление вирусной программой информации на заранее зарегистрированный мошенником хостинг после копирования важной для хищения денежных средств информации (при этом вирусная программа способена блокировать входящие звонки и сообщения с телефонных номеров, которые используются сервисом дистанционного банкинга, содержащих информацию о паролях подтверждения, результатах списания со счета денежных средств, состоявшихся платежах);

беспрепятственное осуществление перевода денежных средств со счета потерпевшего на имеющиеся в распоряжении злоумышленника счета вследствие полного доступа к банковским счетам потерпевшего в результате использование специального программного обеспечения.

Так, МВД по Республике Карелия при расследовании уголовного дела в отношении М. установлено, что с января по июнь 2015 г. М. занимался обналичиванием денежных средств, похищенных с банковских платежных карт вышеуказанным способом. За сутки М. обналичивал денежные средства от 5 до 15 раз суммами от 3 000 до 15 000 р. Использовавшиеся банковские платежные карты были оформлены на подставных лиц, которыми в основном являлись жители другой области. Денежные средства похищались в различных регионах России.

При использовании другого вредоносного программного обеспечения мошенники реализуют следующим алгоритм:

получение полного доступа к мобильному устройству в результате установки на нем вирусной программы;

запрашивание программой через услуги дистанционного банкинга баланса привязанной к нему банковской платежной карты, лицевого счета федерального телефонного номера и других идентификационных данных (при этом об этих действиях пользователь не подозревает);

синхронизация вирусной программы с сервером, находящимся под контролем мошенника, направление сервером на зараженное мобильное устройство списка команд и сведений о других зараженных устройствах, куда должны быть переведены безналичные денежные средства (часть зараженных устройств не используется для списания безналичных денежных средств со счетов своих владельцев, а применяется для сокрытия следов преступления, эти устройства являются промежуточным звеном в серии переводов безналичных денежных средств до вывода их в распоряжение мошенника, при этом используется перевод денежных средств изначально с учетом комиссии за услуги платежных систем).

При расследовании уголовного дела по факту безналичного хищения денежных средств у Р., жителя Володарского района Нижегородской области, было установлено, что с использованием услуги дистанционного банкинга посредством направления СМС-команды осуществлены два безналичных перевода денежных средств на банковские платежные карты, одина из которых принадлежала Е., жителю Курганской области, вторая – К., жителю Приморского края. При анализе сведений о движении безналичных денежных средств по банковской платежной карте и федеральному телефонному номеру Е. установлено, что перевод от Р. поступил на банковскую платежную карту Е., после чего с помощью услуги дистанционного банкинга безналичные денежные средства переведены на лицевой счет федерального телефонного номера Е., а далее направлены на лицевой счет федерального телефонного номера неустановленного лица. Аналогичные переводы согласно полученным сведениям из банковского учреждения и компании сотовой связи осуществлялись по лицевым счетам Е. в течение одного месяца, мобильный телефон использовался для общения в социальных сетях и загрузки развлекательных приложений, постоянно подключен к сети Интернет.

В завершение следует отметить, что с развитием, усовершенствованием и внедрением новых информационных технологий (электронная торговля, предоставление сетью Интернет разного рода услуг, прежде всего финансовых) мошенниками будут совершенствоваться способы совершения дистанционного хищения денежных средств как у физических, так и юридических лиц. Кроме того, появятся новые виды мошенничества. Для улучшения существующего положения необходимы глубокие исследования, основанные на обобщении судебно-следственной практики по раскрытию, расследованию и судебному рассмотрению уголовных дел в сфере информационных технологий.

УДК 343.985.8

А.В. Яскевич, С.В. Пилюшин

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ

Информационное обеспечение в теории ОРД традиционно рассматривается как сложная, многогранная система действий сотрудников оперативных подразделений ОВД по сбору, анализу, систематизации, хранению и последующему использованию оперативно-розыскной информации о лицах и фактах, представляющих оперативный интерес. Основное ее назначение заключается в обеспечении потребностей оперативных подразделений в оперативно-розыскной информации и возможности ее аналитической обработки с целью принятия соответствующих решений.

Необходимо отметить, что ранее в специальной литературе при освещении проблемных вопросов, связанных с информационным обеспечением, использовался термин «оперативный учет». Данное понятие изначально употреблялось в уголовном сыске и определяло процесс систематизации различных видов информации, характеризующей лиц, причастных к совершению преступлений. В последующем он приобрел новое название – уголовная регистрация. С течением времени система регистрации начала расширяться. Наряду с учетом отдельной категорией лиц, представляющих оперативный интерес, стала производиться регистрация фактов преступлений, похищенного, следов, предметов, обнаруженных на месте совершения преступления, и т. п.

Анализ ведомственных нормативных правовых актов советского периода показывает, что вопросы совершенствования информационного обеспечения ОРД оставались предметом дискуссий на протяжении

длительного периода. Ведомственными приказами сотрудникам оперативных подразделений предписывалось систематически проводить поисковые мероприятия по установлению преступных элементов и маргинальных лиц. Решение этой задачи предполагалось достичь при помощи организации централизованного оперативного учета, использование которого являлось неотъемлемой частью оперативной работы. Каждый оперативный сотрудник обязан был пользоваться оперативными учетами и систематически их пополнять, что в целом должно было поспособствовать успешной работе по противодействию преступности. В этих целях предусматривалось ведение соответствующих алфавитных картотек, а также дел оперативного учета (ДОУ).

Однако такая система имела свои очевидные недостатки. В случаях использования картотек возможность выборки по ключевым признакам была существенно ограничена, происходило дублирование карточек, часто их содержание ограничивалось краткой справкой об объекте учета либо сведения, содержащиеся в них, носили непроверенную информацию и т. п.

ДОУ заводились соответственно на лиц, состоящих на картотечном (пофамильном) учете, с целью более глубокого изучения их образа жизни и поведения. В таких делах концентрировалось значительно больше оперативно-розыскной информации, чем в карточках оперативного учета. Однако сложности, связанные с обеспечением режима секретности, создавали проблемы для их изучения и не способствовали оптимизации ОРД. Длительное время оставалась неразрешенной проблема централизации учетов на определенных уровнях (областном, республиканском, всесоюзном). Остро стоял вопрос о разработке эффективной системы обмена оперативно-розыскной информацией между заинтересованными в ее получении оперативными подразделениями.

Только с развитием информационных технологий стало возможным пересмотреть устоявшиеся подходы информационного обеспечения деятельности оперативных подразделений ОВД. В период 70–80-х гг. прошлого века стали разрабатываться концептуальные положения использования ЭВМ в целях информационного обеспечения ОРД. Предусматривалась автоматизация трудоемких процессов сбора, обработки и поиска оперативно-розыскной информации, объединение разрозненных по территориальным оперативным подразделениям массивов оперативных данных и др.

Внедрение информационных технологий позволило в определенной степени еще в советский период, а в последующем и вовсе отказаться от использования традиционных картотек, внедрить в практическую дея-