ТЕНЬ ЦИФРОВОЙ ЭКОНОМИКИ

Сергей Охрименко
Доктор экономических наук, профессор Лаборатория "Информационная безопасность" Молдавская Экономическая Академия

Григорий Бортэ
Докторант Лаборатория "Информационная безопасность" Молдавская Экономическая Академия

Введение

Теневая экономика, возникшая во времена становления товарно-денежных отношений, остается одной из самых злободневных тем для развитых и развивающихся стран. Периодически объявляемые меры и мероприятия по борьбе с теневой экономикой не дают, к сожалению, действенных результатов. Следует отметить, что в основе любой деятельности человека лежит информация, характеризующая многие стороны творческих, производственных и сбытовых процессов. Информация выступает в качестве объекта притязаний (вплоть до криминальных), как предмет обмена и продажи существует с давних пор (с античных времен) и роль и актуальность информации в управлении государством и обществом постоянно возрастает. Построение информационного общества привело к росту потребности в разнообразной информации, характеризующей практически все стороны деятельности личности, общества и государства. Одновременно с этими процессами отмечается рост объемов неправомерной деятельности по отношению к самой информации, процессам ее получения и передачи по каналам связи, местам сосредоточения и хранения информационных ресурсов. Другими словами, добыча информации во всех ее формах, с помощью использования различных продуктов и услуг превратилась для группы предпринимателей в высокодоходный нелегальный бизнес.

Особую актуальность данная проблема противостояния нелегальным процессам добычи, обработки и распространения разнообразной по форме и содержанию информации приобретает в условиях построения цифрового общества и цифровой экономики. Цифровая экономика - подразумевает тотальную глобализацию, создает сверхвысококонкурентную среду, развивается стремительными темпами, немыслима без квалифицированных кадров и качественного образования, убивает

многие традиционные сферы деятельности, обеспечивает новое качество жизни, бизнеса и государственных услуг, в значительной степени является виртуальной, неосязаемой. Но она невозможна без связи с материальным миром. Поэтому базой цифровой экономики является индустриальное развитие.

Основной целью данного исследования является формирование научного представления об основных тенденциях, направлениях и перспективах становления и развития теневой цифровой экономики, мирового рынка продуктов и услуг криминальной направленности в условиях глобализации. Для достижения данной цели авторами поставлены следующие задачи:

- исследовать экономическую категорию “теневая цифровая экономика”, а также факторы, оказывающие влияние на ее уровень и направления развития;
- проанализировать концептуальные подходы к исследованию теневой цифровой экономики, как составной части мирового рынка информационных и коммуникационных технологий криминальной направленности;
- исследовать структурную основу и основные сегменты данной экономической категории;
- провести сравнительный анализ сегментов теневой цифровой экономики с выделением основных функций, причин появления и перспектив “совершенствования”.

Объектом исследования является рынок программных продуктов и информационных услуг в сфере информационных и коммуникационных технологий криминальной направленности. Соответственно, предметом данного исследования является рыночный механизм функционирования мирового рынка теневой цифровой экономики.

В докладе “Цифровые дивиденды” группы Всемирного Банка за 2016 год указывается: “Нынешнее расширение доступа к цифровым технологиям несет многим людям богатство выбора и большие удобства. За счет усиления социальной интеграции, повышения эффективности и внедрения инноваций такой доступ открывает бедным и обездоленным слоям населения возможности, которых они прежде были лишены. (Всемирный банк)” 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 оцифровки личности, обществу и государству.

В коллективной монографии, посвященной рассмотрению цифровой трансформации экономики, указывается: “Новая модель форми-

руется на технологическом базисе очередной четвертой промышленной революции, связанной с оцифровкой экономики не только в области услуг, корпоративного и государственного управления, но и в собственно материальном базисе экономики, в обрабатывающей промышленности и сопряженной с ней логистической инфраструктурой. (Толкачева)" Основными драйверами цифровой трансформации являются: интернет вещей; искусственный интеллект; аналитика больших данных; нейронные сети; блокчейн; облачные вычисления; робототехника; аддитивные технологии (включая 3D-печать); виртуальная и дополненная реальность. Предусматривается внедрение оцифровки в следующих направлениях: государственное регулирование; информационная инфраструктура; исследования и разработки; кадры и образование; информационная безопасность; государственное управление; умный город; цифровое здравоохранение. Особое внимание уделяется информационной безопасности, так как изменение, например, цифрового наполнения такого явления, которым является "цифровой двойник" (digital twin) может привести к катастрофической ситуации не только в области промышленного производства. Потенциальную опасность представляют неправомерные действия по отношению к набору критических технологий, в их числе следует выделить такие, как промышленный интернет или интернет вещей, медицинское оборудование, прежде всего кардиологическое, компьютерные технологии, интегрированные с биологическими организмами и др.

Выделяют три волны цифровых технологий, каждая характеризуется технологическими достижениями и набором угроз. К первой волне относят процессы внедрения информационных и коммуникационных технологий, компьютеризацию основных сфер деятельности, автоматизацию процессов управления (в том числе внедрение и использование ERP, EDI, CRM и др), а также внедрение широкополосного доступа. Вторая волна может быть охарактеризована разработкой и внедрением онлайновых платформ, например, поисковых систем, торговых площадок, дистанционного обучения, социальных сетей. Третья волна предусматривает внедрение таких технологий, как предиктивная аналитика больших данных, промышленный интернет или интернет вещей, робототехника, аддитивные технологии (включая 3D-печать), искусственный интеллект, включая машинное обучение.

Существуют основания предполагать, что интерес к противоправной деятельности в области цифровой экономики будет стремительно нарастать и данный процесс, и действия необходимо исследовать

во всех аспектах, в первую очередь, по отношению к критическим технологиям для предотвращения серьезных последствий.

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” (Даннинг).

Можно предположить, что неправомерный бизнес (именно предпринимательская деятельность отдельных личностей и организованных групп), направленный на получение закрытой информации (например, информации составляющей государственную и, в большей степени, коммерческую тайну) приносит доходы, объем которых может значительно варьироваться и зависеть от множества факторов. Кроме того, отмечается недостаточное исследование информационной составляющей “классической” теневой экономики.

Настоящая работа в качестве главной цели ставит рассмотрение процессов и условий, являющихся основой для формирования нового направления исследований - теневой цифровой (информационной) экономики (ТЦЭ).

Материалы и методы исследования

Многие авторы связывают незаконные действия в области информационных и коммуникационных технологий, являющиеся основой ТЦЭ, с кибертерроризмом и возросшими рисками в управлении обществом (Schneider). Для формирования общей картины считаем необходимым рассмотреть статистические данные, характеризующие некоторые виды деятельности, подпадающие, по нашему мнению, под ТИЭ. В информационную базу данного исследования были положены материалы Юнеско, ООН, МВФ, отчеты таких исследовательских центров, как McAfee, Kaspersky Lab, Ernst & Young, Kroll, ESET, IBM, EuroPol, Imperva, Panda Security, Ponemon, Sophos, Symantec, Verizon, techdirt,

Websense, Bit9, Blue Coat, CyberSource, DELL SecureWorks, Detica и др. Но следует иметь в виду, что приведенные статистические данные получены путем опросов и не в полной мере характеризуют исследуемые явления. Это еще одна из нерешенных проблем, для ее решения следует разработать методологические подходы и методики измерения.

В отчете “The Global Risks Report 2018” (Weforum), который был подготовлен Мировым Экономическим Форумом, информационные угрозы вошли в рейтинг глобальных рисков. Такие угрозы, как “Кибератаки” и “Кража данных и мошенничество” вошли в пятерку высоковероятных, присутствует также угроза критическим инфраструктурам. Там же выделяются основные области рисков: экономические, геополитические, экологические, социальные и технологические. Именно в последней области сосредоточены глобальные преобразования, направленные на: информационную безопасность, информационные технологии, управление интернетом, цифровую экономику и общество, рабочую силу и занятость, будущее экономического прогресса, перспективы молодежи, поставки и транспорт, миграция, 4-ю промышленную революцию.

В глобальном плане наблюдается широкий диапазон киберпреступлений, которые включают преступления, совершаемые в целях получения финансовой выгоды, преступления, связанные с использованием информации, которая содержится в компьютере, а также преступления, направленные против конфиденциальности, целостности и доступности компьютерных систем.

Будапештская Конвенция, принятая Советом Европы 23 ноября 2001 года, как основополагающий документ в сфере борьбы с киберпреступностью, позволяет регулировать действия различных государств при осуществлении борьбы с преступлениями в интернете, предоставляет следующую классификацию киберпреступлений:

1. правонарушения против конфиденциальности, целостности и доступности компьютерных данных и систем, в частности:

a. незаконный доступ, например, путем взлома, обмана и другими средствами;

b. нелегальный перехват компьютерных данных;

c. вмешательства в данные, включая умышленно повреждение, уничтожение, ухудшение, изменение или сокрытие компьютерной информации без права на это;

d. вмешательства в систему, включая умышленное создание серьезных помех функционированию компьютерной системы, напри-

мер, путем распределенных атак на ключевую информационную инфраструктуру;

е. злоупотребления устройствами, то есть изготовление, продажа, приобретение для использования, распространения устройств, компьютерных программ, компьютерных паролей или кодов доступа с целью осуществления киберпреступлений;

2. правонарушения, связанные с компьютерами, включая подделку и мошенничество, совершенные с использованием компьютеров;

3. правонарушения, связанные с содержанием информации, в частности, детская порнография, расизм и ксенофобия;

4. правонарушения, связанные с нарушением авторских и смежных прав, например, незаконное воспроизведение и использование компьютерных программ, аудио/видео и других видов цифровой продукции, а также баз данных и книг.

В то же время, с учетом мотивации преступников, киберпреступления представляется возможным условно разделить на следующие категории:

1. кибермошенничество с целью завладения средствами;

2. кибермошенничество с целью завладения информацией (для собственного пользования или для последующей продажи);

3. вмешательства в работу информационных систем с целью получения доступа к автоматизированным системам управления (для умышленного повреждения за вознаграждение или для нанесения ущерба конкурентам);

4. другие преступления.

К сожалению, данная Конвенция не предусматривает должных мер в отношении современных киберугроз, таких как рассылка спама, сетевое мошенничество и ботнеты.

Выделяются следующие угрозы личности, обществу (eurasiangroup.org) и государству:

1. открытость общества и государства. Созданная на основе компьютерных сетей и информационных технологий удобная инфраструктура для международных поставок товаров, оказания услуг, перевода средств между физическими и юридическими лицами, хранения информации в сети Интернет и подключение к ней каждого компьютера, предоставляет одновременно широкие возможности, как собственно для киберпреступлений, так и для отмывания денег от этих или других преступлений с помощью компьютерных технологий;

2. скорость и невысокая стоимость преступления. Вышеуказанная инфраструктура также предоставляет преступникам возможность быстрого доступа к любой информации, документам и, наконец, част-

ной собственности, и одновременно к дешевым, оперативным и практически анонимным платежным системам, что позволяет быстро, без дополнительных затрат и эффективно скрыть следы преступления и дальнейшего движения незаконно полученных доходов;

3. высокая технологичность. Чрезвычайно быстрое развитие информационных технологий и сложность этой сферы, наряду с относительно длительным и бюрократическим подходом к развитию нормативно-правовых баз, приводит к значительному отставанию мероприятий по предупреждению и борьбе с киберпреступностью;

4. сложный характер преступления. Кроме того, что киберпреступники получают финансовые или другие материальные выгоды от совершения преступления, они используют компьютерные технологии, информационно-коммуникационные сети из социально-психологических соображений. В частности, для дискредитации правительств и государств, создания сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния (что является своего рода дополнением к традиционному виду терроризма);

5. анонимность преступления. Преступников привлекает отсутствие физического контакта с жертвой, относительная мягкость наказания в некоторых странах и, безусловно, сложность обнаружения, фиксации и изъятия криминалистически значимой информации в виртуальном пространстве;

6. транснациональный и популярный характер преступления. Особенностью данного вида преступности является то, что подготовка и совершение преступления, при наличии доступа к сети Интернет, может осуществляться практически с любого места. А учитывая, что компьютерная техника и Интернет-услуги становятся доступными для все более широкого круга лиц, киберпреступность становится все более популярной.

Заслуживает внимания статистика активности киберпреступников, приведенная (McAfee) в таблице 1.

Дж. Льюис приводит региональное распределение киберпреступности (Lewis) по регионам, представленным в таблице 2.

Некоторые наиболее известные компьютерные инциденты и ущерб от них приведены в таблице 3.

Таблица 1
Предполагаемая активность киберпреступности в 2017 году

Разделы киберпреступности	Оценка ежедневной активности
Вредоносные программы	80 миллиардов
Новые вредоносные программы	300000
Фишинг	33000
Программы-вымогатели	4000
Взломанные записи	780000

Таблица 2
Региональное распределение киберпреступности в 2017 году

Регионы	ВВП по регионам (трил.$)	Стоимость киберпреступлений (млрд.$)	Потери от киберпреступности (в % от ВВП)
Северная Америка	20,2	От 140 до 175	От 0,69 до 0,87
Европа и Центральная Азия	20,3	От 160 до 180	От 0,79 до 0,89
Восточная Азия и Тихий Океан	22,5	От 120 до 200	От 0,53 до 0,89
Южная Азия	22,5	От 120 до 200	От 0,53 до 0,89
Латинская Америка и Карибский бассейн	55,3	От 15 до 30	От 0,28 до 0,57
Страны Африки южнее Сахары	1,5	От 1 до 3	От 0,07 до 0,20
Ближний Восток и Северная Африка	3,1	От 2 до 5	От 0,06 до 0,80
Всего по миру	75,8	От 445 до 608	От 0,59 до 0,80

Таблица 3
Ущерб от инцидентов в области теневой цифровой экономики

Год	Инцидент	Ущерб (доллары США)
1998	Эпидемия вируса СШ	20-80 млн.
2000	Эпидемия вируса ILOVEYOU	5,5-15 млрд.
2004	Эпидемия вируса MyDoom	38 млрд.
2009	Эпидемия вируса Conficker	9,1 млрд.
2013	Эпидемия вымогательской программы CryptoLocker	28 млн.
2017	Эпидемия вымогательской программы WannaCry	До 4 млрд.
(Berr) (Garza)		

Данные, приведенные в табл. 3, характеризуют огромный ущерб от компьютерных инцидентов. Так, последние эпидемии вымогательских программ CryptoLocker и WannaCry оцениваются приблизительно в 28 млн. долларов и 4 млрд. долларов. Следует подчеркнуть, что данные о потерях являются оценочными, полученными на основе проведения опросов, и практика свидетельствует о сокрытии ущерба компьютерными фирмами, коммерческими банками и корпорациями из-за нежелания оглашать действительные размеры потерь.

В таблице 4 приведены данные о количестве поступивших сообщений о киберпреступлениях и соответствующих потерях. Эти данные собраны и обработаны Internet Crime Complaint Center (IC3) в партнерстве с ФБР и National White Collar Crime Center (NW3C) в период с 2009 по 2014 годы (Sjouwerman).

Таблица 4
Поступившие сообщения и потери за 2009-2014 г.г.

Год	Количество сообщений	Потери (млн.$)
2014	269,422	800.49
2013	262,813	781.84
2012	289,974	525.44
2011	314,246	485,25
2010	303,809	Нет данных
2009	336,655	559.70

Пик количества сообщений пришелся на 2011 г. – более 314 тыс. с потерями $485,25 млн, затем отмечается снижение до 269 тысяч. Но совершенно иная картина по потерям – с уменьшением количества сообщений потери постоянно увеличиваются и в 2014 г. достигли величины $800 млн.

В табл. 4 приведены данные, характеризующие основные типы компьютерных преступлений, совершенных в США (ic3.gov). Приведенные данные весьма впечатляют. Например, компрометация электронной почты в целях мошенничества, при относительно небольшом количестве (12005 случаев), нанесла потери в более $360 млрд. Наибольшее количество случаев компьютерных преступлений отмечается по направлению “непредставление продуктов и услуг после их оплаты” (81029 случаев) при потерях пользователей более $138 млрд.

Исследовательская компания Trend Micro представила краткое содержание и основные выводы отчета “Программы-вымогатели: прошлое, настоящее и будущее” (Trendmicro):

1. за 2016 г. количество семейств программ-вымогателей выросло на 752%;

2. средняя сумма выкупа за возвращение доступа к файлам составила 0,5-5 биткоинов;

3. киберпреступники заработали в 2016 году на программах-вымогателях более $1 млрд.

Одновременно с ростом количества используемых программ-вымогателей растет количество случаев технических и программных атак на банкоматы (АТМ) с целью завладения денежными средствами. Эту криминальную область деятельности ТЦЭ характеризуют данные, приведенные в табл. 6.

Данные табл. 6 свидетельствуют о росте количества инцидентов (22450 в 2012 году до 23588 в 2016 году). Соответственно объем потерь возрос с 265 (2012 год) до 332 (2016 год).

В 2016 году Центр Infowatch зафиксировал 213 случаев утечек информации из российских компаний и государственных органов, что на 80% больше чем в 2015 г. В девяти из десяти случаев в России утекали персональные данные (ПДн) и платежная информация, а общий объем скомпрометированных за год данных увеличился более чем в 100 раз до 128 млн. записей, но не превысил порог в 4% от мирового объема утечек информации (Infowatch).

В отчете “Актуальные киберугрозы - 2017. Тренды и прогнозы”, который подготовила известная компания Positive Technologies, рассматриваются итоги 2017 года по отношению к существующей инфраструктуре и информационному воздействию в разрезе объектов, мотивов и методов (табл.7).

Таблица 5
Основные типы компьютерных преступлений в США в 2016 году

№	Тип компьютерного преступления	Количество	Потери ($)
1	Компрометация e-mail в целях мошенничества	12,005	360,513,961
2	Мошенничество на доверии	14,546	219,807,760
3	Непредставление продуктов и услуг после их оплаты	81,029	138,228,282
4	Инвестиции на основе ложной информации	2,197	123,407,997
5	Утечка корпоративных данных	3,403	95,869,990
6	Другие преступления	12,619	73,092,101
7	Мошенничество с авансовыми платежами	15,075	60,484,573
8	Утечка личных данных	27,573	59,139,152
9	Кража личных данных	16,878	58,917,398
10	Гражданские иски	1,070	57,688,555
11	“Нигерийские” письма	25,716	56,004,836
12	Мошенничество с кредитными картами	15,895	48,187,993
13	Мошенничество с недвижимостью	12,574	47,875,765
14	Нелегальная трудовая деятельность	17,387	40,517,605
15	Фишинг, вишинг, смишинг, фарминг	19,465	31,679,451
16	Угрозы преследования и насилия	16,385	22,005,655
17	Мошенничество с лотереями	4,231	21,283,769
18	Вымогательство	17,146	15,811,837
19	Искажение информации	5,436	13,725,233
20	Выдача себя за правительственного чиновника	12,344	12,278,714
21	Отказ в обслуживании	979	11,213,566
22	Ложная техническая поддержка	10,850	7,806,416
23	Нарушение авторских прав	2,572	6,829,467
24	Вредоносное программное обеспечение	2,783	3,853,351
25	Программы “вымогатели”, лжеантивирусы	2,673	2,431,261
26	Повторная отправка товара	893	1,932,021
27	Лжеблаготворительность	437	1,660,452
28	Вирусы	1,498	1,635,321
29	Обман в области здравоохранения	369	995,659
30	Азартные игры	137	290,693
31	Терроризм	295	219,935
32	Преступления против детей	1,230	79,173
33	Хактивизм	113	55,500

Таблица 6
Статистика атак на банкоматы (ATM)

Показатели	2012	2013	2014	2015	2016
Количество инцидентов (тыс.шт.)	22450	21346	15702	18738	23588
Объем потерь (млн. евро)	265	248	280	327	332

Следует отметить, что относительно недавно появились данные, характеризующие услуги по превращению результатов криминальной деятельности лиц и групп, в “звонкую монету” (т.е. процесс монетизации) (Ablon). Характерным примером монетизации работы программы-шифровальщика Spora (программы-вымогателя - ransomware), выявленной в августе 2017 года, являются данные, приведенные в докладе Чернышенко И. на конференции “ГГ@ Security Forum”. Перечень услуг программы включает (Чернышенко):

- расшифровку всех файлов ($79);
- покупку иммунитета против будущих инфекций Spora ($50);
- удаление всех связанных со Spora файлов после оплаты выкупа ($20);
- восстановление файла ($30);
- восстановление двух файлов бесплатно.

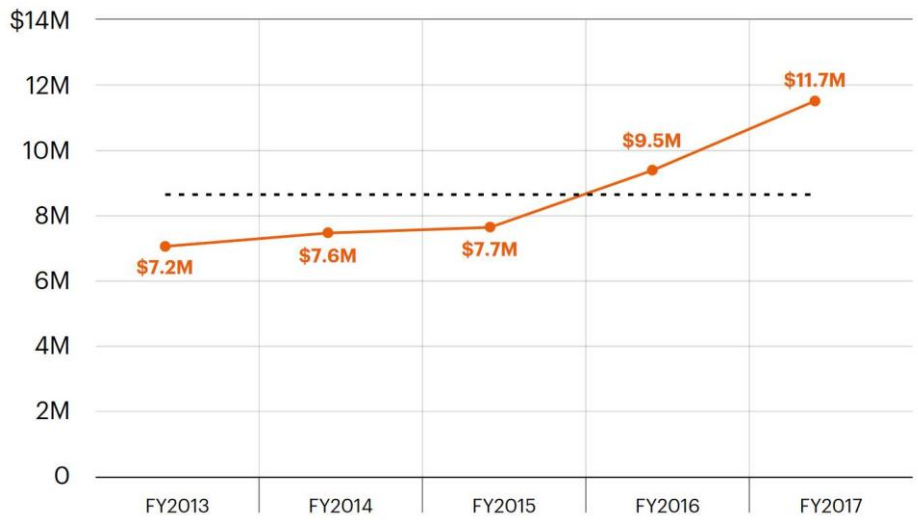
Налицо элементы криминального прайс-листа услуг по результатам деятельности программы-шифровальщика.

Таблица 7
Действия компьютерных злоумышленников в 2017 году

	Инфраструктура	**Веб-ресурсы**	**Пользователи**	**Интернет вещей**	**Мобильные устройства**	**Банкоматы и POS**	**Финансовая выгода**	**Получение данных**	**Хактивизм**	**Кибервойна**	**Вредоносное ПО**	**Уязвимости ПО**	**Учетные данные**	**Веб-уязвимости**	**DDoS**	**Соц. инженерия**	*Другое*
Гос. организации	54	34	6	4	2	-	44	34	17	5	39	20	20	19	19	9	8
Финансовая отрасль	42	32	10	-	-	16	92	8	-	-	37	8	2	9	7	12	2
Онлайн серверы	20	72	7	1	-			85	9	5	-	4	13	27	10	2	3
Мед. учреждения	56	10	34	-	-	-	69	28	3	-	16	8	13	7	1	12	4
Образование	57	17	26	-	-	-	81	17	2	-	16	9	14	8	-	9	2
Сфера услуг	42	30	7	2	6	13	70	21	9	-	17	3	14	9	2	2	6
IT-компании	53	31	5	5	3	3	84	16	-	-	15	5	4	3	4	2	5
Пром. компании	79	4	17	-	-	-	55	24	7	14	12	2	4	1	-	8	2
Розничная торговля	22	52	4	-	-	22	74	26	-	-	8	3	4	5	2	2	3
Частные лица	35	18	18	2	27	-	79	19	1	1	39	20	35	12	-	38	14
Составлено авторами на основании отчета “Актуальные киберугрозы - 2017.Тренды и прогнозы” (ptsecurity.com)																	

Отдельную недостаточно проработанную проблему представляет вопрос определения ущерба от неправомерных воздействий. Отдельные исследования рассматривают урон от воздействия программных злоупотреблений, распределенных атак и т.д. Исследователи и практические работники остро нуждаются в разработке методических основ определения и расчета всесторонних потерь.

Считаем достаточным привести характеристику глобальной средней стоимости киберпреступлений, основываясь на отчете Института Понемон за 2017 (Ponemone). Динамика средней стоимости киберпреступлений приведена на фиг. 1.



Фигура 1. Глобальный средний показатель стоимости киберпреступлений за 5 лет

Следует отметить устойчивый рост стоимости киберпреступлений, а за последний 2017 год по сравнению с 2016 прирост составил 27,4%, а в целом за 5 лет прирост составил 62%.

Считаем необходимым привести общую статистику, характеризующую компьютерный криминал в Республике Молдова. Несмотря на относительно малые размеры и неразвитость информационной инфраструктуры отмечается рост компьютерных преступлений. В 2015 году Центр по борьбе с компьютерными преступлениями Молдовы (ЦБКП) расследовал 43 случая осуществления Интернет-переводов с использованием реквизитов банковских карт, 14 случаев несанкционированного доступа к информационным системам, 6 случаев мошенничества, 42 случая осуществления развратных действий с помощью информацион-

ных технологий, 14 случаев перехвата информации и шантажа. По статистике за 2003-2015 гг. на первом месте - изготовление и подлог банковских платежных инструментов, второе - нарушение авторских и смежных прав. На долю нарушения авторских и смежных прав приходится 256 случаев за указанный период. На третьем месте - нарушение неприкосновенности личной жизни (173 случая), нарушение тайны переписки (55), детская порнография (55). Но все эти данные не отражают полной картины. Например, далеко не все коммерческие банки предоставляют информацию о том, что были попытки взлома их электронных платежных систем.

Определения теневой цифровой (информационной) экономики (ТЦЭ)

Интерес к теневым процессам, протекающим в экономике отдельных стран, возник в середине 20 столетия. Результаты отдельных разрозненных исследований привели к формированию нового научного направления в экономике, на уровне государства начали разработку программ противодействия процессам теневой экономики и вывода их из тени. Проведенные на раннем этапе исследования позволили зафиксировать уровень теневой экономики, ее структуру и, самое главное, был сделан вывод о возможности вывода результатов деятельности из тени.

В основу настоящего исследования положены работы С. Барсуковой, Ю. Латова, Р. Гиляревского, Т. Филипповой, Boehme R., Gaspareniene I., Rentrop C., Krebs C., Shneider F., Passere P., Sjouwerman S.,Korzeniowski L., Libicki M. и многие другие. Необходимо отметить работы австрийского ученого Фридриха Шнейдера, в которых отражены все аспекты проблем теневой экономики не только развитых, но и развивающихся стран.

“Теневая экономика” - это неформальная часть национальной экономики, не учитываемой официальной статистикой. Она охватывает все виды деятельности, неучтенной и незафиксированной официально, в том числе такие как:

- операции, не запрещенные законом (так называемый “серый рынок”);
- криминальная деятельность, запрещенная законом (“черный рынок”);
- внерыночная деятельность, когда продукты и услуги производятся и потребляются в домашних хозяйствах;

- бартерный обмен продуктами и услугами при условии невыхода на рынок.

Рассмотрим сегменты теневой экономики. Основными из них являются следующие:

1. Неформальная экономика (“серый рынок”) - в принципе законные экономические операции, масштаб которых скрывается или занижается хозяйствующими субъектами, как, например, трудовой наем без оформления, нерегистрируемые ремонтно-строительные работы, репетиторство, сдача в аренду недвижимости и другие способы уклонения от налогов.

2. Криминальная экономика (“черный рынок”) - экономическая деятельность, запрещённая законом в любой экономической системе и в подавляющем большинстве стран: наркобизнес, контрабанда, проституция, рэкет и др.

3. Фиктивная экономика - предоставление взяток, индивидуальных льгот и субсидий на основе организованных коррупционных связей.

Наряду с определением “теневая” экономика очень часто используются и другие, такие как “подпольная”, “неосязаемая”, “параллельная”, “серая”, “черная”, “криминальная” экономика.

Считаем важным отметить, что некоторые из этих определений ссылаются на отдельные аспекты теневой экономики, покрывают один из определенных её сегментов. Правда, большинство из этих определений охватывают явление целиком. Например, “серая”, “подпольная”, “теневая”, “параллельная” в основном указывают на целостное явление, в то время как определения “черная” и “криминальная” - ссылаются лишь на его отдельные, более узкие участки незаконной деятельности.

Представим структуру “классической” теневой экономики.

Во-первых, криминальная экономика - “встроенная” в официальную экономику экономическая преступность (хищения, корыстные должностные и хозяйственные преступления); подпольная, полностью скрываемая от всех форм контроля экономическая деятельность (наркобизнес, азартные игры, проституция); общеуголовная преступность против личной собственности граждан как форма внеэкономического перераспределения доходов (грабеж, разбой, кража личного имущества, рэкет).

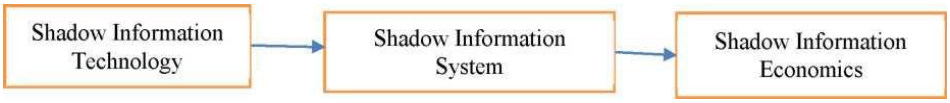
Во-вторых, фиктивная экономика - официальная экономика, дающая фиктивные результаты, отражаемые в действующей системе учета и отчетности как реальные. В-третьих, неформальная экономика - система неформальных взаимодействий между экономическими субъектами, базирующаяся на личных отношениях и непосредственных кон-

тактах между ними и дополняющая или заменяющая официально установленный порядок организации и реализации экономических связей.

Большинство авторов связывает теневую и неформальную экономики. Наиболее емкое определение предложено С.Ю Барсуковой – "…неформальная экономика объединяет качественно разнородные виды деятельности, полностью или частично не подчиненные формальным институтам хозяйствования, не подкрепленные формальными контрактами и не фиксируемые статистическим учетом". Автор отмечает, что при существенном снижении теневой составляющей неформальная экономика сохранит свои позиции за счет других сегментов и видов деятельности, но с изменением последствий для социально-экономического развития страны в целом.

Обобщающим определением теневой экономики, по нашему мнению, следует признать гипотезу, предложенную В.Латовым, а именно – теневая экономика - это социально-экономический институт (комплекс институтов), который выполняет в жизни общества определенные функции, как деструктивные (разрушительные), так и конструктивные (созидательные) (Барсукова).

Рассмотрим структуру ТЦЭ. Начнем с анализа логической цепочки, представленной на фиг. 2.



Фигура 1. Структура теневой цифровой экономики

Таким образом, отправной точкой являются "теневые ИТ" (Shadow IT). Используются различные определения, в частности:

1. Shadow IT - это сторонние ИТ-решения, в том числе облачные приложения и услуги, неподконтрольные корпоративному ИТ-департаменту. Облачные решения, представляющие собой большую часть Shadow IT, могут замещать какую-либо функцию сотрудника или целое подразделение, становиться частью услуг предприятия. Статистика реального использования облачных решений в корпоративном секторе поражает: это сотни решений, а не десятки, как полагают многие специалисты по ИТ и ИБ. Однако с точки зрения безопасности облачные приложения и сервисы представляют собой "слепое пятно" (Орешкина).

2. Shadow IT - они представляют все аппаратное, программное обеспечение или любые другие решения, используемые сотрудниками внутри организационной экосистемы, которые не получили официального одобрения ИТ-отдела (Silic & Back).

3. Бизнес-подразделения и пользователи автономно реализуют ИТ-решения, которые не встроены в организационное управление ИТ-услугами. Это все более растущее явление называется Shadow IT (Zimmermann & Rentrop).

4. Shadow IT - определяется как набор ИТ-инструментов, используемых для выполнения ИТ-функций, но не являющихся частью основной ИТ-организации (Shumarova & Swatman).

5. Авторы определяют Shadow IT как любое ИТ-решение, используемое сотрудниками для выполнения своих рабочих задач без одобрения и официальной поддержки ИТ-отдела (Mallmann, Macada, & Oliveira).

6. Например, так называемые Shadow IT, то есть сторонние ИТ-решения, неподконтрольные корпоративному управлению. И это не всегда облака, это могут быть любые информационные системы, находящиеся вне зоны видимости или контроля. Инфраструктура Shadow IT не всегда зло, часто она возникает из “добрых” побуждений, для оптимизации легитимных бизнес-процессов. Поэтому ее нужно выявлять и анализировать, и только при необходимости предложить альтернативу. Это даст возможность сделать облачную среду контролируемой, удобной и безопасной (Акинин).

7. Shadow IT - это термин, используемый для описания ситуации, когда бизнес-единицы приобретают, владеют и управляют ИТ-ресурсами без помощи ИТ-подразделения. ИТ-подразделения считают теневые ИТ неэффективными, а также источником риска и видят часть своей задачи как сдерживающую ее распространение (Microsoft).

8. Shadow IT становятся все более важными, поскольку цифровые методы работы упрощают работу бизнес-подразделений, создающих собственные ИТ-решения. Предыдущие исследования в области теневых ИТ-систем часто использовали фиксированные отчеты о добре или зле: они были отмечены как мощные движущие силы инноваций или демонизированы как недостающие центрального управления. Мы представляем метод для ИТ-менеджеров и архитекторов, позволяющих более тонкое понимание теневых ИТ-систем в отношении их архитектурной встраиваемости (Fiirstenau & Hannes).

9. Термин “теневые системы” относится к автономным программным решениям или расширениям существующих решений, которые не разрабатываются и не контролируются центральным ИТ-отделом (Fiirstenau, Sandner, & Anapliotis).

Как видно из приведенных определений, “Shadow IT” не всегда воспринимается как отрицательное явление.

Рассмотрим эволюцию термина ТЦЭ и используемые определения:

1. Разграничивая подпольную экономику и деятельность преступного мира, подчеркивается, что государство рассматривает их как одно целое (представители обеих групп сознательно нарушают законы, правила и игнорируют политическую власть), но они радикально отличаются по своей роли в обществе (Sennholz).

2. Криминальная экономическая деятельность охватывает те виды производства товаров или услуг, которые прямо запрещены существующим законодательством и являются незаконными. Она включает производство и продажу наркотиков, производство и продажу в обход установленных правил оружия, проституцию, контрабанду и т.д. (Колесников)

3. Рыночное производство товаров и услуг, законных или незаконных, которое не включено в официальные оценки ВВП (Smith).

4. Примеры киберпреступлений включают атаки типа отказ в обслуживании, киберкражи, киберпреступления, критические атаки на инфраструктуру, онлайн- мошенничество, онлайн-отмывание денег, преступное использование интернет- коммуникаций, мошенничество с идентификационными данными, использование компьютеров для дальнейших традиционных преступлений, и кибервымогательство.

5. Будущее киберпреступности будет экспоненциальным, автоматизированным и трехмерным (Goodman).

6. Неформальная экономика - трудный для исследователя объект. Одни виды неформальной деятельности скрываются в силу своей противоправности (теневая и криминальная экономики), другие — ускользают в силу своей обыденности (домашняя экономика, экономика дара) (Kshetri).

7. Перспективные организационно-экономические механизмы управления производственно-хозяйственной деятельностью предлагается конструировать на основе неформальной информационной экономики будущего (НИЭБ), разрабатываемой как методологическая основа конкретных исследований в области организационно-экономического моделирования (Орлов).

8. Теневая экономика составляет значительную долю в финансовых источниках терроризма, которые в последнее время показывают тенденцию к диверсификации. Кроме того, теневая экономика нарушает законы, принципы государственности, а также подрывает благосостояние и процветание страны, уменьшая бюджет и ВВП, а также значительно ухудшает инвестиционный климат (Орлов А.).

9. Под “теневой информационной экономикой” следует понимать индивидуальную или коллективную противоправную деятельность, связанную с проектированием, производством, распространением, поддержкой и использованием компонента информационно-коммуникационных технологий. Другими словами - это криминальные информационные продукты, услуги и процессы, основанные на ИТ или использующие ИТ (Охрименко & Бортэ).

10. Под теневой информационной экономикой следует понимать всю индивидуальную и коллективную деятельность, являющуюся незаконной, связанную с проектированием, разработкой, распространением, поддержкой и использованием компонента информационных и коммуникационных технологий, скрываемую от общества. То есть, теневая информационная экономика - это все незаконные и скрываемые продукты и услуги, использующие и основывающиеся на информационных технологиях. В качестве наиболее важных экономических элементов данной сферы мы выделяем следующие: незаконные экономические взаимоотношения, незаконную деятельность, связанную с производством, распространением и использованием запрещенных продуктов и услуг (Охрименко, Саркисян, & Бортэ).

11. Под теневой информационной экономикой понимается деятельность, связанная с исследованиями, поддержкой и использованием компонента информационных и коммуникационных технологий, скрываемая от общества и государства, находящаяся вне государственного контроля и учета, а также, чаще всего, являющаяся противоправной (Бортэ).

12. Под теневой информационной экономикой следует понимать всю индивидуальную и коллективную деятельность, являющуюся незаконной, связанную с проектированием, разработкой, распространением, поддержкой и использованием компонента информационных и коммуникационных технологий, скрываемую от общества. То есть, теневая информационная экономика - это все незаконные и скрываемые продукты и услуги, использующие и основывающиеся на информационных технологиях. В качестве наиболее важных экономических элементов данной сферы выделятся следующие: незаконные экономические взаимоотношения, незаконную деятельность, связанную с производством, распространением и использованием запрещенных продуктов и услуг.

13. Теневая информационная экономика - деятельность, связанная с исследованием, проектированием, производством, распространением, поддержкой и использованием компонента информационных и коммуникационных технологий, скрываемая от общества и государства,

находящаяся вне государственного контроля и учёта, а также, чаще всего, являющаяся противоправной. Таким образом, причиной существования теневой информационной экономики является наличие условий, при которых выгодно скрывать свою деятельность, либо отдельные её элементы (Бортэ).

14. Авторы статьи предлагают следующее определение ТИЭ - это коллективная или индивидуальная деятельность, паразитирующая во всех сферах жизни общества, базирующаяся на использовании компонента информационно-коммуникационных технологий. Данный вид нелегальной деятельности должен рассматриваться как особый сегмент, которому присущи следующие системные свойства: всеобщность, целостность, связь с внешней средой, структурность, способность к самоорганизации и непрерывному развитию, наличие конструктивного (производительный сектор) и деструктивного (криминальный сектор) элемента (Охрименко & Бортэ).

Проведенный анализ подходов к определению ТЦЭ позволяет выделить пять основных подходов: юридический, математический, социально-психологический, организационно-управленческий, экономико-финансовый.

Юридический подход описывает данную категорию с позиции юридической науки, акцентируя внимание на противоправной деятельности. Математический рассматривает как модель управления теневой деятельностью участников в информационном секторе с выделением жизненного цикла отдельных продуктов и услуг, а также процессы монетизации.

Организационно-управленческий подход заключается в определении ТЦЭ с точки зрения организационно-правовой формы взаимодействия участников теневых рынков продуктов и услуг.

Социально-психологический анализирует деятельность участников с точки зрения иррационального экономического поведения, привлечения большого количества специалистов в информационных и коммуникационных технологиях.

Экономико-финансовый подход рассматривает ТЦЭ в качестве финансовых структур, отмывающих деньги посредством использования различных махинаций на базе информационно-коммуникационных технологий на легальном рынке товаров и услуг.

Сформулируем определение теневой цифровой экономики, основываясь на ее специфике с точки зрения производства продуктов и услуг, жизненного цикла производства и услуг и т.д. Таким образом, теневая цифровая экономика (ТЦЭ) - сектор экономических отношений, охватывающих все виды производственно-хозяйственной деятельности,

которые по своей направленности, содержанию, характеру и форме противоречат требованиям законодательства и осуществляются вопреки государственному регулированию экономики и в обход контроля над ней.

Основу ТИЭ 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 отчетности;
- 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 ботнетов.

Как отмечает известный специалист по информационной безопасности Лукацкий А.: “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 платежные системы расчетов, партнерские 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”.

Следует отметить, что первыми авторами, которые использовали категорию “теневая информационная экономика” - были авторы монографии “Рынок информационных услуг и продуктов”. В 5 главе монографии выделен параграф 5.2.4 “Теневая информационная экономика”, который начинается с использованием главной посылки нашего исследования – “Рассмотрение теневого сектора информационной экономики и информационной деятельности требуется для оценки ее объема и потенциального ущерба, который она наносит”. Вместе с тем указывается, что реальные потери бюджета России из-за теневого характера частного бизнеса в области информационных услуг и продуктов не так велики и, по сути, данный тип теневого бизнеса является одним из немногих, которые заслуживает вывода из тени путем введения для него безналогового режима в целях поддержки развития. Таким образом, в России определенная часть информационной деятельности и рынка информационных услуг и продуктов находится в тени. Теневой сектор

не имеет криминальной основы и связан с низкой эффективностью информационной деятельности, уровень развития которой не позволяет не только финансировать рост, но и осуществлять простое воспроизводство при условии оплаты всех налогов. Следует обратить внимание на выделение авторами части рынка информационных услуг и продуктов, который находится в тени и отсутствие криминальной основы. За прошедшее время картина кардинальным образом изменилась – часть рынка информационных продуктов и услуг стала подпольной и криминальной, приносящей высокую прибыль.

Несколько иной подход используется в работах авторов Гаспарениене Л.,Ремейкиене Р., Шнейдер Ф., (Ligita Gaspareniene) основанный на процессах всеобщей оцифровки (дигитализации) экономики. В частности, предлагается следующее определение теневой цифровой экономики: “нелегальная деятельность в киберпространстве, позволяющая генерировать нелегальные потоки денег для нелегальных поставщиков услуг и продавцов, а также лишать доходов легальных поставщиков услуг и продавцов”.

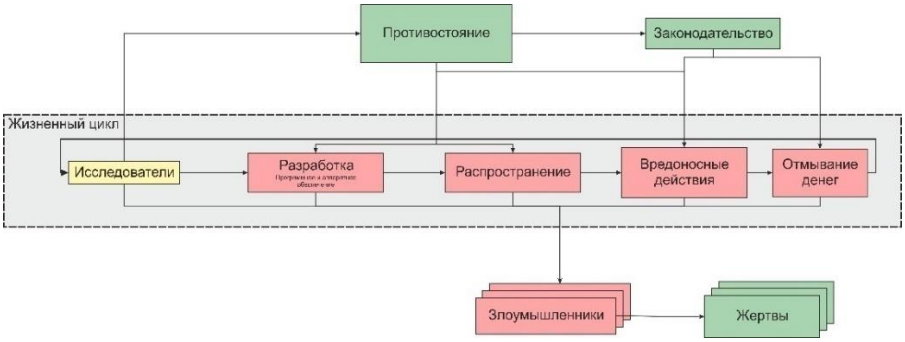
Таким образом, подводя итоги анализа существующих подходов к определению ТЦЭ, авторы настоящего исследования предлагают следующие определения:

- теневая цифровая экономика - специфическая сфера экономической деятельности с присущими ей структурой и системой экономических отношений. Специфичность задается нелегальностью, неофициальностью, а также криминальным характером экономической деятельности и сокрытием доходов;
- с экономической точки зрения - 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 компонента информационных и коммуникационных технологий, скрываемая от общества.

Таким образом, ТИЭ - 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 запрещенных продуктов и услуг.

Вышеприведенное позволяет предложить эмпирическую модель ТЦЭ, которая приведена на следующей фигуре.



Фигура 2. Эмпирическая модель ТЦЭ

Следует выделить особенности, характерные для информационной области теневой экономики. В их числе следующие:

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

2. 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 углубленном 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.

3. В информационной среде куда проще найти клиента или поставщика услуг благодаря глобализации и сети Internet.

4. По сравнению с “классическими” денежными переводами, транзакции осуществляются намного быстрей и надежней, могут быть совершены анонимно благодаря криптовалютам.

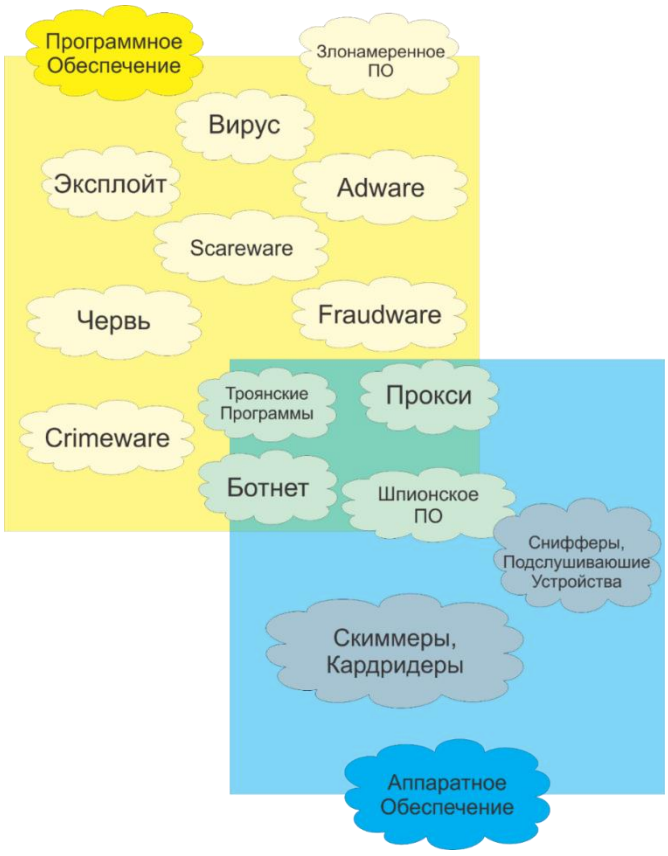
5. Информационные товары и услуги несут в себе меньшие риски по сравнению с продажей, например, оружия и наркотических веществ, при этом объем прибыли может быть сопоставим.

6. Минимальные риски, связанные с ответственностью, в том числе уголовной.

Сегментация теневой цифровой (информационной) экономики

Представляется необходимым проанализировать существующие подходы к классификации продуктов и услуг, а также рассмотреть сегментацию ТЦЭ. Обобщенная структура предусматривает деление на продукты и услуги, с учетом постоянной их изменчивости. Данное свойство является определяющим, поскольку достижения научно-технического прогресса и нововведения в области информационных и коммуникационных технологий обеспечивает достаточно быструю сменяемость аппаратной и программной платформ. В информационной сфере материальные продукты крайне малочисленны и обычно относятся к аппаратному обеспечению, в то время как большая часть данного определения подразумевает программное обеспечение, которое обычно считается нематериальным. Следует отметить, что в практике информационной безопасности используют множество классификаций.

Структура продуктов ТЦЭ приведена на следующей фигуре.



Фигура 3. Структура продуктов ТЦЭ

К продуктам в сфере ТЦЭ следует отнести, прежде всего, специализированное программное обеспечение (вредоносные программы). Это огромный класс программ, состав которого постоянно изменяется и это заставляет специалистов по информационной безопасности предпринимать комплекс мер и выстраивать технические и программные барьеры для исключения их проникновения в информационные системы.

Структура и состав вредоносных программ представлена на фиг. 4 (CheckPoint). Следует иметь в виду, что их состав постоянно изменяется. В литературе вредоносные программы обозначают как malware (англоязычный термин, состоящий из двух слов: malicious – злонамеренный и software – программное обеспечение). Существуют синонимы – badware, computer contaminant, crimeware. К подобным программам относят любое программное обеспечение, способное несанкционированно проникать в информационную систему для нарушения нормальной работы компьютера, хищения личных данных и т.д.

Фигура 4. Структура вредоносных программ

Рассмотрим наиболее известные примеры вредоносных программ, основные из них приведены в следующей таблице.

Таблица 8

Примеры наиболее известных вредоносных программ

Год	Наименование	Тип	Метод распространения	Разработчик
1986	Brain	Virus	Boot sector	Basit and Amjad Farooq Alvi
1988	RTM	Worm	Internet	Robert T. Morris
1999	Melissa	Macro	Email	David Smith
2000	I Love You	Macro	Email	Onel de Guzman
2001	Code Red	Virus/worm hybrid	Email/Internet	Unknown
2001	Nimda	Worm	Email, Internet/network shares	R.P.China
2003	Slammer	Worm	SQL	Unknown
2005	Poison Ivy	Trojan	Typically with PDF, DOC, PPT, and so on	Unknown
2007	Zeus	Crimeware kit	Email, drive-by download, attachment, and so on	Unknown
2008	Agent.btz	Trojan	Thumb drive	Unknown
2009	Confcker	Worm	Thumb drive, network shares	Unknown
2009	Stuxnet	Advanced persistent threat (APT)	Thumb drive, network shares	Unknown
2010	Blackhole exploit kit	Exploit kit	Email, drive-by download, attachment, and so on	Unknown
2014	CryptoLocker	Ransomware	Email, drive-by download, and so on	Unknown
2015	Angler exploit kit	Exploit kit	Email, drive-by download, and so on	Unknown

Есть все основания для проектирования регистра не только вредоносных программ, но и всех продуктов и услуг криминальной

направленности, попадающих под определение инструментов ТЦЭ. В частности, первыми представителями вредоносных программ могут быть следующие:

Adware. В общем случае данным термином называется программное обеспечение содержащее рекламу, однако зачастую подобные программы могут злоупотреблять данным свойством, тем самым мешая комфортной работе, отвлекая пользователя всплывающими окнами и в целом замедляя работу самого компьютера. В ранний период появления этого термина он обозначал программные продукты, которые финансировались рекламой, будучи частью этой программы, и при удалении соответствующего программного продукта исчезали из компьютера. Пользователь был осведомлен о том, что устанавливаемый продукт содержит рекламу. На современном этапе данный термин скорее подразумевает программные продукты, которые могут вводить пользователя в заблуждение своим описанием и отображаемыми сообщениями. Кроме того, не всегда пользователь может от подобных продуктов избавиться без помощи специалиста, поскольку многие из подобных программ могут обладать защитными механизмами самовосстановления, установки дополнительных подобных продуктов. Помимо этого, отображаемая реклама может нести оскорбительный характер. Adware может собирать данные о посещаемых сайтах, запускаемых программах и передавать подобные данные на удаленный сервер для показа “таргетированной” рекламы в дальнейшем без должного оповещения об этом пользователя. К сожалению, не все операционные системы, используемые на сегодняшний день, обладают механизмами, защищающими пользователей от подобных действий. И далеко не все пользователи проявляют достаточную осторожность при установке программного обеспечения.

Шпионское программное обеспечение - программный продукт, собирающий сведения о пользователе и его действиях. Использует программное и аппаратное обеспечение без должного оповещения об этом самого пользователя, без получения на то его согласия и без предоставления достаточного контроля над собираемыми данными.

Crimeware - термин, обозначающий программные продукты, нацеленные на автоматизацию киберпреступлений. Например, кража сохраненных на компьютере жертвы паролей, скрытная установка шпионского программного обеспечения и т.д.

Компьютерные вирусы. Данная группа насчитывает достаточно много разновидностей программного обеспечения и является наибо-лее представительной по сравнению с другими вредоносными программными продуктами. Они отличаются по среде обитания (сетевые, файловые

и загрузочные); по способу заражения (резидентные и нерезидентные); по степени воздействия (неопасные, опасные и очень опасные); по особенностям алгоритмов реализации (паразитические, репликаторы, невидимки, мутанты, троянские, временные логические бомбы, макровирусы и т.д.).

Генератор вредоносного программного обеспечения. Данный вид программного обеспечения является набором специализированных инструментов для создания узконаправленного вредоносного программного обеспечения и объединения зараженных компьютеров в сеть. Например, Zeus и Spy Eye. Имеется одна особенность - Spy Eye может удалять с инфицированного компьютера компоненты конкурирующей системы Zeus.

Компьютерный червь. Вредоносное программное обеспечение, использующее саморепликацию для заражения компьютеров. В отличие от вирусов, черви не прикрепляются к уже существующим программам или файлам, которые вирусы модифицируют (очень часто необратимо). Чаще всего черви используют сетевую инфраструктуру для заражения других компьютеров.

Троянская программа. Тип вредоносного программного обеспечения, который не способен самостоятельно заражать компьютеры пользователей. Чаще всего распространяется благодаря социальной инженерии, выдавая себя за полезную или интересную программу. Троянские программы выполняют несанкционированные пользователем действия. Они могут удалять, изменять, копировать и блокировать данные, существенно замедлять работу компьютера. Обычно подобные программы стремятся украсть конфиденциальные данные пользователя, предоставляют бэкдор и т.д.

Scareware (Fraudware, Fake Anti-Virus). Программное обеспечение, вводящее пользователя в заблуждение ложными сообщениями о том, что его компьютер инфицирован вредоносным программным обеспечением, и вымогающее оплату за очистку компьютера, продление лицензии и т.д. Помимо этого, подобные программы могут содержать бэкдор, позволяющий злоумышленнику получить полный доступ к компьютеру жертвы или же использовать его компьютер для DoS атак, рассылки спама, загрузки дополнительного программного обеспечения (партнерские программы, PPI). Данный класс программ может блокировать некоторые функции системы, запустить определенные процессы, например, командную строку, менеджер задач, редактор реестра, доступ к определенным файлам и веб-сайтам и т.д., утверждая, что эти меры необходимы для обеспечения безопасности.

Потенциально нежелательное программное обеспечение. Специалисты относят к данной категории узкоспециализированное программное обеспечение, предназначенное для упрощения администрирования и т.д., например, подборщики паролей, утилиты удаленного доступа и управления, руткиты, которые нашли добропорядочное применение и в дальнейшем были включены в комплект утилит.

Руткит. Программное обеспечение, чаще всего вредоносное, спроектированное таким образом, что позволяет избежать обнаружения стандартными методами, а также получить наивысший уровень прав на компьютере. Не все руткиты являются вредоносными. Некоторые из них могут выступать в качестве утилит, например, эмуляторы - программное обеспечение, отвечающее за безопасность (антивирусы, брандмауэры и т.д.), защиту от кражи ноутбуков и т.д. Исходные коды для многих руткитов доступны для скачивания в сети Internet, большинство из них появились в качестве доказательства правильности определенной концепции или теории.

Упаковщик. Программное обеспечение, видоизменяющее бинарный код исполняемого файла без изменения его семантики. Зачастую подобное сжатие может применяться для уменьшения размера исполняемого файла, однако может использоваться и злоумышленниками для уклонения от обнаружения, использующего сигнатурный анализ.

TDS (Traffic Direction Script, Скрипт перенаправления траффика). При помощи подобных скриптов злоумышленник может очень гибко разделять посетителей по странам, веб-сайтам, с которых посетитель перешел, их уникальности на основе IP-адреса и Cookies, отслеживать доступность других ресурсов системы. Скрипт также предоставляет возможность разбивать правила переадресации трафика, выступая балансировщиком нагрузки (load balancer) на прочие ресурсы, занимается разделением трафика по времени или переадресацией всего трафика на другой url в том случае, когда какие-то из компонентов системы недоступны. Помимо этого, скрипт позволяет просмотр очень подробной статистики посетителей и возможность предоставления подобной статистики третьим лицам, без предоставления им администраторского доступа. Обычно этот скрипт перенаправляет жертв на наиболее подходящий для заражения их компьютера эксплойт или даже на вредоносное программное обеспечение, включающее в себя множество эксплойтов, например, blackhole, eleonore exploit pack, phoeniex exploit kit, или их аналоги, которые занимаются непосредственно заражением компьютера жертвы вредоносным программным обеспечением, объединяя их в ботнет. Данная категория скриптов значительно повышает отказоустой-

чивость систем распространения вредоносного программного обеспечения.

Криптолокер - вредоносная программа-вымогатель, шифрующая пользовательские файлы или иным способом препятствующая нормальной работе компьютера, а затем вымогающая деньги в обмен на обещание их расшифровки или восстановления нормального функционирования. Примечательно, что далеко не всегда оплата гарантирует восстановление работоспособности, в некоторых случаях злоумышленники продолжают вымогать всё большие и большие суммы денег.

Криптомайнер – несанкционированный майнинг (добыча) криптовалют. По данным Лаборатории Касперского в 2016–2017 гг. с майнерами столкнулись почти 1,9 млн пользователей, то в 2017–2018 гг. их число выросло почти в полтора раза, до 2,7 млн человек. Преступный или черный майнинг отличается от законного только тем, что злоумышленники используют оборудование, которое им не принадлежит. Для этого они либо заражают чужие компьютеры , либо заманивают жертв на сайт со скриптами, запускающими процесс майнинга в браузере. Рост популярности черных криптомайнеров начался ничем не примечательно - с атак на домашние компьютеры. Однако рядовые пользователи приносят злоумышленникам копейки, поэтому те начали искать более денежные цели. Вредоносные майнеры следуют тем же путем, которым уже прошли программы-вымогатели, - от домашних компьютеров к бизнес-машинам. Следующим логическим шагом должны стать целевые атаки, рассчитанные на внедрение майнеров в корпоративную инфраструктуру (Kaspersky).

Шпионское аппаратное обеспечение. Клавиатурные шпионы, устройства считывания электромагнитных импульсов, устройства перехвата беспроводных коммуникаций и т.д. Скрытое оборудование, используемое для наблюдения и считывания сигналов и получения доступа к вычислительной технике. Подобные устройства могут быть заложены как непосредственно в аппаратное обеспечение, так и могут продаваться в свободном доступе в интернете в виде клавиатурных шпионов для USB или PS/2 по цене от пятидесяти до двухсот долларов США. Наиболее дорогие экземпляры клавиатурных шпионов могут содержать модуль Wi-Fi для передачи данных на средние и короткие дистанции. Наиболее простые устройства содержат чип флеш-памяти, сохраняющий все нажатые клавиши. Закладки, установленные непосредственно в аппаратное обеспечение, обычно состоят из микрокомпьютера на базе ARM и коммуникационных модулей. Подобные устройства позволяют получить удаленный доступ, перехватывать изображение с монитора, перехватывать коммуникации между компьюте-

рами или периферийными устройствами и т.д. Наиболее простые устройства содержат чип флеш-памяти, сохраняющий все нажатые клавиши. Закладки, установленные непосредственно в аппаратное обеспечение, обычно состоят из микрокомпьютера на базе ARM и коммуникационных модулей. Подобные устройства позволяют получить удаленный доступ, перехватывать изображение с монитора, перехватывать коммуникации между компьютерами или периферийными устройствами и т.д.

Сайты-генераторы подарочных карт. Мошеннические ресурсы, которые не крадут деньги или персональные данные посетителя. Суть всегда одна - посетителю предлагают совершенно бесплатно сгенерировать код подарочной карты. Чтобы получить код, пользователь должен выбрать на сайте нужную подарочную карту, после чего система начнет “генерацию кода” или “взлом”. Для большей достоверности по экрану в это время, как в кино про хакеров, бегут надписи, сообщающие о подключении к серверам и т. п. “Сгенерированный” код посетителю целиком не покажут: для начала он должен подтвердить, что является человеком, а не роботом. Для этого надо пройти по предложенной ссылке и выполнить некое задание. Итоговый результат выполнения заданий неприятен, но закономерен: жертву либо водят по партнерским сайтам, пока той не надоест заполнять анкеты и играть в лотереи, либо выдают ей в качестве награды случайный набор символов, который не имеет никакого отношения к настоящим кодам и похож на них лишь форматом. Владельцы сайтов-генераторов стараются не прибегать к откровенному мошенничеству или фишингу. Им вполне хватает средств от “продажи действий” пользователей на партнерских сайтах: заработок колеблется от нескольких центов за клик по нужной ссылке до нескольких десятков долларов за заполнение посетителем анкеты или подписки на платные услуги.

Материалы, нарушающие авторские права, пиратство. В данном случае под пиратством понимается правонарушение, при котором используются определенные охраняемые авторским правом произведения науки, литературы или искусства, без разрешения автора или правообладателя, или с нарушением условий договора об использовании этих произведений с использованием компонента информационно-коммуникационных технологий.

Материалы и программные продукты, нарушающие пользовательское соглашение. К этой категории относятся программы, позволяющие жульничать в многопользовательских компьютерных играх. Например, подписка на программу, позволяющую видеть сквозь стены и упрощающую прицеливание в игре Counter Strike: Global

Offesive, стоит порядка 10.95 долларов США в месяц. Однако существуют и дополнительные возможности, и поддержка других игр за более высокую плату. В подписку входит также доступ к форумам, на которых возможно пообщаться с другими пользователями, администраторами и разработчиками. Примечательно отметить, что в упомянутой программе предусмотрены технические средства защиты авторских прав (DRM). Владелец этого сервиса сообщил в интервью, что сайт приносит порядка 1.25 млн долларов США в год. Разработчики игр отмечают особо заметный приток нарушителей во время и после распродаж игр. Разработчики игр заявляют, что борьба с сайтами, распространяющими подобную продукцию юридическими методами, невыгодна, поскольку они чаще всего зарегистрированы в странах, не осуществляющих экстрадицию.

Аппаратура и инструментарий для мошенничества с платежными картами (кардинг). Под кардингом чаще всего понимается правонарушение, при котором используются платежная карта или её реквизиты без должного на то согласия обладателя этой карты. Одним из используемых в данном случае устройств может служить скиммер - инструмент для считывания данных проходящих через него карт, например, магнитной ленты, а также содержащий устройство для хранения считанной информации и интерфейс для подключения к компьютеру. Скиммеры чаще всего устанавливаются в или на картоприемник банкомата. Считав данные с магнитной ленты, злоумышленник в дальнейшем может изготовить копию данной карты. Кроме этого, злоумышленник может использовать накладную клавиатуру или камеру для того, чтобы заполучить PIN-код украденной карты. Помимо этого, злоумышленник может попытаться подобрать номер карты, имея валидную и зная возможные уязвимости алгоритма генерации номеров кредитных карт. Одним из наиболее крупномасштабных преступлений в области кардинга считается взлом сервиса WorldPay, в результате которого злоумышленникам удалось украсть порядка 9 млн. долларов США. Подделка платежных карт и банкоматное мошенничество включают множество операций, в частности: использование утраченных/похищенных/поддельных платежных карт; похищение реквизитов платежных карт, в том числе с применением технических средств их “клонирования”; скимминг – изготовление, сбыт и установка на банкоматы устройств считывания/копирования информации с магнитной полосы платежной карты и получение ПИН-кода к ней; использования “белого пластика” для “клонирования” (подделки) платежной карты и снятия наличных в банкоматах; Transaction Reversal Fraud – вмешательство в работу банкомата при осуществлении операций выдачи налич-

ных, которое оставляет неизменным баланс карточного счета при фактическом получении наличных злоумышленником; Cash Trapping – заклеивание диспенсера для присвоения злоумышленником наличности, которая была списана с карточного счета законного держателя карты.

Уязвимости программного и аппаратного обеспечения. В ISO/IEC 27005 уязвимостью называется слабость актива или группы ресурсов, которая может быть использована одной или несколькими угрозами, где активом считается всё, что представляет ценность для организации, её коммерческой деятельности и её непрерывности, включая информационные ресурсы, поддерживающие цель организации. В NIST SP 800-30 предложено следующее определение уязвимости: изъян или слабость в системных процедурах безопасности, проектировании, внедрении или внутреннем контроле, которые могут быть использованы (преднамеренно или случайно) и привести к обходу системы безопасности или нарушению политики безопасности компании. Следует отметить, что существует “черный” рынок уязвимостей (в том числе, уязвимости 0-дня), на котором предлагается большой набор инструментов.

Персональные данные. Персональные данные — это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия и т.д. Идентифицируемым лицом является лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификационный номер либо на один или несколько факторов, специфичных для его физической, физиологической, психической, экономической, культурной или социальной идентичности; особые категории персональных данных - данные, раскрывающие расовое или этническое происхождение лица, политические убеждения, религиозные или философские воззрения, социальную принадлежность, данные, касающиеся состояния здоровья или половой жизни, а также данные, касающиеся уголовного наказания, принудительных процессуальных мер или санкций за правонарушения.

Кибероружие. Вредоносное программное обеспечение, используемое в военных или разведывательных целях. В последнее время всплывает всё больше и больше случаев подобного использования программного обеспечения. Одна из основных характерных черт подобных атак - узкая направленность, в отличие от киберпреступников, стремящихся заразить как можно большее количество жертв. Чаще всего подобные разработки спонсируются или проводятся государственными

учреждениями. Наиболее яркими примерами подобного программного обеспечения служат Stuxnet, Falme, Duqu, Gauss. Почти всегда в подобных вредоносных программах используются уязвимости нулевого дня.

Приведенные примеры нелегальных продуктов далеко не исчерпывают всего многообразия. Данный набор постоянно совершенствуется и обновляется с завидной скоростью. В связи с этим, разработка реестра подобных продуктов является весьма актуальной и окажет существенную помощь разработчикам программного обеспечения, персоналу, отвечающему за поддержку информационных систем.

Отдельную группу образуют услуги, состав и структура которых постоянно изменяется. Структура услуг в ТЦЭ приведена на следующей фигуре.

Фигура 5. Структура услуг ТЦЭ

Рассмотрим наиболее яркие примеры:

Аналитика, в том числе поиск и анализ уязвимостей программного и аппаратного обеспечения, анализ рынка и законодательного обеспечения.

Кража личных данных - включает такие действия, как перехват идентификационных данных, кредитных карт, логинов и паролей.

Software as a service - сдача в аренду вредоносного программного обеспечения, а также создание компьютерных вирусов и троянских программ для скрытого перехвата управления компьютером клиента с установленным программным обеспечением дистанционного банковского обслуживания.

Фишинг - попытка выдать вредоносный сайт за сайт крупной и известной компании, которой пользователь доверяет. Сайт обычно предлагает пользователю ввести свои данные, логин, пароль, возможно, данные кредитных карт, потом выдает ошибку и просит повторить попытку позже.

Фарминг - атака, целью которой является перенаправление трафика на другой, подставной веб-сайт.

Вымогательство. Угрозы в случае невыплаты требуемой суммы организовать атаки на их сервисы.

“Нигерийские письма”. Жертве обещают крупную сумму денег или прочие материальные ценности в обмен на оплату доставки или данные кредитной карточки.

Саботаж - создание проблем в функционировании определенной информационной системы или её составных частей, а также мотивирование прибылью.

Терроризм - применительно к киберпространству, саботирование систем или их частей, мотивированное убеждениями.

Пиратство - неправомерное копирование материалов в нарушение законов об авторских правах.

Сдача в аренду прокси-серверов. А также шифрование и сокрытие Интернет-трафика. Одной из главных проблем, стоящих перед злоумышленниками, является сокрытие физического местоположения своих серверов и рабочих станций, в случае обнаружения которых органы правопорядка могут прекратить их работу.

Отмывание денег при помощи информационных технологий. Данная услуга является одной из самых распространенных и доходных в рамках ТЦЭ. Киберкриминал постоянно выстраивает новые схемы обналичивания и использования банковских услуг. Отмывание основано на использовании различных видов операций и поставщиков финансовых услуг, начиная с банковских переводов, внесения/снятия наличных,

использования электронных денег и заканчивая “денежными мулами” и услугами по переводу денег. Инструменты и механизмы, которыми пользуются преступники во время осуществления отмывания доходов, полученных в сфере киберпреступности, являются достаточно разнообразными. В частности, при отмывании доходов от киберпреступлений характерным является использование следующих механизмов:

- использование счетов, открытых по утраченным документам или на подставных лиц;
- использование фиктивных (транзитных) предприятий;
- проведения цепи финансовых операций через несколько банковских счетов с помощью удаленного доступа;
- использования наличных на последнем этапе цепи финансовых операций;
- использования альтернативных платежных систем (электронные платежи), как национальных, так и международных;
- покупка электронных денег и использования систем платежей через электронные кошельки;
- конвертация незаконных доходов в товары путем приобретения последних через сеть Интернет.

Компьютерные преступники используют платежные системы, как внутригосударственные, так и международные для легализации преступных доходов. Их использование основывается на нескольких неоспоримых преимуществах, в том числе:

- доступность – открытие собственного электронного счета является бесплатным для любого пользователя;
- простота использования – открытие и использование электронного счета является интуитивно понятным и не требует специальных знаний;
- мобильность – пользователь через сеть Интернет может осуществлять управление своим счетом из любого места;
- оперативность – транзакции по счету происходят в течение нескольких секунд;
- безопасность – передача информации ведется с использованием криптографической защиты.

Электронные деньги дают возможность осуществлять следующие платежи: платежи внутри системы на счета физических и юридических лиц; оплата товаров в Интернет-магазинах; оплата услуг операторов мобильной связи; оплата коммунальных услуг; оплата Интернет-услуг; оплата государственных сборов, пошлин и штрафов; покупка ж/д и авиабилетов; покупка топлива; бронирование отелей и многие др.

Для преступников несомненным преимуществом использования электронных денег является возможность анонимного открытия и пополнения электронных кошельков, а также круглосуточная доступность и скорость проведения транзакций (в течение нескольких секунд). Электронный кошелек физического лица чаще всего имеет привязку к электронной почте или номеру мобильного телефона. Кроме того, для перемещения наличных средств между участниками схемы могут использоваться срочные переводы через международные системы перевода средств.

Одним из относительно новых видов мошенничества и отмывания денежных средств является онлайн компьютерные игры. Так, по сообщениям компании Kromtech Security, они представили доказательства того, что кардеры используют ворованные кредитные карточки для приобретения внутриигровых валют и вещей в мобильных играх вроде Clash of Clans, Clan Royale, и Marvel Contest of Champions. Далее они перепродают все это уже за реальные деньги при помощи разного рода сервисов. Группа злоумышленников использует сложные автоматизированные системы для приобретения внутриигровых ресурсов и отмывает деньги с ворованных кредиток. Торговля игровыми валютами, вещами и разного рода услугами — солидный источник дохода для многих компаний и частных лиц. К примеру, компания Electronic Arts заработала на Star Wars: Battlefront II около $787 млн - это только внутриигровые покупки, а не продажа самой игры. Эксперты по сетевой безопасности и ранее заявляли, что внутриигровые валюты и все, что с ними связано - отличный способ для злоумышленников отмывать “грязные” деньги без особого риска и опасности для себя. Все это было названо “мечтой киберпреступника”. Отследить подобные транзакции, и тем более блокировать их, крайне сложно. Более того, выявить злоумышленника в большинстве случаев тоже не представляется возможным.

Интересные данные приведены в книге С.Сьювермена (Sjouwerman, Cyberheist: The biggest financial threat facing American businesses.) при сравнении цены на различные украденные киберданные на основе отчетов Symantec и Panda Labs, они приведены в следующей таблице.

Следует отметить, что справочная информация, приведенная в табл. 8, может служить отправной точкой при рассмотрении большинства схем по отмыванию денежных средств.

Создание и сдача в аренду ботнетов. На данный момент наиболее популярным примером является упоминавшийся набор инструментария для создания ботнетов, например, Zeus и SpyEye. Оба набора

предлагают модульную систему и предоставляют административную панель на основе веб-интерфейса. Созданный и поддерживаемый ботнет может быть сдан в аренду ботмастером по договоренности. Данная услуга является заказной и весьма доступной в сети DarkNet.

Таблица 9
Цены на украденные данные пользователей (в $)

Показатели	Оценки **Symantec**	Оценки **Panda Labs**
Информация о банковском счете	15-850	80-700
Информация о кредитной карте	1-30	2-90
Информация о регистрации учетной записи электронной почты	1-20	нет
Банковские переводы и проверка наличных денег	50-60% средств	10-40% средств
Интернет-магазины и доступ к ePay	нет	80-1500
Покупка/пересылка товаров	нет	30-300 за штуку
Спам-рента	4-10 и выше	15 и выше
SMTP-рента	нет	20-40 за 90 дней
VPN-рента	нет	20 за 90 дней
Учетные данные веб-администратора	2-60	нет

Процесс развертывания ботнета может быть представлен следующей последовательностью действий: для начала злоумышленник может проверить полученный им ранее список данных доступа на FTP-сервер при помощи утилиты FTP Checker. Другая утилита, FTP Injecter, служит для соединения с проверенными предыдущей программой FTP-серверами и поиском на них файлов с расширением *.php, *.html, *.htm, *.phtml, *.asp и *.cfm. В случае обнаружения таких файлов утилита пытается включить в них замаскированный html-код, создающий фрейм, ссылающийся на адрес, указанный злоумышленником, который, вероятно, попытается заразить компьютер посетителя веб-сайта вредоносным программным обеспечением. В исследовании MalwareIntelligence фрейм ссылался на сайт http://google-analytica.com, который для обычного пользователя может выглядеть как вполне легитимный веб-сайт. Домен использовал Advanced TDS 1.1 (Traffic Direction Script) для управления трафиком, перенаправляя жертв на наиболее подходящий (в

зависимости от операционной системы, браузера и т.д.) для заражения их компьютера эксплойтом.

Данные о стоимости аренды ботнетов приведены в таблице 7 (DELL SecureWorks).

Очевидно, что цена зависит от спроса на ботнеты, расположенные в определенном регионе и возможности его удовлетворения. Спрос может быть продиктован необходимостью проведения DoS-атак или других злонамеренных действий в данном регионе, потому что чем ближе компьютер жертвы находится к компьютеру, с которого производится атака, тем эффективней будет эта атака. Однако, ещё более важным фактором может быть то, что на компьютерах в определенных регионах может содержаться информация, которую возможно монетизировать, например, информация о кредитных картах.

Таблица 10
Стоимость аренды ботнета

Количество арендуемых ботов	**Стоимость, доллары США**
2013 год, боты со всего мира	
1000	20
5000	90
10000	160
2014 год, США (уникальные установки)	
1000	140 – 190
5000	600 – 1000
10000	1100 – 2000
2014 год, Великобритания (уникальные установки)	
1000	100 – 120
5000	400 – 500
10000	700 – 1100
2014 год, Азия (уникальные установки)	
1000	4 – 12

DoS и DDoS-атаки. Благодаря широкому распространению и доступности вредоносного программного обеспечения Zeus и SpyEye, нередко можно встретить в сети предложения по организации DoS- и DDoS-атак. Согласно информации, предоставленной исследователем Данко Данчевым, подобные атаки могут стоить от 5 долларов США за час, до 900 долларов США за атаку продолжительностью в месяц. Цены зависят в основном от длительности атаки, даже могут быть предусмотрены скидки.

Специалисты по информационной безопасности выделяют пять поколений (этапов) развития механизмов противостояния атакам.

Первое поколение было характерно для конца 80-х годов и было представлено, в основном, вирусными атаками на автономные персональные компьютеры предприятий и организаций. В качестве средства противостояния состоялся запуск и использование семейства антивирусных продуктов. Антивирусные продукты сканируют вредоносные файлы, используя сигнатуры. В свою очередь хакеры постоянно создают новые варианты вирусов для обхода антивирусов. Антивирус попрежнему является актуальным инструментарием, поскольку идентифицировал около 60% вредоносных программ того времени. Но этого явно недостаточно, так как около 49% сегодняшних угроз являются безфайловыми атаками (fileless). Появились антивирусы следующего поколения с более широкой зоной покрытия новых угроз с использованием элементов машинного обучения. Разработчики антивирусов постоянно анализируют образцы вредоносных программ и разрабатывают новые модели, с помощью которых сканируют и анализируют зараженные файлы для разработки функций обнаружения новых вредоносных атак.

Второе поколение характеризует развитие сетей в середине 90-х годов. Для этого периода характерны атаки из Интернета, которые затронули весь бизнес и привели к созданию Firewall.

Третье поколение характеризует развитие приложений и относится к началу 2000-х годов. Использование уязвимостей в приложениях затронуло большинство предприятий и привело к появлению и внедрению систем предотвращения вторжений (IPS - Intrusion Prevention System).

Следующее поколение характеризует такую категорию, как полезная нагрузка, и относится приблизительно к 2010 году. Отмечается резкий рост целенаправленных, полиморфных атак, которые затронули большинство предприятий и привели к началу борьбы с ботсистемами.

Пятое (мега) поколение началось примерно в 2017 году и характеризуется многомасштабными, векторными атаками с использованием распространенных инструментов и продвижением профилактических инструментов. Аналитики предполагают, что данный этап будет продолжаться до 2020 года.

Спам. Спам представляет собой массовую рассылку корреспонденции рекламного или иного характера лицам, не выражавшим желания её получать. Большинство из существующих ботнетов были специально спроектированы для рассылки спама. Наиболее характерным представителем подобных ботнетов является Restock. Согласно данным Techworld, зараженный компьютер мог отправлять до 25000 писем в

час. Однако не всегда их создатели пользуются подобным ботнетами самостоятельно, очень часто подобные системы сдаются в аренду заказчикам. Помимо этого, для рассылки спама злоумышленникам необходимы базы данных электронных адресов. Зачастую подобные базы продаются в Интернете, в них могут быть адреса пользователей, живущих на определенном континенте, в определенной стране или же представителей определенной профессии, пола, религиозного исповедания и т.д. Почти всегда спамеры стремятся избежать обнаружения, поэтому в комплект утилит, необходимых для рассылки спама, могут входить и анонимизаторы, а также VPN для доступа к панели управления спамботами.

Изготовление поддельных кредитных карт. Цена на изготовление карт варьируется от производителя к производителю и обходится в среднем в 150 долларов США за карточку, минимальный заказ составляет пять карт. Дополнительные расходы составляют 30$ за карту из белого пластика и 80$ за цветную печать на карте. Изготовитель гарантирует качество изготовления (упоминается качество печати 2800 dpi) и идентичность оригинальной карте, включая голограмму.

Курсы, семинары, обучение. Некоторые хакеры готовы не только осуществить противоправные действия, но и обучить этому других. В том числе есть возможность купить учебные пособия за 30 долларов США. Среди наиболее распространенных курсов и тренингов встречаются следующие: DDoS-атаки, рассылка спама, троянские программы, эксплойты и т.д.

Методы измерения и оценки ТЦЭ

Подавляющее число исследователей разделяют все методы измерения теневой “классической” экономики на прямые и косвенные. Прямые методы – это методы, основанные на информации, полученной при специальных опросах или наблюдениях за участвующими в теневой экономике (хотя бы на правах потребителя). Косвенные методы – это методы, основанные на анализе имеющихся сводных экономических показателей официальной статистики, финансовых органов, налоговых служб.

При оценке масштабов теневой “классической” экономики задачи, стоящие перед статистиками, отличаются от задач представителей налоговых и правоохранительных органов. Статистики оценивают масштабы нерегистрируемой экономики для осуществления в конечном итоге корректировки макроэкономических показателей и сведения к минимуму ошибок при их исчислении. Налоговые и правоохранитель-

ные органы, в свою очередь, должны оценить объемы недополученных в виде налогов доходов государства и попытаться их возвратить.

В случае отсутствия необходимой статистической информации, что характерно для теневой цифровой экономики, предпочтительнее сделать оценку, основанную на определенных допущениях, чем игнорировать вообще факт наличия теневой экономической деятельности в определенном секторе экономики. Вот почему макроэкономические оценки нерегистрируемой экономики во многих случаях носят приблизительный, вероятностный характер и не могут быть использованы для непосредственного выявления фактов теневой экономики на микроуровне.

Одной из сложных проблем в исследовании ТИЭ является разработка аппарата по оценке ее количественных параметров, поскольку возможности оценки масштабов достаточно ограничены в силу самого характера данного явления, предполагающего полное сокрытие. И, как следствие, для оценки используются различные методы, точность результатов которых зависит от соблюдения многих условий, в том числе и от исходной информации.

Прежде всего, необходимо проанализировать методы оценки “классической” теневой экономики. К их числу можно отнести следующие: метод специфических индикаторов, структурный метод, методы мягкого моделирования, экспертные методы, смешанные методы, специальные методы, методы бухгалтерского анализа, методы документального анализа, методы экономического анализа. Каждый из перечисленных методов необходимо проанализировать с точки зрения сути самого метода, преимуществ и недостатков, а также оптимальных условий применения. Например, метод специфических индикаторов использует один показатель, отражающий уровень экономической деятельности и получаемый прямым или косвенным способом, у которых имеются преимущества и недостатки. Необходимо формирование оптимальных условий применения данного метода к исследованию продуктов и услуг ТЦЭ. Кроме того, часть методов предназначена для работы с конкретными субъектами (например, предприятиями, разрабатывающими программные продукты), другая – для работы на макроуровне. Перечисленные особенности позволяют сделать предварительный вывод о том, что оценка ТЦЭ, независимо от выбранного метода, носит стохастический характер и в значительной степени субъективна.

Одним из перспективных направлений совершенствования методов оценки ТЦЭ, по нашему мнению, является использование когнитивного моделирования, как одного из эффективных подходов к исследованию слабоструктурированных систем и процессов. В данном случае

ТЦЭ представляется как набор факторов, процессов и явлений, описывающих с помощью причинно-следственной сети (когнитивной карты). Карта отражает субъективные представления группы экспертов о конкретном явлении, закономерностях, присущих предметной области.

Когнитивный анализ и моделирование влияния ТЦЭ необходимо реализовывать в следующей последовательности. Во-первых, выявление основных угроз и их влияния на безопасность страны. Во-вторых, построение когнитивной карты влияния ТЦЭ – определение основных факторов, характеризующих предметную область с выделением целевых факторов и выделение причинно-следственных связей влияния и взаимосвязи. В-третьих, собственно построение когнитивной карты с определением силы воздействия и взаимосвязи с проверкой модели на устойчивость и адекватность. В-четвертых, сценарное моделирование с определением возможного изменения факторов и сценариев изменения ситуации. И последнее, выбор направлений и мероприятий по реализации оптимального сценария.

В качестве основных факторов могут быть предложены следующие, с учетом необходимого выделения двух противоположных точек зрения и восприятия – защищающейся стороны (жертвы) и атакующей стороны:

• уровень дохода на душу населения. Наличие дешевого наемного труда из-за невысокой средней заработной платы, высокого уровня безработицы в развивающихся странах при условии значительной потенциальной прибыли в странах, являющихся целями атаки (экономически развитые страны). Данный фактор может послужить существенным компонентом высокой привлекательности и конечной прибыли;

• уровень информатизации общества, развитая инфраструктура – в общем случае обозначает наличие, уровень и качество доступа к информационным ресурсам, технологиям и системам. С точки зрения атакующей стороны, чем развитей инфраструктура, тем проще осуществить атаку, пользуясь различными векторами атаки, имея доступ к обширным технологическим, техническим и информационным ресурсам. С позиции жертвы обычно обширная и хорошо развитая инфраструктура свидетельствует о высоком уровне развития страны, а значит и наличия денежных средств у её граждан, что делает их более привлекательными целями для атаки;

• уровень образования. С позиции атакующей стороны высокий уровень образования обозначает углубленные знания и понимание работы программного и аппаратного обеспечения, а значит, возможность проведения комплексных и эффективных атак. С другой стороны, с позиции жертвы высокий уровень образования означает наличие сущест-

венных мер защиты, основанных на том же понимании принципов работы программного и аппаратного обеспечения. Помимо этого образование должно означать понимание того, как правильно вести себя в информационной среде, более ответственное отношение к персональным и корпоративным данным;

• уровень преступности в стране. Чем выше данный показатель в определенной стране, тем выше шанс найти индивида, согласного на информационное правонарушение, т.е. исполнителя.

Приведенные факторы во многом взаимосвязаны. Но необходимо сделать следующие допущения. В общем случае, атакующая сторона стремится выбрать наиболее выгодное (т.е. приносящее максимальную прибыль) соотношение перечисленных факторов. Таким образом, в идеальной для атакующей стороны ситуации исполнителем работы будут выступать граждане страны с развитой инфраструктурой, но низкой оплатой, а жертвой – граждане стран с развитой и стабильной экономикой, высокими доходами.

В заключение нельзя не отметить, что определение объемов ТЦЭ и конкретной экономической деятельности (например, такой как производство и продажа программных злоупотреблений, организация DDOS-атак и др.) в настоящее время, к сожалению, не проводится. Это можно объяснить как отсутствием соответствующих методик, так и соответствующей информационной базы, которая послужила бы основой для подобных расчетов.

Организованные криминальные группы в теневой цифровой экономике

Предпримем попытку рассмотрения, в первую очередь, связи традиционной “классической” организованной преступности с продуктами и услугами ТЦЭ. На вопрос – “Использует ли преступность информационные и коммуникационные технологии в своей деятельности?” - ответ будет положительным. Защищенные средства коммуникаций, цифровая подпись, стеганография, технологии отмывания преступных доходов – все это далеко не полный перечень используемых информационных и коммуникационных технологий. Кроме того, именно представители данных групп являются первыми покупателями и распространителями продуктов и услуг ТЦЭ.

Противостояние между криминальной экономикой и правоохранительными органами в области информационных и коммуникационных технологий началось со смены парадигмы – когда действия одиночек были направлены на извлечение прибыли в результате разработки

специальных программ, компьютерных манипуляций и т.д. Появление на ранних этапах зловредных и разрушающих программных злоупотреблений привело к формированию рынка компьютерных вирусов, червей, троянских коней, репликаторов и т.д. С расширением научной базы исследований стали появляться комплексные механизмы воздействия на ресурсы информационных систем криминальной направленности (например, концепция GRID-систем переросла в концепцию создания бот-систем). Постепенно происходило переливание новых знаний в области организации информационно-вычислительного обслуживания в среду криминальной направленности. Некоторое влияние на данный процесс оказали специальные органы государственной власти, которые разрабатывали соответствующие механизмы воздействия в условиях противостояния между государствами.

Действенным примером использования информационных и коммуникационных технологий, системы SWIFT, судов различных уровней является операция, получившая название “Ландромат”, представленная на фиг. 6. Следует отметить, что подобная схема была реализована в Болгарии, Сербии, Прибалтийских странах, Украине, России и затронула Национальные и коммерческие банки, Правительства и судебную систему. Все это должно стать предметом углубленных исследований общественности и правоохранительных органов.

Фигура 6. Ландромат

Считаем возможным предложить для анализа новую схему организации ТИЭ с точки зрения криминальной направленности. Следует выделить несколько групп горизонтальной направленности: наука и научная деятельность, собственно разработчики, распространители криминальных продуктов и услуг, реализаторы криминальных действий (программ и услуг) в соответствии с требованиями заказчиков, дополнительные действия, обеспечивающие отмывание денежных средств и т.д.

Выделяются следующие виды финансово-ориентированных киберпреступлений: фишинг, кибервымогательство, финансовое мошенничество, киберпреступления, связанные с вторжением в личную жизнь, кража персональных данных, шпионаж, нарушение авторского права, спам, социальные и политически мотивированные киберпреступления, преступления на почве ненависти и домогательства, кибербуллинг, киберпреступления, связанные с недозволенными действиями, противозаконная порнография, груминг, распространение наркотиков и оружия и др.

Следует обратить внимание на последний отчет “Рынок преступных киберуслуг”, подготовленный Positive Technologies и “Актуальные киберугрозы. I квартал 2018 года”. Была дана оценка минимальной и средней стоимости различных инструментов и услуг, которые продаются на площадках DarkWeb. Так, например, взлом сайта с получением полного контроля над веб-приложением обойдется злоумышленнику всего в 150 $, а стоимость целевой атаки на организацию в зависимости от сложности может превысить 4500 $. Наиболее дорогим оказалось вредоносное программное обеспечение (ВПО) для проведения логических атак на банкоматы. Цены на подобное готовое вредоносное программное обеспечение этого класса начинаются от1500$.

На рынке преступных киберуслуг широко распространены криптомайнеры (20%), хакерские утилиты (19%), ВПО для создания ботнетов (14%), RAT (Remote Access Trojans, троянские программы для удаленного доступа) и трояны-вымогатели (доля каждого - 12%), а основным спросом закономерно пользуются услуги, связанные с разработкой и распространением ВПО (55%).

Проведенное исследование показало, что спрос на услуги по созданию ВПО на сегодняшний день превышает предложение в три раза, а по его распространению - в два раза. Такое положение дел позволяет говорить о востребованности среди киберпреступников новых инструментов, которые становятся все доступнее благодаря партнерским программам, сервисам по аренде ВПО и моделям распространения “как услуга”. Как сообщают эксперты, большая часть запросов на взлом в DarkWeb имеет отношение к поиску уязвимостей на сайтах (36%) и получению паролей от электронной почты (32%). Среди предлагаемых

услуг лидируют взлом учетных записей социальных сетей (33%) и электронной почты (33%). Аналитики Positive Technologies связывают эти данные с желанием одних людей получить доступ к переписке других. С другой стороны, эти взломы меньше других требуют от атакующего каких-либо технических навыков.

В соответствии с Глобальным прогнозом (medium.com) ожидается, что размер рынка кибербезопасности вырастет с 137,85 млрд. в 2017 году до 231,94 млрд. дол. США к 2022 году, а нехватка рабочих мест в области кибербезопасности - одна из самых серьезных проблем, с которыми будут сталкиваться предприятия. Основные характеристики приведены в следующей таблице.

Таблица 11

Размер рынка кибербезопасности к 2022 году (mnmks.com)

	Min	**Max**	**CAGR**
Segments "Cyber Security":			
Managed Detection and Response Market	419.7 Million in 2017	1,658.0 Million by 2022	31.6%
Runtime Application Self-Protection Market	294.7 Million in 2017	1,240.1 Million by 2022	33.3%
Segments "Network Security":			
Software-Defined Perimeter (SDP) Market	992.8 Million in 2016	4,396.1 Million by 2021	34.7%
Managed Detection and Response Market	419.7 Million in 2017	1,658.0 Million by 2022	31.6%
Segments "Analytics":			
Enterprise AI Market	845.4 Million in 2017	6,141.5 Million by 2022	48.7%
User and Entity Behavior Analytics Market	131.7 Million in 2016	908.3 Million by 2021	47.1%
Artificial Intelligence in Healthcare Market	667.1 million in 2016	7,988.8 million by 2022	52.68%
Segments "Data Centre & Networking":			
Software-Defined Networking and Network Function Virtualization Market	3.68 Billion in 2017	54.41 Billion by 2022	71.4%
Software-Defined Wide Area Network (SD-WAN) Market	738.9 Million in 2016	9,066.2 Million by 2021	65.11%

SDN Orchestration Market	214.7 Million in 2017	4,458.5 Million by 2022	83.4%
Segments “Mobility & Telecom”:			
Virtualized Evolved Packet Core (vEPC) Market	968.9 million in 2017	7,975.3 million by 2022	52.4%
Low Power Wide Area Network Market	1.01 Billion in 2016	24.46 Billion by 2021,	89.3%
Network Transformation Market	6.01 Billion in 2017	66.86 Billion by 2022	61.9%
Segments “Cloud Computing”:			
Disaster Recovery as a Service Market	2.19 Billion in 2017	12.54 Billion by 2022	41.8%
Personal Cloud Market	12.02 Billion in 2015	80.02 Billion by 2020	46.1%
Cloud/Mobile Backend as a Service (BaaS) Market	1.32 Billion in 2015	28.10 Billion by 2020	84.2%
Segments “Software & Services”:			
Blockchain Market	411.5 Million in 2017	7,683.7 Million by 2022	79.6%
Blockchain Government Market	162.0 Million in 2018	3,458.8 Million by 2023	84.5%
3D Mapping and 3D Modeling Market	1.90 Billion in 2015	16.99 Billion by 2020	55.0%
Segments “Application Security”:			
Managed Detection and Response Market	419.7 Million in 2017	1,658.0 Million by 2022	31.6%
Runtime Application Self-Protection Market	294.7 Million in 2017	1,240.1 Million by 2022	33.3%
Рассчитано авторами на основании источника: https://www.mnmks.com /subscribers/mnm/industry_trends/cyber_security?isguest=true			

Заключение

Представленный материал не исчерпывает всего многообразия проблем подпольного рынка информационных технологий и теневой цифровой экономики. Поставленная задача – рассмотрение экономики теневого рынка информационных и коммуникационных технологий может считаться выполненной только при условии комплексного исследо-

вания всех сегментов, начиная от анализа действий, способствующих поиску уязвимостей в программном обеспечении, организации атак на информационные ресурсы государственных и коммерческих систем, до формирования условий функционирования кибертерроризма.

Следует отметить, что теневая цифровая экономика представляет собой совокупность рынков информационных и коммуникационных технологий, обладает высоким интеллектуальным потенциалом, большим количеством материальных и финансовых средств и огромными экономическими возможностями. По своей структуре рынки неоднородны как с точки зрения объемов, так и перспектив нанесения ущерба личности, обществу и государству.

В результате выполненного обзора и сравнительного анализа современного состояния проблем теневой экономики в сфере информационных технологий подтверждена актуальность поставленной цели исследования, а также сформулированы направления дальнейшей работы. Практическая значимость полученных результатов обусловлена разработкой конкретных мер и практических рекомендаций в сфере противодействия теневой цифровой экономике. Сделаны следующие выводы.

На основании проведенного сравнительного анализа публикаций по данной теме выявлено серьезное противоречие, состоящее в том, что, с одной стороны, существуют объективные предпосылки роста зависимости личности, общества и государства от процессов оцифровки и информационных технологий. С другой стороны, отсутствуют готовые решения (в первую очередь такие, как законодательное обеспечение) и экономико-экономические модели по противостоянию угрозам теневой цифровой экономики.

Цифровая экономика несёт с собой новые вызовы и угрозы, которые напрямую связаны с расширением области применения цифровых технологий и распространением ее, в первую очередь, на физических лиц. В их числе выделяются следующие: снижаются возможности контроля цифровых сервисов и увеличиваются возможности для реализации широкого спектра противозаконных действий; повышаются риски утечек информации, влияния на работу оборудования (например, бытовые приборы, кардиостимуляторы и др.); появляются совершенно новые угрозы, связанные с взрывным ростом значимости социальных сетей в жизни общества и развитием технологии Интернета вещей (IoT).

Ответом на эти угрозы должна стать подготовка квалифицированных специалистов и общества в целом к разработке, осознанному и законному использованию средств и методов цифровой экономики. Основными задачами подготовки кадров в области информационной безопасности являются: постоянно, в соответствии с изменяющимися

запросами общества и профессиональных организаций, требованиями законодательства, совершенствовать подготовку кадров в области информационной безопасности; дифференцировать направления подготовки в соответствии с характером деятельности специалистов различных профилей; интегрировать усилия различных организаций и ведущих специалистов в области образования, информационных технологий и защиты информации; использовать различные формы обучения, привлекая к обучению все слои общества.

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 возможным предложить разработку целостной стратегии противодействия теневой цифровой экономике. Основополагающими принципами этой стратегии могут стать: совершенствование законодательной базы экономического регулирования, нацеленного на создание условий, при которых сокрытие определенных 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; создание рабочих мест, реформирование системы налогообложения с целью ужесточения мер борьбы с отмыванием денег, а также ожесточение борьбы с коррупцией; совершенствовать систему подготовки кадров, способных противостоять явлениям теневой цифровой экономики; расширить базу теоретических исследований и практических разработок, нацеленных на новые группы угроз, в том числе связанных с Интернетом вещей, направленных на медицинское оборудование, криптоманией и др.

Список источников

Ablon, L. *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.*

Berr, J. *“WannaCry” ransomware attack losses could reach $4 billion.*

CheckPoint. *The Check Point 2017. Global Threat Intelligence Trends Report.*

DELL SecureWorks. *The Underground Hacker Markets are Booming with Counterfeit Documents, Premiere Credit Cards, Hacker Tutorials and*

100% Satisfaction Guarantees. eurasiangroup.org. *Киберпреступность и отмывание денег.*

Fiirstenau, D., & Hannes, R. *Shadow IT Systems: Discerning the Good and the Evil.*

Fiirstenau, D., Sandner, M., & Anapliotis, D. *Why do Shadow Systems Fail? An Expert Study on Determinants of Discontinuation.*

Garza, G. *Top 10 worst computer viruses.*

Gaspareniene, L., Remeikiene, R., & Scneider, F. *The factors of digital shadow consumption.*

Goodman, M. *Future Crimes. Inside the Digital Undergraund and the Battle for Our Connected World. .*

ic3.gov. *2016 Internet Crime Report. .*

Infowatch. *Infowatch: Число утечек данных в России приблизилось к численности населения.*

Kaspersky. *Тайный майнинг на ваших серверах. .*

Kshetri, N. *The simple economics of cybercrimes.*

Leszek F. Korzeniowski. *SECURITOLOGIA. Nauka o bezpieczeństwie człowieka i organizacji społecznych.*

Lewis, J. *Economic Impact of Cybercrime - No Slowing Down. .*

Mallmann, G., Macada, A., & Oliveira, M. *Can Shadow IT Facilitate Knowledge Sharing in Organizations? An Exploratory Study.*

McAfee. *Economic Impact of Cybercrime—No Slowing Down.*

medium.com. *How to Make More Money as a Cybersecurity Expert.*

Microsoft. *Every Employee Is a Digital Employee. .*

mnmks.com.

Ponemone. *Cost Of Cyber Crime Study. 2018. Insights On The Security Investments That Make A Difference. .*

ptsecurity.com. *Актуальные киберугрозы -2017.Тренды и прогнозы.*

Schneider, F. *Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime and Terrorism?*

Sennholz , H. *The Underground Economy.*

Shumarova, E., & Swatman, P. *Informal eCollaboration Channels: Shedding Light on "Shadow ICT".*

Silic, M., & Back, A. *Shadow IT - a view from behind the curtain.*

Sjouwerman, S. *Cyberheist: The biggest financial threat facing American businesses.*

Smith, P. *Assessing the Size of the Underground Economy: The Canadian Statistical Perspectives.*

Trendmicro. *Ransomware. Past, Present, and Future. Technical Marketing Team. .*

Weforum. *The Global Risks Report 2018. 13th Edition.*

Zimmermann, S., & Rentrop, C. *On the Emergence of Shadow IT - a Transaction Cost-based Approach.*

Акинин, А. *Shadow IT. Всем выйти из тени!* .

Барсукова, С. *Неформальная экономика: экономико-социологический анализ.*

Бортэ, Г. *Анализ этапов развития теневой информационной экономики.*

Бортэ, Г. *Исторические предпосылки развития теневой информационной экономики.*

Всемирный банк. *Доклад о мировом развитии 2016 "Цифровые дивиденды".*

Даннинг, Т. Д. Retrieved from https://citaty.info/quote/419668

Колесников, С. *Теневая экономика: как её считать.*

Орешкина, Д. *Shadow IT в вашей сети.*

Орлов, А. *Аристотель и неформальная информационная экономика будущего.*

Орлов, И. *Проблемы методологии государственной политики и управления в неформальной информационной экономике будущего.*

Охрименко, С., & Бортэ, Г. *Исследование характеристик теневой информационной экономики.*

Охрименко, С., & Бортэ, Г. *Теневая информационная экономика.*

Охрименко, С., Саркисян, А., & Бортэ, Г. *Противостояние в информационной сфере.*

Толкачева, С. *Промышленная политика в эпоху цифровой трансформации экономики.*

Чернышенко, И. *Победа над кибервымогательством!*

ТЕНЬ ЦИФРОВОЙ ЭКОНОМИКИ

Сергей Охрименко
Доктор экономических наук, профессор Лаборатория "Информационная безопасность" Молдавская Экономическая Академия

Григорий Бортэ
Докторант Лаборатория "Информационная безопасность" Молдавская Экономическая Академия

Резюме

Обсуждается новое направление научных исследований, связанных с выделением нового сегмента теневой экономики – теневая экономика в сфере использования информационных и коммуникационных технологий или теневая цифровая экономика. Поставлена задача формирования научного представления об основных тенденциях, направлениях и перспективах развития мирового рынка продуктов и услуг криминальной направленности в условиях глобализации.

В основу выполненного обзора и сравнительного анализа положены отчеты и доступные статистические материалы известных мировых исследовательских центров, чья деятельность связана с исследованиями проблем информационной безопасности и противостоянием киберпреступности. Проведен анализ современных информационных угроз личности, обществу и государству, которые вошли в рейтинг глобальных рисков. Проанализирован большой объем статистических данных, характеризующих такие аспекты теневой цифровой экономики, как активность киберпреступников, региональное распределение киберпреступности, ущерб от известных компьютерных инцидентов. Выявлен устойчивый рост не только количественных показателей, но и качественных (стоимостных) характеристик киберпреступлений.

Основное внимание уделено разработке и определению категории "теневая цифровая экономика", ее структуре и генезису, с выделением таких составных частей, как "теневые информационные технологии", "теневые информационные системы" и "теневая цифровая экономика". Проведен всесторонний анализ эволюции термина "теневая цифровая экономика" с выделением пяти основных подходов: юридического, математического, социально-психологического, организационно-управленческого и экономико-финансового. Рассмотрена рыночная сегментация с выделением продуктов и услуг. Выделен криминальный фактор производства продуктов и услуг. Предложена новая классификация программных продуктов и информационных услуг криминальной направленности. Проведено выделение группы "перспективных" услуг, способных нанести непоправимый и существенный вред государственным и коммерческим информационным системам. Проведен анализ методов измерения и подходов к оценке уровня теневой цифровой экономики, определены основные факторы, оказывающие влияние на них. Определен уровень поддержки теневой цифровой экономики со стороны организованных криминальных групп и сделан вывод о стимулировании разработки и многократном превышении с их стороны спроса на соответствующие продукты и услуги. Результаты данного исследования могут послужить основой для прогнозов и эффективной борьбы и противостояния проявлениям теневой цифровой экономики.

Ключевые слова: информационная и цифровая экономика, информационная безопасность, криминальные продукты и услуги, теневая цифровая экономика.

JEL: A22, D82, E26, M48, P5.

СЯНКАТА НА ЦИФРОВАТА ИКОНОМИКА

Сергей Охрименко
Доктор на икономическите науки, професор Лаборатория "Информационна безопасност" Молдавска Икономическа Академия

Григорий Борте
Докторант Лаборатория "Информационна безопасност" Молдавска Икономическа Академия

Резюме

Обсъжда се едно ново направление в научните изследвания, свързани с обособяването на нов сегмент в сенчестата икономика, а именно сенчеста икономика в сферата на използване на информационните и комуникационните технологии или сенчеста цифрова икономика. Поставя се задачата да се формира научна представа за основните тенденции, направления и перспективи за развитие на световния пазар на продукти и услуги с криминална насоченост в условията на глобализация.

В основата на направения обзор и сравнителен анализ лежат отчети и достъпни статистически материали на известни световни изследователски центрове, чиято дейност е свързана с изследване проблемите на информационната безопасност и противопоставяне на киберпрестъпността. Извършен е анализ на съвременните информационни заплахи за личността, обществото и държавата, които влизат в рейтинга на глобалните рискове. Анализиран е голям обем статистически данни, характеризиращи такива аспекти на сенчестата цифрова икономика, като активност на киберпрестъпниците, регионално разпределение на киберпрестъпността, вреди от известни компютърни инциденти. Показан е устойчивият ръст не само на количествените показатели, но и на качествените (стойностни) характеристики на киберпрестъпленията.

Специално внимание се обръща на разработването и определянето на категорията "сенчеста цифрова икономика", нейната структура и генезис, с обособяването на такива съставни части, като "сенчести информационни технологии", "сенчести информационни системи" и "сенчеста цифрова икономика". Извършен е всестранен анализ на еволюцията на термина "сенчеста цифрова икономика", като са очертани пет основни подхода: юридически, математически, социално-психологически, организационно-управленчески и икономическо-финансов. Разгледана е пазарната сегментация с обособяването на продукти и услуги. Изтъква се криминалният фактор за производство на продукти и услуги. Предлага се нова класификация на програмните продукти и информационни услуги с криминална насоченост. Обособява се група "перспективни" услуги, които могат да нанесат непоправима и съществена вреда на държавните и търговските информационни системи. Извършен е анализ на методите за измерване и подходите за оценка на нивото на сенчестата цифрова икономика, определени са основните фактори, които им влияят. Установено е нивото на подкрепа на сенчестата цифрова икономика от организираните криминални групи и е направен извода, че от тяхна страна се стимулира разработването и многократно се увеличава търсенето на съответните продукти и услуги. Резултатите от настоящото изследване могат да послужат като основа за прогнози, ефективна борба и противопоставяне на проявите на сенчестата цифрова икономика.

Ключови думи: информационна и цифрова икономика, информационна безопасност, криминални продукти и услуги, сенчеста цифрова икономика.

JEL: A22, D82, E26, M48, P5.

THE SHADOW OF DIGITAL ECONOMICS

Serghei Ohrimenco
Doctor of Science in economics, professor at "Information Security" laboratory
Academy of Economic Studies of Moldova

Grigori Borta
PhD student at "Information Security" laboratory
Academy of Economic Studies of Moldova

Abstract

A new direction of scientific research related to outlining a new segment of the shadow economics is discussed: the shadow economics in the domain of information and communication technologies or the shadow digital economics. The task is to form a scientific understanding of the main trends, directions and prospects of the development of the global market for criminal products and services in the context of globalization.The review and comparative analysis is based on reports and available statistical materials from well-known global research centers, whose activities are related to research on information security problems and struggling against cybercrime. An analysis of modern information threats to the individual, society and the state, which are included in the global risk rating, is carried out. A large amount of statistical data characterizing certain aspects of shadow digital economics such as activities of cybercriminals, regional distribution of cybercrime, and damage from known computer incidents have been analyzed. The steady growth of not only quantitative indicators, but also qualitative characteristics of cybercrime has been revealed.

Great attention has been paid to the development and definition of the category of "shadow digital economics", its structure and genesis, with the identification of such components as "shadow information technologies", "shadow information systems" and "shadow digital economics". A comprehensive analysis of the evolution of the term "shadow digital economics" has been carried out, with five main approaches: legal, mathematical, socio-psychological, organizational, managerial, economic and financial. Market structure is analyzed with the segmentation of products and services. The criminal factor of products and services industry is singled out. A new classification of software products and information services of a criminal nature is proposed. A selection of a group of "prospective" services that can cause irreparable and significant harm to the state and commercial information systems has been carried out. An analysis of measurement methods and approaches to assessing the level of the shadow digital economics is carried out, the main factors influencing them are determined. The level of support for the shadow digital economics by organized criminal groups has been determined, and a conclusion has been drawn about the stimulation of development and their excess of demand for relevant products and services. The results of this study can serve as a basis for predictions, effective struggle and confronting the manifestations of the shadow digital economy.

Keywords*:* information economics, information security, digital economics, underground economics.

JEL: A22, D82, E26, M48, P5.

Съдържание

СЪДЪРЖАНИЕ

TABLE OF CONTENTS

Годишник на СА "Д. А. Ценов" – Свищов
5250 Свищов, ул. "Ем. Чакъров" № 2
www.*uni-svishtov.bg/godishnik*

Начин на цитиране: Годишник/СА "Д. А. Ценов"

За контакти:
Проф. д-р Маргарита Богданова – главен редактор
☏ 0631/66297, e-mail: m.bogdanova@uni-svishtov.bg
Ивелина Станева – технически секретар
☏ 0631/66364, e-mail: i.staneva@uni-svishtov.bg

ISSN 0861-8054

Year-book of D. A. Tsenov Academy of Economics – Svishtov

2 Em Chakarov str., 5250 Svishtov
www.*uni-svishtov.bg/godishnik*

Reference: Yearbook/D. A. Tsenov Academy of Economics

Contact persons:
Prof. Margarita Bogdanova, PhD – Editor-in-chief
☏ 0631/66297, e-mail: m.bogdanova@uni-svishtov.bg
Ivelina Staneva – Technical Secretary
☏ 0631/66364, e-mail: i.staneva@uni-svishtov.bg

ISSN 0861-8054

СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ”
Свищов, ул. Ем. Чакъров, 2

АКАДЕМИЧНО ИЗДАТЕЛСТВО „ЦЕНОВ”
Свищов, ул. Градево, 24

ГОДИШНИК
ТОМ CXXI

Даден за печат на 19.11.2018 г.
Печатни коли 40,5; формат 16/70/100; тираж 100 бр.
Излязъл от печат на 20.12.2018 г.

ISSN 0861–8054