УДК 517.5:004.021

Влияние цифровой экономики на киберпреступность

В. В. Бондаренко
Донецкий национальный технический университет
vadimbond.2000@gmail.com

Аннотация.
В статье анализируются подходы к определению понятия «цифровая экономика», исследуется ее взаимосвязь с развитием преступности в киберпространстве. На основе статистических данных автором изложен ряд уголовно-правовых деяний с использованием ИКТ, которые являются доминирующими и, соответственно, приобрели особую актуальность в настоящее время. Также раскрывается механизм совершения некоторых из них. Предложен комплекс мер, направленных на эффективное противодействие кибепреступности.

Введение в цифровую экономику

«Те страны, которые первыми войдут в информационное общество, приобретут величайшие преимущества: они будут определять условия для тех, кто будет следовать за ними»: - Мартин Бангеманн.

В настоящее время, проблема становления и развития цифровой экономики является актуальной не только в теоретической, но и в практической плоскости, в том числе и на государственном уровне, в связи с пониманием решающей роли цифровых технологий в становлении стратегической конкурентоспособности страны.

Интерес к цифровой экономике обусловлен тем, что исследования ученых, международных организаций, показывают, что информационные технологии приобретают всё большую важность в экономическом развитии всех стран мира без исключения.

Цифровая экономика — понятие многогранное. Существует немало подходов к содержанию данной дефиниции.

По мнению А. Энговатовой - это экономика, основанная на новых методах генерирования, обработки, хранения, передачи данных, а также цифровых компьютерных технологиях [1].

Интересна и точка зрения Юдиной Т. Н., которая раскрывает цифровую экономику как результат трансформационных эффектов новых технологий общего назначения в области информации и коммуникации, которые влияют на все секторы экономики и социальной деятельности [2].

Исследовательский центр журнала Economist и компания IBM отметили важную характеристику такой экономики — способность предоставить высококачественную ИКТ-инфраструктуру и мобилизовать возможности ИКТ на благо потребителей, бизнеса и государства.

Приведенные точки зрения отражают, что такая экономика всегда тесно сопряжена с научными достижениями и уровнем развития информационной инфраструктуры, так как их возможности используются во всех сферах жизни общества.

Киберпреступность

Как следствие, одной из современных тенденций развития мировой экономики является активизация экономической преступной деятельности, но не в традиционном её понимании. Процесс глобализации, помимо многих положительных тенденций, имеет и ряд негативных черт. Экономическая преступность превратилась в одну из наиболее важных проблем, стоящих перед обществом, оказывая деструктивное воздействие как на экономику отдельных государств, так и на развитие мировой экономики. В её состав входит самая прогрессивная, динамичная и научно подкованная разновидность преступности — киберпреступность, ставшая негативным последствием развития информационных технологий. Компьютеры и телекоммуникационные системы, Всемирная сеть Интернет, ставшие неотъемлемыми атрибутами жизнедеятельности современного человека, сформировали новую разновидность экономической преступности.

Киберпреступность — это следствие глобализации информационно-коммуникационных технологий и появления международных компьютерных сетей [3]. Стоит отметить, что любые информационные и технические новшества значительно расширяют сферу киберпреступности и создают условия для повышения эффективности её осуществления.

Такие новации изучаются и модернизируются под определенный вид преступной деятельности, что непременно ведет к усложнению расследования таких дел, ввиду необходимости своевременного правового и технического реагирования со стороны государства на подобные деяния.

Важно отметить, что киберпреступления относительно ненаказуемы и при их высокой доходности считаются привлекательным видом деятельности. Такие преступления зачастую носят трансграничный характер, что дает возможность для совершения хищений и обналичивания денег в диаметрально противоположных местах. Очевидность преступных действий не всегда явная, ибо они могут быть абсолютно скрытными, и пострадавшая сторона узнает об этом через длительный промежуток времени. Благодаря предварительно внедренному программному обеспечению, преступники могут использовать при осуществлении своих действий внушительное количество компьютеров. Определение места нахождения преступника, факт совершения преступных действий, сбор доказательственной базы являются затруднительными для правоохранительных органов, осуществления ими процессуальных действий.

В 2018 году за период с января по декабрь 2018 г. зарегистрировано 174674 преступлений с использованием компьютерных и телекоммуникационных технологий, а выявлено лишь 43362 [4]. Статистика свидетельствует о низкой раскрываемости, ввиду технической сложности таких деяний.

Активное внедрение информационных и телекоммуникационных технологий в экономику обострило проблемы охраны персональных данных, коммерческой, корпоративной и банковской тайны. В структуре преступлений экономической направленности значительно превалируют деяния в финансово-кредитной сфере.

Банковские кражи

Group-IB, международная компания, специализирующейся на предотвращении кибератак, проанализировала высокотехнологичные преступления 2018 года, к реагированию на которые привлекались ее эксперты-киберкриминалисты.

По данным исследования, основная масса хакерских атак пришлась на финансовый сектор, при этом 74 % банков оказались не готовы к кибератакам, у 29 % были обнаружены активные заражения вредоносными программами, а в 52 % случаев выявлены следы совершения атак в прошлом. По данным исследования Group-IB, на банки пришлось порядка 70 % хакерской активности в прошлом году. Схемы для обналичивания денежных средств хакерами остались прежними: через заранее открытые банковские карты, счета юридических фирм-однодневок, платежные системы, банкоматы и сим-карты. При этом скорость обналичивания выросла в несколько раз: если 3 года назад вывод суммы в 200 млн руб., в среднем, занимал около 25–30 часов, то в 2018-м году компания столкнулась с прецедентом, когда такая же сумма была обналичена менее чем за 15 минут единовременно, в разных городах России [5].

Банк, чья инфраструктура оказалась взломанной, может не просто потерять денежные средства, но и стать угрозой для других участников финансового рынка. Получив контроль над системами банка, преступники заинтересованы не только в выводе денег из него, но и в заражении максимального количества новых жертв. Для этой цели запускается «принцип домино» — вредоносная рассылка идет по спискам компаний-партнеров банка. Такой вектор опасен, прежде всего тем, что письма отправляются из реального банка, то есть отправитель не подделан, а это повышает вероятность их открытия в банке-партнере и пополнения числа жертв.

Главной тенденцией того года стало, что грань между киберпреступлениями и другими видами преступной деятельности постепенно размывается. Большая часть инцидентов связана не непосредственно с кражей денег, а только с похищением различной информации, что свидетельствует о том, что взлом компьютерных систем может являться лишь подготовительным этапом в будущих крупных мошеннических схемах или инструментом в кибервойне. Украденные сведения могут быть использованы как против частных лиц, к примеру, для оформления кредитов на чужое имя, получения бесплатных медицинских услуг или дорогостоящих медикаментов, так и против организаций и даже государств — например, с целью присвоения чужих технологий и разработок.

В докладе от Positive Technologies, международная компания, специализирующаяся на разработке программного обеспечения в области информационной безопасности, отмечается, что растет доля атак, направленных на кражу информации. Злоумышленники похищают преимущественно персональные данные (30 %), учетные данные (24 %) и данные платежных карт (14 %). Кроме банковской сферы, внимание преступников привлекли медицинские учреждения в США и Европе: по количеству атак они опередили даже финансовые организации. Хакеров интересует как медицинская информация, так и возможность получить выкуп за восстановление

работоспособности компьютерных систем: медучреждения легче соглашаются заплатить хакерам, поскольку от этого могут зависеть жизнь и здоровье людей. Например, из-за действий хакеров была парализована работа компьютерных систем в американской больнице Hancock Regional, руководство которой решило заплатить вымогателям 55 тысяч долларов) [6].

Схема кражи с банковских карт

Нет оснований отрицать, что электронными средствами платежа, в том числе и платежными картами, сейчас пользуются огромное количество человек по всей планете, и теоретически каждый из них может стать жертвой мошенников. Ведь с появлением пластиковых карт появились и специальные устройства, с помощью которых стало возможным получение наличных денег без траты времени на очереди в кассу банка — это банкоматы. При помощи соответствующих идентификаторов определяется ее держатель карты, а при совершении покупок или снятия денег в банкомате деньги списываются со счета держателя карты. Чтобы мошенникам получить доступ к банковскому счету потерпевшего и завладеть его денежными средствами, необходимо получить реквизиты его банковской карты.

С целью получения доступа к идентификаторам, закрепленным на карте, были придуманы специальные считывающие устройства «скиммеры», которые устанавливаются на банкоматы, а способ совершения кражи денег при их помощи получил название «скимминг». Эти устройства устанавливаются перед гнездом, куда вставляется банковская карта, и считывают информацию с магнитной полосы, а также защитного кода на оборотной стороне карты. Также злоумышленникам необходимо завладеть и пин-кодом, который держатель карты вводит перед осуществлением банковских операций с целью идентификации своей личности как держателя карты. Для кражи пин-кода обычно используется маленькая видео камера, которая крепится к банкомату и снимает, как ничего не подозревающие люди, вводя пин-код, дают злоумышленникам ключ от своего счета в банке. После получение всех необходимых данных карты изготавливается ее дубликат, и злоумышленники снимают деньги жертвы в банкомате.

Интернет-банкинг

Тем не менее, с развитием сети Интернет и для удобства предоставления банковских услуг клиентам стал широко применяться интернет-банкинг. Интернет-банкинг — это общее название технологий дистанционного банковского обслуживания, а также доступ к счетам и операциям (по ним), предоставляющийся в любое время и с любого компьютера, имеющего доступ в интернет. Для того чтобы получить доступ к дистанционному банковскому обслуживанию посредством интернет-банкинга, пользователю необходимо идентифицировать себя при помощи логина и пароля. Для завладения конфиденциальными данными пользователя мошенниками используется «фишинг», который широко распространен для кражи логинов и паролей от аккаунтов страниц в социальных сетях, аккаунтов электронной почты и т. д. В нашем случае происходит создание сайта, внешне неотличимого от настоящего сайта банка. При попадании на фальшивый сайт ничего не подразумевающий пользователь вводит свой логин и пароль в предусмотренные для этого поля, после чего мошенники получают доступ к конфиденциальной информации пользователя и, соответственно, — к его счетам.

Заключение

Усовершенствование технологических разработок, связанных с расширением информационных технологий и автоматизацией деятельности во многих сферах жизнедеятельности, в том числе финансово-кредитной сфере, имеет, несомненно, приоритетное значение. С другой стороны, прогресс в IT-технологиях повлек за собой умышленное злоупотребление этими технологическими достижениями, создавая целый ряд проблем и рисков для отдельных лиц и групп, стран, а также для мирового общества в целом.

Исходя из этого, полагаем, что необходима реализация комплекса мер, направленных на эффективное противодействие кибепреступности, среди которых позволительно выделить следующие:

Основываясь на обобщении и учете зарубежного опыта стран с развитой цифровой экономикой в сфере противодействия преступности, дальнейшая разработка и внесение изменений в законодательство, регламентирующее виды санкций за неправомерное поведение в киберпространстве;

Техническая поддержка правоохранительных органов, включая регулярное обновление программного обеспечения, криминалистической техники, увеличение числа экспертов в органах безопасности и специализированных подразделениях, занимающихся противодействием киберпреступности;

Принятие мер по усилению межведомственного сотрудничества между

различными структурами информационных технологий для предотвращения риска возникновения кибератак. Сотрудничество должно быть не только на уровне национальной безопасности, но также с международными органами безопасности;

Повышение уровня осведомленности общественности о необходимости надлежащего использования ресурсов в информационных технологиях в связи с киберпреступлениями.

Литература

1. Newsru.com — новостной портал. URL: https://www.newsru.com/russia.

2. Мещеряков, Р. В. Криптографические протоколы в системах с ограниченными ресурсами / Р. В. Мещеряков [и др.] // Вычислительные технологии, 2007. - № 12.1. - С. 51–61.

3. Юдина Т. Н. Осмысление цифровой экономики / Т. Н. Юдина // Теоретическая экономика, 2016. — № 3. — С. 12–16.

4. Incident Response: итоги года: https://www.group-ib.ru/blog/incident.

5. Positive Technologies: Актуальные угрозы, 2018. - URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-rus.pdf

6. https://cyberleninka.ru/article/v/kibermoshennichestvo-harakteristika-priemy-i-metody-ego-sovershenіya.

Бондаренко В. В. Влияние цифровой экономики на киберпреступность. *В статье анализируются подходы к определению понятия «цифровая экономика», исследуется ее взаимосвязь с развитием преступности в киберпространстве. На основе статистических данных автором изложен ряд уголовно-правовых деяний с использованием ИКТ, которые являются доминирующими и, соответственно, приобрели особую актуальность в настоящее время. Также раскрывается механизм совершения некоторых из них. Предложен комплекс мер, направленных на эффективное противодействие кибепреступности.*

Ключевые слова: *цифровая экономика, информация, компьютер, надежность, киберперступления.*

Bondarenko V. The impact of the digital economy on cybercrime. *The article analyzes approaches to the definition of the concept of "digital economy", examines its relationship with the development of crime in cyberspace. Based on statistical data, the author presents a number of criminal acts using ICT, which are dominant and, accordingly, have acquired particular relevance at the present time. The mechanism of committing some of them is also revealed. A set of measures aimed at effectively countering cybercrime is proposed.*

Keywords: *digital economy, information, computer, reliability, cybercrime.*

Статья поступила в редакцию 12.05.2022
Рекомендована к публикации профессором Федяевым О. И.