ских трансформаций, требующих использования всего спектра средств правового реагирования на возникающие угрозы в информационной сфере.

Проблемы уголовно-правовой охраны кибербезопасности (компьютерной безопасности) с 90-х гг. XX в. являются предметом пристального анализа отечественных ученых-криминалистов. Однако в белорусской уголовно-правовой доктрине почти не уделялось внимание комплексному исследованию проблем информационной безопасности в гуманитарном аспекте, анализу средств и способов уголовно-правового обеспечения информационно-психологической безопасности. Актуальность обращения к проблемам уголовно-правовой охраны информационно-психологической безопасности субъектов информационных отношений обусловлена динамикой политических, экономических, социальных процессов, резким возрастанием значения информации и знаний в условиях развития информационных и коммуникационных технологий, что подтверждается не только отечественными, но и мировыми тенденциями трансформации правового механизма обеспечения информационного суверенитета государства и информационно-психологической безопасности субъектов всех уровней (личный, корпоративный, государственный). Концепция информационной безопасности Республики Беларусь, утвержденная постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, определяет противодействие деструктивным информационно-психологическим воздействиям на массовое общественное сознание в качестве одного из средств обеспечения безопасности информационно-психологической компоненты информационной сферы. Развитие социальных процессов в информационной среде, изменение условий социального бытия, важной сферой которого становится информационная сфера, требуют адаптации как регулятивных, так и охранительных механизмов обеспечения стабильности и прогрессивного развития информационной сферы прав и интересов субъектов информационных отношений.

Концепция в качестве угроз в информационно-психологической сфере определяет действия по дискредитации конституционных основ государства и его властных структур, размыванию национального менталитета, вовлечению людей в экстремистскую и террористическую деятельность, разжиганию межнациональной и межконфессиональной вражды, формированию радикального и протестного потенциала, действия, направленные на нарушение территориальной целостности государства. Мощным фактором психоманипуляции в современной действительности стало умалчивание и фальсификация исторических фактов, изменение трактовок важнейших исторических событий. В этой связи актуальным направлением правовой политики государства становится противодействие трансформации исторической памяти народа, представляющей угрозу национальной безопасности. Деструктивное информационное воздействие используется как метод социального управления и создает угрозу причинения вреда личным, корпоративным, общественным, государственным интересам. Анализ социальной действительности, обусловливающей трансформацию законодательства, свидетельствует о том, что получает распространение информационное воздействие как вид общественно опасного деяния. Указанное предопределяет необходимость дефинирования информационного воздействия как вида информационного деяния, которое выражается в распространении либо предоставлении, а также утаивании, сокрытии, непредоставлении информации с целью оказания влияния на индивидуальное либо групповое сознание.

Анализ актов деструктивного информационного воздействия, свидетельствующий о расширении спектра информационных угроз, указывает на необходимость определения системы правовых средств противодействия таковым на основе научно обоснованной стратегии правовой охраны национальных интересов в информационной сфере. Самостоятельными задачами совершенствования уголовно-правового механизма обеспечения информационной безопасности как интегративного объекта правовой охраны, полагаем, являются:

определение социальной потребности установления уголовной ответственности за общественно опасные информационные деяния;

определение предмета и пределов уголовно-правовой охраны информационной безопасности личности, общества, государства с постулированием ее как важнейшего базового объекта уголовно-правовой охраны;

совершенствование мер уголовно-правового контроля за преступностью в информационной сфере.

УДК 343.985.8

Б.В. Ковалик

МЕХАНИЗМ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ ДИСТАНЦИОННЫМ СПОСОБОМ

Одним из наиболее распространенных преступлений, совершаемых в сети Интернет, является мошенничество. Актуальность данной проблемы обостряется формированием транснациональных организованных преступных групп в этой сфере, как правило действующих из-за пределов страны проживания жертв данных преступлений. Алгоритм их функционирования отлажен, и по своей структуре они сходны с действующими на законной основе организациями со своими службами поддержки и безопасности, бухгалтерией и т. д. Большинство из них используют идентичные принципы организации, схемы совершения преступлений и имеют четко выстроенную иерархию.

Площадкой для реализации преступных намерений могут стать классифайды, социальные сети, сайты знакомств и другие интернет-ресурсы. В ходе переписки непосредственный исполнитель просит потенциальную жертву перейти по предоставленной ссылке и выполнить условия рекомендуемого им сервиса, который является фишинговым. Большинство площадок по размещению объявлений препятствуют деятельности мошенников, блокируя сторонние ссылки во внутренних чатах.

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