УДК: 33.330.101.5

В ТЕНИ ИНФОРМАЦИОННОЙ ЭКОНОМИКИ
IN THE SHADOW OF INFORMATION ECONOMCS
ÎN TENEBRU ECONOMIEI INFORMAȚIONALE

ОХРИМЕНКО Сергей, доктор хабилитат (д.э.н.), профессор,
Лаборатория информационной безопасности
Молдавская экономическая академия, Кишинэу
БОРТЭ Григорий, докторант
Молдавская экономическая академия, Кишинэу

OHRIMENCO Serghei, PhD, University Professor,
Security Laboratory
Academy of Economic Studies of Moldova (University), Chisinau
BORTA Grigorii, PhD student,
Academy of Economic Studies of Moldova (University), Chisinau

OHRIMENCO Serghei, doctor habilitat, profesor universitar
Laboratorul de securitate informaţională
Academia de Studii Economice a Moldovei, Chișinău
BORTĂ Grigorii, doctorand,
Academia de Studii Economice a Moldovei, Chișinău

***Аннотация**: Настоящая статья в качестве главной цели ставит рассмотрение процессов и условий, являющихся основой для формирования нового направления исследований – теневой информационной экономики (ТИЭ).*

***Annotation:** This paper aims at analyzing the processes and conditions that are the basis of forming of a new research direction – shadow information economics (SIE).*

***Ключевые слова**: теневая экономика, теневая информационная экономика, сегментация теневой информационной экономики, продукты и услуги, вредоносные программы, заказные услуги.*

***Keywords:** shadow economics, shadow information economics, segmentation of shadow information economics, goods and services, malicious software, service rental.*

Введение

Теневая экономика, возникшая во времена становления товарно-денежных отношений, семимильными шагами шествует по планете, не смотря на объявленные меры по ее искоренению. Информация, как объект притязаний, как предмет обмена, существует с давних пор и ее роль и актуальность 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 неправомерной деятельности по отношению к самой информации, процессам ее передачи по каналам связи, местам сосредоточения и хранения информационных ресурсов. Другими словами, добыча информации во всех ее формах, с помощью различных продуктов и услуг превратилась для группы предпринимателей в высокодоходный нелегальный бизнес.

Особую актуальность данная проблема приобретает в условиях построения цифрового общества.

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".

Можно предположить, что неправомерный бизнес, направленный на получение закрытой информации (например, информации составляющей государственную и 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 статья в качестве главной цели ставит рассмотрение процессов и условий, являющихся основой для формирования нового направления исследований – теневой информационной экономики (ТИЭ).

Материалы и методы исследования

Немного статистики

Многие авторы связывают незаконные действия в области информационных и коммуникационных технологий, являющиеся основой ТИЭ, с кибертерроризмом и возросшими рисками в управлении обществом. Для формирования общей картины считаем необходимым рассмотреть статистические данные, характеризующие некоторые виды деятельности, подпадающие под ТИЭ [2; 4; 5; 7; 11; 12; 13; 20].

В отчете «The Global Risks Report 2018» [36], 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 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.

Заслуживает внимания статистика активности киберпреступников, приведенная в Таблице 1.

Таблица 1. Предполагаемая активность киберпреступности в 2017 году [23]

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

Дж. Льюис приводит региональное распределение киберпреступности по регионам (данные Таблицы 2)

Таблица 2. Региональное распределение киберпреступности в 2017 году [23]

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

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

Таблица 3. Ущерб от инцидентов в области теневой информационной экономики [8; 17]

Год	Инцидент	Ущерб (доллары США)
1998	Эпидемия вируса CIH	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.

Данные, приведенные в Таблице 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 и практика свидетельствует о сокрытии ущерба компьютерными фирмами из-за нежелания оглашать действительные цифры потерь.

В Таблице 4 приведены данные, характеризующие основные типы компьютерных преступлений, совершенных в США [3]. 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.

Таблица 4. Основные типы компьютерных преступлений в США, 2016 год
[составлено авторами на основе изученного статистического материала]

№	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

Компания Trend Micro представила краткое содержание и основные выводы отчета «Программы-вымогатели: прошлое, настоящее и будущее» (Ransomware: Past, Present, and Future) [28]:

- за 2016 г. количество семейств программ-вымогателей выросло на 752%;
- средняя сумма выкупа за возвращение доступа к файлам составила 0,5−5 биткоинов;
- киберпреступники заработали в 2016 году на вымогателях $1 млрд.

Результаты и обсуждения

Одновременно с ростом количества используемых программ-вымогателей растет количество случаев атак на банкоматы (АТМ) с целью завладения денежными средствами. Эту криминальную область деятельности ТИЭ характеризуют данные, приведенные в Таблице 5.

Таблица 5. Статистика атак на банкоматы

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

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 4% от мирового объема утечек информации [22].

Следует отметить, что относительно недавно появились данные, характеризующие услуги по превращению результатов деятельности лиц и групп, в «звонкую монету» (т.е. монитизация). Характерным примером монетизации работы программы-шифровальщика Spora (программы-вымогателя – ransomware), выявленной в августе 2017 года, являются данные, приведенные в докладе Чернышенко И. на конференции “IT@ Security Forum”. Перечень услуг программы включает [59]:

- 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.

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 информационных 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 указанных 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 банки предоставляют информацию, что были попытки взлома их электронных платежных систем [47].

Следует иметь в виду, что приведенные статистические данные не исчерпывают всего разнообразия оценок, используемых для характеристики такого сложного явления, каким является ТИЭ. Для формирования полной и комплексной картины следует использовать отечественные и зарубежные научные публикации [1; 9; 18; 21; 24; 29; 30; 45; 50; 58], материалы ЮНЕСКО, ООН, МВФ, отчеты таких специализированных 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.

Определения теневой информационной экономики (ТИЭ)

«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 не выхода 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, запрещенная 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.

Теневая экономика во многих странах является важным объектом экономических исследований. 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 контактах между ними и дополняющая или заменяющая официально установленный порядок организации и реализации экономических связей.

Рассмотрим структуру ТИЭ. Начнем со следующей логической цепочки:

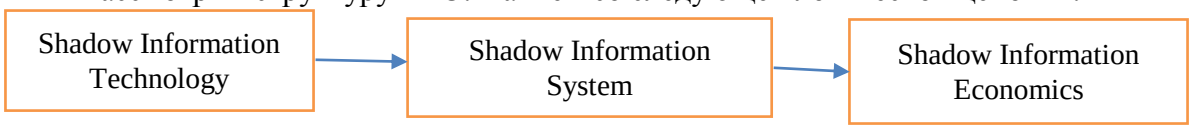

Рисунок 1. Структура ТИЭ [составлено авторами]

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» [51].
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 [33].
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 [37].
4. Shadow IT – определяется как набор ИТ-инструментов, используемых для выполнения ИТ-функций, но не являющихся частью основной ИТ-организации [32].
5. Мы определяем Shadow IT как любое ИТ-решение, используемое сотрудниками для выполнения своих рабочих задач без одобрения и официальной поддержки ИТ-отдела [26].
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 [38].
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 [14].
8. Shadow IT становится 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 [15].

9. Термин «теневые системы» относится к автономным программным решениям или расширениям существующих решений, которые не разрабатываются и не контролируются центральным ИТ-отделом [16].

Как видно из приведенных определений, «Shadow IT» не всегда воспринимается как отрицательное явление.

Эволюция терминологии и используемые определения ТИЭ приведены ниже:

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), они радикально отличаются по своей роли в обществе [31].
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. [49].
3. «Рыночное производство товаров и услуг, законных или незаконных, которое не включено в официальные оценки ВВП» [34].
4. Примеры киберпреступлений включают атаки типа отказ в обслуживании, киберкражы, 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. 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) [25].
6. Перспективные организационно-экономические механизмы управления производственно-хозяйственной деятельностью предлагаем конструировать на основе неформальной информационной экономики будущего (НИЭБ), разрабатываемой как методологическая основа конкретных исследований в области организационно-экономического моделирования [39].
7. 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 [52].
8. Под «теневой информационной экономикой» следует понимать индивидуальную или коллективную противоправную деятельность, связанную с проектированием, производством, распространением, поддержкой и использованием компонент информационно-коммуникационных технологий. Другими словами – это криминальные информационные продукты, услуги и процессы, основанные на ИТ или использующие ИТ [55].
9. Под теневой информационной экономикой мы понимаем деятельность, связанную с исследованием, поддержкой и использованием компонент информационных и коммуникационных технологий, скрываемую от общества и государства,

находящуюся вне государственного контроля и учета, а также, чаще всего, являющуюся противоправной [41].

10. Под теневой информационной экономикой следует понимать всю индивидуальную и коллективную деятельность, являющуюся незаконной, связанную с проектированием, разработкой, распространением, поддержкой и использованием компонент 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 [56].
11. Теневая информационная экономика - деятельность, связанная с исследованием, проектированием, производством, распространением, поддержкой и использованием компонент 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 [40].
12. Авторы статьи предлагают следующее определение ТИЭ – *это коллективная или индивидуальная деятельность, паразитирующая во всех сферах жизни общества, базирующаяся на использовании компонент 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)* [53].

Проведенный анализ подходов к определению ТИЭ позволяет выделить пять основных подходов к определению ТИЭ: 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 процессов монетизации.

Организационно-управленческий подход заключается в определении ТИЭ 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 технология. Экономико-финансовый подход рассматривает ТИЭ в качестве финансовых структур, отмывающих деньги посредством использования различных махинаций на легальном рынке товаров и услуг.

Сформулируем определение теневой информационной экономики (ТИЭ), основываясь на ее специфике с точки зрения производства продуктов и услуг, жизненного цикла производства и т.д. ТИЭ – 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 бот-нетов.

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» [по 44].

Следует отметить, что первое использование категории ТИЭ, отмечается в коллективной монографии под редакцией Гиляревского Р.С. [по 58]. Несколько иной подход используется в работе авторов Гаспарениене Л. и Р. Ремейкиене, основанный на процессах всеобщей цифровизации (дигитализации) экономики [19]. 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».

Авторы предлагают следующие подходы к определению ТИЭ [10; 41; 43; 54; 56]:

- ТИЭ – 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 компонент 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.

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 информационной экономики

Представляется необходимым рассмотреть и проанализировать сегментацию ТИЭ. Обобщенная структура предусматривает деление на продукты и услуги, с учетом постоянной изменчивости. 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 [46].

Предпримем попытку рассмотреть основные. К продуктам в сфере ТИЭ следует отнести:

1. Специализированное программное обеспечение (вредоносные программы). Структура вредоносных программ представлена на Рисунке 2 [35].
   Примеры известных вредоносных программ приведены в Таблице 6.

Таблица 6. Примеры известных вредоносных программ [разработано авторами на основании изученного материала - The Network Security Test Lab: A Step-by-Step Guide]

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

Год	Наименование	Тип	Метод распространения	Разработчик
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

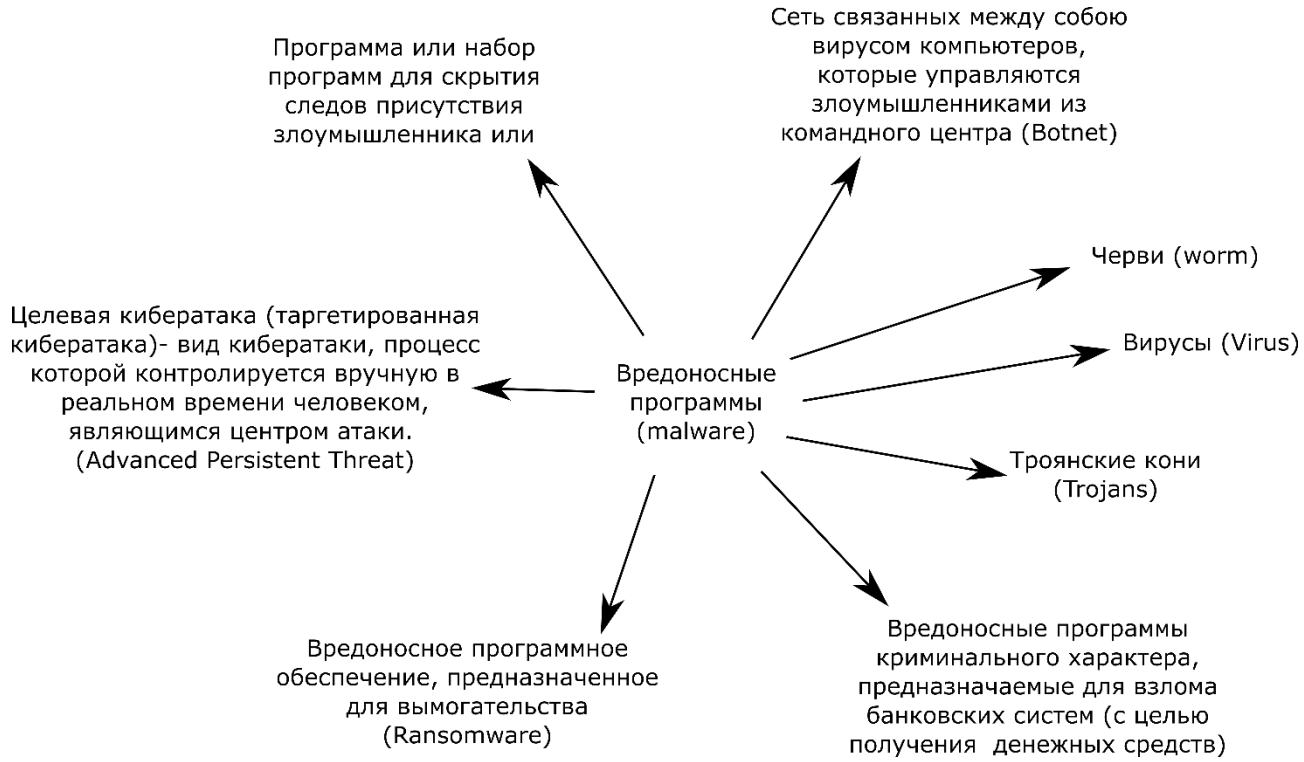

Рисунок 2. Структура вредоносных программ
[разработано авторами на основании изученного материала]

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 его на то согласия и без предоставления достаточного контроля над собираемыми данными.

Crimeware – термин, обозначающий программные продукты, нацеленные на автоматизацию кибер-преступлений. Например, кража сохраненных на компьютере жертвы паролей, скрытная установка шпионского программного обеспечения.

Компьютерные вирусы. Данная группа насчитывает достаточно много разновидностей программного обеспечения.

Генератор вредоносного программного обеспечения. Например, Zeus и SpyEye. Они являются наборами инструментов для создания узконаправленного вредоносного программного обеспечения и объединяют зараженные компьютеры в сеть.

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. 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, запуск определенных процессов, 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 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 отказоустойчивость систем распространения вредоносного программного обеспечения.

Криптолокер – вредоносная программа, 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.

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 может продаваться в свободном виде 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 компьютерами 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.

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.

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.

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.

Персональные данные. 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.

Отдельную группу образуют услуги, состав и структура которых постоянно изменяется. Рассмотрим наиболее яркие примеры:

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

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.

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 траффика. 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.

Создание и сдача в аренду ботнетов. На данный момент наиболее популярным набором инструментария для создания ботнетов являются Zeus и SpyEye. Оба набора предлагают модульную систему и предоставляют административную панель на основе вебинтерфейса.

DoS-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.

Спам. Многие из существующих ныне ботнетов, были специально спроектированы для рассылки спама. 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 желающим. 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.

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 (в источнике, приведенном в отчете, упоминается качество печати 2800 dpi) и идентичность оригинальной карте, включая голограмму.

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

Заказные услуги. Особое внимание следует уделить анализу новых заказных услуг, которые представляются в подпольной сети TOR индивидуальным пользователям и коллективным заказчикам. В их числе такие, как Cybercrime-as-a-Service, Research-as-a-Service, Crimeware-as-a-Service, Cybercrime Infrastructure-as-a-Service, Hacking-as-a-Service, Rent-a-Hacker.

Следует отметить, что рассмотренный перечень продуктов и услуг не является законченным и полным. Это объясняется динамическим развитием компонент информационных и коммуникационных технологий.

Выводы

В заключении, считаем возможным предложить разработку целостной стратегии противодействия теневой информационной экономике. Основополагающими принципами этой стратегии могут являться:

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 информационной экономики.

Создание рабочих мест, реформирование системы налогообложения, с целью ужесточения мер борьбы с отмыванием денег, а также ожесточение борьбы с коррупцией.

Следует полностью исключить элемент стихийности в процессах выработки стратегии.

Библиография

1. 2013 Cyber Attacks Statistics. https://www.hackmageddon.com/2013/07/21/june-2013-cyber-attacks-statistics/
2. 2015 Cost of Cyber Crime Study: Global Benchmark Study of Global Companies. http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf
3. 2016 Internet Crime Report. https://pdf.ic3.gov/2016_IC3Report.pdf
4. 2016: Current State of Cybercrime. https://www.rsa.com/content/_dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf
5. 2017 Cyber Attack Trends and New Global Cyber Threats. https://pages.checkpoint.com/global-cyber-attack-trends-2017.html?utm_source=research&utm_medium=cp-website&utm_campaign=CM_WR_18Q1_WW_Threat_Intelligence_Trends_Report_2017_H2
6. 2017 Cybercrime Report. https://cybersecurityventures.com/2015-wp/wp-content/_uploads/2017/10/2017-Cybercrime-Report.pdf
7. Adjusting the Lens on Economic Crime. https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf
8. Berr J. "WannaCry" ransomware attack losses could reach $4 billion. http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/
9. Bohme R. Vulnerability Markets. What is the economic value of a zero-day exploit? http://wi-web04.uni-muenster.de/security/publications/Boehme2005_22C3_VulnerabilityMarkets.pdf
10. Borta G. The Dark Side of Information Economics. In^ Economica. An. XXIII, nr2. (92), iunie 2015, ISSN 1810-9136, Academia De Studii Economice A Moldovei, Chisinau, Moldova, p. 97-102.
11. Comprehensive Study on Cybercrime. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
12. Cyber security. Report. Special Eurobarometer 423. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf
13. Cybercrimes/e-Crimes: Assessment Report. ITU 2012. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Assessment%20Cybercrimes.pdf
14. Every Employee Is a Digital Employee. https://blogs.msdn.microsoft.com/jmeier/2015/08/23/every-employee-is-a-digital-employee/

15. Fürstenau D., Hannes R. Shadow IT Systems: Discerning the Good and the Evil. https://www.researchgate.net/publication/262809695_Shadow_IT_Systems_Discerning_the_Good_and_the_Evil
16. Fürstenau D., Sandner M., Anapliotis D. Why do Shadow Systems Fail? An Expert Study on Determinants of Discontinuation. https://www.researchgate.net/publication/ 303682057 Why_Do_Shadow_Systems_Fail_An_Expert_Study_on_Determinants_of_Discontinuation
17. Garza G. Top 10 worst computer viruses. http://www.catalogs.com/info/travel-vacations/top-10-worst-computer-viruses.html
18. Gaspareniene L., Remeikiene R. Digital Shadow Economy: a Critical Review of the Literature. http://www.mcser.org/journal/index.php/mjss/article/view/8577
19. Gaspareniene L., Remeikiene R., Schneider F. G. The factors of digital shadow consumption. http://www.econ.jku.at/%5Cmembers%5CSchneider%5Cfiles%5Cpublications%5C2016%5CDigitalShadowConsumption.pdf
20. Hackmageddon. Information Security Timelines and Statistics https://www.hackmageddon.com
21. Hassan M., Schneider F. Size and Development of the Shadow Economies of 157 Worldwide Countries: Updated and New Measures from 1999 to 2013. Journal of Global Economics, 2016. http://www.econ.jku.at/members/Schneider/ files/publications/2016/SizeShadEc157countries_JOGE.pdf
22. Infowatch: Число утечек данных в России приблизилось к численности населения. Инфографика. http://safe.cnews.ru/news/line/2017-06-08_infowatch_chislo_utechek_dannyh_v_rossii_priblizilos
23. James Lewis. Economic Impact of Cybercrime - No Slowing Down. https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf
24. Krebs B. Crimeware Author Funds Exploit Buying Spree. Krebs on Security. http://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/
25. Kshetri N. The simple economics of cybercrimes. In: IEEE Security and Privacy, 2006, 4(1), p. 33–39.
26. Mallmann, G. L., Maçada, A. C. G., Oliveira, M. (2016). Can Shadow IT Facilitate Knowledge Sharing in Organizations? An Exploratory Study. Proceedings of the 17th European Conference on Knowledge Management, Belfast, North Ireland.
27. Markets for Cybercrime Tools and Stolen Data. https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf
28. Ransomware. Past, Present, and Future. Technical Marketing Team. https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf
29. Rentrop C., Zimmermann S. Shadow IT Evaluation Model. https://pdfs.semanticscholar.org/709d/36170b51bce651b15d0c5606b8124bc5fda6.pdf
30. Schneider F., Buehn A., Montenegro C. Shadow Economies All over the World. New Estimates for 162 Countries from 1999 to 2007. http://www.gfintegrity.org/storage/gfip/documents/reports/world_bank_shadow_economies_all_over_the_world.pdf
31. Sennholz Hans F. The Underground Economy. https://studfiles.net/preview/427430/page:2/
32. Shumarova E., Swatman Paul A. Informal eCollaboration Channels: Shedding Light on "Shadow CIT". https://pdfs.semanticscholar.org/90a9/6bff9201c382ad7db0f267c6a5195a90d365.pdf
33. Silic M., Back, A. Shadow IT – a view from behind the curtain. https://www.researchgate.net/publication/263284725_Shadow_IT_-_A_view_from_behind_the_curtain

34. Smith Ph. Assessing the Size of the Underground Economy: The Canadian Statistical Perspectives. Canadian Economic Observer. 1994. Catalogue No. 11-010, 3.16-33, at 3.18.
35. The Check Point 2017. Global Threat Intelligence Trends Report. https://blog.checkpoint.com/2018/01/31/check-point-2017-global-threat-intelligence-trends-report/
36. The Global Risks Report 2018. 13th Edition. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf
37. Zimmermann S., Rentrop C. On the Emergence of Shadow IT - a Transaction Cost-based Approach. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1199&context=ecis2014
38. Акинин Андрей. Shadow IT. Всем выйти из тени! https://journal.ib-bank.ru/post/610
39. Барсукова, С. Ю. Неформальная экономика: экономико-социологический анализ М.: Изд. дом ГУ ВШЭ, 2004. 448 с.
40. Бортэ Г. Анализ этапов развития теневой Информационной экономики. В: Conferinţa Internaţională, ediţia a X-a Jubiliară, 19 Aprilie 2013. с. 53-55.
41. Бортэ Г. Исторические предпосылки развития теневой информационной экономики. В: Системи Обробкі Інформаціі, 2012, №4(102), с. 12-14.
42. Бортэ Г. Теневая Информационная Экономика. В: Materialele Conferinței internaționale, Securitatea Informationala 2011. Ch.: ASEM, 2011, p.93-95.
43. Бортэ Г. Теневая Информационная Экономика. В: Годишен Алманах. Научни Изследвания на Докторанти, Болгария, Книга 5, 2012, с. 485-495.
44. Будущее российского рынка информационной безопасности. https://cyberleninka.ru/article/v/buduschee-rossiyskogo-rynka-informatsionnoy-bezopasnosti
45. Буров В. Исследование теневой экономики. http://eizvestia.isea.ru/pdf.aspx?id=13936
46. Вавренюк А.Б., Васильев Н.П., Вельмякина Е.В., Гуров Д.В., Иванов М.А., Матвейчиков И.В., Мацук Н.А., Михайлов Д.М., Шустова Л.И. Разрушающие программные воздействия. М.: НИЯУ МИФИ, 2011. 328 с.
47. Волков В. Генпрокуратура Молдовы: Мы предложим руководству страны создать специализированную прокуратуру по борьбе с киберпреступностью. https://digital.report/genprokuratura-moldovyi-predlozhit-rukovodstvu-sozdat-spetsprokuraturu-po-borbe-s-kiberprestupnostyu/
48. Классификация вредоносных программю Kasspersky Lab. http://docplayer.ru/43797247-Klassifikaciya-vredonosnyh-programm.html
49. Колесников С. Теневая экономика: как её считать. – 2001. http://www.bnews.narod.ru/economy/invest_ssftrrgg.htm
50. Латов В. Социальные функции теневой экономики в институциональном развитии постсоветской России. https://fdp.hse.ru/data/327/566/1238/avtoref_Latov.pdf
51. Орешкина Д. Shadow IT в вашей сети. http://bis-expert.ru/bdi_source/20/files/assets/basic-html/index.html#32
52. Орлов А.И. Аристотель и неформальная информационная экономика будущего. В: Biocosmology – NEO-ARISTOTELISM ,Vol.2Summer, 2012, p.150-164.
53. Охрименко С., Бортэ Г. Исследование характеристик теневой информационной экономики. В: Юбилейна научна конференция «Предизвикателства пред информационните технологии в контекста на „Хоризонт 2020”, 7 – 8 октомври 2016, с. 53-59.
54. Охрименко С., Бортэ Г. Обратная Сторона Информационного общества. Економічна та інформаційна безпека суб'єктів господарювання: сучасний стан і тенденції розвитку: монографія. Авт. кол.: ред. кол.: Т. С. Смовженко, А. Я. Кузнецова, О. І Барановський, О. М. Тридід, Г. М. Азаренкова та ін., К.: УБС НБУ, 2014, 386 с.

55. Охрименко С., Бортэ Г. Теневая информационная экономика. В: Партнерство кафедр ЮНЕСКО в области применения ИКТ в образовании.
56. Охрименко С., Саркисян А., Бортэ Г. Противостояние в информационной сфере. В: Revista militară, №1 (9) 2013, с. 53-61.
57. Панасенко А. Киберпреступники заработали в 2016 году на вымогателях $1 млрд. https://www.anti-malware.ru/news/2017-06-07/23111
58. Родионов И., Гиляревский Р., Цветкова В., Залаев З. Рынок информационных услуг и продуктов. М: МК-Пародика, 2002. 552 с.
59. Чернышенко И. Победа над кибервымогательством! http://www.itsecurityforum.ru/materials/pobeda-nad-kibervymogatelstvom/