3) «для обороны других лиц, когда никакое иное средство защиты не было возможно».

Оружие могло быть применено и при задержании преступника, оказавшего сопротивление «сему указанными в п.п. 1 и 2 насильственными действиями или когда невозможно будет преследовать или настичь убегающего», а также «при преследовании арестанта, бежавшего из тюрьмы или из-под стражи, когда невозможно настичь его или когда он противится задержанию, предусмотренными выше насильственными действиями».

В перечисленных случаях милиционеры были обязаны обо «всех обстоятельствах и последствиях употребления в дело оружия» немедленно сообщить начальнику милиции.

Таким образом, Инструкция от 10 декабря 1918 г., утвержденная Президиумом Рогачевского уездного исполнительного комитета, созданная для регламентации деятельности органов милиции Рогачевского региона в условиях создавшегося правового вакуума, представляет научный интерес не только для истории ОВД Республики Беларусь, но и всей отечественной истории государства и права. Данный документ любопытен, помимо прочего, тем, что являет собой свидетельство применения белорусскими правоохранителями на практике положений УУС после его юридической отмены.

ЗАРУБЕЖНЫЙ ОПЫТ

УДК 343.72

И.И. Бердинских

ЦИФРОВЫЕ МОШЕННИЧЕСТВА. СОВРЕМЕННОЕ СОСТОЯНИЕ И ПРОФИЛАКТИКА

Современную фазу мирового технологического развития можно идентифицировать как этап формирования и совершенствования разнообразных информационных систем. Стремительный рост технологического процесса влечет за собой динамичное внедрение в жизнь людей процессы цифровизации, такие как использование компьютерной техники, сотовой связи и развитие электронных услуг различного социального характера. В то же время глобальная цифровизация, развитие передовых технологий, внедрение инновационных разработок приводят к дополнительным угрозам и рискам, в том числе и криминогенного характера.

Применение передовых технологий приводит к росту объема персональных данных в информационной среде: при помощи электронной почты происходит обмен различного рода документами, в том числе содержащими персональные данные граждан, в мессенджерах и социальных сетях размещается информация, раскрывающая личную жизнь, при совершении покупок через интернет-магазины направляются реквизиты банковских платежных карточек. Для осуществления противоправных действий мошенники используют персональную информацию, полученную на нелегальном рынке баз данных интернет-магазинов, государственных организаций, финансовых структур.

На сегодня почти каждый современный человек использует в повседневной жизни мобильные устройства и хотя бы раз сталкивался с телефонным мошенничеством. К сожалению, даже современные антивирусные приложения, установленные на мобильных устройствах и персональных компьютерах, не способны в полной мере предотвратить мошеннические действия, как правило, направленные на завладение денежными средствами жертв, так как большинство телефонных мошенничеств осуществляются при помощи методов психологического давления и манипуляций.

Так, согласно статистическим данным информационного центра МВД России, за январь – декабрь 2021 г. ущерб от мошенников, действующих с использованием информационно-телекоммуникационных технологий, составил в России более 45 млрд р., в то же время темп

роста регистрации такого рода преступлений замедлился. По итогам 2021 г. их количество выросло незначительно – на 1,4 %. Примерно половина всех потерпевших сами добровольно передавали секретные данные, пароли и коды. Наиболее распространенным видом мошенничества с использованием информационно-телекоммуникационных технологий является телефонное мошенничество.

Всероссийский центр изучения общественного мнения (ВЦИОМ) в середине 2021 г. представил данные опроса о телефонных мошенниках.

За первое полугодие 2021 г. 57 % опрошенных получали звонки от телефонных мошенников, 19 % – СМС-сообщения, 35 % с действиями телефонных мошенников не сталкивались. Чаще всего мошенники звонили жителям Москвы и Санкт-Петербурга – 70 %, жителям городов с населением более миллиона человек – 69 %, жителям сел – 40 %, малых городов – 55 %.

В результате действий телефонных мошенников понесли денежный ущерб 9 % россиян (из них 6 % сообщили о значительном ущербе).

Представленные данные свидетельствуют о том, что преступления в сфере информационно-коммуникационных технологий становятся одним из наиболее простых способов получения несанкционированного доступа к информации о банковских реквизитах граждан.

Действия телефонных мошенников квалифицируются по ст. 159 Уголовного кодекса Российской Федерации как мошенничество, т. е. умышленные действия, направленные на хищение чужого имущества путем обмана или злоупотребления доверием. Противодействие такому виду мошенничества осуществляется государственными органами не только с помощью регистрации и расследования уголовных преступлений, но и путем информирования граждан о потенциальной опасности.

Можно выделить следующие основные виды мошенничества, совершенные с использованием информационно-телекоммуникационных технологий:

просьбы о помощи от лица друзей или родственников. Чтобы заставить жертву мошенничества поверить и перечислить деньги на счета мошенников, телефонные преступники используют различные методы, применяя высокотехнологичные устройства, например, для имитации голоса или обработки фотографии тех, от чьего имени они звонят;

платные телефонные номера. Способ телефонного обмана, когда жертва пытается дозвониться на платный номер телефона. Используют очень часто и в самых разных вариациях, в результате чего деньги со счета владельца телефона переходят на счет мошенника;

телефонные вирусы. Абонентам присылают сообщение с просьбой перейти по ссылке, после чего происходит списание денежных средств;

«выигрыш в лотерее». Человеку звонит мошенник, представляется, например, ведущим популярной радиостанции и поздравляет его с выигрышем в лотерее, организованной радиостанцией и мобильным оператором. Когда жертва перезванивает, сотрудник «призового отдела» говорит, что для получения приза нужно предоставить реквизиты банковской платежной карточки и заплатить налог на доходы физлиц;

код от оператора связи. Жертве поступает звонок или приходит СМС-сообщение от мошенника, представляющегося сотрудником техподдержки оператора связи, в котором ему предлагают подключить новую эксклюзивную услугу для улучшения качества связи или для защиты от спам-рассылки, после чего происходит списание денежных средств;

звонки с подмененных номеров. Большинство банков имеют специальные номера, которые используются только для сообщений клиентам. Сбербанк, например, рассылает свои уведомления только с номеров 900 или 9000. Но существуют специальные программы, которые маскируют настоящий номер звонящего, и абонент видит знакомый ему идентификатор, после чего теряет бдительность и идет на поводу у мошенников, вследствие чего лишается своих денежных средств.

Чтобы не стать жертвой телефонных мошенников, рекомендуется выполнять следующие действия:

ни при каких обстоятельствах не сообщать по телефону свои конфиденциальные данные. Необходимо помнить, что банки и другие легитимные организации никогда не потребуют озвучить код из СМС, CVV и т. д. Запрос конфиденциальной информации – самый явный признак мошенничества;

при малейшем подозрении нужно завершить звонок и перезвонить на официальный телефон той организации, от которой поступил первичный вызов. В случае банка, например, телефон можно найти на оборотной стороне банковской платежной карточки, либо в личном кабинете онлайн-банкинга. Следует отметить, что помимо финансовых организаций и силовых организаций, мошенники также представляются сотрудниками сотовых операторов;

не реагировать на сообщения с незнакомых номеров, в которых указаны ссылки для скачивания стороннего программного обеспечения или переход на какие-либо веб-страницы с целью получения, например, выигрыша в лотерее (особенно, если ни в каком конкурсе вы не участвовали). Такие действия способствуют установке на телефон жертвы мошенников вирусного программного обеспечения, хищению персональных данных и денежных средств;

необходимо игнорировать сообщения с незнакомых номеров с просьбой перевода денежных средств. Мошенники могут написать от

лица близких родственников. Необходимо совершить звонок с уточнением на номер человека, от лица которого действуют мошенники;

не следует перезванивать на незнакомый номер в виду того, что мошенники часто используют платные номера, при звонке на такой номер с лицевого счета жертвы удерживаются денежные средства.

В связи с тем что цифровая преступность не имеет территориальности, для эффективной борьбы с киберпреступлениями необходимо усиливать межгосударственное взаимодействие правоохранительной системы с целью быстрого реагирования на факты цифрового мошенничества. Кроме того, для повышения эффективности расследования преступлений в сфере информационно-телекоммуникационных технологий целесообразно регулярное проведение профилактических мер в средствах массовой информации, усовершенствование правовой, технической базы, профессиональная подготовка узконаправленных специалистов.

Полагаем, данная статья может способствовать формированию актуальных взглядов на состояние киберпреступности и выработке мер профилактического характера борьбы с ней.

УДК 004.89

В.В. Достов

О НЕКОТОРЫХ ВОПРОСАХ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ В СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ

Несмотря на высокие темпы развития информационных технологий, не стоит полагаться только на информационные системы и современные технологии, чем отличаются современные тенденции развития правоохранительных органов всего мира, однако нужно понимать современное состояние и уровень развития программного обеспечения, способного оказывать непосредственную помощь в организации раскрытия, расследования и предупреждения преступлений, обеспечения охраны общественного порядка и обеспечения общественной безопасности.

Только комплексный подход, как со стороны сотрудников, осуществляющих эксплуатацию и ведение информационных ресурсов правоохранительных структур, так и со стороны сотрудников, являющихся источниками информации для них, позволит обеспечить их эффективное и результативное использование.

Выбор программного обеспечения, которое будет использоваться непосредственно для формирования массивов данных не принципиален,

однако выбор программного обеспечения с постоянной поддержкой и сопровождением будет существенно способствовать нейтрализации рисков как информационной безопасности, так и снижения эргономичности информационных систем.

Размещение в базах данных правоохранительных структур информации о результатах судебных экспертиз может способствовать оперативному раскрытию преступлений прошлых лет и идентификации лиц, их совершивших. Этому аспекту не уделяется должного внимания в области объединения данных информационных ресурсов с ресурсами, находящимися в распоряжении сотрудников, непосредственно занятых в раскрытии и расследовании преступлений.

Значимым фактором повышения эффективности использования информационных систем правоохранительных органов является возможность консолидации всей оперативно значимой информации в единой информационной системе, формируемой на основе банков данных различных государственных структур, так или иначе занятых в правоохранительной деятельности и обеспечении государственной безопасности. При формировании и проектировании информационных систем необходимо учитывать технические, правовые и программно-аппаратные возможности интеграции ресурсов взаимодействующих правоохранительных структур и систем межведомственного взаимодействия. Нужна глубокая проработка точек взаимодействия, рамок и объемов предоставления информации в строгом соответствии с законодательством и обеспечением мер информационной безопасности. Реализация данных мер возможна в рамках межведомственных соглашений об информационном обмене.

Для обеспечения своевременного и качественного наполнения банков данных правоохранительных органов должен быть обеспечен максимальный охват источников информации. При обеспечении данного свойства системы сбора, обработки и хранения оперативной информации, ее достоверность по каждому отдельному случаю не будет представлять значения, за счет того, что информация из разных источников будет оцениваться по признаку идентификации совпадающих значений. Для реализации данных мер в информационные системы правоохранительных органов необходимо осуществить внедрение инструментария нейросетей различного назначения, отвечающих как за идентификацию лиц, явлений, предметов и событий, так и за систему поддержки принятия решений. Использование нейросетей позволит существенно повысить эффективность и оперативность использования информационных ресурсов правоохранительных структур, так как за счет взаимодействия с субъектами правоохранительной деятельности они будут обучаться и