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

постановление Пленума Верховного Суда Республики Беларусь «О судебной практике по делам о преступлениях против информационной безопасности».

Важным документом, определяющим политику Республики Беларусь в сфере информационной безопасности, является Концепция национальной безопасности Республики Беларусь. В документе определены национальные интересы Республики Беларусь, внутренние и внешние источники угроз безопасности в информационной сфере, основные направления обеспечения информационной безопасности.

Принципы государственной политики Республики Беларусь в сфере информатизации и основные направления развития информационного общества с учетом совокупности факторов, влияющих на его прогресс, указаны в Стратегии развития информатизации в Республике Беларусь на 2016–2022 годы. Так, с учетом цифрового доверия, защиты информационных ресурсов и информационно-коммуникационной инфраструктуры Стратегия определяет основные направления обеспечения информационной безопасности:

организация научных исследований, разработка и производство собственных аппаратных и программных средств защиты информации, ключевых элементов информационно-коммуникационной инфраструктуры, совершенствование системы их стандартизации, сертификации и аттестации в целях создания «цифрового суверенитета» Республики Беларусь;

совершенствование нормативной правовой и нормативно-технической базы для доступного, эффективного и беспрепятственного информационного взаимодействия государства, бизнеса и граждан;

организация хранения персональных данных граждан Республики Беларусь исключительно в центрах обработки данных и дата-центрах на территории Республики Беларусь;

создание необходимого уровня защиты информации, содержащейся в государственных информационных ресурсах;

резервирование информационных сетей республиканских органов государственного управления;

активное использование возможностей белорусского спутника связи и вещания для увеличения информационного присутствия страны в мировом информационном пространстве.

В связи с постоянным ростом преступности в области информационной безопасности, масштабностью причиненного ею ущерба для физических и юридических лиц такие преступления представляют серьезную угрозу для общества, а борьба с ними является серьезной проблемой для правоохранительных органов, особенно в части, касающейся оперативного установления злоумышленников, самого факта и места совершения преступления. Для противодействия данным преступлениям в 2001 г. в Министерстве внутренних дел Республики Беларусь создано управление по раскрытию преступлений в сфере высоких технологий (УРПСВТ, или управление «К»). Приоритетной задачей управления является координация деятельности подразделений МВД Республики Беларусь при выявлении ими преступлений против информационной безопасности. Также управление «К» осуществляет международное сотрудничество по оперативному обмену информацией в рамках противодействия преступлениям в сфере высоких технологий посредством международной сети НКП (Национальный контактный пункт), функционирующей под эгидой Римско-Лионской подгруппы «Группы Восьми». Наиболее эффективное взаимодействие осуществляется с Российской Федерацией.

Следует отметить, что Следственный комитет Республики Беларусь выступил с инициативой создания в Республике Беларусь центра противодействия киберпреступности. Центр передового опыта с целью решения теоретических и практических проблем противодействия киберпреступлениям предлагается создать на базе одного из учебных заведений Республики Беларусь. В центре должны будут работать как преподаватели вузов, так и сотрудники правоохранительных органов, специалисты в области расследования таких преступлений. Предполагается, что будут осуществляться исследования в области уголовного права, уголовного процесса, криминалистики, будут проводиться регулярные встречи ученых, представителей правоохранительных органов и частного сектора для обмена опытом и поиска решений существующих проблем, выработки стратегических подходов в борьбе с киберпреступностью, создания учебных и образовательных программ по данной тематике. Создание центра противодействия киберпреступности, несомненно, повысит уровень информационной безопасности в стране.

Таким образом, для обеспечения информационной безопасности в Республике Беларусь осуществляется эффективное правовое регулирование в информационной сфере, работают специальные подразделения для борьбы с преступлениями в области информационной безопасности, ведется взаимодействие с правоохранительными органами разных стран.

Приоритетными направлениями в развитии обеспечения информационной безопасности является совершенствование нормативной правовой базы, завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования дея-

тельности в этой сфере. При этом важное значение отводится усилению деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством.

УДК 343.8

А.Е. Сушко

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита граждан, их прав и свобод, интересов общества и государства являются основными задачами, стоящими перед правоохранительными органами Республики Беларусь.

На современном этапе столь динамичного развития и применения информационных технологий неизбежно возникает проблема защиты от их использования в преступных целях. Преступность в сфере высоких технологий не имеет границ и составляет угрозу международной безопасности.

Киберпреступность является проблемой мирового уровня, так как подобные преступления совершаются, как правило, транснациональными организованными преступными группами, члены которых, используя возможности сети Интернет, виртуально пересекают границы между государствами и пользуются несовершенством законодательства различных государств. Преступления против информационной безопасности приобретают транснациональный и организованный характер. Преступление с использованием компьютерной техники и ресурсов интернета может быть совершено на территории другой страны и даже нескольких государств одновременно. При этом злоумышленник потратит на его совершение всего несколько минут, общаясь с представителями различных организаций (банковские учреждения, интернет-магазины, платежные системы, различные сервисы интернета) не выходя из своего дома.

Концепция национальной безопасности Республики Беларусь определяет информационную безопасность как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере и выделяет ее в самостоятельную составляющую национальной безопасности. К таким угрозам относятся и преступления против информационной безопасности, впервые отраженные в Уголовном кодексе Республики Беларусь

1999 г. Статистика последних лет свидетельствует об увеличении количества этих преступлений.

В 2016 г. в сравнении с 2015 г. количество выявленных преступлений в сфере высоких технологий увеличилось на 1,3 % (с 2 440 до 2 471), притом прирост преступлений против информационной безопасности (гл. 31 УК Беларуси) составил 63,6 % (с 404 до 651). Количество же фактов несанкционированного доступа к компьютерной информации возросло на 152,9 % (со 102 до 258).

Национальными интересами России в сфере информационных технологий является обеспечение прав и свобод граждан, а также неприкосновенность частной жизни, как определено в Доктрине информационной безопасности Российской Федерации.

Информационная безопасность приобрела особое значение в условиях глобализации и интенсивного информационного обмена в мировом масштабе. Дело бывшего сотрудника ЦРУ и агентства национальной безопасности США Эдварда Сноудена, хакерские атаки на серверы Демократической партии США, серверы Европейской комиссии подтверждают это.

Практически каждый белорус в настоящее время активно использует множество высокотехнологичных устройств (Smart TV, компьютеры, планшеты, мобильные телефоны и иные электронные устройства, банковские карточки). Международный союз электросвязи отметил, что Беларусь в 2016 г. улучшила позиции в рейтинге развития информационно-коммуникационных технологий (ИКТ) и заняла 31-е место среди 175 стран.

Очевидно, что в настоящее время подлежит защите любая информация, имеющая отношение к физическому лицу, которая включает его персональные данные, сведения о регистрации на различных сайтах в сети Интернет или в социальных сетях, сведения о покупках в интернет-магазинах. Минимизировать риски в указанной сфере, в частности со стороны операторов персональных данных, позволит принятие Закона «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Так как проблема информационной безопасности не носит региональный характер, а охватывает все государства мира, при разработке указанного Закона целесообразно ориентироваться на европейское и российское законодательства в данной сфере.

Управлением Следственного комитета по Минской области в январе 2017 г. завершено расследование уголовного дела в отношении группы лиц, занимавшихся хищениями денежных средств граждан.