УДК 343.7

Д.И. Шнейдерова, преподаватель кафедры уголовного процесса и криминалистики учреждения образования «Могилевский институт МВД Республики Беларусь»
galuzodi@mail.ru

ХИЩЕНИЕ ЦИФРОВЫХ ВАЛЮТ КАК ВИД КИБЕРПРЕСТУПНОСТИ

Стремительное развитие информационных технологий способствует не только качественному преобразованию и упрощению жизни современного человека, но и появлению новых способов совершения хищений. Рост киберпреступности объясняется доступностью средств ее совершения (компьютеры, мобильные телефоны, сеть Интернет и др.), популярностью виртуального пространства и повышенным интересом к новым технологиям, а также сложностью и длительностью выявления и раскрытия такого вида преступлений.

К числу преступлений в сфере информационных технологий, к которым до недавнего времени относили распространение по локальным и глобальной сетям вредоносных вирусных программ и поддельных сайтов, взлом аккаунтов пользователей различных мессенджеров и социальных сетей с целью использования их личных данных в корыстных целях, завладение номерами банковских платежных карточек и др., добавился новый вид – хищение цифровых валют.

С момента вступления в законную силу Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» цифровые валюты, к которым приравнивается и криптовалюта с растущим числом ее видов, приобрели легализованный статус имущества, которые, как и любое другое имущество, могут быть отчуждены у своего владельца незаконным путем. При этом необходимо отметить, что законным владение криптовалютами будет считаться только при условии, если они были приобретены через зарегистрированные в Парке высоких технологий биржи. Однако официальная регистрация биржи и ее участников лишает их возможности оставаться анонимными, что противоречит принципам блокчейна, лежащего в основе распределительных систем, где и происходит «добывание» цифровых активов. Ввиду чего для совершения анонимных сделок пользователи выбирают в большинстве случаев любую из предлагаемых в сети Интернет распределительную базу, что лишает их средства правовой защиты.

Несмотря на вышеизложенное, риск быть обманутым и потерять внушительную часть реальных денежных средств, вложенных в цифровые валюты, присутствует в любой ситуации. Следует обратить

внимание на способы хищения криптовалют и токенов, получившие за последний год наибольшую популярность.

Большая часть криптоплатформ и бирж в качестве дополнительной защиты электронных хранилищ пользователей использует двухфазную систему безопасности, которая предполагает не только знание личного ключа, но и проверку пользователя посредством смс-оповещения с уникальным кодом для авторизации. Такая система заложила начало развития сим-свопинга, т. е. процедуры обмена сим-карт, который позволяет получить номер владельца электронного кошелька и код доступа к его цифровым валютам. Сим-свопинг включает в себя два этапа: получение логина криптокошелька и номера телефона пользователя, с последующим переводом его на новую сим-карту.

Активные пользователи социальных сетей и мессенджеров, пренебрегая безопасностью, публикуют свои персональные данные в открытом доступе в сети Интернет, привязывают аккаунты к номеру мобильного телефона, а также хранят персональные данные и пороли в файлах на различных носителях. Данное обстоятельство позволяет компетентным злоумышленникам получить необходимую информацию и использовать ее в корыстных целях, например, посредством вредоносных программ, внедряющихся на персональные устройства и копирующие личную информацию (логины, пароли, ключи и т. д.).

Второй этап сим-свопинга может вызвать затруднения, так как напрямую зависит от политики мобильного оператора. Чтобы перенести номер на новую сим-карту, прежде всего необходимо обратиться к оператору с просьбой о блокировке старой сим-карты, например, в связи с ее потерей или порчей. Следующий шаг – убедить оператора в необходимости перенести старый номер на новую сим-карту и выдать ее злоумышленнику. В данной ситуации возможно два варианта: если степень защиты данных пользователей мобильной сети низкая, то получение сим-карты возможно и без личного присутствия, например, по почте или курьером. В ином случае доступ к услугам оператора мобильной сети затруднен и возможен только через взаимодействие с недобросовестными сотрудниками компании. Используя сим-карту с номером пользователя, мошенник получает и доступ к его криптокошельку, откуда переводит на свой счет цифровые монеты и в последующем обналичивает их через любую криптобиржу на реальные деньги.

Существуют еще несколько вариантов доступа к электронным кошелькам через номер мобильного телефона. Так операторы мобильной связи предоставляют своим пользователям возможность управлять услугами через онлайн-сервис, где каждому номеру телефона отводится личный кабинет. Мошенник, получив доступ к такому кабинету, подключает услугу переадресации входящих смс-сообщений на свой

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