УДК 343.9 + 316.77 + 330

С.В. Масленченко

ЭКОНОМИЧЕСКИЕ УСЛОВИЯ РАЗВИТИЯ КИБЕРПРЕСТУПНОСТИ

В условиях информационного общества наша страна заинтересована в наращивании своего медийного и сетевого влияния в интернете, а также в защите национальных интересов в киберпространстве. Основные тенденции развития глобальной сети демонстрируют не только стремление государств, крупных компаний и отдельных пользователей к более продолжительному и интенсивному интернет-участию, но и стремление криминальных структур использовать кибертехнологии для осуществления своей противоправной деятельности.

Можно выделить ряд условий, способствующих криминализации киберпространства: политические, технологические, технические, общекультурные. Доминирующее значение среди них отводится экономике, которая выступает фундаментом объективации форм общественного сознания, «обслуживающих» ее интересы.

Активизация киберпреступности определяется следующими экономическими условиями:

1. Рост интернет-аудитории, активно пользующейся сетевыми возможностями интернет-коммерции. К началу 2014 г. интернетом пользовалось более 2,8 млрд человек, из них 45,1 % проживали в Азии, 20,2 % – в Европе, 10,7 % – в Северной Америке, 10,8 % – в Южной Америке, 8,6 % – в Африке, 3,7 % – на Ближнем Востоке, 0,9 % – в Океании и Австралии. В 2014 г. по данным Белстата количество интернет-абонентов в стране составило 8,4 млн человек, а число подключенных устройств – 9,4 млн. Однако число активных пользователей значительно меньше.

2. Рост e-commerce. Мировой объем доходов в интернете за 2013 г. превысил 500 млрд USD, лидерами являются: США – 264 млрд USD, Китай – 193 млрд USD, Германия – 52 млрд USD, Россия – 17 млрд USD, Бразилия – 12 млрд USD. По итогам 2013 г. наша страна опередила традиционных лидеров по экспорту компьютерных услуг на душу населения (Беларусь – 60 USD, Индия – 41 USD, США – 36 USD), что составило в общем объеме 480 млн USD. Среди стран Таможенного союза только Беларусь имеет положительное сальдо компьютерных услуг, причем на протяжении последних пяти лет страна постоянно увеличивает этот показатель. Так, в 2009 г. сальдо равнялось 121,5 млн USD, в 2010 – 172,1 млн USD, в 2011 – 227,6 млн USD, в 2012 – 352,1 млн USD, в 2013 – 480 млн USD.

3. Виртуализация денежных средств. С появлением электронных денег как денежных обязательств эмитента в электронном виде, которые находятся на электронном носителе в распоряжении пользователя и соответствуют трем критериям (фиксируются и хранятся на электронном носителе; выпускаются эмитентом при получении от иных лиц денежных средств в объеме, не меньшем, чем эмитированная денежная стоимость; принимаются как средство платежа другими (помимо эмитента) организациями»), не остановило процесс виртуализации offline-денег. Начало XXI в. стало временем актуализации виртуальных денег как одного из видов нерегулируемых государством цифровых денег, которые создаются и контролируются обычно разработчиками, принимаются среди членов определенного виртуального сообщества. Как правило, виртуальные валюты обладают ценностью только внутри и для определенных интернет-сообществ.

В 2009 г. происходит важное событие. В процессах виртуализации денег появляется криптовалюта bitcoin, во многом задавшая направление дальнейшего развития остальных криптовалют, – пиринговая система электронной наличности, использующая одноименную цифровую валюту. Bitcoin могут использовать для оплаты товаров или услуг у продавцов, готовых их принимать. Есть возможность обмена на обычные деньги через специализированные площадки для торгов или обменники. Одна из особенностей – эмиссия новых bitcoin, которая децентрализована, лимитирована по объему и времени, распределяется относительно случайно среди желающих, использующих вычислительные мощности своего оборудования для защиты платежной системы методом proof-of-work от повторного расходования средств.

4. Виртуализация товаров. В условиях развития игровой онлайн-индустрии происходит формирование отдельного класса объектов нематериального характера, которые пользуются спросом со стороны интернет-пользователей и геймеров: игровые очки, улучшения и другие опции, средства брендинга в социальных сетях, особые подарки в онлайн-сообществах и т. д.

Внутренняя стратификация интернет-сообществ в последние 10 лет привела к появлению ряда «специализаций» в среде хакеров: кардеры, фрикиры, спамеры, шпионы и т. д. Совершенствование технических и технологических навыков и определенные маркетинговые умения позволили представителям данного сообщества получать прибыли, не занимаясь своим непосредственным ремеслом – «хакингом»: создание фишинговых страниц, продажа «вирусов» на заказ, криптографических программ сегодня находят своего покупателя среди тех интернет-пользователей, которые приняли решение получить выгоды в киберпространстве незаконным путем.

Согласно отчету Лаборатории Касперского (лето 2014 г.) доходы киберпреступников могут более чем в 20 раз превышать их затраты на организацию атак. В качестве показательных моделей реализации противоправных устремлений можно отметить:

1. Создание в популярной социальной сети фишинговой страницы для заманивания доверчивых пользователей на мошеннический сайт и организация спам-рассылки с упоминанием этого сайта-подделки обходятся мошенникам сегодня в среднем в 150 долларов. Если же на их удочку «клюнут» хотя бы 100 человек, то злоумышленники смогут заработать до 10 тыс. USD, продав похищенные таким образом конфиденциальные данные пользователей.

2. Программа-троянец, блокирующая экран устройства, обойдется примерно в 1 тыс. USD – цена, которую злоумышленники запрашивают со своей жертвы. Таким образом, со 100 пострадавших можно получить до 20 тыс. USD.

3. Стоимость программ, шифрующих данные пользователей, составляет на черном рынке около 2 тыс. USD. В этом случае, как правило, объектами атак становятся корпоративные сети доходных компаний. Запрашиваемая разблокировка содержимого, особенно информации, касающейся текущих сделок, в разы превышает расходы хакеров.

3. Наибольшую же доходность мошенникам обеспечивает применение банковских троянцев, которые «охотятся» напрямую за деньгами пользователей. Потратив около 3 тыс. USD на приобретение вируса в комплекте с эксплойтом (исполняемой программой для его внедрения) и специально организованной для этого спам-рассылкой, киберпреступники имеют шанс получить до 72 тыс. USD от 100 успешных атак.

При этом для потенциальных киберпреступников не составляет труда отыскать требуемый криминальный инструмент на многочисленных форумах и сайтах хакеров, а его относительная дешевизна и высокая доходность выступают предпосылками роста аудитории, подумывающей о совершении киберпреступления.

Очевидно, что цивилизационные тренды в глобальной экономике, а также внутрисистемные изменения в стратегиях поведения и ценностном комплексе среди интернет-пользователей выступают одной из предпосылок актуализации криминальной активности в киберпространстве.

Кроме того, вследствие взятого нашим государством курса на активное развитие коммуникационной сферы, расширения присутствия Беларуси в мировом информационном пространстве, увеличения скорости и доли участия граждан в интернете национальные интересы неизбежно будут испытывать на себе возрастающее давление как внутренних, так и внешних рисков, вызовов и угроз в области кибербезо-

пасности. В целях защиты национальных интересов уже сегодня необходимо осуществлять мероприятия по мониторингу происходящих трендов и трансформаций, готовить правовую базу и создавать учреждения, призванные минимизировать потенциальные негативные процессы в киберпространстве, а в перспективе функционирующие на профилактику и упреждение киберпреступности.

УДК 340.15

Н.В. Мисаревич

ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА БЕЛОРУССКИХ ЗЕМЛЯХ: ИСТОРИЧЕСКИЙ АСПЕКТ

Экономическая безопасность рассматривается как один из элементов национальной безопасности любого государства. Только в условиях экономической безопасности страна может в полной мере реализовать свои национальные интересы и сохранить государственный суверенитет и территориальную целостность.

Конституция Республики Беларусь устанавливает, что государство осуществляет регулирование экономической деятельности в интересах человека и общества (ст. 13). Элементом стратегических интересов безопасности государства является создание системы гибкого регулирования рыночной экономики.

Следует отметить, что экономическая безопасность всегда находилась в центре внимания государства. Достаточно интересным представляется период XIV–XVII вв., когда белорусские города получали привилеи на самоуправление, в которых среди прочего содержались положения, направленные на обеспечение реальных условий для экономического развития города. Рассмотрим следующие моменты, исследовав их через призму современных подходов к государственному регулированию экономических процессов.

Общенормативное регулирование экономической жизни. Общим правилом получения экономической самостоятельности города было получение привилея за подписью главы государства. Причем в преамбуле привилея в качестве главной цели указывался именно экономический приоритет. В акте Минску 1499 г. говорилось: «Иж маючы взгляд посполитого доброго розмноженья и хотечи положенье места нашого Менского в мере лепшое поставити, абы люди наши там мешкаючыи, через врад добрый а справедлівый былі размножены...». В привилее