УДК 343.985.8

***Г.А. Казакевич**, заместитель министра внутренних дел Республики Беларусь – начальник криминальной милиции*

О МЕРАХ, ПРИНИМАЕМЫХ МВД РЕСПУБЛИКИ БЕЛАРУСЬ, ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ НА СОВРЕМЕННОМ ЭТАПЕ

Проанализированы современные меры, предпринимаемые МВД Республики Беларусь, по противодействию киберпреступности. Рассмотрен порядок действий правоохранительных органов с целью профилактики киберпреступлений и минимизации вызовов и угроз в мире информационных технологий. Представлен комплекс мероприятий, направленный на повышение цифровой грамотности и информационной защищенности граждан Республики Беларусь от киберугроз.

Ключевые слова: противодействие киберпреступности, сеть Интернет, фишинг, вишинг, сваттинг, идентификация пользователя, электронные платежные системы, профилактика киберпреступности.

Сегодня государство уделяет особо повышенное внимание обеспечению защищенности информационного пространства. Согласно Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, в нашей стране создана система предупреждения, выявления, пресечения и всестороннего расследования киберпреступлений. Эффективность противостояния правоохранительной системы данному преступному вызову зависит как от состояния правопорядка, защищенности прав и интересов граждан, так и от обеспечения информационной безопасности общества и государства.

Статистика свидетельствует, что количество регистрируемых киберпреступлений ежегодно увеличивается более чем в два раза. В общем объеме зарегистрированных преступлений этот показатель вырос в три раза в основном за счет хищений путем использования компьютерной техники. В действительности преступлений такого вида намного больше, и с учетом высокой степени латентности раскрываемость киберпреступлений составляет около 10 %.

Изучение международного опыта показывает, что распространение киберпреступности свойственно большинству государств мира. Например, в Российской Федерации количество таких уголовно наказуемых деяний в 2020 г. увеличилось на 73,4 %, а их удельный вес в общей структуре преступности составил 25 %.

Значительный рост киберпреступлений обусловлен повсеместным и нарастающим использованием всевозможных форм дистанционного обслуживания. Беларусь, как и все мировое сообщество, ориентирована на развитие и популяризацию безналичных расчетов, сопровождающихся увеличением количества устройств, осуществляющих финансовые транзакции, ростом числа пользователей разнообразных электронных платежных систем в сети Интернет. Не последнюю роль в распространении и росте преступности в данной сфере сыграли последствия коронавирусной инфекции (Covid-19), в частности переключение на интернет-пространство многих сфер общественных отношений, в том числе удаленный режим работы, товарный и денежный обороты.

Согласно данным Национального банка Республики Беларусь, объем платежей с использованием банковских платежных карточек по оплате товаров (работ, услуг), прочих безналичных операций в 2020 г. постоянно увеличивался и достиг 60,2 % от всех платежей.

В сети Интернет количество пользователей, недостаточно осведомленных об угрозах информационной безопасности, составляет довольно широкую, привлекательную и уязвимую целевую группу для киберпреступников, активно использующих методы социальной инженерии.

Наиболее распространенным способом совершения киберпреступлений в настоящее время является фишинг[1]. Основной способ совершения данного вида киберпреступлений – применение CNP-фрода[2] совместно с методами социальной инженерии посредством телефонных и интернет-коммуникаций, а также использование фишинговых интернет-ресурсов.

В Республике Беларусь в 2020 г. злоумышленники массово использовали интернет-площадку Kufar[3] в качестве источника поиска жертв преступлений среди лиц, размещавших объявления о продаже (покупке) товаров. Организованные группы, взаимодействуя через закрытые чаты мессенджера Telegram, осуществляли «отработку» потенциальных потерпевших, получая реквизиты банковских платежных карточек путем обмана или направления ссылки на фишинговый интернет-ресурс. Похищенные средства переводились на электронные кошельки, оформленные на подставных лиц, либо в криптовалюту[4].

В результате проведенных по инициативе МВД Республики Беларусь организационных и технических мероприятий во взаимодействии с ООО «Адевинта» (интернет-площадка Kufar) количество совершаемых с использованием данного ресурса преступлений в 2021 г. значительно снизилось. Для этого были приняты соответствующие меры: логирование доступов к объявлениям и абонентским номерам неавторизованными пользователями; ограничение доступа к просмотру телефонных номеров и регистрация учетных записей с иностранных IP-адресов; сокрытие абонентских номеров с целью ведения диалога через сайт; создание и внедрение сервиса «Куфар Оплата», когда зачисление денежных средств продавцу осуществляется после подтверждения доставки товара соответствующей службой покупателю. Так, во втором полугодии 2020 г. от общего количества зарегистрированных хищений путем использования компьютерной техники преступления с использованием интернет-площадки Kufar составляли около 19 %, а за январь – май 2021 г. их доля сократилась до 9 %.

Другим наиболее распространенным способом совершения преступлений в данной сфере является вишинг[5]. Масштабность данной проблемы подтверждает следующий пример: в апреле 2021 г. сотрудниками МВД Республики Беларусь совместно со Следственным комитетом Республики Беларусь пресечена деятельность преступной группы, занимавшейся хищением денежных средств со счетов клиентов белорусских банков путем применения социальной инженерии. Злоумышленники, используя современные средства IP-телефонии (мессенджер Viber), выдавая себя за сотрудников служб безопасности банков, побуждали потенциальных жертв передавать им конфиденциальные данные (одноразовые смс-коды, личные идентификационные номера, реквизиты банковских платежных карточек). В результате совместно проведенной работы подозреваемыми признаны 28 граждан, в одном производстве соединено 134 уголовных дела. Причиненный преступными действиями ущерб составил более 1,5 млн белорусских рублей.

Широкий общественный резонанс также получило социально опасное явление «сваттинг», связанное с заведомо ложными сообщениями об опасности (например, минирование различных социально значимых объектов). Сегодня наблюдается значительный рост подобных сообщений, поступающих в государственные органы и организации с использованием возможностей сети Интернет.

[1] Фишинг (англ. phishing, от phone phreaking – взлом телефонных автоматов и fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Наиболее ярким примером фишинговой атаки может служить сообщение, отправленное жертве по электронной почте и подделанное под официальное письмо (от банка или платежной системы), требующее проверки определенной информации или совершения определенных действий. В подобных письмах обычно содержится ссылка на фальшивую веб-страницу, сходную с официальной и содержащую форму, требующую ввода конфиденциальной информации.

[2] CNP-фрод (от англ. card not present) – операции без присутствия карточек.

[3] Интернет-площадка Kufar использовалась в 2018 г. для совершения более 50 преступлений, в 2019 г. – около 125, в первом полугодии 2020 г. – более 100, во втором полугодии 2020 г. – около 3 780.

[4] Криптовалюта – разновидность цифровой валюты (электронных денег).

[5] Вишинг (от англ. vishing, от voice phishing – голосовой фишинг) – один из методов мошенничества с использованием социальной инженерии, заключающийся в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудник банка, покупатель товара и др.), под разными предлогами выманивают у держателя банковской платежной карточки конфиденциальную информацию или стимулируют к совершению действий со своим банковским счетом.

Аналогичные тенденции роста рассматриваемого вида преступлений на протяжении нескольких последних лет имеют место в соседних государствах (Российская Федерация, Украина).

Подростки, объединенные общим интересом (как правило, участники сетевых игр), от имени своего соперника по игре сообщают в органы правопорядка о минировании, тем самым «подставляя» его. Основными мотивами при этом являются развлечение и получение хайпа[1], причинение максимума неприятностей недругу. Общественная опасность подобных деяний заключается в том, что заведомо недостоверные сведения об опасности дезорганизуют нормальную работу транспорта, предприятий, государственных органов и учреждений, а также причиняют существенный экономический вред и организациям, и гражданам. Все сообщения об опасности воспринимаются серьезно и подвергаются тщательной проверке.

Следует отметить, что в связи с использованием преступниками различных механизмов анонимности в сети Интернет имеющимися в настоящее время в распоряжении правоохранительных органов техническими средствами оперативно отреагировать и установить злоумышленника не всегда представляется возможным.

Обычно для направления ложных сообщений о минировании преступники используют систему соблюдения анонимности TOR, электронную почту ProtonMail, совершают телефонный звонок посредством сервисов IP-телефонии с абонентского номера оператора связи иностранного государства.

Так, сотрудниками подразделений по противодействию киберпреступности Республики Беларусь только в 2020 г. установлено свыше 2 100 лиц (+14 %), виновных в совершении киберпреступлений. Около 1 600 (+11 %) из них привлечены к уголовной ответственности. Сумма установленного ущерба от совершения киберпреступлений превысила 1,5 млн белорусских рублей, а уровень ее возмещения потерпевшим достиг 61 %.

Сегодня можно с уверенностью говорить о международной специализации преступников по определенным способам совершения киберпреступлений, для которых не существует границ и карантинных ограничений.

Показательным в данном случае является следующий пример. Шестеро граждан Украины на протяжении 2017–2019 гг. совершили в отношении граждан Беларуси более 1 000 преступлений, связанных с хищением денежных средств в особо крупном размере в системах дистанционного банковского обслуживания путем применения методов социальной инженерии. Фигуранты признаны подозреваемыми по 302 уголовным делам (ст. 208, 209, 212, 349 УК Республики Беларусь).

Для повышения эффективности противостояния росту киберпреступлений разработана специализированная база данных в МВД Республики Беларусь. Система в режиме реального времени накапливает информацию обо всем, что связано с преступлениями в сфере высоких технологий: адреса, телефоны, электронные кошельки, транзакции и многое другое. База позволяет анализировать, обобщать сведения и координировать работу.

Так, анализ преступлений, совершенных в 2017–2020 гг. и связанных с хищением денежных средств с карт-счетов белорусских граждан, позволил возбудить 4,5 тыс. уголовных дел, к которым могут быть причастны члены организованной преступной группы граждан Украины. В настоящее время МВД Республики Беларусь совместно с СК Республики Беларусь проводится работа для объединения данных дел в одно производство.

МВД Республики Беларусь с целью профилактики киберпреступлений реализует комплекс масштабных мероприятий, направленных на повышение цифровой грамотности населения, и мер по обеспечению информационной безопасности.

Для подготовки школьников по предмету «Обеспечение безопасности жизнедеятельности» МВД Республики Беларусь специально разработана памятка о последствиях ложных сообщений об опасности с целью повышения осведомленности учащихся в этом вопросе. Работа выстроена с участием психологов, чтобы профилактика не превратилась в антирекламу. Родители являются особой целевой группой профилактики данных правонарушений. Задача правоохранительных органов – довести до их понимания, что бесконтрольные действия в сети Интернет чреваты проблемами не только для детей, но и для них самих (как минимум в виде внушительной материальной ответственности).

[1] Хайп (от англ. hype – шумиха) – надувательство, обман, трюк с привлечением внимания.

По инициативе МВД Республики Беларусь Администрацией Президента Республики Беларусь тема «Основные аспекты профилактики киберпреступности в Республике Беларусь» была определена в мае текущего года к изучению в рамках единого дня информирования.

По распоряжению министра внутренних дел Республики Беларусь в мае текущего года проведена декада кибербезопасности, в ходе которой основные усилия были сосредоточены на организации широкомасштабной воспитательно-профилактической работы с населением. В период проведения акции организовано и осуществлено 21 выступление в газетах «СБ. Беларусь сегодня», «Народная газета», журнале «Милиция Беларуси»; выступления на основных республиканских телеканалах, в эфире Первого национального канала Белорусского радио, радиостанций «Альфа Радио», «Радиус ФМ», размещена тематическая информация на официальном интернет-сайте и в телеграм-канале «Пресс-секретарь МВД Беларуси».

Во исполнение поручения Совета Министров Республики Беларусь МВД совместно с заинтересованными государственными органами подготовлен и проходит согласование проект Указа Главы государства «О совершенствовании деятельности по пресечению противоправной деятельности в сети Интернет». Цель проекта – обеспечение оперативной блокировки для пользователей белорусского сегмента сети Интернет вредоносных сайтов и ссылок с максимальным сокращением при этом бюрократических процедур.

МВД Республики Беларусь принимает активное участие в разработке проекта Указа Президента Республики Беларусь «О противодействии мошенничеству в банковской сфере», реализация которого упростит механизм взаимодействия между Национальным банком Республики Беларусь, банками и правоохранительными органами; а также в разработке Закона Республики Беларусь «Об изменении законов по вопросам банковской деятельности», предусматривающего корректировку Банковского кодекса Республики Беларусь в части совершенствования регулирования вопросов обеспечения информационной безопасности банков, усиления противодействия компьютерным атакам и мошенничеству с использованием электронных платежных инструментов.

Значимым этапом в совершенствовании противодействия киберпреступлениям на государственном уровне стала подготовка МВД Республики Беларусь и утверждение 26 марта текущего года заместителем Премьер-министра Республики Беларусь Ю.В. Назаровым Комплексного плана мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2021–2022 годы, основными направлениями которого являются повышение уровня компьютерной грамотности граждан, развитие и совершенствование систем обеспечения кибербезопасности, мониторинг и нейтрализация угроз из киберпространства, обеспечение защищенности информационных ресурсов от кибератак, создание и совершенствование системы подготовки кадров в сфере противодействия киберпреступлениям и их профилактики, развитие международного сотрудничества.

Таким образом, выстраиваемая комплексная система реагирования государственных органов на проявления киберпреступности учитывает постоянную трансформацию вызовов и угроз в мире информационных технологий, способствует повышению цифровой грамотности и защищенности наших граждан, обеспечивает реализацию государством принципа неотвратимости наказания за совершенные преступления.

***G.A. Kazakevich**, Deputy Minister of the Interior of the Republic of Belarus – Chief of the Criminal Militia*

MEASURES, TAKEN BY THE MINISTRY OF THE INTERIOR OF THE REPUBLIC OF BELARUS, TO COUNTER CYBERCRIME AT THE PRESENT STAGE

Analyzed current measures, undertaken by the Ministry of the Interior of the Republic of Belarus, to counteract cybercrime. Operating procedure for the law enforcement bodies to prevent cybercrime and minimize challenges and threats in the information technology world is considered. A set of measures to increase digital literacy and provide information security for citizens of the Republic of Belarus against cyber-threats is submitted.

Keywords: cybercrime counteraction, Internet, phishing, vishing, swatting, user identification, electronic payment systems, cybercrime prevention.