Мошенники обходят данное средство защиты, предлагая потенциальной жертве продолжить общение в стороннем мессенджере, либо изначально ведут переписку в Viber, Telegram и т. д., если в объявлении указан номер пользователя.

Определенные механизмы противодействия злоумышленникам заложены и в мессенджеры. Как правило, мошенник регистрирует аккаунт на ранее не задействованный, приобретенный в теневом сегменте сети Интернет номер. Рассылка потенциальным жертвам осуществляется массово, что может повлечь за собой блокировку аккаунта. Например, алгоритмы Viber могут заблокировать новый аккаунт, с которого происходит непрерывная отправка однотипных сообщений различным пользователям, за спам. На этот случай у кураторов преступных групп имеются инструкции с описанием модели поведения как для предотвращения блокировки, так и для разблокировки уже скомпрометированного аккаунта, дабы не приобретать новый подложный номер.

Для генерации отправляемых жертвам фишинговых ссылок используется доступ к телеграм-ботам, которые автоматизировали данный процесс: необходимо отправить в бот ссылку на нужный товар и т. п., после чего искусственный интеллект самостоятельно создает подложную страницу по образу популярных сервисов в зависимости от заданной конфигурации. Для каждого из них организаторы пишут инструкции для непосредственных исполнителей. В них содержатся рекомендации по подбору потенциальной жертвы и выбору легенды мошенничества, под которой следует понимать сведения, предоставляемые преступником потерпевшему с целью убеждения последнего в том, что злоумышленник действительно является тем, за кого себя выдает.

Визуальная составляющая подложных ресурсов чаще всего качественно проработана и не вызывает подозрений. Очевидным признаком, выдающим преступный замысел, является ссылка на ресурс. Мошенники заранее регистрируют «рабочие» домены, напоминающие адреса реальных сервисов. Фишинговый двойник для условного сайта dostavka.by может выглядеть как dostavka.me, dostavka.be – вместо домена первого уровня by окажется иной. Адрес на первый взгляд может выглядеть так же, но стать длиннее: dostavka.by.com, dostavka.belarus.com и т. д.

Страница, отображаемая после перехода по ссылке, является оболочкой для сбора данных о карточке потерпевшего – маской платежной системы для P2P-перевода. После ввода данных банковской платежной карточки в предоставленную форму жертва передает их мошенникам. Так злоумышленники получают возможность для списания денежных средств с банковской платежной карточки потенциального потерпевшего.

Алгоритмы, по которым работают мошенники, отличаются друг от друга, однако их объединяет одно: с использованием социальной инженерии преступник пытается вызвать у человека сильные эмоции, связанные, как правило, с возможностью получения выгоды либо, напротив, избежания наступления серьезных негативных последствий. В данном контексте социальная инженерия является собирательным термином и применяется для обозначения социопсихологических манипуляций, используемых злоумышленниками для получения доступа к защищенным системам с целью получения доступа к определенной информации, паролям и т. п. Предлоги могут разниться: продажа либо покупка товара по выгодной цене, возможность легко и быстро заработать значительную сумму денег, встреча интимного характера с привлекательной девушкой (парнем) и т. д.

Таким образом, неизменным в большинстве преступных схем остается то, что для достижения заманчивой цели потерпевшему необходимо выполнить определенные условия: внести предоплату за покупку (доставку) товара либо привязать карточку к определенному сервису для вывода полученной прибыли; заказать такси либо подарок для девушки, которая готова к встрече. При этом механизм достижения обозначенной выше цели существенно не меняется вне зависимости от адаптации мошеннической схемы для ее реализации на различных ресурсах сети Интернет.

УДК 343

В.Е. Козлов

СИСТЕМА НАУЧНО-ТЕХНИЧЕСКИХ СРЕДСТВ, ИСПОЛЬЗУЕМЫХ В ПРОЦЕССЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

Рассматривая организационно-тактические основы применения научно-технических средств (НТС) в деятельности правоохранительных органов, связанной с противодействием киберпреступлениям, можно выделить два уровня общественной деятельности.

Управленческий уровень – создание условий постоянной готовности подразделений и служб правоохранительных органов к применению НТС. Он проявляется в технической оснащенности подразделений и профессиональной высокотехнологичной, криминалистической, тактико-технической грамотности их сотрудников.

Исполнительский уровень – решение организационных, тактических и ситуационных задач. Они решаются руководителями, а также непосредственно сотрудниками правоохранительных органов. На этом уровне реализуется постоянная готовность применения НТС, формируемая на управленческом уровне.

Весь комплекс НТС правоохранительных органов применяется с соответствующими организационно-тактическими основами при строгом соблюдении закона, т. е. правообоснованность применения НТС в противодействии киберпреступлениям распространяется на все виды НТС, а также формы и тактические приемы их применения. Это означает, что в отношении лиц, совершивших киберпреступление либо подозреваемых в его совершении, могут быть применены НТС для пресечения подготавливаемых или раскрытия (расследования) совершенных преступлений. Такие НТС имеют право использовать только компетентные лица, наделенные особыми полномочиями, и лишь в строго определенном законом порядке. В каждом конкретном случае правомерным должен быть выбор не только самого НТС, но и метода его применения, т. е. технологии в целом. Таким образом, под правообоснованностью применения НТС и технологий в противодействии киберпреступлениям может пониматься подтвержденная нормами морали и закона допустимость их эффективного и безопасного использования

для людей и окружающей среды, а также полученных результатов в целях защиты личности, общества и государства от преступных посягательств.

Существующие НТС (как основополагающая категория) по области применения можно разделить на две группы: НТС, используемые в деятельности правоохранительной системы, и НТС, используемые в других областях общественной деятельности, связанных с обработкой компьютерной информации (КИ). НТС первой группы призваны обеспечивать функционирование только одной отрасли общественных отношений, которые складываются в области функционирования правовых институтов. В то время как вторая группа НТС обеспечивает функционирование всех институтов общественных отношений. На первом управленческом уровне учитываются следующие факторы, влияющие на эффективность искомого противодействия: готовность субъектов противодействия, разработка и внедрение средств противодействия, разработка и внедрение методов противодействия.

Внедрение средств противодействия неэффективно без совершенствования методики их применения. Эффективно оценить и внедрить в практическую деятельность правоохранительных органов достижения смежных с криминалистикой и теорией оперативно-розыскной деятельностьи отраслей науки применительно к процессу противодействия компьютерной преступности возможно по следующим направлениям: во-первых, воздействуя на процесс формирования фундаментальных и прикладных криминалистических знаний, прежде всего подразумеваются знания, раскрывающие сущность механизма следообразования; во-вторых, формируя основные положения тактики использования специальных знаний в противодействии (в узком смысле) киберпреступления, при производстве следственных действий и проведении оперативно-розыскных мероприятий.

Специфика осуществления противодействия данным преступлениям предопределена необходимостью работы с КИ, а именно совершением действий по ее поиску, обнаружению, фиксации, изъятию, сохранению и исследованию. Такая деятельность сопровождается обнаружением, аутентификацией, восстановлением и преобразованием КИ в отображаемую, доступную для непосредственного восприятия человеком форму. Следовательно, наибольший теоретико-прикладной интерес представляет исследование НТС, применяемых для обнаружения, фиксации, изъятия и исследования следов компьютерных преступлений с целью повышения эффективности их применения. Очевидно, что наиболее полное и быстрое раскрытие компьютерных преступлений может быть осуществлено в тех случаях, когда при производстве следственных действий и проведении оперативно-розыскных мероприятий, направленных на собирание и исследование доказательств, используются все реально способствовавшие установлению истины по делу НТС.

Ранее нами были сформулированы системные требования к НТС, используемым, например, при проведении осмотра места происшествия по делам рассматриваемой категории, а именно: безопасность, универсальность, защищенность, эффективность, целесообразность, мобильность. Отметим непрерывность процессов заимствования достижений научно-технического прогресса в отрасли информатизации и комплексной защиты КИ. Очевидно, что технологии ее обработки, накопления и хранения усложняются, что объективно требует оперативного реагирования. Наиболее эффективным оно может быть в случае непрерывного мониторинга и анализа характера и уровня развития аппаратно-программных средств, используемых как для обработки и хранения КИ, так и для обеспечения компьютерной безопасности с последующим внедрением отобранных таким образом НТС в деятельность правоохранительных органов. Для проведения наиболее сложных, специфических исследований НТС могут также специально разрабатываться (конструироваться). В этом случае осуществляется заимствование не самих НТС, а информации, необходимой для формирования технических заданий разработчикам НТС. Субъектами, осуществляющими анализ, прежде всего должны быть сотрудники научно-исследовательских и научно-педагогических коллективов систем МВД, прокуратуры и органов государственной безопасности, распространение накопленных ими знаний осуществляется через систему криминалистического и специального образования в рамках деятельности по криминалистическому и оперативно-техническому обеспечению противодействия компьютерной преступности. В качестве критериев заимствования НТС могут быть использованы системные требования к ним, сформулированные выше. Глубина такого заимствования отражается на конструктивных особенностях НТС.

Таким образом, на основании объекта криминалистического исследования можно представить следующую классификацию НТС:

предназначенные для криминалистического исследования КИ (исследование качества КИ – ее целостности и доступности; исследование следовой КИ; восстановление КИ; исследование и использование каналов утечки КИ; поиск КИ);

предназначенные для криминалистического исследования носителей КИ (исследование свойств средств компьютерной техники; исследование инженерно-технических средств защиты КИ, в том числе вскрытие систем защиты; исследование сетей).

УДК 343.985

С.В. Король

СОДЕЙСТВИЕ ГРАЖДАН ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ

Преступность – один из главных факторов, препятствующих осуществлению позитивных социальных и экономических реформ в стране. Укрепление правового порядка и борьба с преступностью в Республике Беларусь являются одной из главных общенациональных задач, требующих принятия серьезного комплекса мер.

Значимое место среди наиболее эффективных средств борьбы с преступностью занимает оперативно-розыскная деятельность (ОРД). Наиболее приоритетными задачами ОРД согласно ст. 3 Закона Республики Беларусь от 15 июля 2015 г.