2) уязвимые места КВОИ – те его участки, зоны или сегменты критических элементов КВОИ, в отношении которых в силу их недостаточной устойчивости или низкого уровня защищенности могут быть успешно реализованы незаконные действия (электрокабели, провода связи, мотивация и здоровье персонала объекта и т. п.);

3) деяния, совершаемые в отношении критических элементов или уязвимых мест КВОИ, либо иные деяния, создающие угрозу безопасности КВОИ.

Адекватная и эффективная режимная деятельность должна основываться на знании и прогнозировании возможных действий лиц, создающих угрозы безопасности КВОИ, – нарушителей безопасности КВОИ.

4. Режимная деятельность уполномоченных субъектов по установлению, поддержанию и прекращению действия СКАПР при обеспечении безопасности КВОИ.

Целью осуществления режимной деятельности субъектов СКАПР при обеспечении безопасности КВОИ является охрана и защита, обеспечивающие соблюдение интересов государства и общества, а также нормальное функционирование объекта или поддержание его функционирования в случае выхода из строя его компонентов.

Установление СКАПР осуществляется принятием соответствующего законодательного акта, который регламентирует отношения в рассматриваемой области, определяет критическую информационно-коммуникационную инфраструктуру с выделением КВОИ и включением таких объектов в Государственный реестр КВОИ. Рассматриваемый СКАРП фактически установлен принятием Указа № 486. Одновременно сформирован соответствующий Государственный реестр.

Содержанием деятельности субъектов рассматриваемого СКАПР по поддержанию данного режима должна стать реализация соответствующих правовых, организационных, инженерно-технических, аппаратно-программных и специальных мер обеспечения безопасности КВОИ. Вместе с тем очевидно, что система мер обеспечения безопасности КВОИ сформирована еще не в полной мере, так как основной упор пока делается на аппаратно-программные и инженерно-технические меры.

Действия по прекращению действия СКАПР при обеспечении безопасности КВОИ будут заключаться в выводе соответствующих объектов из числа критически важных и в исключении их из Государственного реестра КВОИ.

УДК 343

Д.Г. Полещук

НЕЗАКОННЫЙ ОБОРОТ ПАРОЛЕЙ, КОДОВ ДОСТУПА К КОМПЬЮТЕРНОЙ СИСТЕМЕ, СЕТИ ИЛИ МАШИННОМУ НОСИТЕЛЮ: ПЕРСПЕКТИВЫ КРИМИНАЛИЗАЦИИ

Общество XXI в. характеризуется скоростными темпами развития информационных технологий, повышением значения информации и подавляющим воздействием глобальной компьютерной сети Интернет на повседневную жизнь большинства людей. На рабочих местах, в домашних условиях, в транспорте используются компьютеры, планшеты, смартфоны и иные устройства, позволяющие осуществлять быстрый доступ к различным информационным системам или сетям (в том числе социальным). В основном такой доступ носит санкционированный характер, то есть для его осуществления требуется идентификация пользователя путем введения его логина и пароля (кода) доступа, только пароля (кода) доступа либо использования дополнительных средств защиты от незаконного доступа (например, подтверждение доступа посредством SMS-информирования). Одновременно на многих машинных носителях (компьютеры, мобильные устройства и др.) также устанавливаются пароли (коды) доступа и даже сканеры отпечатков пальцев с целью ограничения доступа к таким устройствам посторонних лиц. Осуществление указанных технических мер обусловлено необходимостью защиты хранящейся в компьютерной системе, сети или на машинных носителях информации, ценной для их пользователей, владельцев и собственников.

Вместе с тем попытки несанкционированного доступа к защищенной информации приобрели маштабность мирового значения, а борьба с ними стала одной из ключевых проблем в сфере обеспечения информационной безопасности.

В то же время вопросам оборота паролей, кодов доступа к компьютерной системе, сети или машинному носителю (далее – пароли), полученным незаконным путем, в национальном охранительном законодательстве и в юридической литературе особого внимания не уделяется. С точки зрения действующего законодательства незаконные действия с паролями (продажа, отчуждение в иной форме, приобретение и др.) теоретически не могут рассматриваться как приготовление к преступлению (ст. 349 УК Республики Беларусь) или административному правонарушению (ст. 22.6 КоАП Республики Беларусь), поскольку КоАП не выделяет приготовление к административному правонарушению как основание наступления административной ответственно-

сти, а приготовление в рамках УК возможно только к умышленному преступлению, кроме преступлений, не представляющих большой общественной опасности.

Что касается возможности квалификации незаконного оборота паролей по ст. 353 УК «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети», по нашему мнению, она является некорректной, поскольку предмет указанного преступления по своему смысловому содержанию пароли не охватывает.

Таким образом, меры правового воздействия на лиц, занимающихся незаконным оборотом паролей, в Республике Беларусь отсутствуют.

Общественная опасность рассматриваемого деяния заключается в возможности неконтролируемого использования паролей, добытых незаконным путем, для подготовки и совершения более тяжких преступлений. При этом миллионы паролей ежедневно похищаются и передаются хакерами друг другу в сети Интернет. Особую роль при их незаконной передаче играет даркнет (частная сеть, соединения которой устанавливаются только между доверенными участниками, нередко с применением специального программного обеспечения).

Случаи масштабных похищений и продаж паролей непосредственно затрагивают и граждан государств – членов СНГ. Так, в мае 2016 г. на одном из специализированных форумов молодой русскоязычный хакер похвастался массивом из 1,17 млрд взломанных учетных записей (большинство из них аккаунты Mail.ru), который он готов продать. В июне 2016 г. в средствах массовой информации сообщалось о том, что хакер под ником Peace на одной из онлайн-платформ выставил на продажу пароли 70 млн пользователей «Вконтакте» за 1 биткоин (примерно $1300), полученные в результате кибератаки на сайт в период между 2011 и 2013 гг. Уже в марте 2017 г. в даркнете были выставлены на торги 5 млн паролей к почтовым ящикам Gmail и Yahoo.

Международные основы борьбы с незаконным оборотом паролей установлены Конвенцией Совета Европы от 23 ноября 2001 г. «О преступности в сфере компьютерной информации» (ETS № 185) (далее – Конвенция). Пункт 1 ст. 6 Конвенции предусматривает необходимость установления уголовной ответственности за умышленное производство, продажу, приобретение для использования, импорт, оптовую продажу или иные формы предоставления в пользование компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части, с намерением использовать их в целях совершения противозаконного доступа, неправомерного перехвата, воздействия на данные или воздействия на функционирование системы. Кроме того, Конвенция ориентирует на принятие законодательных мер, необходимых для того, чтобы квалифицировать в качестве преступления владение одним или несколькими паролями с намерением использовать их для совершения указанных выше преступлений.

Уголовная ответственность за рассматриваемые действия не наступает, если они связаны с разрешенным испытанием или защитой компьютерной системы.

Следует отметить, что сторона, присоединяющаяся к Конвенции, может сохранить за собой право не применять положения об уголовной ответственности за незаконные действия с паролями при условии, что такая оговорка не будет касаться продажи, оптовой продажи или иных форм предоставления в пользование паролей, кодов доступа или иных аналогичных данных.

Многие уголовные законы зарубежных государств содержат специальные нормы об уголовной ответственности за незаконный оборот паролей.

В частности, ст. 260-4 УК Молдовы предусматривает ответственность за неправомерные производство, импорт, продажу или предоставление паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к информационной системе в целом или ее части с целью совершения одного из преступлений, предусмотренных ст. 237, 259, 260-1–260-3, 260-5 и 260-6, если эти действия повлекли причинение ущерба в крупных размерах.

Статья 285 УК Грузии устанавливается уголовная ответственность за самовольные изготовление, хранение, продажу, распространение пароля, кода допуска, необходимого для проникновения в компьютерную систему, или иных подобных данных либо иное обеспечение доступа к ним с целью совершения киберпреступления либо нарушения тайны личной переписки, телефонных переговоров или сообщений.

Согласно ст. 231 УК Чехии подлежит уголовной ответственности тот, кто с намерением совершить нарушение тайны переписки или неавторизованный доступ к компьютерной системе и компьютерной информации производит, вводит в оборот, импортирует, экспортирует, перенаправляет, предлагает, предоставляет, продает или иным образом предоставляет, приобретает для себя или для другого лица либо обрабатывает пароль компьютера, код доступа, данные, процесс или любые другие аналогичные средства, с помощью которых можно получить доступ к компьютерной системе или ее части.

В ст. 615-4 УК Италии также предусмотрена ответственность за незаконную закупку, воспроизведение, распространение, передачу или предоставление кодов, паролей либо других средств доступа к компьютерной или телекоммуникационной системе.

Учитывая мировые тенденции консолидации усилий всех государств в борьбе с преступлениями против информационной безопасно-

сти и унификации норм материального уголовного права с положениями Конвенции, полагаем целесообразным рассмотреть вопрос установления уголовной ответственности за отдельные незаконные действия с паролями и в Республике Беларусь.

Предложенный подход будет иметь следующие результаты:

установление уголовной ответственности за незаконный оборот паролей будет способствовать вовлечению Республики Беларусь в борьбу с транснациональной киберпреступностью и позволит реагировать на рассматриваемые незаконные действия, совершенные на ее территории;

для возможного присоединения к Конвенции положения национального уголовного права будут приведены в соответствие с ее требованиями;

признание рассматриваемого деяния преступлением позволит предупредить совершение иных преступлений против информационной безопасности (ст. 349–352 УК Республики Беларусь).

На основании изложенного и принимая во внимание особенности действующего уголовного закона, предлагаем дополнить гл. 31 УК Республики Беларусь статьей следующего содержания:

«Статья 353^1. Незаконные изготовление, приобретение либо сбыт паролей, кодов доступа или иных аналогичных данных

Незаконные изготовление с целью сбыта, приобретение либо сбыт паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к защищенному машинному носителю, защищенной компьютерной системе или сети в целом или любой их части для совершения преступлений, предусмотренных ст. 349, 350, 351 и 352 настоящего Кодекса, –

наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет».

УДК 004:34

Ю.В. Полковниченко, Т.Г. Чудиловская

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время фиксируется все больше случаев использования информационно-коммуникационных технологий в целях нарушения работоспособности информационных систем и информационно-коммуникационных сетей, а также нарушения права граждан на неприкосновенность частной жизни, личной и семейной тайны, осуществления промышленного шпионажа, нарушения прав интеллектуальной собственности. Обеспечение информационной безопасности является актуальной проблемой ввиду наличия многообразных факторов и угроз. В обращении с ежегодным Посланием к белорусскому народу и Национальному собранию 21 апреля 2017 г. Президент Республики Беларусь А.Г. Лукашенко отметил: «Обеспечение национальной безопасности невозможно без надежной защиты от деструктивных информационных атак, которые стали средством вмешательства во внутренние дела суверенных государств».

Вопросы обеспечения информационной безопасности государства, наряду с организационными и программно-техническими мерами, должны регулироваться нормами права. Правовое обеспечение информационной безопасности в Республике Беларусь включает в себя огромный комплекс норм, содержащихся в различных нормативных правовых актах Республики Беларусь и международных договорах.

Правовое регулирование в области информационных отношений в Республике Беларусь осуществляется Законом Республики Беларусь «Об информации, информатизации и защите информации». Основной функцией Закона является регулирование отношений, возникающих в процессе жизненного цикла информации, при создании и использовании информационных технологий, систем, сетей, ресурсов, а также при организации и обеспечении защиты информации. Этот Закон устанавливает требования по защите информации, а также ссылается на иные законодательные акты Республики Беларусь, в которых закреплена ответственность за нарушение законодательства об информации, информатизации и защите информации.

Составы правонарушений в информационной сфере находят свое отражение в Кодексе Республики Беларусь об административных правонарушениях, в котором данному аспекту посвящена гл. 22 «Административные правонарушения в области связи и информации».

Одними из важнейших правовых средств обеспечения информационной безопасности являются нормы уголовного законодательства, устанавливающие преступные деяния, посягающие на отношения в различных сферах информационной безопасности и определяющие санкции за их совершение. Они представлены в Уголовном Кодексе Республики Беларусь в разделе XII «Преступления против информационной безопасности» (одноименная гл. 31, ст. 349–355). Преступления, посягающие на состояние защищенности жизненно важных интересов физических и юридических лиц в информационной сфере, содержатся и в других разделах и главах УК. С целью единообразного применения законодательства об ответственности за совершение преступлений против информационной безопасности целесообразно было бы принять