номер и тем самым имеет возможность перехватить уникальный код доступа к криптокошельку владельца. Стоит обратить внимание и на использование злоумышленниками специальных протоколов, которые позволяют отслеживать в мобильной сети поступающие на определенный номер смс-сообщения и информацию, содержащуюся в них, которая, соответственно, и дает возможность доступа к электронному криптокошельку и совершению хищения.

Среди мошенников пользуется популярностью метод фишинга, т. е. обмана пользователей путем создания поддельных сайтов, где владельцы криптокошельков добровольно вводят свои личные данные, используемые в последующем для совершения хищения. Фишинг может осуществляться как посредством рассылки писем на электронную почту, так и через создание чатов и открытых групп в социальных сетях и мобильных мессенджерах. Однако принцип механизма аналогичный в обоих вариантах: пользователь получает письмо или уведомление от имени криптоплатформы или биржи о необходимости пройти дополнительную авторизацию и прямую ссылку на сайт, переходя по которой попадает на идентичный настоящему по внешним признакам сайт мошенника. Следует отметить, что копированию подвергается даже доменное имя ресурса, в котором достаточно изменить всего один символ для его запуска. Доверчивый пользователь вводит необходимые злоумышленнику логин и пароль к своему криптокошельку, чем помогает последнему получить доступ к хранилищу и перевести все цифровые активы на сторонний кошелек. Кроме того, фишинговые сайты нередко ссылаются на рекомендации от знаменитых и влиятельных людей, которые как бы рекомендуют использовать именно этот сайт, как проверенный на личном опыте, что вводит неграмотных пользователей в заблуждение.

Еще один способ хищения криптомонет – внедрение вредоносного программного обеспечения (трояна), которое может быть загружено на устройство также посредством фишинг-атаки. Троян, попадая на незащищенное и уязвимое устройство, способен копировать всю информацию о системе и ее пользователе (его личные данные, информацию о банковских платежных карточках и счетах, логины и пороли к аккаунтам, ключи к криптокошелькам), с последующей передачей управляющему серверу, за которым и стоят мошенники, умело использующие полученные данные в корыстных целях.

Таким образом, перед правоохранительными органами стоит задача предупреждения и профилактики совершения такого рода хищений посредством пропаганды цифровой культуры в средствах массовой информации, сети Интернет или посредством личных бесед с гражданами и коллективами, которая должна включать в себя комплекс мер

по обеспечению безопасности личных данных пользователей при регистрации и использовании социальных сетей, мессенджеров и иных ресурсов сети Интернет.

УДК 343.4

Шукюров Шахин Тейюб оглы, доктор философии по праву, доцент кафедры «Административная деятельность в ОВД» Академии Полиции МВД Азербайджанской Республики
shahin 1967@mail.ru

КОНСТИТУЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ И ЕГО ВЗАИМОСВЯЗЬ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Компьютерная преступность – один из новых видов злостных правонарушений в нашем современном обществе. Она обладает характерными особенностями, среди которых способность быстро приспосабливаться к новым условиям и проникать во все сферы нашей жизни – ее главная цель.

В настоящее время преступления, совершаемые с использованием информационных технологий, создают особо глобальную угрозу национальной безопасности государств, открывают безграничные возможности, порождают все новые проблемы для развития общества. Информационные технологии в руках недоброжелателей служат удобным инструментом и быстро досягаемым рычагом для совершения других особо опасных видов преступлений, таких как терроризм, экстремизм, наркомания, тем самым создавая серьезные проблемы для его решений.

Несмотря на то что преступления, совершаемые с использованием информационных технологий, приобретают транснациональный характер, непосредственно находят свое глубокое отражение во внутренних делах государства.

На заседании Кабинета Министров Азербайджанской Республики, посвященном итогам 2013 г., Президент Азербайджанской Республики Ильхам Алиев, раскрывая характерные черты современной информационно-коммуникационной политики в государствах мира, отметил важную роль в формировании международного общественного мнения, расширяющихся с каждым днем интернет-ресурсов и транснациональных информационных систем, тенденцию перешагивания виртуальных связей через все национальные границы в мире. Президент Азербайджанской Республики особо подчеркнул, что на современном

этапе мирового развития одним из главных приоритетов национальной безопасности каждой страны является обеспечение информационной безопасности.

В обращении с ежегодным Посланием к белорусскому народу и Национальному собранию 21 апреля 2017 г. Президент Республики Беларусь А.Г. Лукашенко отметил следующее: «Обеспечение национальной безопасности невозможно без надежной защиты от деструктивных информационных атак, которые стали средством вмешательства во внутренние дела суверенных государств».

Конституционно-правовое обеспечение борьбы с компьютерной преступностью заключается в том, что Конституция – Основной Закон и акты, исходящие из него, устанавливая определенные права, свободы и обязанности граждан в сфере информационных отношений, запрещают выход за пределы указанных прав, свобод, обязанностей, а уголовное законодательство определяет уголовную ответственность за невыполнение требований содержания Конституции и законодательства.

Согласно содержанию конституций государств – участников СНГ в основном права и свободы граждан в сфере информационных отношений идентичны и основываются на конституционных принципах.

Право человека на информацию – одно из прав, закрепленных в действующих конституциях государств – участников СНГ. Допустим, это можно увидеть на примере Конституции Российской Федерации. Права и свободы человека и гражданина в сфере информационных отношений определены Конституцией Российской Федерации и включают в себя право доступа к информации, затрагивающей права, свободы и обязанности человека и гражданина; право на тайну частной жизни (ст. 23, 24), тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23); право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29); свободу слова (ст. 29).

В Конституции Азербайджанской Республики 12 ноября 1995 г. также закреплено положение о свободе слова, мысли и информации, право каждого гражданина на получение и распространение информации.

Конституции по своему содержанию также определяют ряд ограничений и запретов, связанных с информационными отношениями в целях правовой защиты ряда немаловажных институтов, таких как безопасность государства, оборона государства, личные права и интересы граждан, здоровье, государственный строй и др.

Кроме Основного Закона информационные отношения внутри государств – участников СНГ регулируются рядом актуальных документов: концепциями, программами, декретами и другими нормативными правовыми актами, тем самым предотвращая компьютерную преступность. Как указывают Ю.В. Полковниченко, Т.Г. Чудиловская в науч-

ной статье «Правовое регулирование в области информационных отношений в области информационной безопасности», правовое регулирование в области информационных отношений в Республике Беларусь осуществляется Законом Республики Беларусь «Об информации, информатизации и защите информации». Основной функцией данного 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. Важным документом, определяющим политику Республики Беларусь в сфере информационной безопасности, предотвращении компьютерной преступности является Концепция информационной безопасности Республики Беларусь от 18 марта 2019 г. В документе определены национальные интересы Республики Беларусь, внутренние и внешние источники угроз безопасности в информационной сфере, основные направления обеспечения информационной безопасности.

Следует отметить, что вопросы обеспечения информационной безопасности Азербайджана в общей форме нашли свое отражение в Концепции национальной безопасности от 23 мая 2007 г. и в Законе Азербайджанской Республики от 29 июня 2004 г. «О национальной безопасности». Политика информационной безопасности Азербайджанской Республики состоит в осуществлении комплекса мер, направленных на охрану государственных, общественных и частных информационных ресурсов, а также защиту национальных интересов в сфере информации.

Как указал А.М. Гасанов в монографии «Политика национального развития и безопасности Азербайджанской Республики»: «Проводимая в современном глобальном мире транснациональная политика в этой области создает в Азербайджане необходимость дальнейшего совершенствования правовых основ своей национальной политики информационной безопасности и повышения эффективности практической работы. По мнению экспертов, в современном мире обеспечение информационной безопасности каждой страны зависит от четкого определения приоритетов государственной информационной политики, точной, правильной, объективной, научно-теоретической оценки среды информационной безопасности и организации эффективной деятельности в этой области. Поэтому в настоящее время большое значение имеет определение и систематизация ключевых факторов, влияющих на среду информационной безопасности, и их отражение в отдельной Концепции Информационной Безопасности».

Развитие и совершенствование конституционно-правовых основ в области информационной безопасности создаст условия для обеспечения борьбы с компьютерной преступностью.