Григорий Русланович БОРТЭ[1]
Сергей Антонович ОХРИМЕНКО[2]
Николай Витальевич ЖУРАВЛЕВ[3]
Елена Юрьевна БАЖЕНОВА[4]
Сергей Витальевич БАЖЕНОВ[5]

ТЕНЕВАЯ ЦИФРОВАЯ ЭКОНОМИКА

В условиях бурного развития цифровой и индустриальной революции недостаточно внимания уделяется вопросам формирования негативных тенденций информационного общества. Особая роль в этих негативных процессах принадлежит теневой экономике. В работе представлены результаты исследований по определению категории «теневая цифровая экономика». Обсуждаются возможные определения и наполнения теневой цифровой экономики (ТЦЭ), структура основных сегментов компонент вычислительно-коммуникационной техники и программного обеспечения. Исследуются связи теневой цифровой экономики и криминальной деятельности - киберкриминала. Определена основа ТЦЭ, которую составляет теневая предпринимательская деятельность, общими чертами являются такие, как скрытый, латентный (тайный) характер, охват всех фаз процесса общественного воспроизводства (производство, распределение, обмен и потребление) и паразитический характер всех процессов.

Ключевые слова: *цифровая экономика, теневая цифровая экономика; информационная безопасность, угрозы информационной безопасности; киберкриминал*

УДК*: 330.101.541*

Grigori BORTA[6]
Serghei OHRIMENCO[7]
Nikolay ZHURAVLEV[8]
Elena BAZHENOVA[9]
Sergey BAZHENOV[10]

SHADOW DIGITAL ECONOMY

Insufficient attention is paid to the formation of negative trends in the information society in the context of the rapid development of the digital and industrial revolution. A special role in these negative processes belongs to the shadow economy. The paper presents

[1] Молдавская Экономическая Академия (Кишинёв, Республика Молдова)
[2] Молдавская Экономическая Академия (Кишинёв, Республика Молдова)
[3] Представительство Россотрудничества в Республике Молдова (Кишинёв, Республика Молдова)
[4] Южный федеральный университет (Ростов-на-Дону, Россия)
[5] Science Horizons Foundation (Москва, Россия)
[6] Laboratory of Information Security, Academy of Economic Studies of Moldova (Chisinau, Republic of Moldova)
[7] Laboratory of Information Security, Academy of Economic Studies of Moldova (Chisinau, Republic of Moldova)
[8] Representative Office of Rossotrudnichestvo in Republic of Moldova (Chisinau, Republic of Moldova)
[9] Southern Federal University (Rostov-on-Don, Russia)
[10] Science Horizons Foundation (Moscow, Russia)

the results of research on the definition of the category "shadow digital economy". Possible definitions and content of the shadow digital economy (SDE), the structure of the main segments of the components of computing and communication technology and software are discussed. The links between the shadow digital economy and criminal activity - cybercrime - are investigated. The basis of the SDE, which is the shadow entrepreneurial activity, has been determined; common features are such as a hidden, latent (secret) nature, coverage of all phases of the process of social reproduction (production, distribution, exchange and consumption) and the parasitic nature of all processes.

***Keywords**: digital economy, shadow digital economy; information security, threats to information security; cybercriminal*

***UDC**: 330.101.541*

Теневая экономика, возникшая во времена становления товарно-денежных отношений, и по сей день остаётся одной из самых актуальных тем для научных исследований в развитых и развивающихся странах *(Dallago, 1991; Gutmann, 1977; Hart, 1973).* Периодически объявляемые меры и мероприятия по борьбе с теневой экономикой не дают, к сожалению, действенных результатов.

В основе любой деятельности человека лежит информация, характеризующая многие стороны творческих, производственных и сбытовых процессов. Именно поэтому с широким внедрением в жизнь общества новейших информационных технологий зародилась новая отрасль знаний – *теневая цифровая экономика* (ТЦЭ), которая объединяет деятельность по продвижению продуктов и услуг криминальной направленности. Она представляет собой специфическую сферу экономической деятельности с присущими ей структурой и системой экономических отношений. Специфичность задаётся нелегальностью, неофициальностью, а также криминальным характером экономической деятельности и сокрытием доходов.

С экономической точки зрения ТЦЭ — это сектор экономических отношений, охватывающих все виды производственно-хозяйственной деятельности, которые по своей направленности, содержанию, характеру и форме противоречат требованиям существующего законодательства и осуществляются вопреки государственному регулированию экономики и в обход контроля над ней.

С технологической точки зрения — это индивидуальная и коллективная деятельность, являющаяся незаконной, связанная с

проектированием, разработкой, распространением, поддержкой и использованием компонент информационных и коммуникационных технологий, скрываемая от общества.

Мы предлагаем определять теневую цифровую экономику следующим образом. Теневая цифровая экономика — это все незаконные и скрываемые продукты и услуги, использующие и основывающиеся на информационных технологиях. В качестве наиболее важных экономических элементов данной сферы выделяются следующие: незаконные экономические взаимоотношения, незаконная деятельность, связанная с производством, распространением и использованием запрещённых продуктов и услуг *(Borta, 2015; Бортэ, 2012b, 2012a; Охрименко & Бортэ, 2018, 2019)*.

Авторы известной и популярной книги «*Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок*» отмечают, что общество само по себе быстро и непрерывно меняется.

«*Цифровые технологии и онлайн-вычисления находятся в эпицентре этих изменений, преобразуя принципы организации общества, общественных отношений и деловых связей, ведь все стороны нашей жизни все больше и больше зависят от мощности компьютеров и сетевых коммуникаций*» *(Кейси & Винья, 2015).*

В докладе «Цифровые дивиденды» группы Всемирного Банка за 2016 год указывается:

«*Нынешнее расширение доступа к цифровым технологиям несёт многим людям богатство выбора и большие удобства. За счёт усиления социальной интеграции, повышения эффективности и внедрения инноваций такой доступ открывает бедным и обездоленным слоям населения возможности, которых они прежде были лишены*».

И с этим нельзя не согласиться. Но любая монета или медаль имеет и оборотную сторону. Кроме явных и понятных достижений необходимо анализировать явные и скрытые угрозы, которые несут

процессы цифровизации личности, обществу и государству *(Всемирный банк, 2016).*

22 января 2020 года Генеральный секретарь ООН Антониу Гутерриш назвал «четырьмя всадниками Апокалипсиса» главные угрозы человечеству: геостратегическую напряжённость, изменение климата, рост недоверия на глобальном уровне и опасность новых технологий («Обратная сторона» цифровой революции). По словам Генерального секретаря, новые технологии развиваются настолько быстро, что мы не успеваем не только отреагировать на них, но порой даже понять их суть. При том, что они сулят огромные преимущества, цифровые технологии и искусственный интеллект становятся инструментом подстрекательства, распространения ложной информации, вмешательства в частную жизнь, эксплуатации людей и совершения преступлений.

Так, он считает неприемлемым использование боевых автономных систем – «*машин, способных убивать без всякого участия человека и не несущих никакой ответственности», и призывает запретить применение «роботов-убийц*».

Гутерриш настоятельно рекомендовал навести порядок и в киберпространстве, которое он назвал цифровым «Диким западом».

«*Террористы, поборники чистоты белой расы и другие им подобные злоупотребляют интернетом и социальными сетями, - отметил глава ООН. – Боты распространяют дезинформацию, подталкивают к поляризации и подрывают демократию. В следующем году киберпреступность обойдётся нам в 6 триллионов долларов*» *(Новости ООН).*

Ещё один фронт борьбы с издержками новых технологий – это рынок труда, где, как предсказывает Гутерриш, автоматика в ближайшее десятилетие лишит работы сотни миллионов трудящихся. Он видит выход в реформе системы образования, задачей которой будет научить людей учиться в течение всей жизни. По словам Генерального секретаря, ООН – это самая подходящая платформа для того, чтобы правительства, частный сектор, гражданское общество

смогли противопоставить «цифровому расколу» глобальное сотрудничество.

Актуальными остаются слова английского публициста XIX века Томаса Даннинга, повторенные К. Марксом в «Капитале»:

«*Капитал ... избегает шума и брани и отличается боязливой натурой. Это правда, но это ещё не вся правда. Капитал боится отсутствия прибыли или слишком маленькой прибыли, как природа боится пустоты. Но раз имеется в наличии достаточная прибыль, капитал становится смелым. Обеспечьте 10 %, и капитал согласен на всякое применение, при 20 % он становится оживлённым, при 50 % положительно готов сломать себе голову, при 100 % он попирает все человеческие законы, при 300 % нет такого преступления, на которое он не рискнул бы, хотя бы под страхом виселицы. Если шум и брань приносят прибыль, капитал станет способствовать тому и другому. Доказательство: контрабанда и торговля рабами*».

В настоящее время наиболее актуальными угрозами признаны следующие:

Раскрытие персональных данных.

Социально-опасный контент (кибербулинг, призывы к суициду).

Вмешательство в выборы, атаки на электронные системы голосования и обработки информации.

Атаки на устройства интернета вещей (промышленный интернет).

Атаки на электронные системы, которые обслуживают физическую инфраструктуру поставок различных товаров.

Кибератаки входят в десятку основных глобальных рисков с точки зрения вероятности и воздействия. Эта обеспокоенность не нова и не удивительна, учитывая анонимность, которую кибератаки предоставляют как преступникам, так и жертвам *(World Economic Forum, 2019).*

В Отчёте за 2020 г. в материалах Всемирного экономического форума рассматриваются последствия цифровой сегментации. В то

время как цифровые технологии приносят огромные экономические и социальные выгоды большей части населения мира, такие проблемы, как неравный доступ к Интернету, отсутствие глобальной системы управления технологиями и небезопасность киберпространства - все это создаёт значительный риск. «Отказ информационной инфраструктуры» - шестой по значимости риск до 2030 года *(World Economic Forum, 2020).*

Основу ТЦЭ составляет теневая предпринимательская деятельность, общими чертами которой являются:

скрытый, латентный (тайный) характер, то есть та деятельность, которая не регистрируется государственными органами и не находит отражение в официальной отчётности;

охват всех фаз процесса общественного воспроизводства (производство, распределение, обмен и потребление);

паразитический характер всех процессов, от раскрытия исходного кода программного продукта до монетизации сдачи в аренду бот-нетов.

Как отмечает известный специалист по информационной безопасности А. Лукацкий:

«*Мы отмечаем переход киберпреступности на качественно новый уровень, заключающийся в превращении теневого рынка киберкриминала в хорошо отлаженную индустрию, которая полностью повторяет законы мира обычного. Своя разработка, своя поддержка, возврат средств в случае недовольства купленным товаром, сдача в аренду технологий и оборудования, услуги посредников, неотслеживаемые платёжные системы расчётов, партнёрские программы, обналичивание денежных средств и многое другое. Не случайно появляется термин Crime-as-a-Service, означающий превращение рынка киберпреступности в хорошо налаженную машину, работающую со знаком минус*» *(Лукацкий, 2015)*

Специалисты ведущей информационной фирмы в области противостояния теневой цифровой экономике Digital Shadows определила основные категории злоумышленников, у которых есть

мотив для злоупотреблений и использования труда удалённых сотрудников *(Fuentes, 2020; Kropotov et al., 2020a, 2020b).* К ним относят:

организованная преступность: группы, занимающиеся киберпреступностью, обладают возможностями и навыками для проведения целевых атак на конечных пользователей из-за надомной работы. Использование личных устройств с меньшим количеством мер безопасности и контроля делает пользовательские приложения более привлекательными для таких операций. Доступ к корпоративным услугам и ресурсам, даже с собственных устройств конечного пользователя, делает цель более привлекательной, поскольку вероятность получения несанкционированного доступа значительно увеличивается;

мошенники: ожидается рост числа попыток мошенничества из-за вспышки COVID-19. Они, вероятно, будут особенно эффективны против сотрудников, которые не привыкли работать на личных и / или мобильных устройствах;

злонамеренные инсайдеры: те пользователи, кто не привык к удалённой работе, могут столкнуться с проблемами из-за случайного раскрытия конфиденциальных данных, ошибок при обмене файлами и т. д.;

хактивисты: фишинговые атаки будут развиваться, особенно сейчас, когда конечный пользователь более уязвим в Интернете.

Следует выделить особенности, характерные для информационной области теневой экономики.

Риск быть пойманным и наказанным за преступление, совершенное в сфере теневой информационной экономики, минимален по сравнению с «классической» теневой экономикой.

Начальный порог вхождения низок как с точки зрения материальных, так и временных затрат. Для начала работы необходимо всего лишь иметь компьютер с доступом в сеть Internet. Более того, для начального получения прибыли нет необходимости в углублённом понимании принципов работы как информационных технологий вообще, так и электронной коммерции в частности. Многие инструменты легко или свободно доступны. Интерфейсы управления

подобным инструментарием интуитивно понятны и легко осваиваемы. Персональные данные и данные кредитных карт возможно купить, не имея каких-либо технических навыков.

В информационной среде куда проще найти клиента или поставщика услуг благодаря процессу глобализации и сети интернет.

По сравнению с «классическими» денежными переводами, транзакции осуществляются намного быстрей и надёжней, могут быть совершены анонимно благодаря криптовалютам.

Информационные товары и услуги несут в себе меньшие риски по сравнению с продажей, например, оружия и наркотических веществ, при этом объем прибыли может быть сопоставим.

*Заключение***.** За последние несколько лет киберпреступность перешагнула через многие технические и программные преграды и перешла из узкоспециализированной ниши в один из наиболее значительных стратегических рисков, стоящих сегодня перед всем миром. Развитие цифровых форм мошенничества (криптовалюты и ICO, заражение вирусом-вымогателем, установка приложения на смартфон, фишинг и др.) во многом способствует развитие технического прогресса.

Отметим прогнозы относительно теневых ИТ (Shadow IT), представленные ведущими исследовательскими и консалтинговыми компаниями *(FireCompass, 2019).*

Так, по прогнозам *Gartner* к 2020 году 30% нарушений в информационной сфере будет вызвано теневыми ИТ, при этом расходы составят от 30 до 40 % всех расходов на ИТ в целом. В отчёте консалтинговой компании *Frost & Sullivan* говорится, что более 80% респондентов признают, что используют неутверждённые (теневые) приложения в своей работе. Исследования, проведённые компанией IDG, свидетельствуют, что распространение теневых ИТ ежегодно увеличивается на 5 % и составляют около 30% ИТ-бюджетов предприятий. Исследования *Everest Group* зафиксировали, что доля теневых ИТ составляет 50% и более в расходах на ИТ в целом.

Dixon & Samartsev (2019) указывают на три основные технологии, которые будут наиболее востребованными и с большой вероятностью определят достижения следующего десятилетия.

В первую очередь к ним относят, новое поколение сетей 5G, которые представляют самую сложную проблему в сфере кибербезопасности. Это объясняется тем, что критически важные приложения и инфраструктура будут запускаться почти в 1000 раз быстрее, чем сегодняшний Интернет. Это может обеспечить кибермошенникам реализацию атак в новом темпе 5G *(OECD, 2019).*

Второй основной технологией является *искусственный интеллект* (ИИ). Безусловно, ИИ призван способствовать созданию глобальной защиты общества и государства от киберугроз, однако, он уже активно используется и киберпреступным сообществом *(Brundage et al., 2018).*

Третья технология – *биометрия*, которая получила широкое применение в различных секторах экономики. Биометрия и аутентификация следующего поколения требуют больших объёмов данных о человеке. Голоса, лица, малейшие детали движения и поведенческие следы должны будут храниться в глобальном масштабе, и это заставит киберпреступников использовать новое поколение персональных данных.

Цифровая экономика несёт с собой вызовы и угрозы, которые напрямую связаны с расширением области применения цифровых технологий и распространением её на физических лиц:

снижаются возможности контроля цифровых сервисов и увеличиваются возможности для противозаконных действий;

повышаются риски утечек информации, влияния на работу оборудования;

появляются новые угрозы, связанные с взрывным ростом значимости социальных сетей в жизни общества и развитием технологии Интернета-вещей.

Считаем необходимым обратить внимание на малую изученность следующих направлений исследований: возможность реализации угроз в отношении медицинского оборудования (в частности,

применительно к кардиостимуляторам); криптомания – как социально-экономическое явление; Wetware – компьютерные технологии, интегрированные с биологическим организмом; концепция «цифровой двойник» (Digital Twin) и др.

В заключении, считаем необходимым предложить разработку целостной стратегии противодействия теневой цифровой экономике. Основополагающими принципами этой стратегии должны являться:

Совершенствование законодательной базы экономического регулирования, нацеленного на создание условий, при которых сокрытие определённых видов деятельности или их элементов, как и любая незаконная деятельность станут невыгодными.

Развитие сотрудничества на государственном, региональном и международном уровнях с целью понижения уровня теневой цифровой экономики.

Литература

Бортэ, Г. Р. (2012a). Исторические предпосылки развития теневой информационной экономики. *Системи Обробки Інформації*, *4*(102), 12–14.

Бортэ, Г. Р. (2012b). Теневая информационная экономика. *Годишен Алманах «Научни Изследвания На Докторанта». Стопанска Академия «Д.А. Ценов»*, *5*.

Всемирный банк. (2016). *Доклад о мировом развитии 2016 «Цифровые дивиденды». Обзор.*

Кейси, М., & Винья, П. (2015). *Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок*. Манн, Иванов и Фербер.

Лукацкий, А. (2015). Будущее российского рынка информационной безопасности. *Век Качества*, *2*, 58–59. https://cyberleninka.ru/article/n/buduschee-rossiyskogo-rynka-informatsionnoy-bezopasnosti

Новости ООН. (б.д.). *Глава ООН рассказал о своих приоритетах на 2020 год.* Получено из https://bit.ly/2HbLKUm

Охрименко, С. А., & Бортэ, Г. Р. (2018). Тень цифровой экономики. *Годишник На Стопанска Академия «Д.А. Ценов»*, *121*.

Охрименко, С. А., & Бортэ, Г. Р. (2019). Новое наполнение науки секьюритологии. In A. Kozera & E. Sadowska (Eds.), *Nauka i praktyka bezpieczeństwa : księga pamiątkowa Leszka Fryderyka Korzeniowskiego profesora Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie* (pp. 112–147). Wydawnictwo EAS.

Borta, G. (2015). The Dark Side of Information Economics. *Economica*, *XXIII*(2 (92)), 97–102.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., HÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., … Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. In *Workshop "Bad Actor Risks in Artificial Intelligence" (19-20 February, 2017, Oxford, United Kingdom)*. https://doi.org/10.17863/CAM.22520

Dallago, B. (1991). The «Second Economy»: A Mechanism for the Functioning of Society in Eastern Europe. *Journal of the Washington Institute for Valuesitin Public Policy*, *1*(1), 76–113.

Dixon, W., & Samartsev, D. (2019). 3 technologies that could define the next decade of cybersecurity. *Annual Meeting of the New Champions 2019 (1-3 July 2019, Dalian, People's Republic of China)*.

FireCompass. (2019). *Short guide on shadow IT: Digital footprinting, continuous monitoring &digital risk protection*. https://www.firecompass.com/wp-content/uploads/2019/05/Short-Guide-On-Shadow-IT.pdf

Fuentes, M. R. (2020). *Trading in the Dark: An Investigation into the Current Condition of Underground Markets and Cybercriminal Forums*. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/trading-in-the-dark

Gutmann, P. M. (1977). The Subterranean Economy. *Financial Analysts Journal*. https://doi.org/10.2469/faj.v33.n6.26

Hart, K. (1973). Informal income opportunities and urban employment in Ghana. *The Journal of Modern African Studies*. https://doi.org/10.1017/S0022278X00008089

Kropotov, V., McArdle, R., & Yarochkin, F. (2020a). *Commodified Cybercrime Infrastructure: Exploring the Underground Services Market for Cybercriminals*. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/commodified-cybercrime-infrastructure-exploring-the-underground-services-market-for-cybercriminals

Kropotov, V., McArdle, R., & Yarochkin, F. (2020b). *The Hacker Infrastructure and Underground Hosting: Services Used by Criminals*. https://documents.trendmicro.com/assets/white_papers/wp-the-hacker-infrastructure-and-underground-hosting-services-used-by-criminals.pdf

OECD. (2019). The road to 5G networks: Experience to date and future developments. *OECD Digital Economy Papers*, *284*. https://doi.org/10.1787/2f880843-en

World Economic Forum. (2019). *The Global Risks Report 2019 14th Edition.* Получено из https://bit.ly/3dz2Oj0

World Economic Forum. (2020). *The Global RisksReport 2020.* Получено из https://bit.ly/2ICptQ1