ЭКОНОМИЧЕСКАЯ АКАДЕМИЯ РЕСПУБЛИКИ МОЛДОВА
КАФЕДРА «КИБЕРНЕТИКИ И ЭКОНОМИЧЕСКОЙ ИНФОРМАТИКИ»

На правах рукописи

УДК: 330.47

БОРТЭ ГРИГОРИЙ

ИССЛЕДОВАНИЕ ТЕНЕВОЙ ЭКОНОМИКИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

523.01 КИБЕРНЕТИКА И ЭКОНОМИЧЕСКАЯ ИНФОРМАТИКА

Диссертация доктора экономических наук

Научный руководитель: Охрименко Сергей Антонович
доктор хабилитат экономических наук, профессор университар

Автор:

КИШИНЁВ, 2018

ACADEMIA DE STUDII ECONOMICE A MOLDOVEI
CATEDRA "CIBERNETICĂ ŞI INFORMATICĂ ECONOMICĂ"

Cu titlu de manuscris

C.Z.U: 330.47

BORTĂ GRIGORI

CERCETAREA ECONOMIEI TENEBRE ÎN DOMENIUL TEHNOLOGIILOR INFORMAŢIONALE

523.01 CIBERNETICĂ ŞI INFORMATICĂ ECONOMICĂ

Teză de doctor în economie

Conducător științific: Ohrimenco Serghei

Doctor habilitat în economie,
profesor universitar

Autorul:

CHIŞINĂU, 2018

СОДЕРЖАНИЕ

АННОТАЦИЯ

Диссертационная работа «Теневая экономика в сфере информационных технологий» подготовлена Бортэ Григорием на соискание степени доктора экономических наук. Работа включает введение, три главы, выводы по главам, общие выводы и предложения, библиографию из 179 литературных источников, 2 приложения, 100 страниц текста, 40 рисунков, 11 таблиц, 10 формул. Результаты исследования были опубликованы в 21 научных работах в Республике Молдова и за рубежом.

Ключевые слова: теневая информационная экономика, теневые информационные технологии, информационная безопасность, теневая экономика, экономика информационных технологий, экономика информационной безопасности.

Областью исследования является феномен теневой информационной экономики (ТИЭ), охватывающий стадии жизненного цикла продуктов и услуг.

Решенная научная проблема заключается в формировании целостного взгляда на феномен ТИЭ в целом и его структуру в частности, что позволило предложить методологические и методические основы для его исследования.

Целью работы является рассмотрение феномена ТИЭ, определение базиса, структуры, рисков и ущерба.

Для достижения цели были поставлены и решены следующие **задачи**: исследована природа ТИЭ; исследована, определена и предложена структурная основа и состав её сегментов, продуктов и услуг, проведён их сравнительный анализ сквозь призму функций, причин появления и перспектив развития; построены модели элементов её прибыльности.

Научная новизна диссертации состоит в том, что разработаны и предложены методологические основы исследования ТИЭ; предложены определения категории ТИЭ; разработан оригинальный комплекс моделей структуры ТИЭ, включающий криминализированные товары и услуги в сфере информационных технологий; предложена классификация секторов ТИЭ, и проведена параллель со «светлыми» аналогами; предложена и описана секторальная структура ТИЭ; проанализирована эволюция ТИЭ; определены институциональные основы ТИЭ.

Результаты диссертационного исследования были положены в основу учебной программы и курса лекций по предмету «Теневая Информационная Экономика» в Молдавской Экономической Академии, а также были внедрены в Национальном Банке Республики Молдова и используются для оценки проектов по информационной безопасности, а также для обучения сотрудников. Предложенные методические подходы рекомендованы для использования в дальнейших исследованиях ТИЭ.

ADNOTARE

Teza de doctorat cu titlul "Economia tenebră în domeniul tehnologiilor informaționale", a fost elaborată de aspirantul la titlul de doctor în economie Bortă Grigori. Lucrarea include partea introductivă, trei capitole, concluzii pe capitole, concluzii generale și recomandări, bibliografia cu 179 de referințe, 1 anexă, 100 de pagini, 40 figuri, 11 tabele și 10 relații matematice. Rezultatele cercetărilor, cuprinse în disertație, au fost publicate în 21 de lucrări științifice și comunicări în cadrul diverselor conferințe naționale și internaționale.

Cuvinte-cheie: economia informațională tenebră (EIT), tehnologia informațională tenebră, securitatea informației, economia subterană/informală, economia tehnologiei informației, economia securității informațiilor.

Domeniul de cercetare al disertației îl constituie economia informațională tenebră, care cuprinde ciclul de viață al produselor și serviciilor.

Problema științifică importantă soluționată constă în formarea viziunii complete asupra fenomenului EIT în general și structura lui în particular, ce a permis propunerea bazele metodologice și metodice pentru cercetarea lui.

Obiectivul acestei lucrări rezidă în examinarea fenomenului economiei informaționale tenebre (EIT), determinarea bazei, structurii, riscurilor și daunelor provocate de aceasta.

În scopul realizării acestui obiectiv, au fost stabilite și soluționate un șir de probleme: cercetarea naturii EIT; cercetarea, identificarea și elaborarea bazei structurale și componenței segmentelor, produselor și serviciilor, precum și analiza comparativă prin intermediul funcțiilor, cauzelor și perspectivelor de dezvoltare; elaborarea modelului elementelor de profitabilitate.

Noutatea științifică a tezei constă în faptul că au fost dezvoltate și propuse bazele metodologice ale cercetării EIT; au fost definite categoriile EIT; s-a dezvoltat o gamă originală de modele ale structurii EIT, care cuprind bunuri și servicii infracționale, în domeniul tehnologiei informației; au fost clasificate sectoarelor EIT și trasate paralele cu omologiile "strălucite"; a fost elaborată și desfășurată structura sectorială a EIT; au fost analizate evoluția și tendințele EIT; a fost definit cadrul instituțional a EIT.

Rezultatele cercetării incluse în disertație sunt reflectate în procesul educațional din cadrul Academiei de Studii Economice a Moldovei, fiind plasate la baza elaborării curriculum-ului unui curs de prelegeri la disciplina "Economia informațională subterană", precum și implementate în activitățile Băncii Naționale a Republicii Moldova, și utilizate în scopul evaluării proiectelor de dezvoltare a domeniilor de securitate a informațiilor, și pentru perfecționarea personalului din domeniu. Abordările metodologice elaborate sunt recomandate pentru dezvoltarea în continuare a cercetărilor teoretice și aplicative a EIT.

ANNOTATION

Grigori Borta wrote this thesis paper titled "Shadow Economics in Information Technologies Domain", claiming the title of PhD in economics. The paper includes introduction, three chapters, conclusions for each chapter, general conclusions, bibliography of 179 sources, 1 annex, 100 pages of text, 40 figures, 11 tables, 10 formulae. The results of the thesis were published in 21 scientific papers and reports on national and international conferences.

Keywords: shadow information economics, shadow information technologies, information security, shadow economics, economics of information technologies, and economics of information security.

The domain of research comprises shadow information economics (SIE), encompassing the stages of products and services lifecycle.

Important solved problem is to form a holistic view of the phenomenon of SIE as a whole and its structure in particular, opening the possibility to offer methodological and methodological bases for its further study.

The aim of this work is analyzing the phenomenon of SIE, defining its basis, structure, risks, and damage.

The aim was achieved by solving the following **tasks**: research the nature of SIE; research and define the structural basis and the composition of its segments, products and services, perform their comparative analysis through the prism of functions, reasons of appearance, and development perspectives; build models of its profitability elements.

Scientific novelty of this paper is defined by the development and introduction of methodological basics of SIE research; three SIE category definitions are proposed; an original model complex was developed, describing SIE structure, including criminalized goods and services in the domain of information technologies; a classification of SIE sectors is proposed and a parallel with their "legal" analogues is drawn; SIE sectoral structure is proposed and described; SIE evolution is analyzed; SIE institutional bases are defined.

The results of this thesis paper were reflected in educational process at Academy of Economic Studies of Moldova, serving as the basis of "Shadow Information Economics" course. The results were also implemented at the National Bank of Moldova, helping in information security projects estimation, and in employees' education. Proposed methodological approaches are recommended for further theoretic and empiric researches of SIE.

СПИСОК АББРЕВИАТУР И СОКРАЩЕНИЙ

- CEO – Chief Executive Officer (англ. главный исполнительный директор)
- CERT/CC – Computer Emergency Response Team Coordination Center
- DDoS – Distributed Denial of Service (англ. распределенный отказ в обслуживании)
- DoS – Denial of Service (англ. отказ в обслуживании)
- PPI – Pay-per-Install (англ. оплата за установку)
- SQL – Structured query language (англ. язык структурированных запросов)
- VPN – Virtual private network (англ. виртуальная частная сеть)
- WWF – World Wide Fund for Nature (англ. Всемирный фонд природы)
- XSS – Cross-site scripting (англ. межсайтовый скриптинг)
- АО – аппаратное обеспечение
- ВВП – валовой внутренний продукт
- ЕС – Европейский Союз
- ИБ – информационная безопасность
- ИКТ – информационно-коммуникационные технологии
- ИТ – информационные технологии
- МВФ – Международный валютный фонд
- ООН – Организация объединенных наций
- ОС (OS) – операционная система (Operating System)
- ПО – программное обеспечение
- США – Соединенные Штаты Америки
- ТИЭ – теневая информационная экономика
- ТЭ – теневая экономика
- ФБР (FBI) – Федеральное бюро расследований (Federal Bureau of Investigation)

ВВЕДЕНИЕ

Актуальность темы. В данной работе впервые поднята проблема информационного сектора в общем контексте теневой экономики, впервые предложена методология и методики её исследования и анализа. Теневая экономика состоит из различных типов деятельности, целиком или частично не подчиняющихся общепринятым нормам жизни и законодательствам. Учитывая тот факт, что в современном мире существенная часть деятельности человека подходит под данное определение, значимость исследования теневой экономики становится очевидной.

Кроме того, актуальность работы определяется фактом малой изученности информационной составляющей теневой экономики. Глобализация экономики и рынков, как следствие стремительного развития информационных технологий и их повсеместного проникновения также являются важным фактором обоснования актуальности данного исследования.

Кроме практической применимости, необходимо подчеркнуть и научную актуальность. Она подтверждается тем, что большая часть информационных технологий, относимых к теневым, не попадает под действие существующего законодательства, в т. ч. уголовного кодекса и существует на частных договоренностях и контрактах. Совершенно очевидным является тот факт, что наличие теневой информационной экономики является существенным препятствием на пути формирования информационного общества и цифровой экономики.

Необходимость изучения теневой информационной экономики, её структуры и механизмов в различных аспектах обуславливает актуальность темы данной диссертационной работы.

Борьба с теневой экономикой в общем и её информационной составляющей в частности приведет к увеличению темпов роста малого и среднего бизнеса, и, как следствие, оздоровит экономику в целом.

Тема исследования предельно актуальна с учетом тех проблем и угроз, с которыми сталкивается на данный момент не только Республика Молдова, но и весь мир. Данная проблема будет в поле зрения и в краткосрочной, и в среднесрочной, и долгосрочной перспективах. В условиях промышленной революции 4.0, когда всё большую актуальность приобретают машинное обучение, большие данные, трехмерная печать, краудсорсинг и краудфандинг (коллективное финансирование на добровольных взносах), облачные технологии, проблема защиты от информационных угроз становится как никогда актуальной [28].

Объектом исследования является рынок продуктов и услуг в сфере ИКТ криминальной направленности.

Предмет исследования – механизм функционирования мирового рынка ТИЭ.

Цель и задачи исследования. Целью данной диссертационной работы является решение задачи формирования научного представления об основных тенденциях, направлениях и перспективах развития ТИЭ, мирового рынка продуктов и услуг криминальной направленности в условиях глобализации.

Для достижения данной цели предполагается решить следующие **задачи**:

1. Исследовать категорию теневой информационной экономики, в том числе факторы, влияющие на её уровень.
2. Определить концептуальные подходы к исследованию ТИЭ, как составной части мирового рынка ИТ.
3. Исследовать, определить и предложить структурную основу и состав сегментов теневой информационной экономики.
4. Определить институты теневой информационной экономики, их состав и спецификацию.
5. Провести сравнительный анализ сегментов теневой информационной экономики сквозь призму их функций, причин появления и перспектив развития.
6. Построить модели прибыльности элементов теневой информационной экономики.
7. Предложить возможные векторы противодействия преступлениям в области информационных технологий.

В процессе исследования были применены общенаучные подходы и **методы** научного познания, такие как анализ и синтез, историческое и логическое моделирование, качественный и количественный анализ, системный подход; экономико-статистические методы, такие как, сравнение, группировка и т.д.; экономико-математические методы, позволяющие установить и подробно описать взаимосвязь определенных факторов и их влияние на различные феномены.

Методологическую основу исследования составил категориальный аппарат экономической теории, институциональной теории, методы диалектики, экономико-статистические приемы, метод моделирования и сценарного подхода, принципы формальной логики, конкретно-исторический и системный подходы. Кроме того, важным элементом методологической основы работы является системный подход,

предполагающий исследование современного рынка теневых информационных продуктов в качестве сложной системы взаимодействующих между собой участников, акторов.

Научная новизна работы.

Научная новизна данного диссертационного исследования состоит в следующем:

1. Разработаны и предложены методологические основы исследования теневой информационной экономики.

2. Предложены определения категории теневой информационной экономики (общее, экономическое, технико-технологическое).

3. Разработан оригинальный комплекс моделей структуры теневой информационной экономики, включающий криминальные товары и услуги в сфере информационных технологий. Предложена сегментация секторов теневой информационной экономики, базирующаяся на структуре её «светлых» аналогов. Проанализирована и описана секторальная структура ТИЭ.

4. Продемонстрирована эволюция теневой информационной экономики как объекта исследования в контексте социально-экономических условий современности.

5. Определены институциональные основы теневой информационной экономики.

6. Разработаны методические основы моделей «эффективности» продуктов и услуг криминальной направленности.

7. Выявлены возможные инструменты противодействия преступлениям в сфере информационных технологий.

Теоретическая и практическая значимость исследования. Результаты данного диссертационного исследования используются в учебном процессе в Молдавской Экономической Академии, разработана учебная программа и прочитан курс лекций по предмету «Теневая Информационная Экономика». Помимо этого, результаты диссертационного исследования внедрены в Национальном Банке Республики Молдова, используются при разработке проектов развития отрасли информационной безопасности, в формировании стратегии информационной безопасности, а также для повышения квалификации и общего уровня осведомленности сотрудников. Кроме того, предложенные методические подходы могут быть использованы для дальнейшего развития теоретических и эмпирических исследований теневой информационной экономики и методов противостояния данному явлению. Основные положения диссертационного исследования вписываются в задачи, определенные национальной стратегией развития информационного общества «Цифровая Молдова 2020».

Степень разработанности научной проблемы. Теоретическими основами для анализа ТИЭ, ее влияния на развитие ИТ и мировой экономики стали работы ряда зарубежных учёных: Фридриха Шнейдера (Friedrich Schneider, Австрия), Райнера Бёма (Rainer Böhme, Германия), Брайана Кребса (Brian Krebs, США), Паоло Пассери (Paolo Passeri, Италия), Лигиты Гаспарениене (Ligita Gaspareniene, Литва), Риты Ремейкиене (Rita Remeikiene, Литва).

Ряд основополагающих проблем формирования «классической» ТЭ, её воздействие на глобализацию и бизнес был исследован в работах российских ученых: Ю. Латова, С. Колесникова, А. Барсуковой, Р. Гиляревского и других, а также в работах австрийского ученого Фридриха Шнейдера.

Информационную базу исследования составляют законодательная база и нормативно-правовые акты, постановления правительства Республики Молдова, так и других стран, монографии, научные публикации, 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.

Решенная научная проблема заключается в формировании целостного взгляда на феномен ТИЭ в целом и его структуру в частности, что позволило предложить методологические и методические основы для его исследования.

Апробация результатов работы. Результаты данного диссертационного исследования нашли отражение в главах двух коллективных монографий, изданных в Республике Польша и Украине, а также в 19-ти научных статьях, опубликованных в материалах международных конференций в Молдове, Болгарии, Украине, России и Польше, из которых две в рецензируемых научных журналах и 8 работ одного автора. Общий объем публикаций составил 4.76 авторских листа. Результаты данного исследования были доложены на следующих научных конференциях:

- 1st - 5th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education, 2011 - 2015, Университет национальной и мировой экономики, София, Болгария;
- ITSEC-2012, International Conference on Information Technologies and Security, Кишинев, Молдова, 15-16 октября 2012;
- Формирование Современного Информационного Общества – Проблемы, Перспективы, Инновационные Подходы, 5-10 сентября, 2012, Санкт-Петербург, Россия;
- Securitatea Informațională 2009 - 2015, Кишинев, Молдова, ASEM, 2009 - 2015.

Структура работы. Диссертация состоит из введения, трех глав, общих выводов и предложений, библиографии.

В первой главе анализируется текущая ситуация в области ТИЭ, предлагается ряд её определений, анализируются существующие методологии и методики оценки уровня ТИЭ, а также факторы, влияющие на формирование и её уровень.

Во второй главе рассматривается генезис ТИЭ, а также подробно анализируется структура продуктов и услуг в области ТИЭ и способы их монетизации.

В третьей главе рассматриваются проблемы противостояния ТИЭ и предлагаются две модели: модель доходности и модель денежных потоков в ТИЭ.

Основные положения диссертационной работы, выносимые на защиту:

1. Результаты исследования мировых тенденций развития ИКТ продуктов и услуг криминальной направленности
2. Впервые предложены определения теневой информационной экономики, основывающиеся на анализе существующих определений «классической» теневой экономики.
3. Анализ структуры теневой информационной экономики, в том числе состава продуктов и услуг, задействованных в данной сфере.
4. Модель процесса монетизации продуктов и услуг в сфере ТИЭ.
5. Генезис теневой информационной экономики. В том числе, выделение трех основных этапов в ее формировании на основе научного исследования и анализа хронологической последовательности.
6. Модель доходности ботнета, описывающая источники прибыли и затрат с точки зрения бот-мастера.
7. Модель денежных потоков в теневой информационной экономике, описывающая кругооборот денежных средств, а также действия основных игроков в данной области.

Ключевые слова: теневая информационная экономика, теневые информационные технологии, информационная безопасность, теневая экономика, экономика информационных технологий, экономика информационной безопасности.

1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ИССЛЕДОВАНИЯ ФЕНОМЕНА ТЕНЕВОЙ ИНФОРМАЦИОННОЙ ЭКОНОМИКИ

1.1. Концептуальные основы формирования теневой информационной экономики; актуальность проблемы теневой информационной экономики.

Явление теневой информационной экономики стало изучаться в 1930-х годах зарубежными учеными. Первые эмпирические исследования теневой экономики появились в начале 1970-ых годов. Они проводились под эгидой Всемирного банка и Международной организации труда. Термин «неформальный сектор экономики» был впервые предложен в этот же период Кейтом Хартом (Keith Hart), который изучал малый и средний бизнес в Гане и Кении. В 1977 году П.М. Гутманом была опубликована статья «Подпольная экономика», в которой автор анализировал проблемную ситуацию теневой экономики в развитых странах, особенно в США. Другим важным, по мнению автора, исследователем в области «классической» теневой экономики выступает перуанский ученый Эрнандо де Сото, который в своих трудах «Загадка капитала» и «Другой путь» показал значимость проблемы теневой экономики, а также продемонстрировал роль государства в её снижении. Ещё двумя важными работами стали «Теория прав собственности» Р. Кроуза и «Преступление и наказание: экономический подход» Беккера. Первым исследователем проблемы, охватившим в своей работе 145 стран, был австрийский экономист Фридрих Шнайдер. В работе был сделан вывод о том, что в развивающихся странах теневой сектор проявляет тенденцию к расширению, в то время как в развитых – к сокращению. На территории стран СНГ первые исследования начали проводиться в 1980-ые годы, и доля теневого сектора была оценена в 9-10 % от ВВП. Важно отметить, что в данных исследованиях учитывалась только криминальная составляющая.

В своей работе «Социальные функции теневой экономики в институциональном развитии постсоветской России» В. Ю. Латов отмечает [24], что «теневая экономика является социально-экономическим феноменом не последних четырех десятилетий, когда ее стали активно изучать, а практически всей цивилизованной истории человечества».

Проблема теневой экономики для государств отнюдь не нова. Согласно исследованию Всемирного Банка [121], опубликованному в 2010 году и данным Journal of Global Economics [78], опубликованным в 2016 году, эта проблема присутствует повсеместно, различен лишь её уровень. Данные из исследований приведены на рисунке 1.1. Несмотря на небольшую тенденцию снижения уровня общей теневой экономики,

исследование отчетливо демонстрирует стабильность её уровня на протяжении всего проанализированного периода. Однако почти никто не уделяет внимания информационной составляющей данного явления.

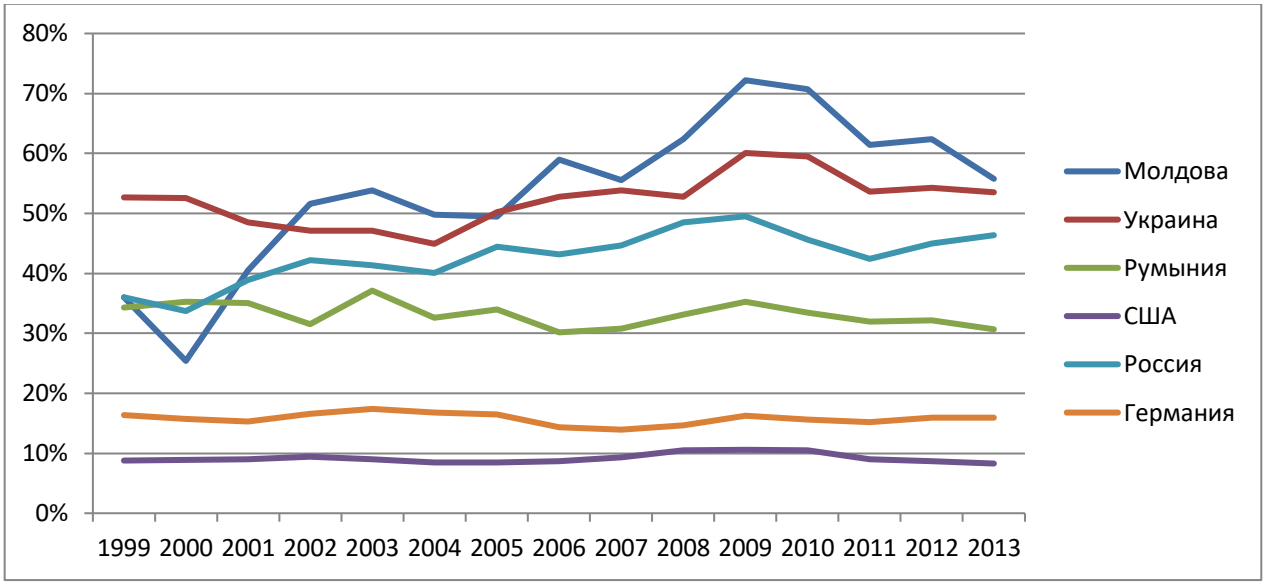

Рисунок 1.1. Тенденция изменения объема теневой экономики в разных странах, в процентах от ВВП данных стран, по данным Всемирного Банка [121] и Journal of Global Economics [78].

Ущерб от существования данной области очевиден. Например, по данным ФБР за последние 14 месяцев злоумышленники украли около 215 миллионов долларов США при помощи всего одной мошеннической схемы, связанной с компрометированными корпоративными адресами электронной почты. Жертвами стали 1198 граждан США и 928 граждан других стран, т.е. в общей сложности пострадали 2126 человек. Примечательно, что гражданам США был нанесен куда больший ущерб, составивший порядка 180 млн. долларов США, т.е. около 84% от общей суммы.

В 1998 году эпидемия вируса CIH, также известного, как «Чернобыль», нанесла урон, объемы которого оцениваются порядка 20-80 миллионов долларов США, не считая огромных объемов потерянной информации и уничтоженного аппаратного обеспечения [72].

В 2000 году эпидемия вируса ILOVEYOU, написанного на VB Script, поразила более пятидесяти миллионов компьютеров за несколько дней, что на тот момент составляло порядка 10% общего числа компьютеров, подключенных к сети Internet. Ущерб, причиненный вирусом, оценивается от 5,5 до 8,7 млрд. долларов США [72].

В 2009 году эпидемия вируса Conficker смогла поразить даже военные подразделения европейских стран. Так, например, во Франции были вынуждены посадить несколько самолетов, находившихся в это время в воздухе в связи с невозможностью скачивания их планов полета. Министерство Обороны Великобритании сообщило о заражении более 800 компьютеров, в Бундесвере заражению подверглись более ста компьютеров. Суммарно, вирус был замечен в 190 странах, заразив при этом миллионы компьютеров. Корпорация Майкрософт назначила награду в размере 250 тысяч долларов США в обмен на информацию, которая приведет к поимке автора данного вируса.

В сентябре 2013 года эпидемия вымогательской троянской программы CryptoLocker, распространяемой посредством ботнета Gameover ZeuS и почтовых вложений, смогла собрать с пользователей 41,928 биткоинов в виде откупа, что на тот момент составило ущерб почти 28 миллионов долларов США [138]. Вышеперечисленные инциденты наглядно представлены в таблице 1.1.

Таблица 1.1. Ущерб от инцидентов в области теневой информационной экономики по данным исследователей George Garza [72], CBS [42]

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.

Согласно данным, представленным в «Национальной программе кибербезопасности Республики Молдова на 2016-2020 годы» [37], в Республике Молдова в период с 2013 года и до августа 2015 было совершено 72 правонарушения в области информационных технологий с ущербом в размере около 21588 тысяч леев и 57 преступлений в области нарушений авторского права и смежных прав, с суммарными наложенными штрафами в размере 99 тысяч леев. Кроме того, по данным CTS, в 2014 году по сравнению с 2013 годом на 26% увеличилось количество атак на веб-сервисы, а вероятность заражения компьютерными вирусами увеличилась на 27%.

Таблица 1.2. Процент компаний, подвергшихся упомянутому типу мошенничества, по данным Kroll [138]

Тип мошенничества	2013	2012
Кража аппаратного обеспечения	28%	24%
Кража информации	22%	21%
Конфликт интересов	20%	14%
Мошенничество с поставками товара	19%	12%
Внутреннее финансовое мошенничество	16%	12%
Нарушение норм или устава	16%	11%
Коррупция и взяточничество	14%	11%
Кража интеллектуальной собственности	11%	8%
Сговор на рынке	8%	3%
Растрата бюджета	8%	-
Отмывание денег	3%	1%

Таблица 1.3. Процент компаний, считающих себя уязвимыми перед упомянутыми угрозами, по данным Kroll [138]

Тип мошенничества	2013	2012
Кража информации	21%	7%
Коррупция и взяточничество	20%	10%
Кража аппаратного обеспечения	18%	6%
Кража интеллектуальной собственности	18%	7%
Мошенничество с поставками товара	18%	5%
Нарушение норм или устава	18%	5%
Конфликт интересов	17%	4%
Сговор на рынке	14%	5%
Растрата бюджета	13%	-
Отмывание денег	11%	4%

Согласно отчёту Group IB [27], по сравнению с 2011-2012 годами, в 2013-2014 годах объем рынка высокотехнологичных преступлений вырос приблизительно на 0,5 миллиарда долларов США. В отчете были рассмотрены такие категории преступлений как интернет-мошенничество, кардинг, спам, внутренний рынок (C2C), DDoS-атаки.

Согласно отчёту компании Kroll за 2014 год [138], в 2013 году по сравнению с 2012 годом всё больше и больше компаний подвергается всем видам электронного мошенничества, более подробные данные приведены в таблицах 1.2 и 1.3.

Исследование, проведенное в Университете Южной Австралии [54], свидетельствует о постоянном росте объемов криминальной кибер-активности в период с 2000 по 2009 годы. Более подробные данные приведены в таблице 1.4.

Таблица 1.4. Динамика роста вредоносной активности в киберпространстве, по данным Университета Южной Австралии [54]

Год	Количество известных инцидентов вредоносной кибер-активности	Процентный рост по сравнению с предыдущим годом
2000	1415	-
2001	3651	158%
2002	4352	19%
2003	9919	128%
2004	16110	62%
2005	23031	43%
2006	30215	31%
2007	43880	45%
2008	54640	25%
2009	71661	31%

Другое исследование, ссылаясь на CERT/CC [118], приводит куда более пугающие данные о динамике роста подобной активности. Данные наглядно представлены на рисунке 1.2.

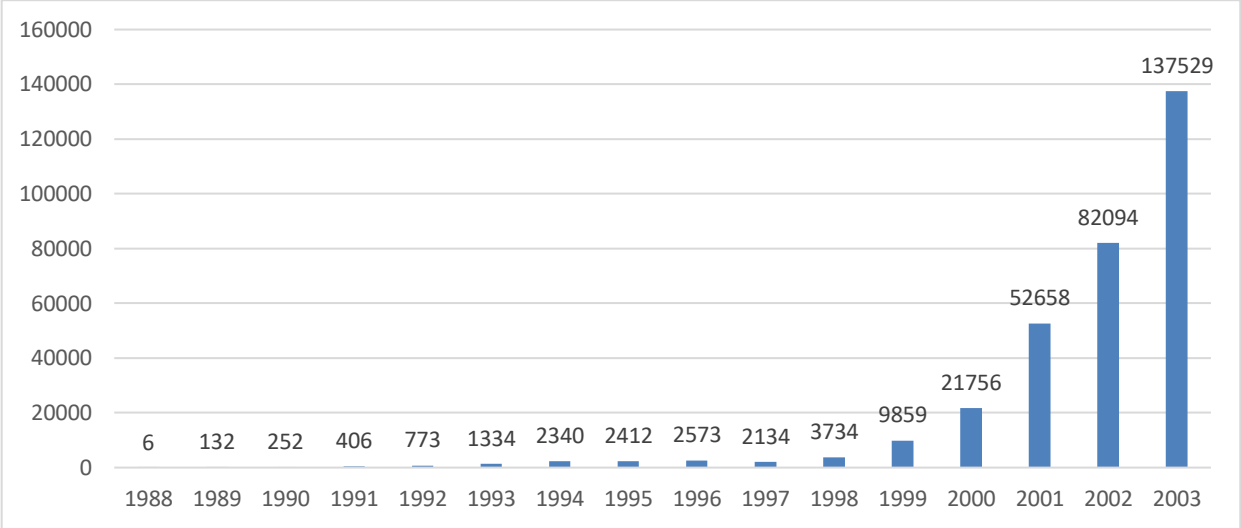

Рисунок 1.2. Динамика роста количества инцидентов компьютерной безопасности, согласно CERT/CC [118].

В своем ежегодном отчете компания Verizon [186] приводит статистику по преступлениям в промышленных секторах за 2015 год. Данная статистика, представленная в таблице 1.5, явно свидетельствует о том, что абсолютно все области воспроизводства подвержены информационным рискам.

В отчёте «The Cost of Cyber Crime» за 2011 год компания Detica [179] оценила ущерб, нанесенный частным лицам в результате кражи персональных данных, в 1,7 миллиарда фунтов стерлингов, ущерб от онлайн-мошенничества в 1,4 миллиарда фунтов стерлингов, а ущерб от фальшивых антивирусов и прочего scareware в 30 миллионов фунтов стерлингов. В этом же отчете объем ущерба государственным структурам оценивается в 2,2 миллиарда фунтов стерлингов. Однако, согласно отчету, больше всего от кибер-преступлений пострадал частный бизнес. Так, ущерб от кражи интеллектуальной собственности оценивается в 7 миллиардов фунтов стерлингов в год, ущерб от промышленного шпионажа оценивается в 7,6 миллиардов, ущерб от кражи данных клиентов в 1,44 миллиарда, ущерб от онлайн-краж и вымогательства по 2,7 миллиардов фунтов стерлингов в год. Таким образом, суммарный ущерб для бизнеса по оценке данного отчета может составить до 21.44 миллиардов фунтов стерлингов в год.

Таблица 1.5. Количество инцидентов в киберпространстве по отраслям, согласно данным компании Verizon [186]

Сфера деятельности	Итого	Мелкие	Крупные	Неизвестно
Гостиничный бизнес	368	181	90	97
Администрация	205	11	13	181
Сельское хозяйство	2	0	0	
Строительство	3	1	2	0
Образование	165	18	17	130
Развлечения	27	17	0	10
Финансовые услуги	642	44	177	421
Здравоохранение	234	51	38	145
Информационные технологии	1496	36	34	1426
Менеджмент	4	0	2	2
Производство	525	18	43	464
Горная промышленность	22	1	12	9
Прочие услуги	263	12	2	249
Профессиональные услуги	347	27	11	309
Публичный сектор	50315	19	49596	700
Недвижимость	14	2	1	11
Розничная торговля	523	99	30	394
Торговля	14	10	1	3
Услуги перевозки	44	2	9	33
Коммунальные услуги	73	1	2	70
Неизвестно	24504	144	1	24359
Итого	79790	694	50081	29015

В исследовании компании Nasuni [175] проводится параллель между использованием сервиса dropbox и использованием теневых технологий на предприятии, а также прослежена корреляция с секторами индустрии. Данные представлены на рисунках 1.3 и 1.4.

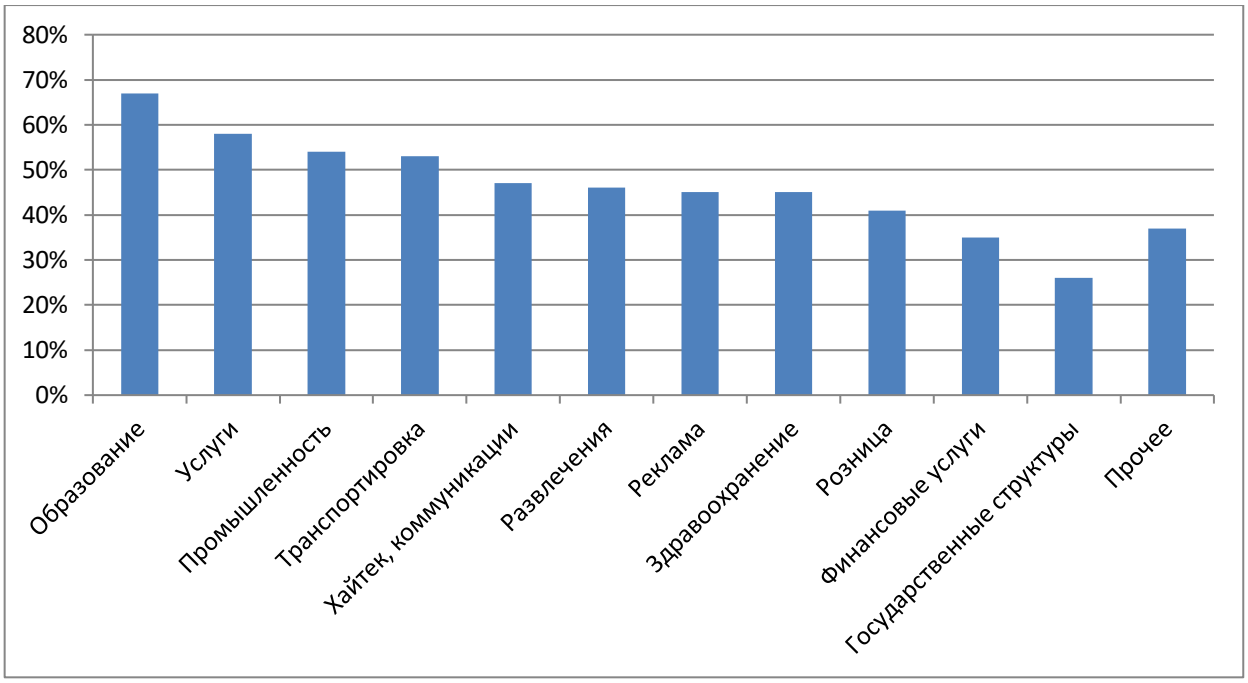

Рисунок 1.3. Распространенность теневых сервисов по секторам, по данным отчета Nasuni [175].

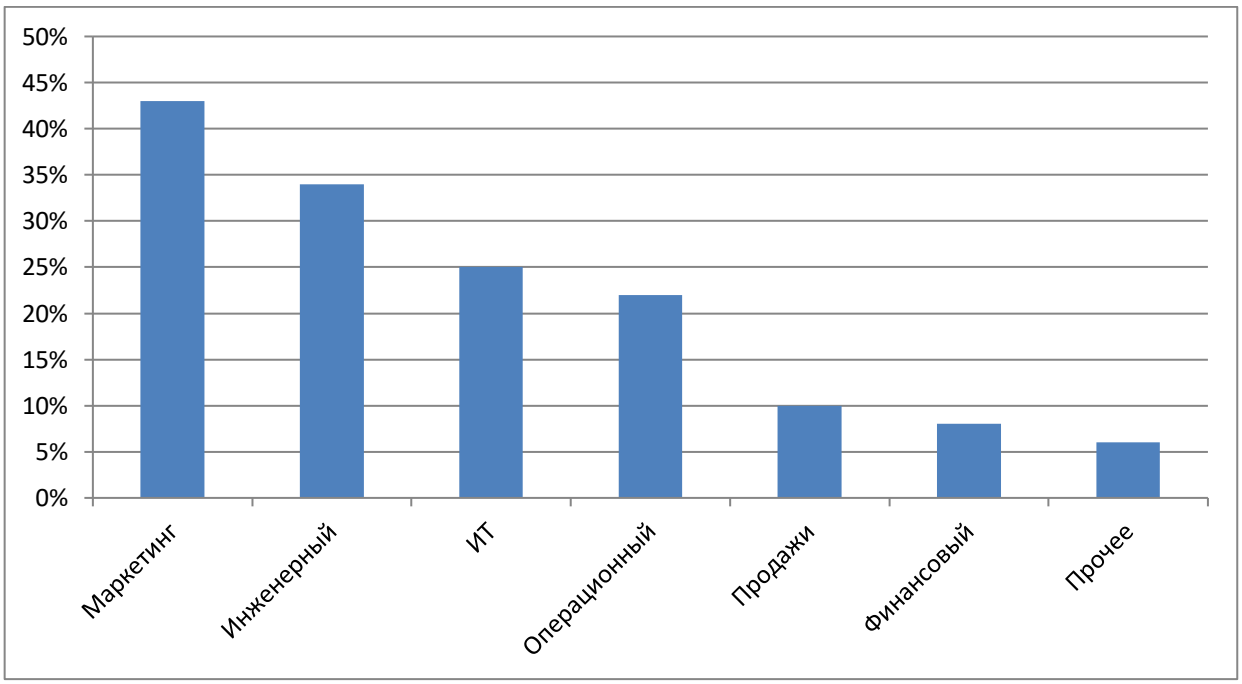

Рисунок 1.4. Использование теневых технологий по отделам, по данным отчета Nasuni [175].

Согласно исследованию Ironpaper [163], рынок информационных технологий продолжает расти. В 2014 году объём рынка составил 2081,9 миллиардов долларов США, и согласно прогнозу данного исследования, в 2019 году рынок информационных технологий вырастет до 2461,1 миллиардов долларов США. Более подробно данные о развитии рынка информационных технологий представлены на рисунке 1.5.

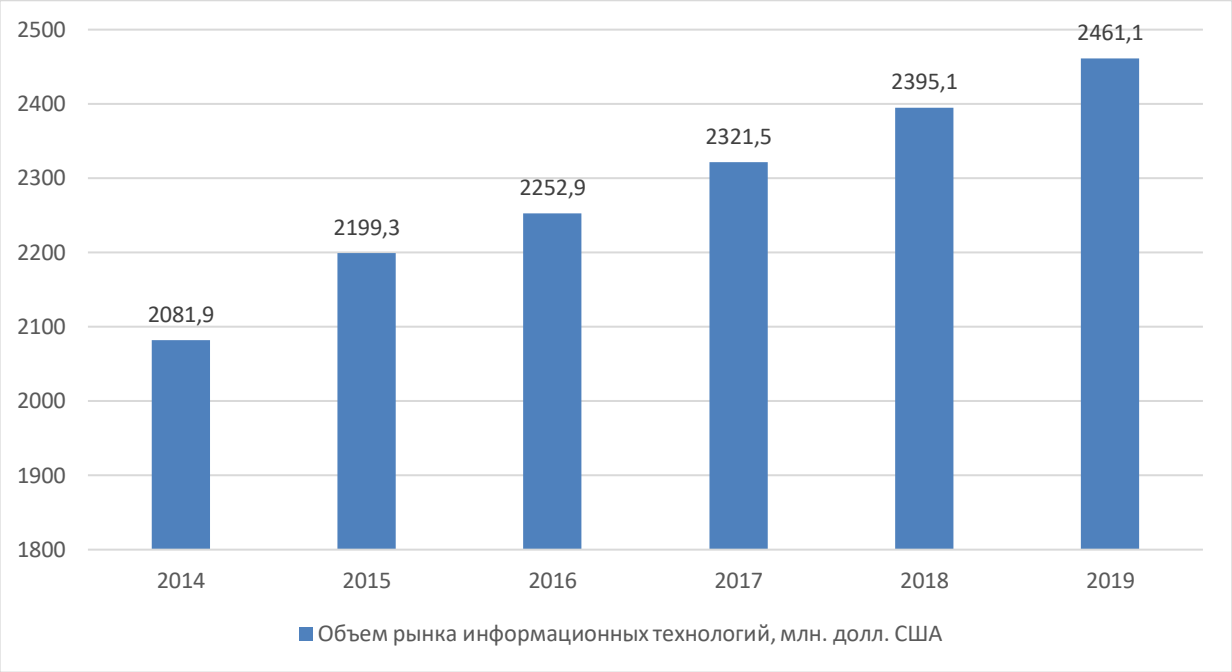

Рисунок 1.5. Объём рынка информационных технологий, млн. долл. США, согласно исследованию Ironpaper [163].

В таблице 1.6 приведены данные об основных типах компьютерных преступлений в США.

Количественные данные 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 1.6 Основные типы компьютерных преступлений в США [141] по данным Internet Crime Complaint Center за 2016 г.

№	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

Как свидетельствуют данные, приведенные в таблице 1.7 ущерб является весьма существенным. По предварительным данным только ущерб от деятельности вымогательской программы WannaCry составил до $4 млрд.

Компания Trend Micro представила краткое содержание и основные выводы отчета «Программы-вымогатели: прошлое, настоящее и будущее» [169]:

- 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.

Таблица 1.7 Статистика атак на банкоматы по данным сайта anti-malware.ru [34].

№	**Показатели**	**2012**	**2013**	**2014**	**2015**	**2016**
1.	Количество инцидентов (тыс.шт)	22450	21346	15702	18738	23588
2.	Объем потерь (млн. евро)	265	248	280	327	332

Теневая экономика во многих странах является важным объектом экономического исследования. Многие ученые и исследователи пытались предложить достойное определение для данного феномена, обозначить его границы. Наряду с определением «теневая» экономика очень часто используются и другие, такие как «подпольная», «неосязаемая», «параллельная», «серая», «черная», «криминальная» экономика. Считается 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.

В статье «Теневая экономика: как ее считать» Сергея Колесникова [22] предлагается следующее определение: «Это скрытая (или теневая) деятельность, неформальная деятельность и нелегальная деятельность. ... Скрытая экономическая деятельность включает в себя в большинстве случаев экономическую деятельность, разрешенную законом, но скрываемую или преуменьшаемую по объему с целью уклонения от уплаты налогов, социальных взносов или выполнения определенных административных обязанностей или предписаний по охране труда, выполнению санитарных и других норм. ... Неформальная экономическая деятельность осуществляется в основном на законном основании индивидуальными производителями или так называемыми некорпорированными предприятиями, т.е. предприятиями, принадлежащими отдельным лицам, домашним хозяйствам, которые часто не оформляются в установленном порядке, основаны на неформальных отношениях между участниками производства (производителем и потребителем) и могут (полностью или частично) производить продукты или услуги для собственного потребления или на продажу (производство продукции сельского хозяйства в личных подсобных хозяйствах, продажа товаров на вещевых и смешанных рынках отдельными гражданами, индивидуальное строительство жилья, частный извоз, оказание бытовых услуг населением по ремонту бытовых изделий, услуг частных парикмахеров и др.). Часто неформальная деятельность бывает основана на вторичной занятости, во многих случаях ею занимаются непрофессионально. Неформальная экономическая деятельность, как правило, бывает распространена в развивающихся странах. ... Нелегальная экономическая деятельность является незаконной, т.е. она охватывает те виды производства товаров или услуг, которые прямо запрещены существующим законодательством. ... В каждом из перечисленных случаев речь идет об экономической деятельности, т.е. о деятельности с целью получения экономической выгоды от производства товаров или услуг и их последующей реализации на рынке, конечного потребления или валового накопления в собственном домашнем хозяйстве, за исключением производства бытовых услуг, потребляемых в собственном домашнем хозяйстве, если они не оказываются оплачиваемой».

Толковый словарь экономики [5] предлагает следующее определение: «Экономическая деятельность, о которой не сообщается в органы социального обеспечения, налоговые и прочие государственные учреждения. Термину намеренно придается несколько уничижительное значение, так как участие в теневой экономике обычно связано с уклонением от уплаты налогов и отчислений в социальные фонды, а

люди, занятые в ней, иногда лишаются права на получение социальных выплат и льгот (social security benefits). Кроме того, в теневой экономике нарушаются законы, касающиеся охраны и безопасности труда, ответственности работодателя, гарантий занятости, найма иностранных работников и т.д. Отсутствие документально подтвержденной информации о деятельности в теневой экономике снижает достоверность официальных статистических данных о доходах и занятости».

Современный экономический словарь [25] предлагает следующее определение теневой экономики: «экономические процессы, которые не афишируются, скрываются их участниками, не контролируются государством и обществом, не фиксируются официальной государственной статистикой. Это невидимые невооруженным глазом, со стороны процессы производства, распределения, обмена, потребления товаров и услуг, экономические отношения, в которых заинтересованы отдельные люди и группы людей. Теневая экономика включает: криминогенную, запретную, противозаконную; скрытую, укрываемую в целях избежать налогов или в связи с нежеланием экономических субъектов придавать известность своим действиям и доходам; неформальную, не подлежащую учету в связи с ее индивидуальностью, личным или семейным характером, отсутствием измерителей».

Большой экономический словарь [6] предлагает следующее определение: «не контролируемое обществом производство, распределение, обмен и потребление товарно-материальных ценностей и услуг, то есть скрываемые от органов государственного управления и общественности социально-экономические отношения между отдельными гражданами, социальными группами по использованию государственной собственности в корыстных личных или групповых интересах. Структура теневой экономики: 1) 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) 2) фиктивная экономика – официальная экономика, дающая фиктивные результаты, отражаемые в действующей системе учета и отчетности как реальные 3) 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».

Канадский исследователь Филип Смит [126] предлагает следующее определение: «рыночное производство товаров и услуг, законных или незаконных, что избежало обнаружения в официальных оценках ВВП».

Разграничивая подпольную экономику и деятельность преступного мира, Hans F. Sennholz [125] подчеркивает, что, хотя 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.

Впервые определение Теневой информационной экономики было предложено в работе коллектива авторов под руководством И. Родионова и Р. Гиляревского, однако, в своём определении авторы описывают несколько иное явление [26]. В своей работе Гаспарениене Л. и Ремейкиене Р. предлагают 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» [73]. Данное определение несмотря на свою уникальность, тем не менее, является слишком узким, что требует проведения исследования с целью поиска новых объективных определений, рассматривающих проблему ТИЭ с разных точек зрения.

В исследовании Gartner [131] предлагается термин «теневые ИТ» (“shadow IT”), под которым понимается ситуация, в которой лица приобретают, владеют и пользуются информационными ресурсами без помощи специализированного персонала. По мнению автора, данное определение подходит лишь для некоторых конкретизированных и узкоспециализированных ситуаций.

В результате исследований автором предложены следующие три определения [7, стр. 485-486]:

1. Говоря обобщенно, 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 [45, стр. 97].

2. С экономической точки зрения, ТИЭ – 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 [45, стр. 98].

3. С технико-технологической точки зрения, ТИЭ – это индивидуальная и коллективная деятельность, являющаяся незаконной, связанная с проектированием, разработкой, распространением, поддержкой и использованием компонент информационных и коммуникационных технологий, скрываемая от общества. Подобие между теневой экономикой и ТИЭ заключается в сходстве характеристик, функций, а также описаний [45, стр. 98].

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 [32, стр. 138].

Для характеристики ТИЭ можно также использовать следующие категории, характерные для теневой деятельности – «вторая экономика», «эксполярная экономика», «теневая экономика – подпольный капитализм», «элемент нетократии», «способность капитализировать негативные знания» и др.

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).

В истории развития ТИЭ выделяются три следующих основных этапа [7, стр. 486], представленных на разработанном автором рисунке 1.6:

Рисунок 1.6. Этапы становления теневой информационной экономики.

1. Докомпьютерный – на данном этапе наблюдается возникновение предпосылок развития теневой информационной экономики в виде формирования финансовых, экономических, правовых, законодательных и информационных систем. Также, многие

страны на этом этапе уже столкнулись с проблемой «классической» теневой экономики [7, стр. 486-487].

2. Ранний – данный этап характеризуется существенным ускорением темпов развития вычислительной техники, появляется первое злонамеренное программное обеспечение, носящее по большей части, вредоносный характер [7, стр. 487-488].

3. Современный – характерной чертой данного этапа выступает объединение злоумышленников в группировки. Кроме того, появляются такие понятия, как кибероружие, хактивизм, набирают популярность облачные технологии [7, стр. 488-489].

Среди основных причин возникновения такого явления, как информационная экономика, выделяется глобализация – как явление, результатом которого является, в первую очередь, интеграция экономик и информационных пространств.

Выделяются несколько элементов, являющихся основополагающими компонентами, составляющими жизненный цикл ТИЭ:

- Исследователи;
- Разработка;
- Распространение;
- Вредоносные действия;
- Отмывание денег.

Противодействие им возможно на двух основных уровнях:

- Программно-технический комплекс мер;
- Законодательство.

На данном рынке наблюдается два основных участника:

- Злоумышленник;
- Жертва.

Обзор существующих моделей, связанных с темой исследования.

В работе «Botnet Economics: Uncertainty Matters» [97] авторами анализируются преступления, связанные с бот-нетами как результат принятия решений о максимизации дохода с точки зрения бот-мастера и арендатора/атакующей стороны. Данная модель помогает понять оптимальные размеры бот-нета, позволяющие максимизировать прибыль бот-мастера и атакующего. Модель, предложенная авторами работы, принимает следующий вид с точки зрения атакующей стороны (формула 1.1) и для бот-мастера (формула 1.2):

$$\max_{n}(Profit) = M - P * n \quad (1.1)$$

$$\max_{k,N}(Profit) = P * n - m * k - a(N) \quad (1.2)$$

Где N – размер типичного ботнета, т.е. количество зараженных машин; a(N) – штрафная функция для бот-мастера, выражающая потери в случае обнаружения и ареста. Контролируемыми переменными для атакующей стороны выступает количество арендованных машин. Для бот-мастера контролируемыми переменными выступают количество командных каналов (k) и размер поддерживаемого ботнета (N).

Несмотря на очевидную новизну и полезность данной модели, по мнению автора, она не учитывает некоторых элементов, важных для создания и поддержания жизнеспособности ботнета.

Вышеупомянутая модель получила некоторое развитие в более поздней работе под названием «Fighting botnets with economic uncertainty» [96], в которой предлагается использовать финансовые рычаги в противостоянии бот-нетам. Авторы предлагают оптимизационную модель с использованием виртуальных ботов и приходят к выводам, что наиболее эффективным способом противостояния бот-нетам может выступать затруднение вычисления оптимального размера бот-нета для его создателя.

В работе «Modeling Botnet Propagation Using Time Zones» [59] авторами анализируется зависимость распространения вредоносного программного обеспечения в зависимости от часовых поясов на примере ботнетов. В своем исследовании, авторы на протяжении шести месяцев наблюдали за десятками ботнетов, объединяющих миллионы жертв. В процессе наблюдения было замечено изменение в поведении ботнетов в зависимости от времени суток, которое, по мнению авторов, вызвано тем, что ерты выключают свои компьютеры на ночь. Кроме того, в результате анализа, авторами было выявлено, что некоторые ботнеты отдают предпочтение заражению компьютеров в определенных регионах. Основываясь на том, что выключенные компьютеры не представляют опасности заражения и любые региональные предпочтения в заражении влияют на общий рост ботнета, авторами была построена модель дневного заражения компьютеров. Основываясь на модели заражения, представленной формулой 1.3, была построена модель дневного распространения, представленная в формуле 1.4.

$$\frac{dI(t)}{dt} = \beta I'(t)S'(t) - \frac{dR(t)}{dt} \quad (1.3)$$

$$\frac{dI(t)}{dt} = \beta\alpha^2(t)I(t)[N(t) - I(t) - R(t)] - \gamma\alpha(t)I(t) \quad (1.4)$$

Где I(t) – количество зараженных машин в момент времени t; S(t) – количество уязвимых машин в момент времени t; N(t) – количество машин изначально уязвимых для рассматриваемого вредоносного программного обеспечения. $I'(t) = \alpha(t)I(t)$ – количество доступных зараженных машин, $S'(t) = \alpha(t)S(t)$ – количество доступных уязвимых машин, $N'(t) = \alpha(t)N(t)$ – количество доступных машин из числа $N(t)$. Под функцией $R(t)$ подразумеваются машины, которые будут удалены из ботнета из-за технических неисправностей, или в случае обнаружения заражения и его удаления, а γ – параметр удаления. Под функцией $\alpha(t)$ подразумевается функция дневного заражения. Наконец, в исследовании предлагается модель, охватывающая различные часовые зоны, представленная в формуле 1.5.

$$\frac{dI_i(t)}{dt} = \alpha_i(t)[N_i(t) - I_i(t) - R_i(t)] \sum_{j=1}^{K} \beta_{ji}\alpha_j(t)I_j(t) - \gamma_i\alpha_i(t)I_i(t) \quad (1.5)$$

Где $N_i(t), S_i(t), I_i(t), R_i(t), \alpha_i(t), \gamma_i$ – соответствующие параметры из предыдущей модели, но с поправкой на то, что машины находятся в часовом поясе i. Параметр β_{ji} – попарная степень заражения машин из пояса j машинами из пояса i. Таким образом, авторы пытаются предсказывать возможное заражение машин между определенными часовыми поясами и демонстрируют важность часовых поясов в динамике роста ботнетов.

В работе «Modeling Peer-to-Peer Botnets» [118] авторами анализируется определенный типа ботнетов – peer-to-peer, появившихся в 2007 году. В отличие от существовавших до этого ботнетов, работавших посредством каналов IRC, Storm Worm использует для коммуникации децентрализованную сеть peer-to-peer. В то время, как централизованная структура управления может быть относительно легко обнаружена и деактивирована посредством отключения управляющей «головы», сети типа peer-to-peer намного сложнее разоружить. Исходя из этого, необходим поиск новых путей противодействия подобным угрозам. Для достижения этой цели, авторами была предложена сетевая модель стохастической активности peer-to-peer ботнетов, которая может предоставить новые пути противостояния им. Предложенная в работе модель представлена на рисунке 1.7.

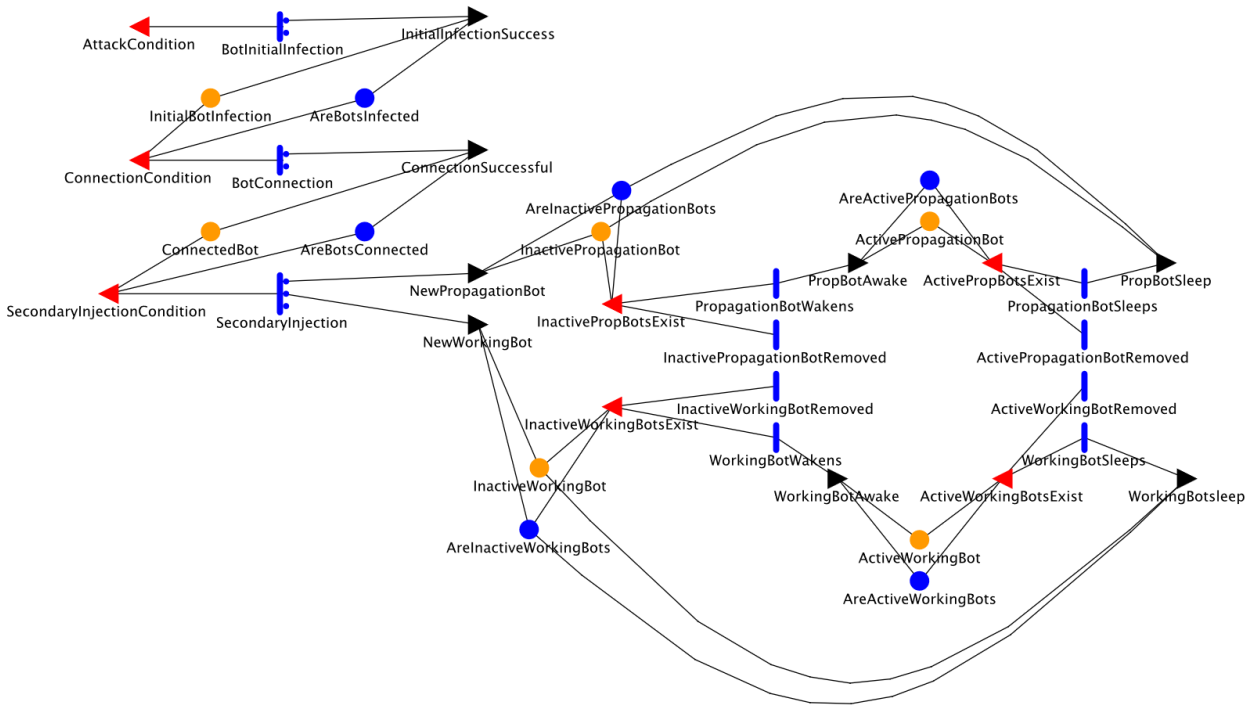

Рисунок 1.7. Сетевая модель стохастической активности peer-to-peer ботнетов, представленная в работе «Modeling Peer-to-Peer Botnets» [118].

Обзор существующих диссертаций, связанных с темой данного исследования.

В диссертации на соискание степени доктора наук «Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы» автор Зиновьева Елена [20] анализирует основные характеристики, природу и движущие силы международного сотрудничества по обеспечению информационной безопасности и определяет особенности основных проблемных сфер международного сотрудничества, субъектов и перспектив взаимодействия в данной области. В своей работе автор подчеркивает важность международного сотрудничества в области информационной безопасности, которое в данный момент находится на этапе переговоров.

В диссертационном исследовании «Performance Enhancement of Intrusion Detection Systems using Advances in Sensor Fusion» [57] автор исследует возможные улучшения систем обнаружения проникновения, как уже существующих, устоявшихся, так и новых типов атак. Автором подробно исследуется так называемое слияние сенсоров. В исследовании рассматриваются отношения между атакующей и защищающейся сторонами с точки зрения моделирования возможных сценариев обнаружения. Автором также анализируются различные метрики, которые возможно использовать в системах обнаружения проникновения. Целью работы выступает исследование возможностей

комбинирования данных из различных систем обнаружения проникновений и их корреляция для повышения эффективности обнаружения злонамеренных действий.

В диссертационной работе «Using Malware Analysis to Evaluate Botnet Resilience» [118] автор анализирует возможные способы противостояния ботнетам, путем исследования их прочности посредством проведения экспериментов со злонамеренным программным обеспечением. В начале, автор анализирует, возможности проектирования платформы для динамического анализа вредоносного программного обеспечения, таким образом, чтобы предоставлять возможности проведения одновременно реалистичных и безопасных экспериментов. Затем, автор анализирует техники и инфраструктуры, используемые злоумышленниками для установки вредоносного программного обеспечения на компьютеры жертв, а также, что именно способствует обеспечению их отказоустойчивости. Наконец, автор анализирует структуру ботнета, с точки зрения независимости от единого контрольного центра, а также выделяет методы систематического разрушения ботнетов типа peer-to-peer и анализирует их эффективность.

В диссертации «Detection of Botnet Command and Control Traffic in Enterprise Networks» [54], автор анализирует возможные способы отслеживания траффика, генерируемого контрольными серверами в ботнетах в корпоративных сетях. Актуальность данной работы продиктована тем, что ботнеты могут атаковать подобные сети с целью шпионажа, воспрепятствования нормальной работе, а также в целях манипулирования процессами и информацией. Одной из главных проблем в обнаружении подобного траффика в корпоративных сетях является тот факт, что он достаточно незаметен для большинства антивирусных систем, а также систем обнаружения проникновений, и, чаще всего, маскируется под «обычный» траффик в сети Internet и сами по себе управляющие команды появляются относительно редко. Обнаружение затрудняется и там фактом, что ботнеты, нацеливающиеся на атаку корпоративных сетей не производят обычный для них объем траффика, возникающий, например, во время атак типа DDoS и рассылки спама. Однако, несмотря на все перечисленные трудности и препятствия, обнаружение на сетевом уровне достаточно привлекательно тем, что оно обычно вне доступа вредоносного программного обеспечения, а также независимо от наблюдаемых платформ. В первой части исследования автор анализирует существующие методы обнаружения злонамеренного траффика, а затем предлагает три новых метода, каждый из которых отличается от уже существующих.

В диссертационном исследовании «Информационное мошенничество: уголовно-правовой анализ преступления» автор Дрэган Алин Теодорус [1] анализирует

юридические аспекты информационных преступлений, а также возможные доработки в плане законодательной базы.

Большинство существующих в области исследования работ носят технический характер, в то время, как по мнению автора, технические меры, несмотря, на свою эффективность, должны дополнять экономические рычаги противодействия злоупотреблениям в сфере ТИЭ, действенность которых выше.

Методики и методологии оценки уровня теневой экономики

Существуют две основных категории методов оценки уровня теневой экономики: прямые и косвенные, которые ещё называют микрометодами и макрометодами. У каждой из групп этих методов есть свои недостатки, связанные с точностью полученной оценки: прямые, чаще всего, предоставляют слишком низкую оценку, в то время, как косвенные склонны её завышать [29].

Используются несколько прямых методик оценки уровня ТЭ в целом. В данной категории методов сопоставляются различные отчетные данные, данные опросов и т.д. Рассмотрим некоторые из них:

- Наиболее простым методом является проведение прямого опроса продавцов и покупателей определенных товаров и услуг. Подобный опрос предоставит данные о структуре рынка, однако, эффективность этого метода подвергается сомнению из-за боязни большинства участников признавать своё участие в нелегальных операциях.
- Другим прямым методом является проверка налоговой отчетности, её сопоставление с информацией из органов налогообложения и социального обеспечения. Данный метод предоставит информацию о попытках уклонения от налогов, однако, подобные проверки не всегда дают желаемый результат.
- Наконец, третьим популярным методом является так называемый «итальянский метод», в основе которого лежит выборочный опрос домохозяйств, в ходе которого выясняют, сколько времени респондент проработал дополнительно в определенных отраслях. Важно подчеркнуть, что вопрос об объеме полученной прибыли не ставится, так как считается, что от ответов на подобные вопросы респонденты склонны уклоняться, или предоставлять искаженные данные, однако зная средний доход по экономике в данной области, эти данные возможно рассчитать. Очевидно, что для того, чтобы данный метод работал эффективно, необходима хорошо отлаженная система проведения опросов и достаточно большая и репрезентативная выборка респондентов. Также очевидно, что данная оценка достаточно расплывчата и приблизительна, однако, она может применяться

для оценки объемов информационной составляющей теневой экономики в целом, но не позволит выделить непосредственно криминальный сегмент.

Однако, по мнению автора, рассмотренные методики обладают существенным недостатком: они опираются только на опросные, статистические и отчетные данные. С другой стороны, эти методы могут предоставить информацию о структуре теневой экономики, её объектах и субъектах. Кроме того, данные методы не очень подходят для оценки динамики развития рассматриваемого сектора.

Существуют также косвенные методы оценки уровня теневой экономики. Эти методы опираются на следующие макроэкономические показатели:

- Несоответствия между уровнем национальных расходов и уровнем доходов. Данная методика основана на различиях между доходами и расходами. Теоретически, объем израсходованного ВВП должен совпадать с объемом произведённого ВВП. Имея данные о доходах населения за отчётный период и данные независимого исследования о расходах, представляется возможным их сопоставление и разница между ними как раз и будет указывать на объем теневого сектора экономики. В качестве недостатка данного метода можно выделить сложность объективной оценки объема расходов населения.
- Несоответствия между уровнями официальной и реальной занятости. Данный метод основан на предположении о том, что при снижении уровня занятости и повышении уровня безработицы, уровень занятости в теневом секторе возрастает. При условии сохранения численности трудоспособного населения, понижение официального уровня занятости может служить индикатором повышения уровня занятости в теневом секторе. Однако, у подобного снижения могут быть и другие причины. Более того, население, занятое в официальном секторе, может параллельно с этим принимать участие и в теневом секторе.
- Метод сделок. Данный метод основан на теории, утверждающей, что существует связь между стоимостью всех совершаемых сделок. Недостатком данного метода являются трудности анализа всех задействованных переменных и коэффициентов, а также наличие прочих причин увеличения обращения денег.
- Метод спроса на наличные. Данный метод основан на связи между спросом на наличные деньги и налогообложением. Предполагается, что сделки на черном рынке совершаются с использованием наличных денег для того, чтобы ограничить возможность наблюдения со стороны органов налогообложения, тем самым увеличивая спрос на наличные деньги. Данный метод является наиболее распространенным для подсчета

уровня теневой экономики, однако его применимость для информационной области крайне сомнительна ввиду того, что подавляющее большинство сделок в данной отрасли совершается при помощи безналичных расчетов, а также криптовалют.

Косвенные методы хороши для оценки масштабов и тенденций развития теневой экономики.

Метод оценки уровня теневой экономики через совокупное энергопотребление, называемый методом Кауфмана-Калиберды, был впервые предложен в работе «Теневая экономика и динамика экономики постсоциалистических стран» Д. Кауфмана и Д. Калиберды.

Выбор конкретного метода может зависеть от возможности получения достоверных данных необходимых для проведения расчётов, в то время, как недоступность данных может воспрепятствовать применению какого-либо конкретного метода. На практике, обычно применяется комбинация нескольких методов для расчета уровня теневой экономики.

Как видно из анализа, большинство существующих методов не подходят для оценки теневой информационной экономики, её объёмов, а те, которые могут быть применимы предоставляют крайне расплывчатые данные.

1.2. Основные черты и характеристики теневой информационной экономики; факторы, формирующие теневую информационную экономику

В своей работе В. Буров [17] выделяет четыре предпосылки возникновения теневой информационной экономики:

1. Деструктивные потребности человека, которые существуют независимо от прочих факторов.

2. Неспособность экономики государства обеспечить достаточно высокий уровень качества жизни населения страны.

3. Противоречие между потребительской стоимостью факторов производства и их меновой стоимостью.

4. Деформация отношений собственности. В качестве ярких примеров автор приводит «военный коммунизм», национализацию частной собственности и «раскулачивание».

Также, в своей работе автор соглашается [17] с выводами А. Смирнова и Е. Рогозинского, которые выделяют следующие функции теневой экономики:

1. Стабилизационная функция позволяет восстанавливать равновесие системы посредством способности разрешения деструктивных противоречий, что в свою очередь ведет к восстановлению системы и уменьшению теневого сектора.

2. Конструктивная функция в отличие от стабилизационной функции, сохраняющей и восстанавливающей существующую систему, меняет качественные характеристики системы, т.е. развивает её.

3. Паразитическая функция заключается в стремлении к сохранению качественных характеристик экономической системы для сохранения возможности дальнейшего паразитирования.

4. Деструктивная функция заключается в разрушении целостности экономической системы, утрате её качественных характеристик.

Таким образом, мы отчетливо видим, что согласно данной классификации функции теневой экономики достаточно противоречивы.

В работе В. Бурова [17] выделяются три основные функции теневой экономики:

1. Функция механизма институциональных инноваций – зачастую новаторский подход к определенным проблемам может наталкиваться на неприятие со стороны приверженцев более консервативных норм. Так как законодательные нормы отражают мнение большей доли законодательных органов и населения, возникновение новых методов заработка может нарушать законы.

2. Функция дубликата государственных институтов – конкуренция между государственными институтами, выполняющими сходные функции, приводит к их постоянному совершенствованию и отбору наилучших.

3. Функция институциональной утилизации – в область теневой экономики зачастую попадают элементы отживших социально-экономических систем. Однако в теневом секторе эти институты всё ещё имеют шанс на возврат, будучи подпитываемыми развитием теневых отношений, что в свою очередь может вести к торможению развития общества.

По мнению В. Бурова [17], все три вышеперечисленные функции могут более активно проявляться на определенных этапах развития общества. Например, инновационная и утилизационная функции наиболее ярко проявляются в периоды рождения нового социально-экономического строя, в то время как дублирующая функция наиболее активно проявляется в тот период, когда качественные перестройки уже закончены.

Из вышеперечисленных классификаций можно выделить наиболее значимые факторы, влияющие на теневую экономику, её состав и уровень.

1. Уровень развитости экономики страны, т.е. уровень жизни населения. Чем выше уровень жизни населения, тем меньше доля теневой экономики. Эти показатели не всегда имеют прямую корреляцию, но тенденция очевидна: в наиболее развитых странах доля теневой экономики значительно ниже, чем в развивающихся.

2. Стабильность состояния общества. Другими словами, находится ли общество и государство в данный момент в переходном состоянии. Если да, то доля теневой экономики, скорее всего, существенно возрастет.

Эти факторы, несомненно, важны для «классической» теневой экономики, однако в теневой информационной экономике мы считаем важным выделить факторы, представленные ниже. Некоторые из этих факторов необходимо анализировать с двух точек зрения: с позиции жертвы и с позиции атакующей стороны.

1. 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.

2. 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.

3. 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 существенных 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.

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

Данные факторы могут быть во многом взаимосвязаны. 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 малой оплатой, а жертвой – граждане стран с развитой экономикой и стабильной, высокими доходами.

Выделим особенности, характерные для информационной области теневой экономики:

1. Риск быть пойманным и наказанным за преступление, совершенное в сфере теневой информационной экономики, уменьшен 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. Сниженные риски, связанные с ответственностью, в том числе уголовной.

Таким образом, появляется возможность построить логическую модель социальных факторов, влияющих на шансы возникновения злоумышленников или жертв в определенной социальной среде. Объективная возможность появления злоумышленника намного выше в среде с высокой преступностью, низким доходом, развитой инфраструктурой и хорошим образованием. Жертва же, скорее всего, появится в среде с низким уровнем преступности, но высоким уровнем дохода. Данная модель представлена на рисунке 1.8. По мнению автора, представленная модель характерна как для глобального уровня, так и для Республики Молдова в частности.

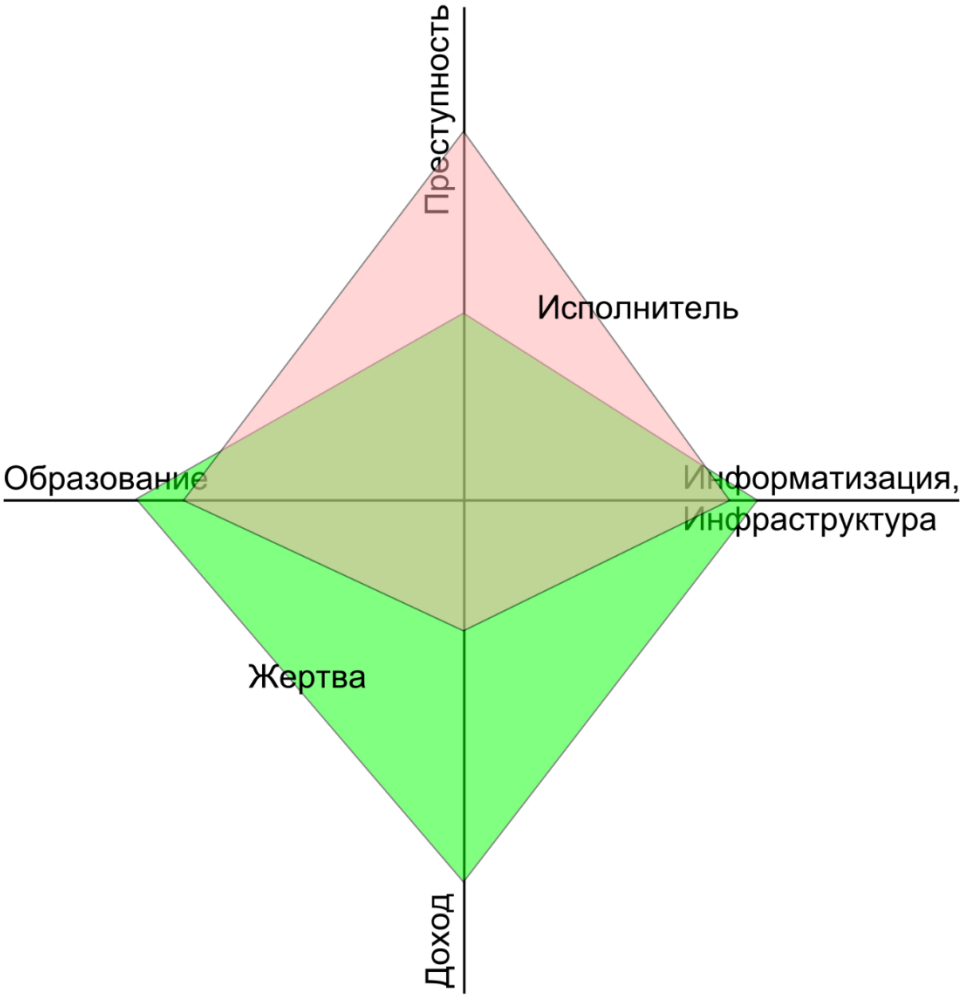

Рисунок 1.8. Социальные факторы, характеризующие жертв и злоумышленников.

1.3. Выводы по первой главе

Проведенный анализ литературных источников, отчётов, посвященных теневой информационной экономике, позволил:

1. Сформулировать и показать актуальность проблемы теневой информационной экономики на основе работы, проделанной с литературными источниками.

2. В результате анализа технологических, правовых и организационных аспектов сформулировать и предложить несколько определений теневой информационной экономики, раскрывающих её сущность и особенности.

3. Определить предметную область теневой информационной экономики, в том числе сформулировать факторы, влияющие на её формирование и поддержание жизнеспособности.

4. Проанализировать существующие методы оценки уровня теневой экономики и их применимость по отношению к её информационному сектору.

Рассмотренный материал, а также анализ существующих моделей и диссертационных работ в области исследования предполагает проведение дальнейших исследований, направленных на поиск возможных экономических путей противостояния злоупотреблениям в сфере информационных технологий, а именно:

1. Исследование генезиса ТИЭ;
2. Построение моделей рынка продуктов и услуг в сфере ТИЭ;
3. Построение модели монетизации продуктов и услуг в сфере ТИЭ;
4. Построение модели доходности ботнета;
5. Построение модели денежных потоков в ТИЭ.

2. ФОРМЫ ПРОЯВЛЕНИЯ ТЕНЕВОЙ ИНФОРМАЦИОННОЙ ЭКОНОМИКИ

2.1. Генезис теневой информационной экономики

В становлении ТИЭ автором выделяются три основных этапа, как уже было упомянуто в первой главе. Рассмотрим каждый из этих этапов подробнее, опираясь на наиболее значимые основополагающие для них события [7, стр. 486].

Докомпьютерный этап. На этой стадии возникают предпосылки развития ТИЭ: появляются первые законодательные системы, первые прототипы компьютеров. На данном этапе большинство стран уже столкнулись с проблемой теневой информационной экономики. Ведь даже в древние времена ценная информация могла продаваться и покупаться, очень часто с недобрыми намерениями, например, шпионская информация (в том числе промышленный шпионаж), военные тайны. На рисунке 2.1 в хронологическом порядке представлены наиболее значимые события данной эпохи:

1. **Начало чеканки монет** (VII в. до н.э.). С их появлением сразу же объявились фальшивомонетчики, штамповавшие поддельные монеты. Среди наиболее известных примеров упомянем варварские подделки чеканных монет древнего Рима.

2. **Изобретение абака** (ок. V в. до н.э.). Это было одно из первых вычислительных устройств, придуманных человечеством.

3. **Римское право** (V — III вв. до н.э.). Служит основой почти всех ныне существующих законодательных систем. Первые шаги в развитии римского права относят к Двенадцати Таблицам, обычно датируемым 439 годом до н.э. Одной из причин существования «классической» теневой экономики является высокое налоговое бремя, создающее условия, при которых юридическим лицам выгодно уклоняться от уплаты налогов и показывать меньший доход в своих бухгалтерских отчетах. Последнее привело к очередному этапу развития ТИЭ.

4. **Программируемые устройства** (ок. 100 г. до н.э.). Первым программируемым устройством считается антикитерский механизм, найденный 4 апреля 1900 г. на дне Средиземного моря. Механизм был предназначен для расчета движения небесных тел. Другим важным прорывом в данной области можно считать работы выдающегося арабского механика и математика аль-Джазари. Важнейшим его изобретением являются модели человекоподобных роботов.

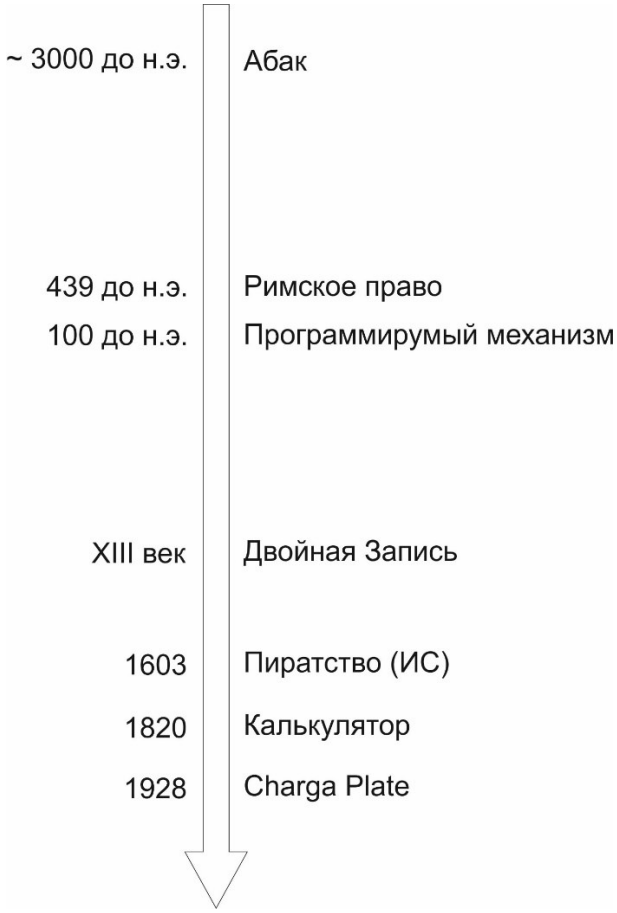

Рисунок 2.1. Основополагающие события докомпьютерной эпохи развития теневой информационной экономики.

5. **Двойная запись** (ок. XIII — ок. XV вв.). Это набор бухгалтерских правил. Они были представлены где-то около XIII в. и систематизированы около XV в.

6. **Пиратство по отношению к авторскому праву** (1603 г.). Оно связано с интеллектуальной собственностью. Впервые данное понятие было использовано в суде Великобритании.

7. **Механический калькулятор Лейбница** (1673 г.). Это был следующий, революционный скачек в развитии вычислительной техники.

8. **Рассылка спама** (1864 г.). Первая зарегистрированная рассылка спама осуществлена в Великобритании.

9. **Начало выпуска эмбоссированных (именных) карт Charga Plate** (1928 г.). Хотя им предшествовали картонные карты компании Mobil Oil (1914 г.) и металлические «карты учтивости» (courtes cards) прочих нефтяных компаний (1920-е гг.), именно Charga Plate считается прародительницей современных пластиковых кредитных карт. Мы относим данное событие к основополагающим в развитии ТИЭ в связи с тем, что в наше

время кража данных кредитных карт является одним из наиболее прибыльных и часто встречающихся видов правонарушений в сфере ТИЭ.

Ранний этап. Начало данного этапа относится к середине XX века и связывается со значительным ускорением темпов развития вычислительной техники и появлением первых хакеров, которые ближе к окончанию этого периода начинают объединяться в группировки. Большая часть вредоносного программного обеспечения, появившегося на данном этапе, носит деструктивный характер. Экономические и юридические основы и принципы принимают свою современную форму и почти не меняются. Совершается относительно мало принципиальных прорывов в данной области, даже несмотря на то, что данные области науки всё больше и больше адаптируются к новым реалиям. Среди наиболее значимых событий, представленных на рисунке 2.2, выделяются следующие:

1. **Первый программируемый компьютер** «Колосс» (the Colossus) был спроектирован и построен в годы Второй мировой войны британскими криптоаналитиками для расшифровки немецких сообщений.

Рисунок 2.2. Основополагающие события ранней эпохи развития теневой информационной экономики.

2. Важным событием в развитии вычислительной техники было **появление мейнфреймов** (1964 г.). Некоторые исследователи даже выделяют именно это событие в качестве основополагающего [85].

3. **«Теория самовоспроизводящихся машин»** – знаменитая работа Джона фон Неймана, опубликованная в 1966 году. Данный труд считается одной из основ дальнейшего развития вредоносного программного обеспечения.

4. **ARPANET** – первая компьютерная сеть, использующая технологию коммутации пакетов. Была представлена в 1969 году и в дальнейшем легла в основу глобальной сети Internet.

5. **Internet** (1969 г.). В наши дни, одна из самых распространенных сред общения, передачи данных, распространения вредоносного программного обеспечения и отмывания денег. Вероятно, одна из самых важных вех в истории развития ТИЭ.

6. **TCP/IP** – стек протоколов, лежащих в основе сети Internet (1980-е гг.).

7. **Intel 80386** – другая очень важная веха в развитии ТИЭ. Во-первых, компьютеры, основанные на технологии Intel-30386, привнесли существенный вклад в дело популяризации компьютеров среди широкой публики. Затем, обширный спрос на процессоры данной модели привел к появлению большого количества i386-совместимых аналогов, например, AMD 5x86, Harris 286, Cyrix Cx486-SLC, OKI M80C86 и т.д. Наконец, ещё одним крайне важным для ТИЭ последствием распространения процессоров i386 мы считаем выделение различных «цветов», присваиваемых аппаратному обеспечению, в зависимости от страны их происхождения и официальности их продажи.

8. **Червь Морриса** (Morris worm) – один их первых компьютерных червей. Был впервые замечен в сети Internet в 1988 году и привлек к себе крайне много внимания со стороны СМИ. Данное вредоносное программное обеспечение могло заражать компьютеры благодаря некоторым уязвимостям в программном обеспечении, при этом червь мог заражать один и тот же компьютер по нескольку раз, приводя тем самым к значительному снижению скорости работы, вплоть до полной неработоспособности. Сам автор отрицал какой-либо злой умысел при написании этого вируса.

9. **MS DOS** – ещё одна крайне значимая веха в развитии ТИЭ. Данная операционная система одновременно помогла распространению компьютеров в широкие массы и стала одним из первых программных продуктов, пострадавших от пиратства.

10. **Антивирусы** – как следствие появления первых вирусов, появляются и первые средства противостояния им. Один из первых антивирусных программных продуктов был разработан для платформы Atari ST компанией G Data Software в 1987 году. Позже, с развитием вирусов, в этом периоде, антивирусные продукты перерастают в целую индустрию. Появляются такие именитые компании как Kaspersky, McAfee, Panda Security, F-Secure, Avira. Symantec, Sophos, AVG, Bitdefender, которые специализируются на исследовании программных угроз и предлагают на рынке свои решения по защите вычислительной техники. Чаще всего, используются сигнатурные методы обнаружения вредоносного программного обеспечения, эффективность которых ограничивается, главным образом, уже известными вирусами, и неэффективна с точки зрения обнаружения новых угроз. Для поиска неизвестных вредоносных программных продуктов применяются технологии эвристического анализа.

Современный этап. Одной из наиболее характерных черт данного этапа выступает тенденция злоумышленников к объединению в хорошо продуманные и эффективно действующие группировки. Единичные случаи правонарушений перерастают в систему. Очень часто члены группировки выполняют узкие и высокоспециализированные задачи и могут даже не подозревать о целях группировки и существовании остальных её членов. Их задачи могут варьироваться от сугубо научных исследований программного и аппаратного обеспечения, рынка, тенденций и течений, законов, возможностей проектирования и разработки программного обеспечения, отмывания денег — и до практических задач по реализации всего вышеперечисленного. Подобные группировки, скорее всего, управляются высококвалифицированными лицами, и их структура (возможно, древовидная) может соответствовать «классической» структуре криминальных группировок. Некоторые исследователи предполагают, что подобные группировки имеют древовидную структуру, схожую с классической структурой мафиозных группировок. На данном этапе вредоносное программное обеспечение приобретает материальный, монетарный характер: крадёт личные данные (в частности, данные кредитных карт), использует вычислительные мощности компьютера, его сетевые ресурсы с конечной целью, заключающейся в получении прибыли. Согласно данным RAND Corporation [40], в начале двухтысячных годов доля злоумышленников-фрилансеров составляла порядка 80 %, к лету 2014 года она уменьшилась до 20 %. Киберпреступность всё более и более напоминает преступления, совершаемые в реальной жизни: вымогательство, шпионаж, даже появляется такой термин, как кибервойны (англ.

cyberwarfare). Люди, бывшие хакерами на предыдущем этапе развития ТИЭ, сейчас становятся экспертами в области информационной безопасности. Ещё одной важной чертой данного этапа является большое количество вирусных эпидемий. Также существенно увеличивается объем пиратского программного обеспечения, он оказывается на одном уровне с увеличением комплексности и сложности защиты. Ещё одним важным явлением выступает хактивизм (hacktivism) — использование компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации. Люди стремятся посредством компьютеров высказывать своё отношение к событиям реальной жизни. Согласно исследованию Hackmageddon [112], на долю хактивизма в 2013 пришлось 44 % всех атак на веб-сайты. И, наконец, последней важной тенденцией, на которую необходимо обратить внимание, является существенное повышение уровня распространенности мобильных устройств, а также связанных с ними мошенничеств. Средства защиты информации также выходят на новый уровень: для поиска вредоносного программного обеспечения применяются технологии анализа поведения в «песочнице» (англ. sandbox – запуск и анализ поведения неизвестных программных продуктов в виртуальной среде), технологии машинного обучения, data mining, а эвристический и сигнатурный анализ применяются всё реже и реже. Среди наиболее значимых событий, представленных на рисунке 2.3, выделяются следующие:

1. **ZeuS** (2007 г.). Троянская программа, крадущая данные кредитных карт и банковских счетов, а также объединяющая все зараженные компьютеры в ботнет. Исследователи отмечают, что эпидемия поразила 196 стран, заразив порядка 3.6 млн компьютеров только в США. Впервые данная программа была обнаружена в 2007 году, а в 2010 году её создатель опубликовал исходный код.

2. Вредоносная программа **Conficker** (2008 г.). Количество зараженных компьютеров оценивается от 9-ти до 15-и млн машин. Даже несмотря на то, что Microsoft выпустила патч, как только разработчикам компании стала известна уязвимость, которую использует вирус, на огромное количество компьютеров программная заплатка установлена не была, что позволило вирусу распространяться быстрыми темпами. Это привело к огромному количеству зараженных машин. От вируса пострадали, среди прочих, Национальные военно-морские силы Франции, Министерство обороны Великобритании и Бундесвер.

3. Вирусы **Stuxnet, DuQu, Flame**. У всех трех общее происхождение. О них часто говорят, как о кибероружии.

4. **DDoS атаки на Amazon, Visa, PayPal, Mastercard**. Это один из наиболее ярких примеров хактивизма [153, 154]. Посредством DDoS атаки люди смогли выразить свой протест по делу Джулиана Ассанжа, владельца проекта Wikileaks. Благодаря своему огромному количеству, протестующие смогли замедлить работу сайтов крупных компаний [11, стр. 217-218].

5. **Облачные технологии**. Это одна из главных тенденций последних лет ввиду свой экономической эффективности [70, 63], гибкости предоставляемых услуг и объема ресурсов. Однако у данной технологии есть ряд неоспоримых недостатков, как присущих именно облакам, так и более общих, возникших вследствие некорректной конфигурации. К недостаткам облаков можно отнести: возможность вырваться за пределы виртуальной среды; нарушение конфиденциальности, целостности или доступности пользовательской сессии и данных; недостаточные или неэффективные криптографические средства защиты пользовательских данных в облаке. Кроме того, можно упомянуть и сложность восстановления данных в случае форс-мажора, а также (с точки зрения поставщика услуг) возможность уклонения от уплаты всех используемых услуг [77]. Ко второй категории уязвимостей можно отнести: SQL Injection; XSS; слабые пароли; блокирование учетных записей многократным повторением неверного пароля; недостаточные журналирование и мониторинг; а также все недостатки, присущие однофакторной аутентификации.

6. **Кибероружие**. Под термином «кибероружие» понимается специализированное программное обеспечение, разработанное для применения в военных, военизированных или разведывательных целях. По оценкам некоторых экспертов, многие страны прибегают к применению DDoS-атак [192], а также экономическому и промышленному шпионажу. Кроме того, известны случаи слежки за гражданами [53].

7. **Криптовалюты**. В 2009 году была запущенна криптовалюта Bitcoin [63]. Со временем криптовалюты начали набирать популярность, использоваться для перевода средств, торгов на биржах и отмывания денег. Летом 2017 года [86] был задержан гражданин Российской Федерации по подозрению в отмывании 4 миллиардов долларов США при помощи Bitcoin.

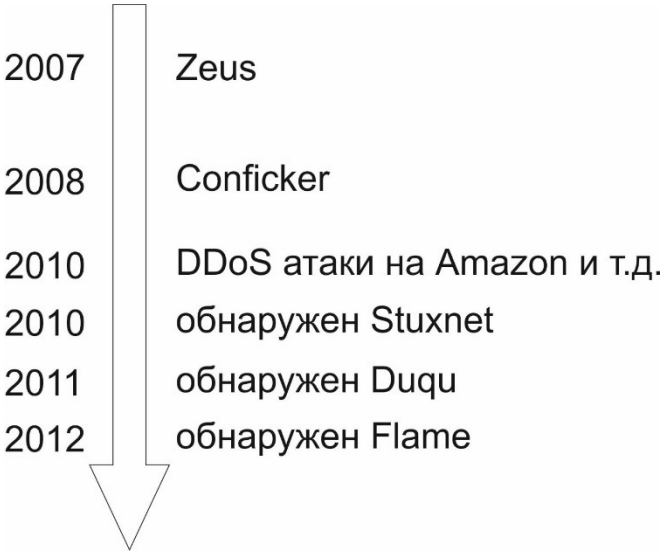

Рисунок 2.3. Основополагающие события современной эпохи развития теневой информационной экономики.

Мобильные устройства

Отдельного внимания заслуживает такая категория, как мобильные устройства. Рассмотрим представленные на рисунке 2.4 наиболее важные этапы развития угроз в данной области [10, стр. 414, 138, 145].

Одним из основополагающих событий в мобильной индустрии было появление «умных» операционных систем, предоставляющих интерфейсы программирования приложений (API) и позволяющих установку дополнительного программного обеспечения на мобильное устройство. Среди них отдельного внимания заслуживают следующие:

- Palm OS, представленная в 1996 году;
- Symbian, представленная в 1997 году;
- Blackberry OS, представленная в 1999 году;
- Pocket PC (в дальнейшем именуемый Windows Mobile, а затем Windows Phone), представленный корпорацией Microsoft в 2003 году;
- Android, купленный корпорацией Google в 2005 году;
- iOS, представленный корпорацией Apple в 2007 году.

Одним из первых вирусов, нацеленных на мобильные платформы, считается Timofonica, обнаруженный в июне 2000 года в Испании. Этот вирус заражал компьютеры, рассылая SMS-сообщения на мобильные номера телефонов [186]. На тот момент вычислительных мощностей телефонов было недостаточно для самостоятельного

заражения, поэтому автор придумал более остроумную схему: зараженные компьютеры рассылали электронные сообщения, которые затем посредством SMS-шлюзов рассылались на телефоны.

Одной из первых вредоносных программ непосредственно для мобильных телефонов считается игра Mosquito, отправлявшая SMS-сообщения без ведома пользователя.

Первым компьютерным червем, способным заражать мобильные телефоны, считается Cabir, разработанный для Symbian S60 в 2004 году в качестве доказательства концепции. Вредоносная программа отображала на экране телефона надпись “Caribe” и пыталась распространиться по сети Bluetooth на другие телефоны. Важно отметить, что без ведома пользователя червь не может заразить телефон. При передаче по Bluetooth, пользователь должен вручную принять файл, и некоторые телефоны даже выдают сообщение о том, что производитель ПО не проверен. Другая разновидность этого червя, известная под названием Mabir, способна рассылать себя не только по Bluetooth, но и при помощи MMS. Червь не был выпущен «на свободу», а был разослан производителям антивирусной продукции в качестве доказательства возможных атак на мобильные телефоны. Первым вирусом для Symbian OS, способным рассылать свои копии посредством MMS-сообщений, стал Commwarrior-A, впервые обнаруженный в марте 2005 года.

В качестве следующего значительного примера мобильного вредоносного программного обеспечения исследователи выделяют Duts, нацеленный на платформу Windows CE. Данный червь был подтверждением концепции. Вредоносное ПО не распространялось самостоятельно, а запрашивало согласие пользователя.

Другим важным шагом в развитии мобильных угроз стало вредоносное программное обеспечение Skulls, написанное для телефона Nokia 7610, работающего на платформе Symbian [67, 173]. Программа была впервые обнаружена в ноябре 2004 года. Её работа заключалась в существенном ограничении функциональности телефона. Программа не могла самостоятельно распространяться, для заражения требовалось, чтобы пользователь вручную запустил вредоносный файл.

Первым вирусом для iOS стал червь Ikee, впервые обнаруженный осенью 2009. Червь заражал телефоны с выполненным jailbreak и установленным сервером ssh, в котором пользователи не поменяли пароль по умолчанию. Вирус менял обои на рабочем столе и сканировал сеть мобильного оператора на наличие других телефонов с подобной уязвимостью [57].

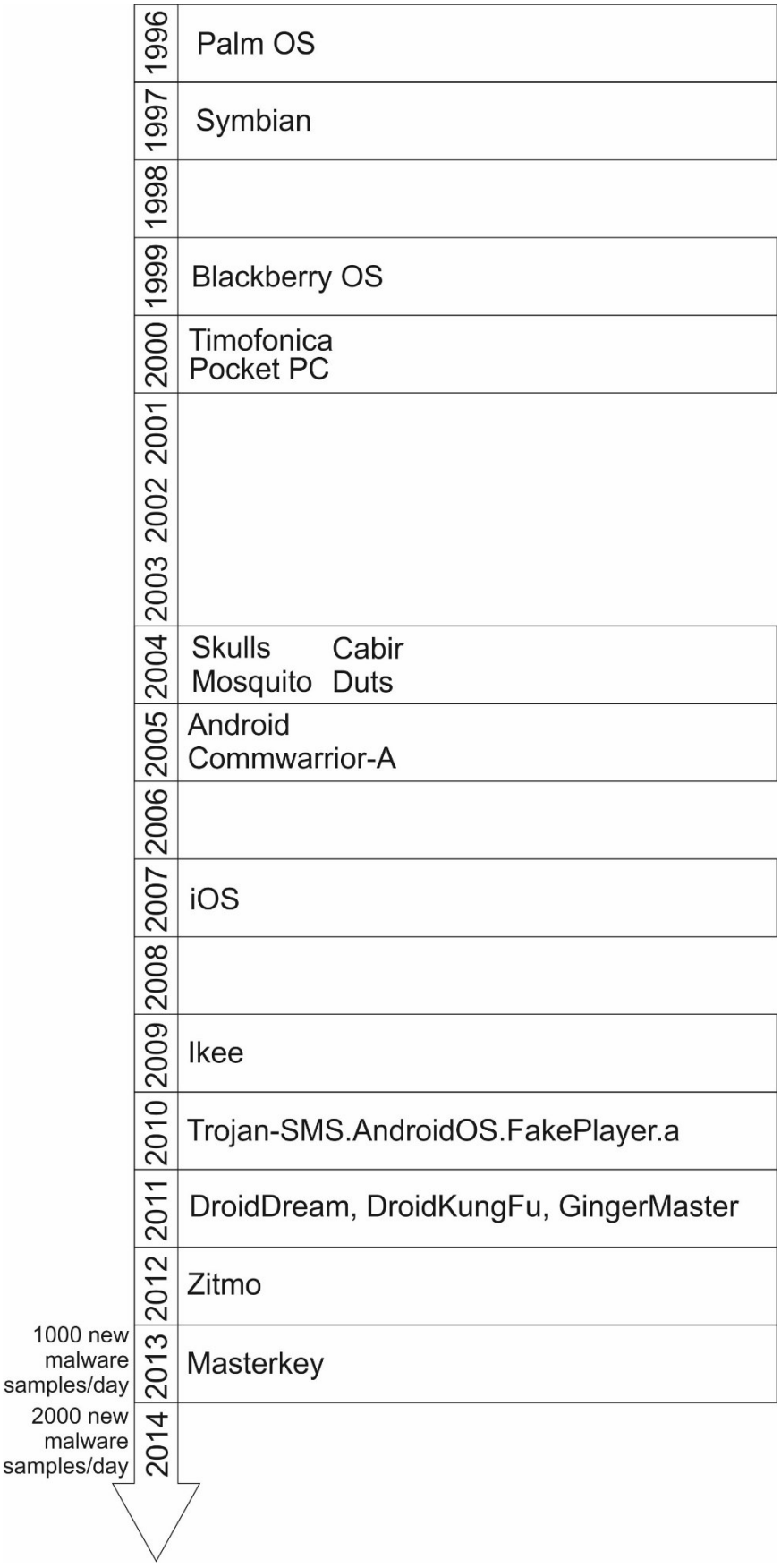

Рисунок 2.4. Основополагающие события развития мобильного сегмента теневой информационной экономики.

В августе 2010 года была обнаружена троянская программа FakePlayer, считающаяся первой в своём роде, нацеленной на операционную систему Android [104]. Программа рассылала СМС-сообщения на премиум-номера, за что со счета пользователя снимались значительные суммы денег. Пользователю предлагалось установить проигрыватель медиа-файлов размером немногим более 13 килобайт, который на самом деле был троянской программой. Как и все приложения для устройств, работающих на Android, это приложение при установке показывало список необходимых для корректной работы привилегий, среди которых числилась и отправка СМС с подсказкой о том, что данная услуга платная. Кроме того, приложение запрашивало права на чтение и изменение данных, а также на сбор информации об устройстве. Сразу после установки приложение начинало рассылать СМС-сообщения, которые обходились пользователям в несколько долларов без какого-либо оповещения владельца устройства. Программа была обнаружена и работала только в Российской Федерации и в российских сетях. В Android Market приложение обнаружено не было.

В противовес предыдущему примеру, DroidDream, обнаруженный весной 2011, был упакован в другие приложения, кажущиеся легитимными. Таким образом, вирус попадал на устройства пользователей, при этом в отличие от распространявшихся таким же способом Geinimi и HongTouTou, ориентированных на региональные рынки приложений, DroidDream был доступен в официальном Android Market [44]. Используя определенные уязвимости, этот вирус мог получить права уровня root на устройстве пользователя. По мнению исследователей компании Sophos [128], подобная эпидемия была вполне предсказуема благодаря очень низкому порогу вхождения на рынок для разработчиков. На тот момент он составлял 25 долларов США. С одной стороны, понятно желание корпорации Google привлечь как можно больше разработчиков на рынок, но с другой стороны, туда слишком просто попасть и злоумышленникам. В качестве меры по пресечению исследователь предлагает повысить ценовой порог вхождения.

Следующим важным шагом стало обнаружение вредоносного ПО DroidKungFu 31 мая 2011 года [82]. Программа распространялась на китайском рынке приложений и содержала в себе два рут-эксплойта в зашифрованном виде. После запуска приложение расшифровывало эксплойты и запускало атаку. Исследователь отмечает, что ни один из существовавших на тот момент антивирусных продуктов, предназначенных для устройств Android, не обнаруживал данное вредоносное ПО.

Эта же исследовательская группа в скором времени обнаружила новое вредоносное ПО, GingerMaster, которое распространялось аналогичным образом, однако использовало

куда более новую версию эксплойта [84]. Очень интересным наблюдением был тот факт, что после установки GingerMaster подключался к удаленному серверу для получения дальнейших инструкций. Исследователи отмечают, что данное вредоносное ПО способно скачивать с удаленного сервера файлы *.apk и устанавливать их, пользуясь правами root. Таким образом, мы наблюдаем явное применение принципов «классического» вредоносного ПО в мобильной среде. GingerMaster вполне попадает под классификацию downloader и может использоваться в схемах Pay-per-Install, описанных во второй главе.

Другим подтверждением данной тенденции может служить печально известное вредоносное ПО ZitMo, впервые обнаруженное в сентябре 2010 года [101]. Название его расшифровывается как ZeuS-in-the-Mobile. ZitMo является мобильной версией троянской программы ZeuS, которая обсуждалась ранее. Исследователи лаборатории Касперского обнаружили версии для ОС Android и Blackberry [102], причем для Blackberry было обнаружено сразу 4 образца. Примечательно, что платформа Blackberry редко становилась целью злоумышленников вследствие своей малой популярности. Это наталкивает на мысль о том, что атака могла быть целенаправленной. ZitMo был спроектирован для быстрой и незаметной кражи конфиденциальных данных жертвы. Схема обычно работает следующим образом: компьютерный ZeuS крадет данные о банковских счетах жертвы и номер мобильного телефона. Затем на мобильный телефон приходит СМС с просьбой установить обновленный сертификат или любое другое полезное ПО, однако ссылка из сообщения устанавливает на аппарат пользователя ZitMo. Получив доступ к мобильному телефону жертвы, злоумышленники могут совершать денежные переводы со счета жертвы, и когда банк отправит СМС-сообщение с кодом авторизации на мобильный телефон, злоумышленники смогут его перехватить и завершить операцию.

В августе 2013 года была обнаружена волна нового вредоносного ПО для Android, которое использовало уязвимость в процессе проверки прав приложения во время установки. Таким образом, приложение, представляющееся легитимным и запросившее достаточно скромный перечень привилегий, на самом деле могло выполнять практически любые действия на зараженном устройстве [63].

Компания Sophos в своём отчете утверждает, что в 2013 году каждый день в среднем появлялось около одной тысячи новых образцов вредоносного программного обеспечения для мобильных платформ. В первые месяцы 2014 года данная цифра выросла до двух тысяч.

2.2. Структура теневой информационной экономики

В сфере информационных технологий в общем, и в теневой информационной экономике в частности, продукты и услуги очень тесно взаимосвязаны и взаимозаменяемы. Зачастую между ними сложно провести четкую границу. Это в первую очередь связано с нематериальным характером информации и программного обеспечения. Структуру теневой информационной экономики сложно однозначно описать ввиду её быстрой и постоянной изменчивости, а также колоссальных масштабов. Кроме того, существует так называемый Dark Web, представленный на рисунке 2.5, границы и рамки которого крайне затруднительно очертить [105].

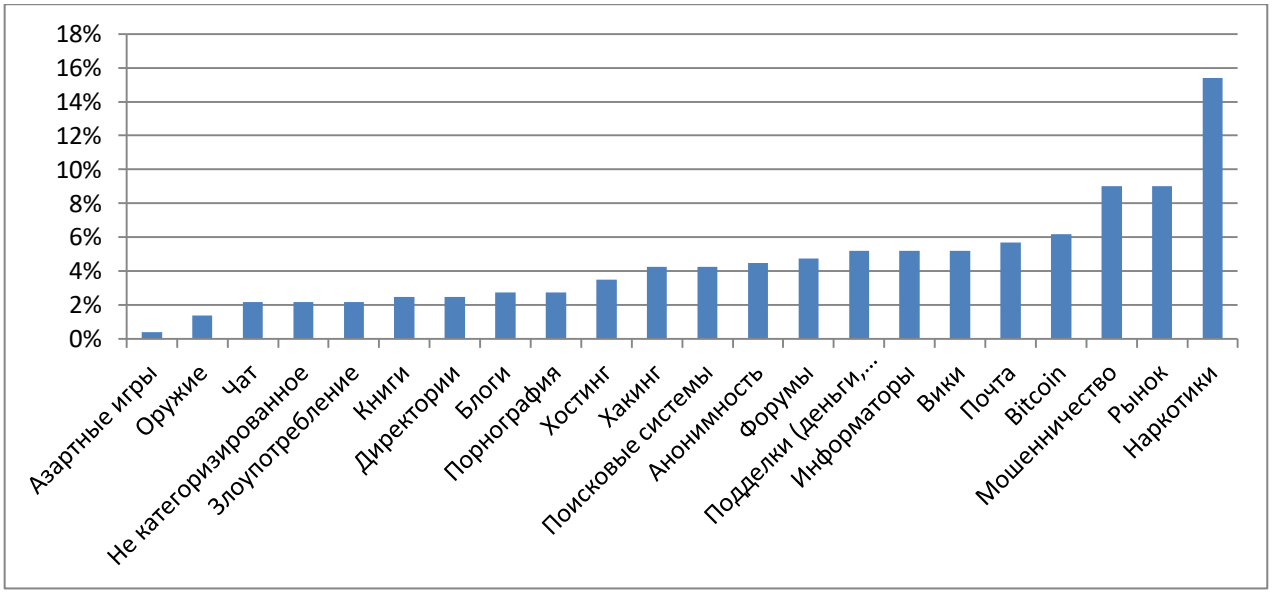

Рисунок 2.5. Состав Dark Web, процент от общего количества сайтов Dark Web, по данным исследователя Оуена Гарета [105].

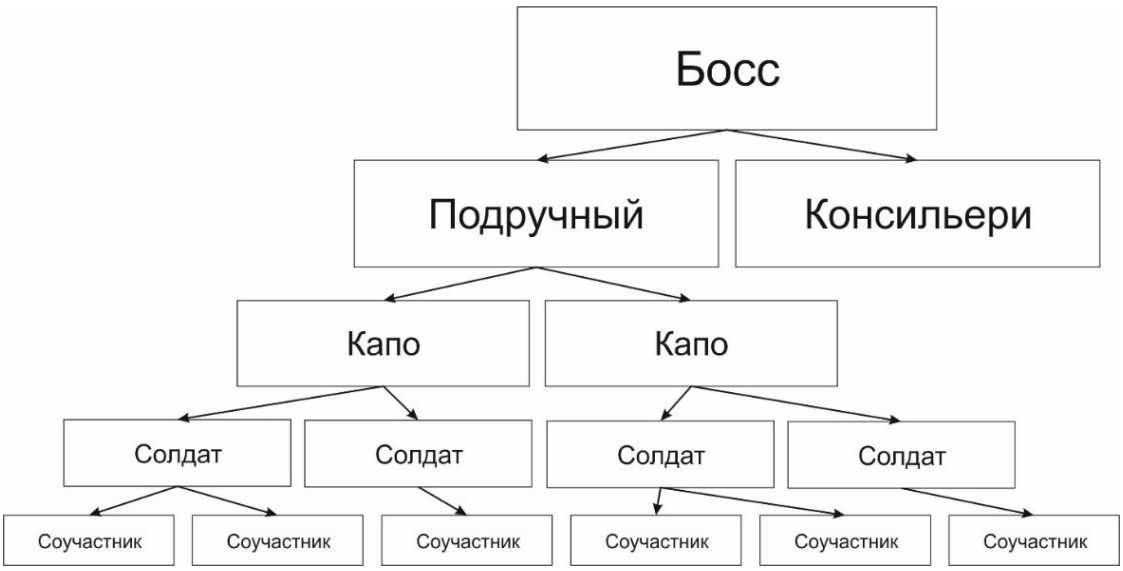

Рисунок 2.6. Типичная структура криминальной организации, разработано автором.

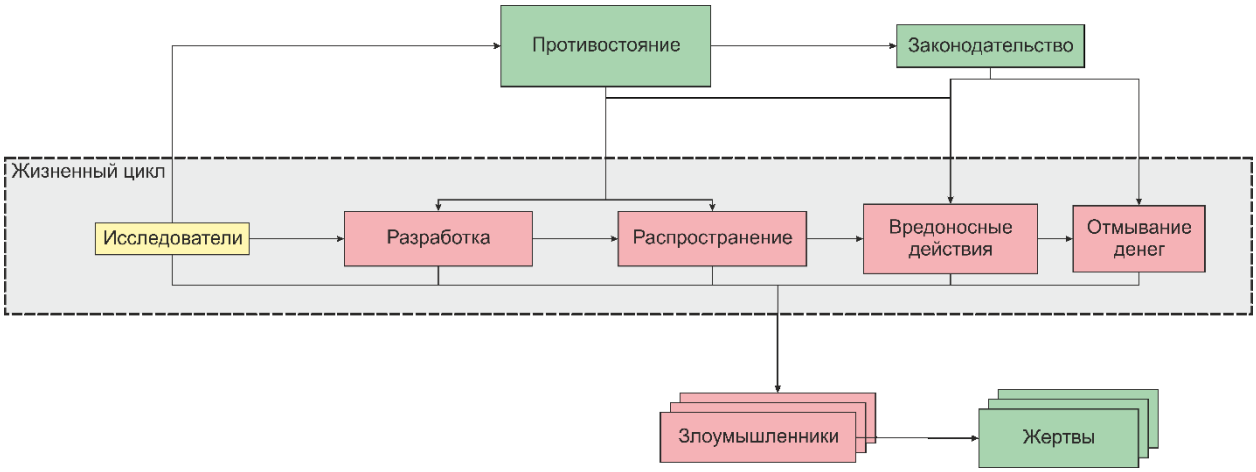

Рисунок 2.7. Обобщенная структура теневой информационной экономики, разработано автором.

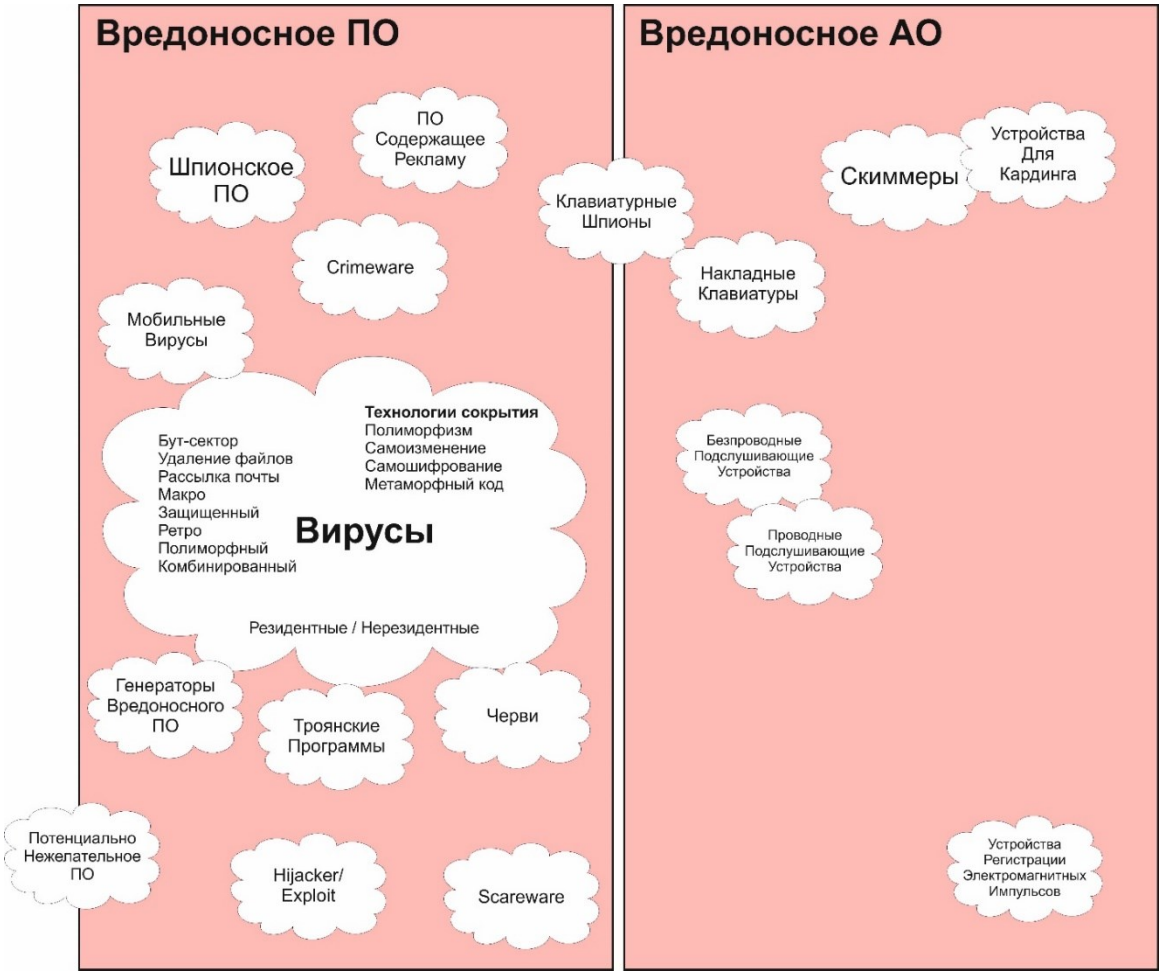

Рисунок 2.8. Детальная структура вредоносного программного и аппаратного обеспечения, присутствующих на рынке теневой информационной экономики, разработано автором.

Рисунок 2.9. Методики распространения вредоносного программного обеспечения, разработано автором.

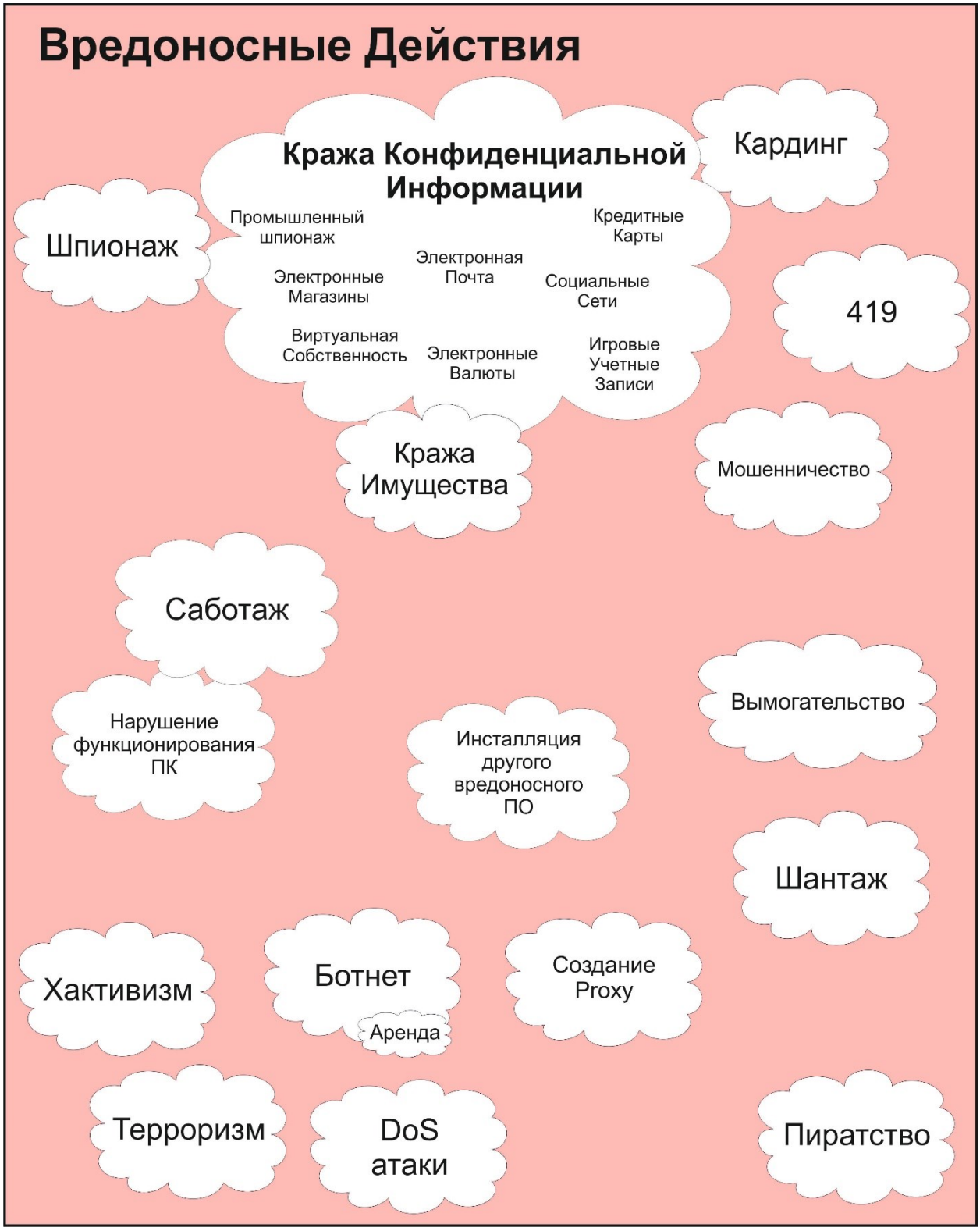

Рисунок 2.10. Типы вредоносных действий, обеспечивающих достижение целей злоумышленников, разработано автором.

Рисунок 2.11. Способы отмывания денег, заработанных в сфере теневой информационной экономики, разработано автором.

Среди правонарушений, характерных теневой информационной экономике, все чаще встречаются преступления, характерные для «классической» теневой экономики и криминала. Кроме того, их организационная структура может напоминать типичные структуры мафиозных сообществ, наподобие представленной на рисунке 2.6 древовидной структуры, характеризующей структуру сицилийских мафиозных группировок. Тем не менее, зачастую криминальные элементы в теневой информационной экономике действуют намного самостоятельней и структуры состоят из меньшего количества уровней, формируя более плоские модели [175, 182].

Обобщенная структура ТИЭ представлена на рисунках 2.7, 2.8, 2.9, 2.10, 2.11.

Продукты.

Продуктом в экономике называется нечто, предназначенное для удовлетворения потребностей и зачастую являющееся материальным. 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 [7, стр. 489-491, 32, стр. 138-140].

Модель жизненного цикла вредоносного ПО представлена на рисунке 2.12 и состоит из 6 этапов:

1. Анализ рынка – исследование популярности существующих программных продуктов, анализ вероятности нахождения уязвимости в них и т.д. Данный шаг позволяет выделить наиболее перспективные с точки зрения эффективности монетизации найденных уязвимостей программные продукты.
2. Анализ ПО – после того, как был выбран определенный программный продукт, начинается углубленный его анализ, поиск уязвимостей.
3. Разработка вредоносного ПО – на данном этапе осуществляется непосредственно реализация уязвимости в программный продукт, который на последующих шагах будет установлен на компьютер жертв с целью монетизации.
4. Распространение вредоносного ПО – заражение компьютеров жертв. Чаще всего используются так называемые дропперы, специализированные вредоносные программные продукты, устанавливающиеся на компьютеры жертв с целью предоставления возможности дальнейшей установки вредоносного программного обеспечения. Более подробно данная схема рассмотрена далее.

5. Использование вредоносного ПО с целью получения прибыли. Например, создание бот-нета, кража данных, добыча криптовалют и т.д.

6. Отмывание полученных на предыдущем этапе доходов, причём отмывание может осуществляться как при помощи информационных технологий, так и «классическими» способами. Важно подчеркнуть, что в информационной сфере могут отмываться и денежные средства, заработанные за её пределами.

Рисунок 2.12. Этапы жизненного цикла вредоносного ПО в сфере теневой информационной экономики, разработано автором.

К продуктам в сфере теневой информационной экономики, схематическая структура которых представлена на рисунке 2.13, относятся:

1. **Специализированное программное обеспечение**:

Рисунок 2.13. Схема структуры продуктов в сфере ТИЭ, разработано автором.

- **Adware** [100, 124]. 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** [100, 124] – 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. Согласно определению, данному лабораторией Касперского [150], к crimeware относится вредоносное программное обеспечение, скрытно устанавливаемое на компьютер жертвы. Также приводится информация о том, что большинство подобных программ является троянскими. Компания Panda Security считает [148], что crimeware не является самостоятельной категорией информационных угроз, а характеризует всё вредоносное программное обеспечение, объединенное общей целью: неправомерное получение денег

[61] или доступа к конфиденциальной информации. Компания относит к данной категории даже социальную инженерию, которая сама по себе не является программным обеспечением.

- **Вирусы** [107, стр. 28]:

a. **Загрузочный сектор**. Исторически является одним из векторов атаки компьютерных вирусов в связи с тем, что код из этих секторов выполняется при загрузке компьютера. Одним из исторических векторов заражения были дискеты, оставленные в дисководе, информация с которых читалась при запуске компьютера.

b. **Удаление файлов**. Архаичный вид злонамеренного программного обеспечения. В настоящее время почти не встречается ввиду своей экономической неэффективности.

c. **Макровирусы**. Написанные на языке макросов (например, скриптовые) языки, встроенные в текстовые редакторы. Поскольку некоторые программные продукты позволяют встраивать макроскрипты в документы и автоматически исполнять их при открытии, данный вектор заражения приводил к серьёзным вирусным эпидемиям в прошлом.

d. **Защищенный** – вирус, препятствующий попыткам уничтожить его.

e. **Ретро-вирус**. По аналогии с биологическими вирусами, носящими такое же название, ретро-вирус стремится обнаружить, атаковать и нейтрализовать установленный на заражаемом компьютере антивирус, если таковой имеется. Подобные вирусы также иногда называются анти-антивирусами.

f. **Полиморфный**. Технология изменения кода при каждом запуске, при этом она сохраняет свою функциональную нагрузку (программную семантику) и позволяет многим вредоносным программам избегать обнаружения, использующего сигнатурный метод анализа. К данной категории можно отнести и возможности самошифрования.

g. **Комбинированный**. Наиболее часто встречающийся вид вредоносного программного обеспечения, сочетающий в себе одновременно несколько технологий, упомянутых выше.

- **Генератор вредоносного программного обеспечения**. Например, Zeus [96], SpyEye. Они являются наборами инструментов для создания узконаправленного вредоносного программного обеспечения и объединяют зараженные компьютеры в сеть.

- **Hijacker/Exploit**. Под эксплоитом понимается программное обеспечение, набор команд, направленные на использование определённой уязвимости в программном обеспечении с целью заставить его вести себя непредвиденным образом. Чаще всего, подобные действия направлены на получение управления компьютером, повышение

привилегий, или отказ в обслуживании. Также могут использоваться целые наборы эксплойтов, такие, как, например, Blackhole [131].

- **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. Ярким примером может служить Blackshades. Согласно данным, предоставленным Брайаном Кребсом, данная программа была достаточно легкодоступна для приобретения в сети Интернет. В последние годы цена поднялась до нескольких сотен евро, однако ранние версии продукта стоили порядка 40 долларов США при покупке посредством PayPal. Доступны были и форумы, на которых пользователь мог получить поддержку по установке и настройке троянской программы. Уровень доступной поддержки позволял пользоваться программой, даже не имея технических знаний и навыков [88, 160].

- **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. [125, 178], пример представлен на рисунке 2.14. 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. Согласно исследованию [169], известны случаи, когда жертвы платили сто долларов США за подобное фиктивное программное обеспечение, а количество жертв измеряется миллионами. Исследователи утверждают, что три наиболее крупных представителя данной отрасли заработали в сумме более 130 млн долларов США. Согласно упомянутому

выше исследованию, scareware обычно используют три вектора заражения компьютеров: социальную инженерию, drive-by-download и ботнеты. Наиболее типичным вектором заражения выступает социальная инженерия: вредоносный или зараженный сайт показывает жертве сообщение о том, что его компьютер заражен, и предлагает скачать утилиту для его очистки.

Рисунок 2.14. Пример сообщения, отображаемого scareware, Association of Certified Fraud Examiners [169].

Первая из рассмотренных в вышеупомянутом исследовании программ предлагала три вида лицензии: на полгода, стоимостью 49,95$; на год, стоимостью 59,95$; на два года, стоимостью 69,95$. Примечательно, что все лицензии покупались в примерно равных пропорциях: на первую пришлось 34,8 %, на вторую 32,9 %, и на третью 32,3 %. Вторая программа предлагала лицензии на полгода (49,95$), год (69,95$) и пожизненную (89,95$). В данном случае, наиболее популярным оказался первый тип лицензии (61,9 %), за ним пожизненная лицензия (24,6 %) и годовая лицензия (13,5 %). Третий рассмотренный продукт предлагал всего два вида лицензии: на год за 59,95$ или пожизненную за 79,95$. Данный продукт также предлагал дополнительную круглосуточную поддержку за 19,95$, что подняло общую цену до 79,90$ за годовую лицензию (купленную 83,2 % жертв), и 99,90$ за пожизненную лицензию (16,8 % жертв). В общей сложности, пробная версия продукта 1 была установлена 8.403.088 раз, что привело к 189.342 продажам всего за три месяца (конверсия составила 2,4 %). Вторая

программа была установлена 6.624.508 раз, что привело к 137.219 продажам за 16 месяцев (конверсия 2.1 %). Третий продукт был куплен 1.969.953 раза, при количестве установок, равном 91.305.640 раз в период с марта 2008 по август 2010 (конверсия 2.2 %). Таким образом, жертвы scareware за рассмотренные периоды потеряли 11.303.494$ в случае первой программы, 5.046.508$ в случае второй и 116.941.854$ в случае третьей. Итого, если экстраполировать результаты первой компании на год, то они бы заработали 45 млн долларов США, вторая компания заработала 3,8 млн за год, а третья, будучи наиболее прибыльной, 48.4 млн долларов в год. Согласно данным, полученным исследователями, около 10 % жертв потребовали возврата денег.

- **Потенциально нежелательное программное обеспечение**. В своём исследовании McAfee [163] относит 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 [23]. 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. Не редки случаи заражения подобными вредоносными программами и в Республике Молдова.

2. **Шпионское аппаратное обеспечение**. Клавиатурные шпионы, устройства считывания электромагнитных импульсов, устройства перехвата беспроводных коммуникаций и т.д. [86]. Скрытое оборудование, используемое для наблюдения и считывания сигналов и получения доступа к вычислительной технике. Подобные устройства могут быть заложены как непосредственно в аппаратное обеспечение [41, 165], 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.

3. **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. Ущерб от подобных действий может оцениваться десятками и даже сотнями миллиардов долларов США, однако некоторые исследователи скептически относятся к подобным оценкам. Например, «Вашингтон Пост» в своей статье за 2006 год приводит оценку ущерба в размере 250 млрд. долларов [103], ссылаясь на представителей официальных властей, однако, Ричард Мента в своей статье подвергает подобный уровень ущерба сомнению [103]. Другие источники указывают меньшие, однако, всё равно, значительные цифры. Например, Business Software Alliance в своём ежегодном исследовании приводит рост размера рынка пиратского программного обеспечения с 58.8 млрд. долларов США в 2010 году до 63 млрд. долларов США в 2011 [53]. Однако и их данные ставятся под сомнение (techdirt) другими исследователями, утверждающими, что опрос в некоторых из заявленных стран проведен не был, а приведенные цифры являются всего лишь догадками [75] (techdirt). Счетная палата США в своём исследовании [150], затрагивающем не только информационную область пиратства, но и область подделки потребительских товаров, отмечает, что у оценки уровня пиратства, приведенной ФБР в своём отчете за 2002 год (200-250 млрд долларов США), на которые ссылаются многие исследования, отсутствуют описание использованной методологии оценки, ссылки на источники приводимых данных, а значит, их данные не подкреплены [80, 81]. Кроме того, в исследовании утверждается, что, несмотря на то, что некоторые ученые приводят в своих работах доводы в пользу пиратства, большинство из них сходятся во мнении о том, что негативные эффекты перевешивают позитивные. Однако, не имея конкретных данных, подтверждающих или опровергающих данные домыслы, в исследовании Счетной Палаты США говорится, что точный эффект для экономики (положительный или негативный) от наличия пиратства неизвестен.

В информационном пространстве существует такая субкультура, сообщество, которую обычно называют «Сцена». Участники данного сообщества занимаются тем, что модифицируют программное обеспечение таким образом, чтобы убрать из него защиту от пиратства или каким-либо другим способом его преодолеть (например, создав генератор ключей для данного программного продукта). При этом чаще всего они не преследуют материальные выгоды, а гонятся лишь за славой, стремясь «взломать» программный продукт раньше других [36]. Важно отметить, что помимо пиратской сцены существуют также и вирусная сцена, демосцена и т.д.

4. **Материалы и программные продукты, нарушающие пользовательское соглашение**. К этой категории относятся программы, позволяющие жульничать в многопользовательских компьютерных играх [99, 115]. 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 компании Bohemia Interactive предполагают, что около одного процента игроков готовы платить за возможность жульничества в этом и без того недешевом хобби. Таким образом, если взять официальные данные о количестве игроков в Counter Strike: Global Offensive в марте 2014 года, то есть 2.5 млн человек, то один процент составит 25 тысяч игроков, пользующихся подобными услугами. Вполне возможно, что многие пользуются подобными услугами дольше одного месяца. 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.

5. **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. Другим примером мошенничества в данной области может служить дело банка Heartland, в результате использования уязвимости в системе безопасности которого злоумышленники получили доступ к данным, принадлежащим 160-ти банкам. Ущерб, нанесенный банку Heartland, оценивается в 12,6 млн. долларов США. В мае-августе 2008 года группой злоумышленников из сети магазинов TJX и некоторых других были украдены данные 40 млн кредитных и дебетовых карт. Согласно отчету Panda Security [179], цены на аппаратуру для копирования кредитных карт составляют от 200 до 1000 долларов США. Поддельные банкоматы могут обойтись злоумышленникам в 3500$. Подобные устройства выглядят, как настоящие банкоматы, однако при попытке проведения операции они выдают пользователю ошибку, сохраняя при этом все данные об использованной карте: её номер, PIN-код и т.д. Они также могут быть использованы для кражи карт [36, 76].

6. **Уязвимости программного и аппаратного обеспечения** [8, стр. 278-281, 13, стр. 326-330]. В ISO/IEC 27005 [158] 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 [128] 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. Согласно отчету компании IBM [156], в 2013 году наиболее часто встречающимися уязвимостями были уязвимости, связанные с аутентификацией на веб-сайтах, в частности, уязвимости CSRF (23%), перехват сессии (23%), XSS (17%). На рисунке 2.16 предлагается модель, описывающая жизненный цикл типичной программной уязвимости.

На рисунке 2.15 представлено общее количество опубликованных эксплойтов для уязвимостей из базы данных CVE по годам, начиная с 1999 года.

7. **Персональные данные** [46, 48]. Согласно закону 133 от 08.07.2011, персональными данным считается «любая информация, связанная с идентифицированным или идентифицируемым физическим лицом (субъектом персональных данных). 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».

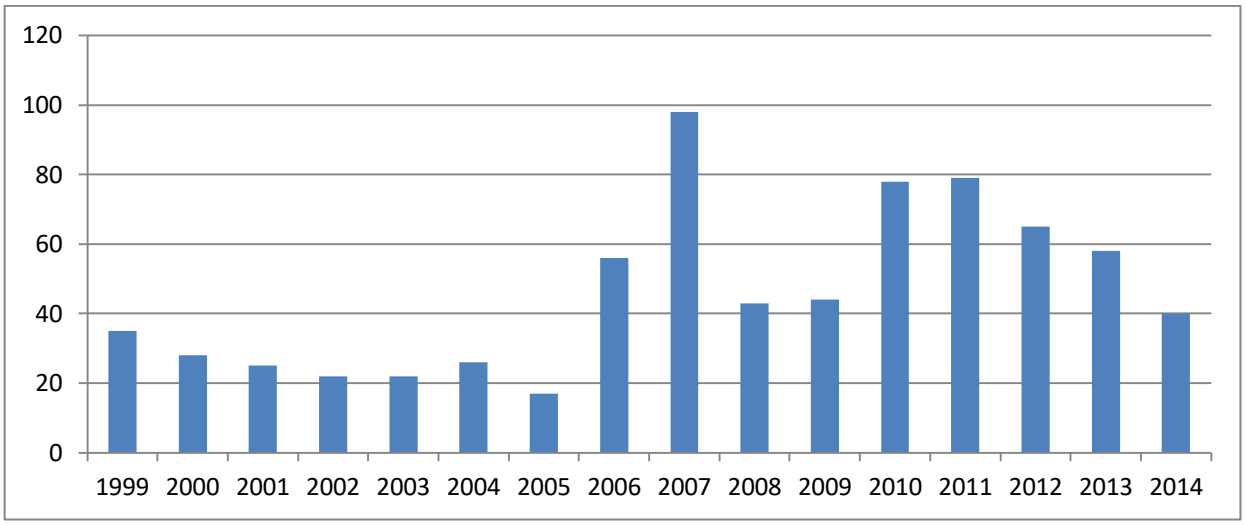

Рисунок 2.15. Количество выпущенных эксплойтов для уязвимостей из базы данных Common Vulnerabilities and Exposures, Verizon [186].

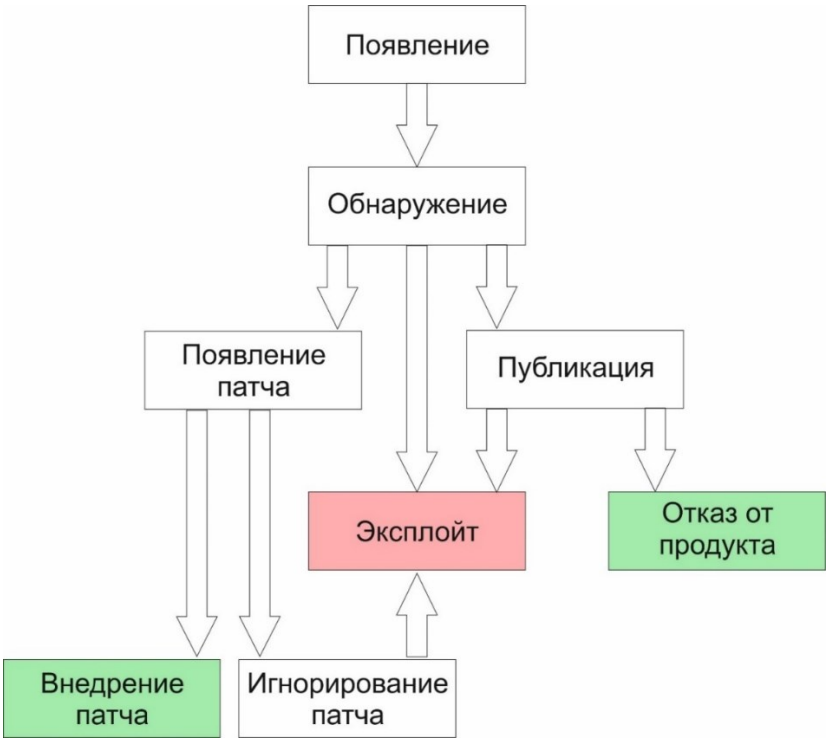

Рисунок 2.16. Этапы жизненного цикла уязвимостей, разработано автором.

Защита персональных данных должна быть одним из приоритетных направлений работы любой компании, обладающей, или имеющей доступ к подобным данным [14, стр. 323-327]. Утечка подобной информации может привести к так называемой «краже личности»: правонарушению, при котором преступник пытается выдать себя за другое лицо [107, стр. 28-29]. Кроме того, утечка информации может повлечь за собой отток клиентов и нанести катастрофический ущерб репутации компании, допустившей подобную утечку, что, несомненно, скажется на доходах. Согласно исследованию, проведенному компанией Symantec в 2012 году [160], в котором приняли участие 4506 респондентов из разных компаний, информация составляет порядка 49% стоимости их компании. Эта информация включает в себя, но не ограничивается персональными данными клиентов. Будучи спрошенными о том, какие последствия может повлечь за собой утечка информации, 20% опрошенных назвали падение цен на акции, 39% назвали увеличение издержек, 41% назвали снижение прибыли, 47% назвали ущерб репутации компании и 49% назвали потерю клиентов. Последствия утечки конфиденциальных данных представлены на рисунке 2.17.

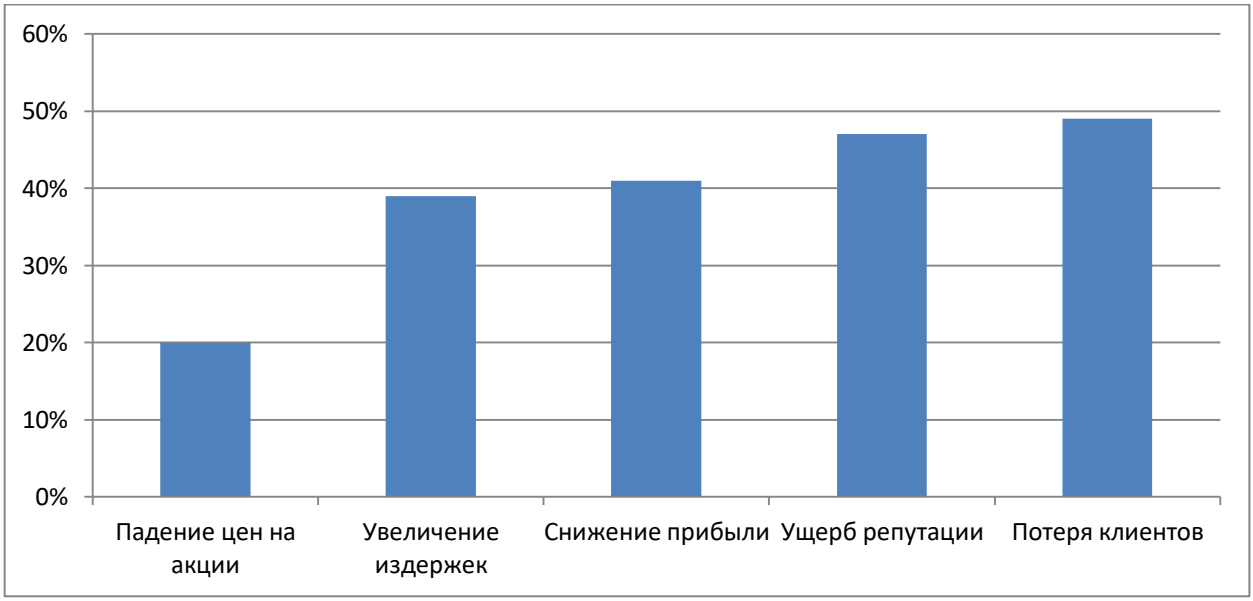

Рисунок 2.17. Последствия утечки информации, на основе данных Symantec [160].

Таким образом, по мнению Symantec, утечка информации повлечет за собой катастрофический ущерб. Приведенные цифры свидетельствуют о том, что компании осведомлены о возможных рисках, но, тем не менее, в течение 12-ти месяцев, предшествовавших исследованию, 69% компаний допустили утечку конфиденциальной информации, 69% допустили утечку информации, связанной с коммерческой тайной или бизнесом, а 31 % не соответствовали заявленным требованиям. Согласно исследованию,

проведенному компанией Digital Forensics Association [183] в 2011 году среди 3700 респондентов из 28-ми стран, основными векторами утечки конфиденциальной информации (рисунок 2.18) служат взломы, мобильные накопители информации, всемирная паутина, в то время как утечки информации вообще (рисунок 2.19), чаще всего происходят благодаря утере ноутбуков, взломам, нарушению процедур уничтожения отработанных материалов или их утере (чаще всего, бумажных носителей), социальной инженерии и всемирной паутине.

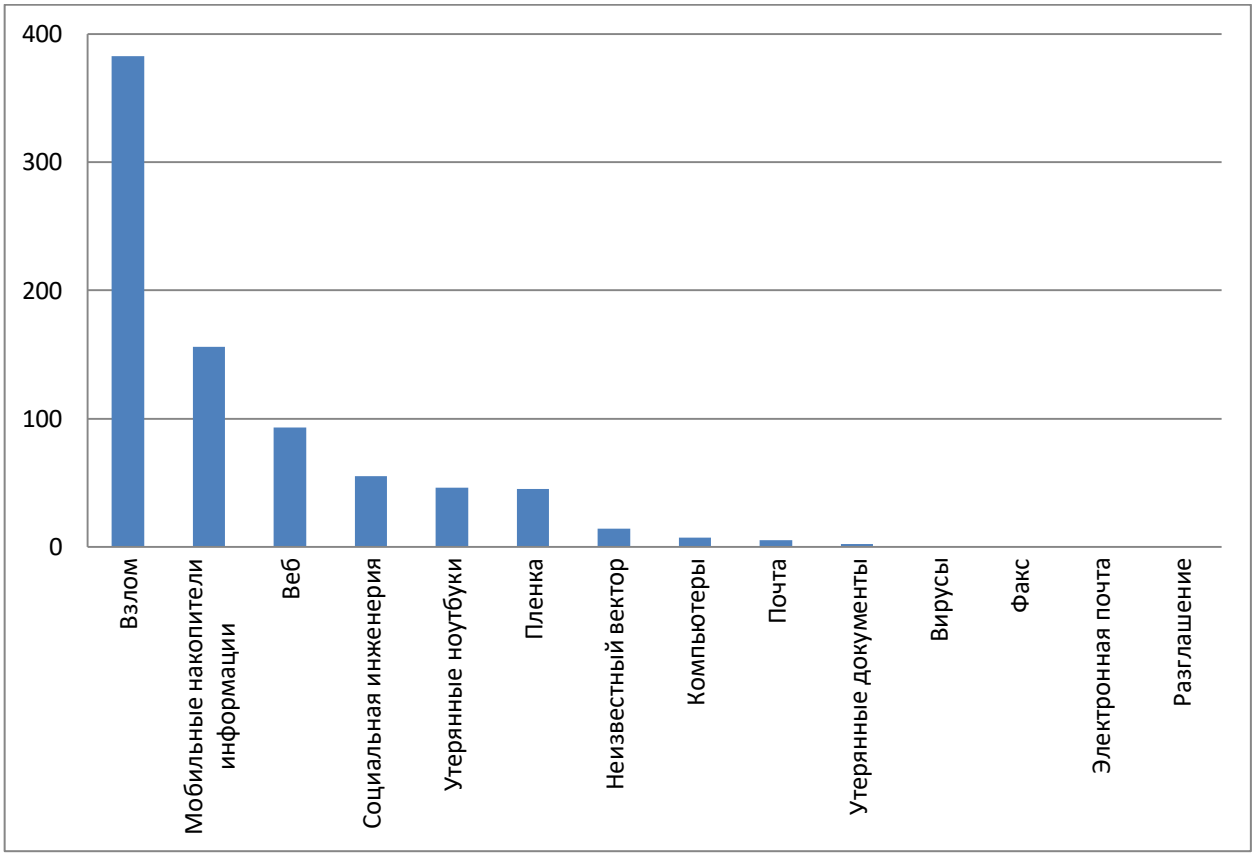

Рисунок 2.18. Векторы утечки конфиденциальной информации, по количеству инцидентов, согласно отчёту Digital Forensics Association [183].

Взломы чаще всего происходят из-за вредоносного программного обеспечения (35%), SQL injection (22%), скиммеров (14%) и украденных данных для аутентификации. Кроме того, значимым объектом атаки злоумышленников могут выступать и социальные сети, в связи с тем, что пользователи охотно хранят там свои персональные данные: имена, дни рождения, фотографии, сферы интересов и контактные данные.

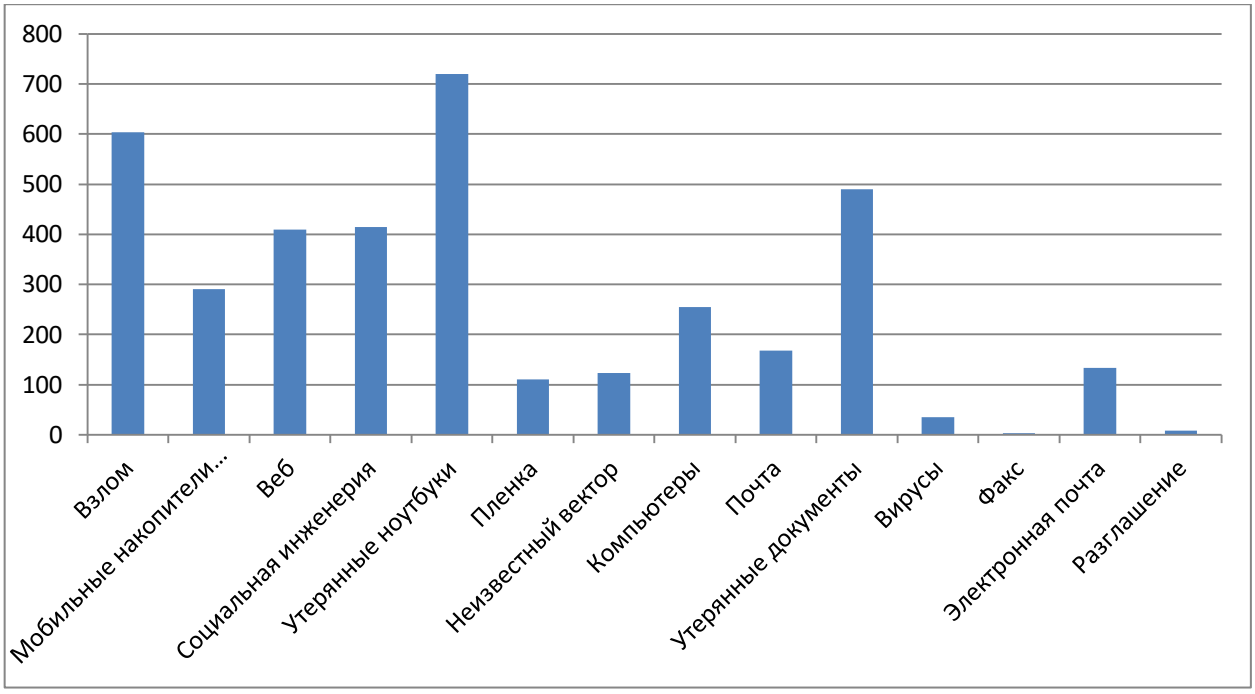

Рисунок 2.19. Векторы утечки информации, по количеству инцидентов, согласно отчёту Digital Forensics Association [183].

Кроме того, часто целью атаки становятся социальные сети, поскольку пользователи охотно публикуют свои персональные данные в открытом доступе. Согласно исследованию, проведенному компанией Imperva (рисунок 2.20) на хакерских форумах [153, 154], чаще всего целью злоумышленников становятся социальные сети Facebook (39%) и Twitter (37%).

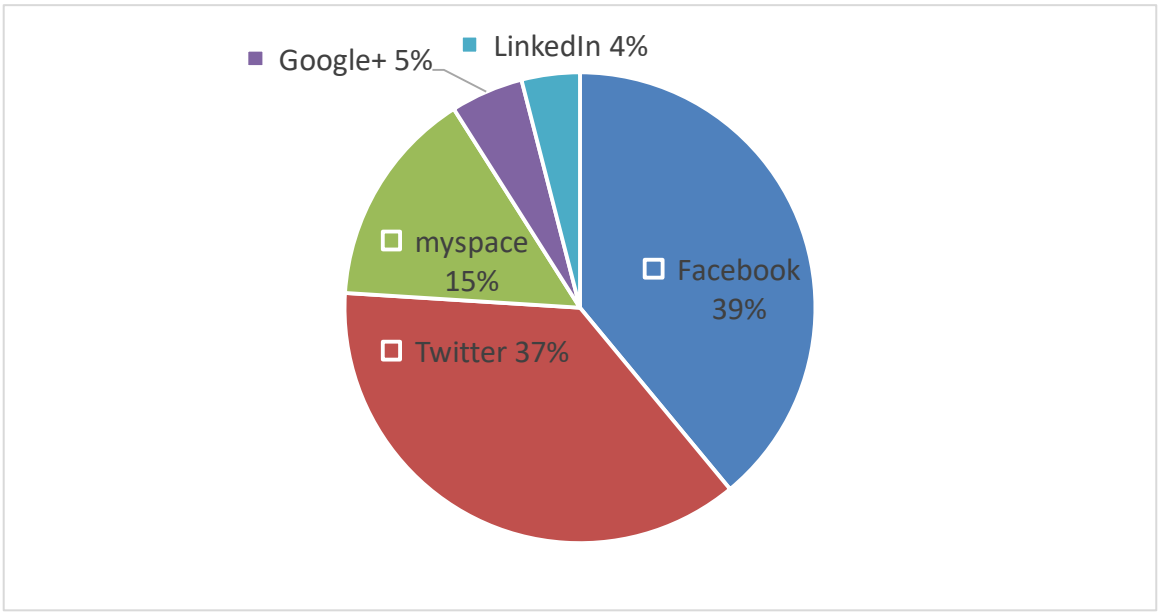

Рисунок 2.20. Социальные сети, наиболее часто подвергающиеся атакам со стороны злоумышленников, согласно отчёту Imperva [153, 154].

Imperva приводит эти данные на основе анализа частоты упоминания ключевых слов на форумах.

8. **Кибероружие** [68]. 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. Государственные структуры готовы платить значительные суммы денег за подобные уязвимости. Наиболее крупными компаниями, занимающимися исследованием программного обеспечения, являются ReVuln, Vupen, Exodus Intelligence, Netragard. Подобные компании не раскрывают своих клиентов, однако Шауки Бекрар, CEO компании Vupen, в одном из интервью признался, что их компания не продает уязвимости странам, имеющим конфликты со странами Европы или США [113, 165].

Услуги.

Как говорилось ранее, в ТИЭ категория услуг настолько плотно переплетена с категорией продуктов, что зачастую между ними достаточно сложно провести границу [7, стр. 491-493, 32, стр. 140]. Структура услуг в ТИЭ схематически представлена на рисунке 2.21. Рассмотрим наиболее яркие примеры услуг в сфере ТИЭ:

1. **Аналитика**, в том числе поиск и анализ уязвимостей программного и аппаратного обеспечения, анализ рынка и законодательства.

2. **Кража личных данных**, например, перехват идентификационных данных, кредитных карт, логинов и паролей. В исследовании Imperva [153, 154] утверждается, что очень часто на хакерских форумах пользователи предлагают вознаграждение за взлом чужих учетных записей в социальных сетях, чаще всего их целями является шпионаж, месть или просто развлечение. Большинство запросов сводятся к восстановлению или сбросу пароля, контрольного вопроса. Ещё одним важным течением в данной области в последнее время можно назвать мобильные кошельки. Данная технология пока не получила глобального распространения, однако, даже в тех немногочисленных странах, где её удалось внедрить, пользователи могут испытывать проблемы, связанные с

безопасностью данных [151]. Исследователи уже продемонстрировали некоторые уязвимости в NFC, используемой в мобильных телефонах для мобильных кошельков. Одной из основных уязвимостей является тот факт, что мобильные телефоны часто теряются и их владельцы очень редко предпринимают достаточные меры для защиты своей информации от злоумышленников.

3. **Software as a service** – сдача в аренду вредоносного программного обеспечения.

4. **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.

5. **Фарминг** (англ. pharming) – атака, целью которой является перенаправление трафика на другой, подставной веб-сайт.

6. **Вымогательство**. Согласно сообщению Риа Новости [94, 134], трех хакеров приговорили к 8-ми годам тюремного заключения за вымогательство денег у крупных интернет-казино. Они угрожали в случае невыплаты организовать атаки на их сервисы.

7. **«Нигерийские письма»**. Жертве обещают крупную сумму денег или прочие материальные ценности в обмен на оплату доставки или данные кредитной карточки. Примечательны случаи, когда у жертвы с каждым разом вымогают всё большие и большие суммы денег, ведь «вложив» определенную сумму денег, остановиться оказывается всё сложней. Особенно достоверно выглядят письма, отправленные с почтового ящика, знакомого жертве. Согласно исследованиям, в 2006 году общий ущерб от интернет-мошенничеств обошелся гражданам США в 198.4 млн долларов, большая часть этого ущерба пришлась именно на «Нигерийские письма» [116].

8. **Саботаж** – создание проблем в функционировании определенной системы или её частей, мотивирование прибылью.

9. **Терроризм** – применительно к киберпространству, саботирование систем или их частей, мотивированное убеждениями.

10. **Пиратство** – неправомерное копирование материалов в нарушение законов об авторских правах.

11. **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. Одним из интересных решений данной проблемы, используемых хакерами, является пропускание

интернет-трафика через спутниковые каналы связи. К такой методике прибегает, например, группа злоумышленников, называющаяся Turla [130].

12. **Отмывание денег при помощи информационных технологий**. Термин «отмывание» был впервые использован в США в 1980-ых годах и обозначал процесс преобразования нелегально заработанных денег в легальные доходы [20].

13. **Создание и сдача в аренду ботнетов**. На данный момент наиболее популярным набором инструментария для создания ботнетов являются Zeus и SpyEye. По данным исследования, проведенного MalwareIntelligence, оба набора предлагают модульную систему и предоставляют административную панель на основе веб-интерфейса. Процесс развертывания ботнета может выглядеть следующим образом: для начала злоумышленник может проверить полученный им ранее список данных доступа на фтп-сервера при помощи утилиты FTP Checker. Другая утилита, FTP Injecter, служит для соединения с проверенными предыдущей программой фтп-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 эксплойт. Данные о стоимости аренды ботнетов приведены в таблице 2.1. 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.

Рисунок 2.21. Структура услуг в сфере ТИЭ, разработано автором.

Таблица 2.1. Стоимость аренды ботнета, по данным корпорации DELL [184]

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

14. **DoS-атаки** [11, стр. 217-218, 69, 150, 179]. 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 [59]. Некоторые злоумышленники также загружают на взломанные веб-сайты так называемые шеллы (англ. shell), небольшие бэкдор-скрипты, позволяющие им загружать, удалять, просматривать и запускать файлы на скомпрометированный веб-сайт, а также организовывать DDoS-атаки [89]. Подобный подход эффективен благодаря куда большим вычислительным мощностям и пропускным

способностям, доступным на веб-серверах по сравнению с обычными пользовательскими компьютерами. Подобные услуги были доступны на сайте absoboot.com, также доступном по адресу twbooter.com. Любой желающий мог зарегистрироваться, рассчитаться при помощи какой-либо виртуальной валюты и начать пользоваться услугами сайта. Минимальная покупка составляла 15 долларов США при оплате PayPal и гарантировала 5 часов DDoS-атаки [92]. Кроме того, сервис предлагал услуги по организации DDoS-атак на определенного пользователя. Злоумышленникам предлагалось отправить жертве ссылку на изображение, которая имитировала популярный сервис хранения изображений imageshack.us и записывала IP-адрес пользователя, открывшего его. Получив IP-адрес жертвы, злоумышленник мог начинать атаку. Статистика, представленная на сайте, утверждала, что зарегистрировано более 450 пользователей, которые использовали сайт для запуска более 5816 DDoS-атак, другими словами, каждый пользователь использовал в среднем около 13 раз [146].

15. **Спам** [105]. Согласно отчету Panda Security [179], многие из существующих ныне 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 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. Почти всегда спамеры стремятся избежать обнаружения, поэтому в комплект утилит, необходимых для рассылки спама, могут входить и анонимизаторы, и VPN для доступа к панели управления спамботами. В своём квартальном отчёте компания IBM [156] исследует корреляцию между количеством разосланного спама и использованием операционной системы Windows XP. В связи с прекращением поддержки этой операционной системы разработчиком, обнаруженные уязвимости не исправляются, что в купе с широкой распространенностью данной системы развязывает руки злоумышленникам. IBM утверждает, что на момент исследования около 95 % банкоматов в США работали на операционной системе Windows XP. Сходную ситуацию можно наблюдать и в Республике Молдова, что способствует возможности использовать данную уязвимость [66].

16. **Изготовление поддельных кредитных карт**. Согласно отчету компании Panda Security [179], 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.

17. **Курсы, семинары, обучение** [184]. Некоторые хакеры готовы не только осуществить 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.

2.3. Монетизация продуктов и услуг в сфере теневой информационной экономики

Под монетизацией понимается процесс извлечения прибыли из злонамеренных продуктов и услуг в области теневой информационной экономики [45, стр. 100-101].

Для начала рассмотрим процесс монетизации уязвимостей в сфере теневой информационной экономики.

1. **PPI** (pay-per-install, англ. оплата за установку) – услуга, предлагающая посредничество в установке вредоносного программного обеспечения на компьютеры жертв. Оплата производится за каждую подтвержденную установку. Таким образом, злоумышленники могут монетизировать уязвимости, позволяющие установку вредоносного программного обеспечения. Обычно сначала устанавливается так называемый downloader (загрузчик), который в дальнейшем скачивает дополнительные программы, получая команды от контролирующего сервера. Данная схема получила широкое распространение благодаря возможности получения существенного заработка за счёт установки множества вредоносных программ на каждый зараженный компьютер, а также дополнительной автоматизации процесса установки. Данная услуга также может предлагать установку лишь определенному типу жертв, например, жителям определенной страны или представителям определенных профессий. Цены могут варьироваться в зависимости от эффективности сервиса, используемого аппаратного обеспечения, количества успешных установок, определенных категорий жертв и т.д., например, сервис blackhole стоит 50$ в сутки при использовании сервера, предоставляемого сервисом, или 700$ за три месяца при условии использования оборудования заказчика. Данная компания

также проводит периодические закупки существующих эксплойтов. Примечательно то, что некоторые сервисы установки пытаются обнаружить присутствие конкурирующих сервисов в зараженной системе и предпринимают попытки их удаления [19, 51, 54, 88, 93, 138]. Модель процесса монетизации представлена на рисунке 2.22.

2. **Продажа** [13, стр. 326-330]. Как демонстрирует Rainer Boehme в своей работе Vulnerability Markets [44], на рынке существует четкая система продажи и покупки уязвимостей и багов в программном и аппаратном обеспечении. Среди наиболее распространенных типов рынков уязвимостей, исследователь выделяет конкурсы, аукционы, брокерство, производные уязвимостей и киберстрахование. Под конкурсами понимаются программы, организованные разработчиком программного обеспечения, стимулирующие поиск уязвимостей и их дальнейшее разглашение только разработчику за определенное вознаграждение, которое чаще всего оговаривается заранее и его размер может варьироваться в зависимости от серьёзности найденной уязвимости. Подобные программы организовывали Mozilla, Google, Microsoft и многие другие. Также под конкурсом могут пониматься соревнования, на которых ИТ-специалистам предлагается найти уязвимость в определенном программном обеспечении за отведенное время, а победители получают призы. Например, конкурс Pwn2own, участникам которого предлагается заполучить полный контроль над устройством, пользователь которого всего лишь нажал на ссылку. В качестве вознаграждения участникам выдается само устройство, в котором была найдена уязвимость. Чаще всего участники приезжают на конкурс с заранее заготовленными эксплойтами. Аукционы отличаются от конкурсов, а также обуславливают свое существование, по мнению исследователя, главным образом инициативностью продавца. Продавец может быстро и самостоятельно начать аукцион, не дожидаясь приглашения. Под брокерами чаще всего понимаются узкие круги обмена уязвимостями, которые платят деньги за новые уязвимости, а потом могут рассылать их своим клиентам, подписавшимся на услуги данной компании. Обычно, уязвимости намного выгодней продавать брокерам, чем непосредственно разработчикам на конкурсах. Цены на уязвимости приведены в таблицах 2.2 и 2.3.

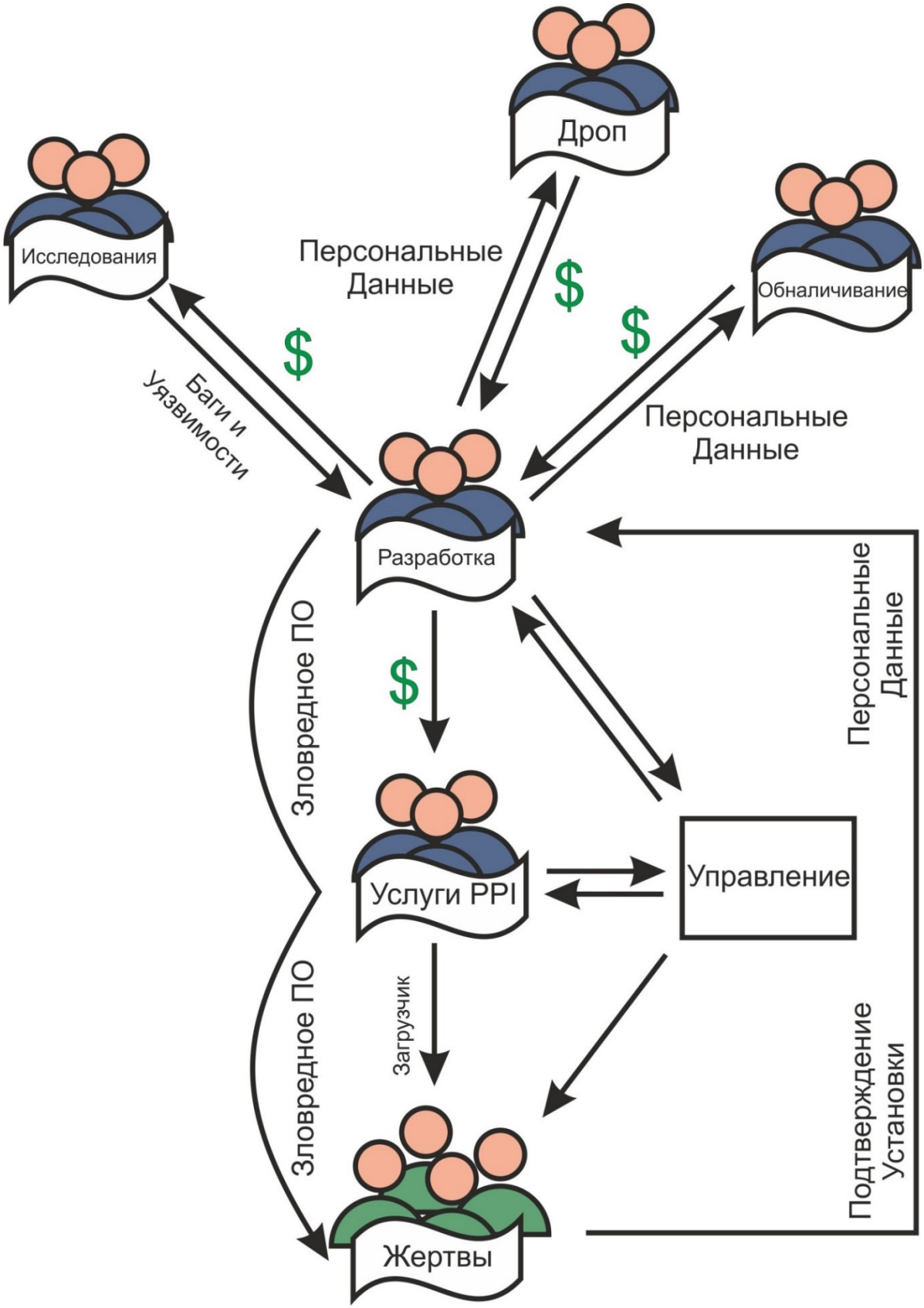

Рисунок 2.22. Схема монетизации PPI.

Таблица 2.2. Цены на уязвимости в программном обеспечении, expocod.com, январь 2017

	Программный продукт	Стоимость уязвимости, доллары США
1	Adobe Acrobat	55,000
2	Adobe Flash	55,000
3	Chrome	60,000
4	Internet Explorer	50,000
5	Edge	50,000
6	Safari	55,000
7	Firefox	45,000
8	Opera	35,000
9	Tor	80,000
10	Microsoft Excel, Word	60,000
11	Windows	55,000
12	OS X	45,000
13	Linux	35,000
14	VM	50,000
15	Android	50,000
16	iOS	80,000
17	Apache HTTP Server	60,000
18	OpenSSL	60,000
19	PHP	50,000
20	vBulletin, phpBB, myBB, Drupal, Joomla, Wordpress	15,000

Таблица 2.3. Цены на уязвимости в программном обеспечении, по данным исследователя Rainer Boehme [44]

	Программный продукт	Стоимость уязвимости, доллары США
1	Adobe Reader	5,000 - 30,000
2	MAC OSX	20,000 - 50,000
3	Android	30,000 - 60,000
4	Flash or Java Browser Plug-ins	40,000 - 100,000
5	Microsoft Word	50,000 - 100,000
6	Windows	60,000 - 120,000
7	Firefox or Safari	60,000 - 150,000
8	Chrome or Internet Explorer	80,000 - 200,000
9	IOS	100,000 - 250,000

Механизм работы рынка производных отличается от ранее упомянутых тем, что вместо того, чтобы покупать уязвимости, заключается контракт, согласно которому одна из сторон обязуется заплатить определенную сумму в случае наступления определенных событий, связанных с безопасностью. В качестве примера приводится контракт, гарантирующий владельцу определенную сумму денег в том случае, когда в определенный момент времени будет существовать эксплойт, позволяющий получить root права в конкретно заданной версии SSH на определенной платформе. В случае же страховки клиент застрахован от финансовых потерь, связанных с брешами в информационной безопасности. В своей статье Brian Krebs утверждает [92], что продавать уязвимости на черном рынке или частным покупателям куда выгодней, чем производителям программного обеспечения, даже несмотря на то, что в последнее время они стали предлагать более значительные вознаграждения. Как уже было упомянуто ранее, стоимость уязвимости напрямую зависит от программного продукта, в котором она была найдена, однако, это не единственный фактор, влияющий на её цену. Наиболее важные факторы, влияющие на цену уязвимости, приведены ниже:

- Популярность программного продукта, в котором была найдена уязвимость. Соответственно, чем популярней определенный продукт, тем больше жертв возможно заразить при помощи уязвимости и тем она может быть дороже. Цены на уязвимости в

таблицах 2.2 и 2.6 обоснованы, главным образом, популярностью перечисленных программных продуктов.

- Статус Zero Day. Известно ли разработчику или кому-то ещё о данной уязвимости. Статус Zero Day повышает цену уязвимости, однако, нет никаких гарантий долгосрочного сохранения этого статуса, поэтому, продавец зачастую заинтересован продать её в кратчайшие сроки, а покупатель может быть вынужден использовать её как можно скорее.
- Эксклюзивность. Определенная уязвимость может быть продана одному лицу, или же группе лиц. Если уязвимость продается эксклюзивно одному единственному покупателю, то и стоит она значительно дороже.
- Версия программного продукта, в котором была найдена уязвимость. Уязвимости, исправленные в более новых версиях программного продукта, будут стоить меньше, даже если о них неизвестно широкой публике.
- Возможность эксплуатации и стабильность эксплойта. Некоторые уязвимости невозможно использовать самостоятельно, а только в тандеме с другими уязвимостями.
- Вектор применения. Чем меньше действий должен совершить пользователь, чтобы запустить вредоносный код, тем дороже уязвимость.
- Насыщенность рынка. Очевидно, что в некоторых странах больше исследователей, чем в других. В цифровом мире эти границы не столь очевидны и значимы, тем не менее, некоторые исследователи предпочитают продавать уязвимости только на рынке своей страны. Хорошим, годным примером такой страны может служить Китай. Таким образом, на некоторых рынках уязвимости стоят дешевле, чем на других.
- Доступность других уязвимостей для данного продукта. Очевидно, что чем больше уязвимостей доступно для определенного программного продукта, тем ниже ценность каждой из них.
- Время между запуском уязвимости и получением ответа. В наши дни с развитием вычислительных мощностей и скорости передачи данных по сети этот фактор потерял свою практическую значимость, однако ранее он имел определенное значение.

3. **Кража** – первый этап. Например, получение неправомерного доступа к базе данных веб-сайта, занимающегося продажами и хранящего данные кредитных карт пользователей. Затем дальнейшее использование или продажа персональных данных. Важно отметить, что цена на данные о кредитных картах может варьироваться в зависимости от того, гражданином какой страны является её обладатель, от недавних

крупных брешей в информационной безопасности, в результате которых на рынок единовременно попало значительное количество данных об украденных кредитных картах [40].

Затем, рассмотрим способы монетизации личных данных [78]. Например, данных кредитных карт, социальных сетей. Рассмотрим каждую из этих категорий подробней:

2. **Данные кредитных карт**, номера банковских счетов [11, стр. 218, 134, 135, 136, 138]

- **Дроп** [10, стр. 416] – передача незаконно заработанных денег или товаров, купленных на такие деньги через посредников. Главной функцией данной операции выступает увеличение количества звеньев в цепи отмывания денег и, как следствие, усложнение поиска всех участников. Чаще всего в подобной схеме выделяют трех участников: Покупатель, Мул и Продавец. Покупатель приобретает в интернет-магазинах товары, рассчитываясь за них при помощи украденных карточек, указывая в качестве получателя адрес Мула. Затем Мул пересылает полученный товар Продавцу, а тот в свою очередь сбывает товар на местном рынке, разделяя прибыль между всеми участниками. Подобная схема затрудняет выявление всех задействованных лиц, а также помогает преодолеть межгосударственные барьеры в тех случаях, когда они накладываются интернет-магазинами (например, ограничение стран, в которые интернет-магазин доставляет свои товары). Данная схема может быть применена и к обналичиванию денег с поддельных карт. В отчете Panda Security приводятся данные о наличии специализированных дроп-сервисов [179], цены на которые приведены в таблице 2.4. Сервис обещает доставить товар в любую точку мира и даже выполнить за клиента покупку в любом электронном магазине. Чаще всего совершаются покупки в крупных, известных интернет-магазинах, таких как amazon, newegg, ebay и т.д.
- **Оффшор** [10, стр. 416]. Привлечение иностранного капитала путем предоставления налоговых льгот или прочих привлекательных финансовых условий. В сфере теневой информационной экономики под данной категорией чаще всего подразумевается проведение денежных сумм через нескольких посредников таким образом, чтобы максимально усложнить задачу отслеживания их происхождения. Согласно отчету Panda Security [179], подобные операции обходятся в 10-40 % от общей суммы перевода, в зависимости от самой суммы. Приведенный в отчете источник указывает градацию, представленную в таблице 2.5.

Таблица 2.4. Стоимость доставки продуктов при использовании дроп-схем, по данным Panda Security [179]

Тип товара	Стоимость доставки, $
Ноутбук	300
Мобильный телефон	60
Цифровая камера	30
Телевизор	100
Переносной DVD-проигрыватель	30
Видеокамера	30
Домашний кинотеатр	50
Проектор	150

Таблица 2.5. Комиссия при отмывании денег посредством оффшора, по данным Panda Security [179]

Сумма транзакции, доллары США	Комиссия, %
200 – 399	40
400 – 599	30
600 – 999	20
1000 и более	15

При этом чаще всего различные провайдеры услуг соревнуются не в уровне взимаемой комиссии, а в скорости и надежности самой транзакции. Представленный в отчете источник утверждает, что способен провести транзакцию за 15-30 минут от момента получения заказа.

- **Продажа кредитных карт**, номеров банковских счетов. Данный метод монетизации выгоден тем, что злоумышленник, укравший данные, значительно уменьшает риск поимки, так как не обналичивает деньги с украденных карт самостоятельно. В интернете существуют порталы, предлагающие свои услуги посредничества и предоставления платформы для покупки и продажи украденных данных

кредитных карт. Цены варьируются в зависимости от страны-эмитента, типа карты (кредитная/дебитная), количества покупаемых карт. Некоторые источники утверждают [114], что цены на карты могут варьироваться от 10$ за кредитную карту американского банка до 50$ за европейскую кредитную карту, объясняя это простотой монетизации и соотношением спроса и предложения на рынке. Например, если в сеть утекла база данных американских карточек, цена на них заметно упадет. Отчет об исследовании, проведенном компанией Panda Security [179], приводит минимальную стоимость одной кредитной карты Visa/MasterCard американского банка 2$ в качестве наиболее дешевой карты, и 30$ за карту из Великобритании. Продавец может гарантировать наличие денег на счету, начиная от двадцати тысяч, вплоть до полумиллиона долларов США. Подобная информация может стоить от 80$ до 700$. В отчете также отмечается, что продавцы проводят очень четкую границу между счетами, принадлежащими физическим и юридическим лицам, поскольку последние чаще всего содержат куда более значительные суммы. Счета PayPal могут стоить от 10 до 1500 долларов США, в зависимости от наличия на них подтвержденной суммы денег [62]. Согласно отчету компании DELL [184], стоимость золотых и платиновых кредитных карт может составлять 35 долларов США, в то время, как обычные карты стоили по 17 долларов. Карты виза премиум стоят 23 доллара. Авторы сайта заявили, что у них в наличии есть 14 миллионов кредитных карт граждан США, 294 тысячи карт Бразильского происхождения, 212 тысяч карт из Канады, 76 тысяч карт из Великобритании, 27 тысяч кредитных карт, выпущенных в ЕС и 342 тысячи карт из всех остальных стран. Другой сервис предлагал кредитные карты оптом, предоставляя существенную скидку. Так, при покупке 10-ти карт, цена за единицу составляет 13 долларов, в то время, как при покупке 2000 и более карт, цена за единицу составляет 9 долларов США. Ещё одним интересным трендом, отмеченным исследователями является то, что злоумышленники предоставляют гарантию на продаваемые карты, обещая заменить их в том случае, если они не будут работать.

- **Системы электронных платежей**, таких как Hawala [133], основанные на взаимном доверии и неформальных связях. В официальных платежных системах, таких как Swift, любые денежные переводы журналируются, а переводы крупнее определенной суммы (например, 10000 долларов США в Америке, 15000 евро в Европе) должны быть проанализированы, в том числе их источник. В неформальных же подобные данные могут не храниться, доступ к ним может быть затруднен или ограничен [10, стр. 416].

- **Поддельные документы** [184]: удостоверения личности (100-200 долларов), паспорта (200-500 долларов), водительские удостоверения (100-150 долларов). В том же

отчете со ссылкой на ФБР утверждается, что в период с 30-го декабря 2013 года по 23 июня 2014 было продано 1514 водительских удостоверений на общую сумму 232.660 долларов США.

- **Триангуляция** [89] – вид мошенничества, при котором злоумышленник продает востребованные вещи на интернет-аукционах по заниженным ценам, которых у него на тот момент ещё нет. Как только аукцион заканчивается, злоумышленник покупает вещь в интернет-магазине, расплачиваясь украденной карточкой и в качестве адреса доставки, указывают адрес победившего на аукционе пользователя.

3. **Учетные записи социальных сетей, электронные адреса, контактные данные** [88]. Важно подчеркнуть, что подобные данные могут быть как украдены, так и созданы автоматизировано, используя уязвимости процесса регистрации (например, автоматизированное распознавание captcha), что зачастую является нарушением пользовательского соглашения. В последнее время создавать фиктивные аккаунты в социальных сетях, почтовых службах становится всё сложней в связи с новыми технологиями защиты. Например, компания Google требует при регистрации указать валидный, ранее незарегистрированный номер телефона, который будет в дальнейшем проверен отправкой СМС-сообщения. Компания Twitter проводила исследование, в ходе которого на теневом рынке покупались аккаунты данной компании. В общей сложности за 10 месяцев было потрачено 5000 долларов США. Типичная стоимость аккаунтов данной социальной сети составила 0.02 – 0.10 долларов. Данное исследование помогло выявить закономерности в регистрации поддельных аккаунтов. В дальнейшем оно позволило компании закрыть 95% из них. После проведения данного закрытия, исследователи снова купили несколько тысяч аккаунтов Twitter, 90% которых оказались нерабочими вследствие проведенной ранее работы. Однако через несколько недель, когда исследователи купили ещё несколько тысяч аккаунтов, нерабочими из них оказались только 54%. В заключении компания подчеркивает, что необходимо усложнять процесс регистрации, например, посредством использования подтверждения регистрации через номер телефона и т.д. В отчете Panda Security [179] упоминается, что стоимость аккаунта может зависеть от того, насколько давно он был создан, объясняя это тем, что обычно более новые аккаунты проявляют большую активность. Так, например, аккаунт, созданный не позднее последних трех месяцев, может стоить на 80% дороже, чем тот, дата создания которого неизвестна. Подобные учетные записи могут быть использованы злоумышленниками для:

- Рассылки спама;

- Рассылки сообщений со ссылками на сайты, распространяющие вредоносное программное обеспечение.

4. **Покупки, совершаемые непосредственно жертвами**. Например, покупка лицензии scareware, плата за разблокировку компьютера и т.д. На первом этапе жертва предоставляет данные своей кредитной карты злоумышленнику. Эти данные передаются обработчику платежей (англ. payment processor), который затем передаёт эти данные какой-либо из купных платежных систем (например, Visa, MasterCard и т.д.). Платежная система в свою очередь запрашивает авторизацию платежа у эмитента карты. Если эмитент подтверждает транзакцию, то деньги снимаются со счета жертвы, и платежная система уведомляет обработчика платежей об успешной транзакции. Периодически (например, раз в неделю, месяц и т.д.) обработчик платежей депонирует накопленные средства на банковский счет злоумышленника, который обналичивает эти средства и оплачивает комиссию партнерам.

Обработчик платежей в данном случае является очень важным звеном в цепи обработки платежа, поскольку без них злоумышленники не смогли бы получать деньги с карт жертв, что, в свою очередь, заставило бы искать альтернативные способы оплаты. Важно отметить, что компании, не принимающие оплату при помощи карт, теряют свою репутацию в глазах покупателей, которые могут сразу заподозрить обман. Обработчики платежей должны поддерживать определенный уровень легитимности, иначе они могут потерять возможность обрабатывать карты крупных платежных систем, как это случилось с компанией ePassporte, которая потеряла возможность обрабатывать карты Visa в связи с большим количеством мошеннических операций, в том числе и по отмыванию денег. Одним из наиболее известных обработчиков онлайн-платежей является сервис Chronopay. Этим сервисом пользуются многие, как добросовестные (например, Electronic Arts, Kaspersky, WWF, Greenpeace, UNICEF), так и преступные компании [82].

2.4. Выводы по второй главе

Проведенная работа по анализу отчётов ООН, государственных и коммерческих организаций, отчетов европейского сотрудничества, описывающих отдельные элементы теневой информационной экономики, а также их совокупности, позволила:

1. Предложить генезис формирования предпосылок и возникновения непосредственно теневой информационной экономики. В том числе было выделено три основных стадии становления теневой информационной экономики и проанализированы основополагающие этапы.

2. Смоделировать структуру рыночного механизма теневой информационной экономики, в частности была предложена структура всего спектра продуктов и услуг, задействованных в данной сфере.

3. Предложить и уточнить определения категорий, составляющих продукты и услуги в сфере теневой информационной экономики.

4. Изучить процесс и способы, а также предложить определение монетизации продуктов и услуг в сфере теневой информационной экономики. Кроме того, был формализован сам процесс и предложена модель процесса монетизации.

5. Разработанные логические и структурные модели рынка и монетизации продуктов и услуг в сфере ТИЭ, позволяют построить модели, необходимые для выявления рычагов противостояния злоупотреблениям в сфере информационных технологий.

3. ПРОБЛЕМЫ ПРОТИВОСТОЯНИЯ ТЕНЕВОЙ ИНФОРМАЦИОННОЙ ЭКОНОМИКЕ

3.1. Построение модели доходности ботнета

В современном периоде цели злоумышленников сместились с нанесения прямого ущерба и самоутверждения в пользу максимизации своей прибыли, как уже упоминалось в параграфе 2.1. В связи с этим для эффективного противостояния бот-мастерам и пользователям ботнетов необходимо использовать экономический подход. Основой этого подхода должен служить анализ источников доходов и прибыли злоумышленников с целью создания условий, при которых прибыль будет нулевой или отрицательной. В том случае, когда существует возможность получения прибыли, всегда найдутся желающие воспользоваться ею.

Бот-мастер стремится увеличивать свою прибыль за счёт заражения как можно большего количества устройств, используя при этом как можно меньшее количество ресурсов, таких как оплата услуг PPI, каналы управления и т.д. с последующей сдачей ботнета в аренду или использованием его вычислительных и пропускных мощностей самому. Таким образом, проанализировав источники доходов злоумышленников, можно предложить возможные инструменты противостояния им.

Основой для модели доходности ботнета послужили работа «Botnet Economics: Uncertainty Matters» [97] в которой анализируются правонарушения, связанные с ботнетами, а также развитие данной модели в работе «Fighting botnets with economic uncertainty» [96], в которой предлагается использовать финансовые рычаги в противостоянии бот-нетам. Несмотря на многие сильные стороны данной модели, по мнению автора, она нуждается в некоторых доработках, заключающихся в учете большего количества важных, на взгляд автора, параметров.

До недавнего времени в качестве объекта ренты рассматривались только лишь природные ресурсы, однако в последнее время всё чаще упоминается рента нематериальных активов, например, продуктов и услуг в сфере информационных технологий. Таким образом, можно выделить категорию неприродной ренты.

В литературе также рассматривается термин квази-рента, под которым понимается сверхприбыль от собственности на неприродные производственные ресурсы, носящая временный характер.

Предлагаются две модели, максимизирующие доходы двух типов злоумышленников: бот-мастера и арендатора ботнета. Под бот-мастером в рамках данной модели понимается лицо, занимающееся непосредственно созданием бот-нета – сети

компьютеров, зараженных специфическим вредоносным программным обеспечением, предоставляющим злоумышленникам контроль над ними. Под арендатором в рамках данной модели понимается лицо, покупающее доступ к уже созданному бот-нету с целью извлечения прибыли из зараженных компьютеров.

С точки зрения **бот-мастера**:

$$y_1 = P * b - k - a(B) - i(B) \quad (3.1)$$

С точки зрения **арендатора**:

$$y_2 = M(b) - O - P * b \quad (3.2)$$

Где:

- P – стоимость аренды одного зараженного компьютера. Данный фактор является контролируемым для бот-мастера, а также для арендатора, принимая во внимание наличие острой конкуренции на данном рынке, а соответственно и наличие выбора.
- b – количество арендуемых зараженных компьютеров, ботов. Данный фактор является контролируемым для арендатора и неконтролируемым для бот-мастера. Стоит однако отметить, что зомби машины обычно сдаются в аренду тысячами и даже десятками тысяч.
- k – плата за услуги провайдера каналов связи, а также средств управления ботнетом. Схематически каналы связи представлены на рисунке 3.1. Данный фактор является контролируемым для бот-мастера в том случае, когда есть выбор между несколькими провайдерами связи.

$$k = k_1 + k_2 + \cdots + k_j + \cdots + k_n; n \in \mathrm{N} \quad (3.3)$$

где k_j – плата за поддержание одного отдельно взятого канала.

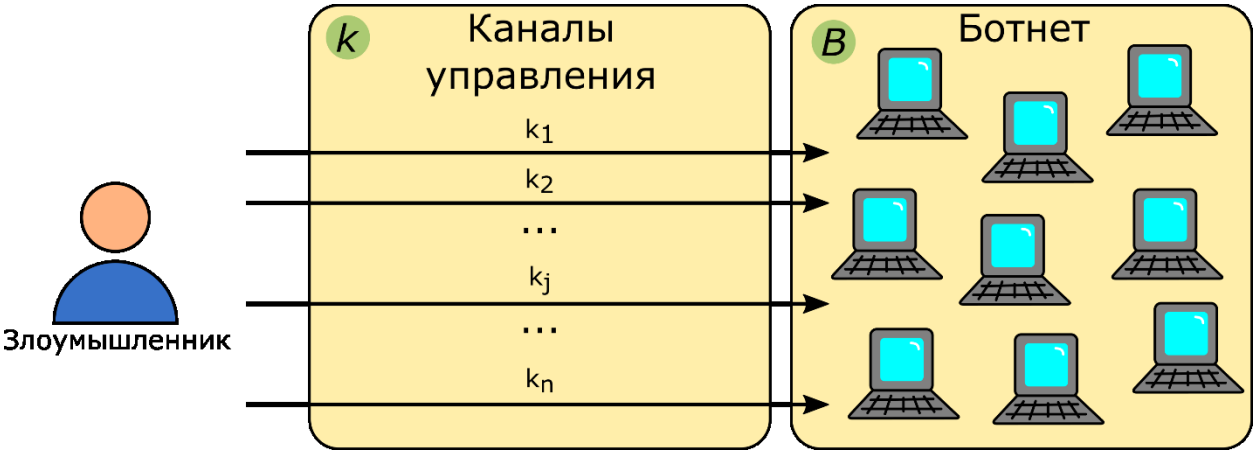

Рисунок 3.1. Каналы связи и управления, используемые злоумышленником.

- B – размер ботнета, т.е. количество зараженных зомби-машин, причём характеристики каждой отдельно взятой машины значения не имеют, во внимание берется лишь их количество. Таким образом, $b \leq B$. Данный фактор является контролируемым для бот-мастера в определенных рамках. Не имеет смысла заражение слишком малого числа машин, поскольку затраты не окупятся, однако, чем выше количество зараженных машин, тем выше риски быть обнаруженным и тем сложнее сохранять нам ними контроль.
- a(B) – потери злоумышленника в случае обнаружения ботнета правоохранительными органами или конкурентами, стоимость восстановления ботнета в случае форс-мажора. Потери, вызванные данной функцией могут нивелировать все доходы, полученные злоумышленником, например, в том случае, когда он был арестован. Данная штрафная функция может принимать различные виды: линейный, логарифмический, экспоненциальный и зависеть от законодательства, конкуренции и т.д. Функция зависит от размера бот-нета в связи с тем, что именно от величины бот-нета зависит насколько легко его будет обнаружить, а также количество ресурсов, потраченных на его создание. Этот фактор является неконтролируемым для злоумышленников.
- i(B) – стоимость заражения компьютеров, их объединение в ботнет. К данной категории относятся, например, затраты на поиск или приобретение уязвимостей. Данная функция может принимать различные виды и зависеть от разнообразия используемых конечными жертвами программных продуктов, развитости инфраструктуры, как с точки зрения атакующего, так и защищающегося лица.
- M(b) – суммарные доходы арендатора за время аренды ботнета. Объём зависит от количества арендованных ботов, и соответственно является контролируемым для арендатора, учитывая возможность контроля фактора b и контролируемым для бот-мастера, учитывая возможность контроля цены аренды. Величина данного параметра определяет прибыльность и экономическую эффективность взятия в аренду зараженных компьютеров.
- O – затраты на поддержание инфраструктуры арендатором. Например, в случае интернет-магазина, затраты на поддержку самого сайта, склада, закупка и пересылка товара. Ботнет в таком случае может арендоваться, например, в целях рассылки спама. Данный фактор является контролируемым для арендатора.

Схематически все вышеперечисленные компоненты модели представлены на рисунке 3.2.

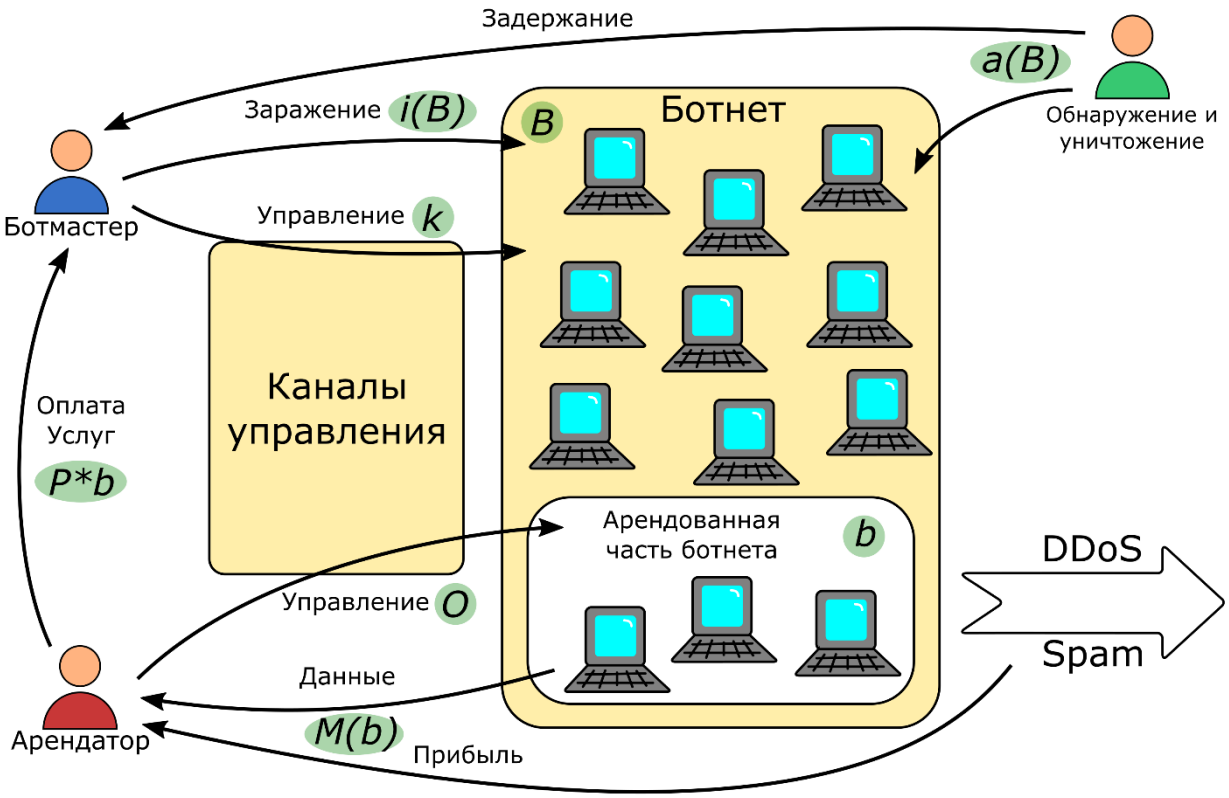

Рисунок 3.2. Схематическое представление модели доходности ботнета.

Параметр $P * b$ встречается в обеих моделях, однако, с точки зрения бот-мастера это – доход, получаемый от сдачи в аренду зараженных компьютеров, который для достижения прибыльности должен перекрыть все связанные с созданием и поддержанием функционирования ботнета затраты. Для арендатора же это – затраты, которые ему необходимо преодолеть для достижения прибыльности.

Также возможен частный случай данной модели, когда бот-мастер и арендатор – одно лицо. В таком случае, соответственно, плата аренды не осуществляется и P = 0 и, возможно, b = B. Кроме того, в таком случае может появиться недополученная прибыль, в том случае, когда самостоятельное использование бот-нета приносит меньший доход, чем его сдача в аренду. В таком случае модель принимает следующий вид:

$$y' = M(b) - k - a(B) - i(B) \quad (3.4)$$

Таким образом, преследуемой целью для органов поддержания правопорядка должно выступать минимизация данных видов доходов.

Как было упомянуто ранее, аренда ботнета обходится порядка 200 долларов США за 10000 зомби-машин. Таким образом, можно построить простой график доходности ботнета для арендатора без учета затрат на поддержку собственной инфраструктуры. Для визуализации трехмерных графиков применятся программный пакет GNU Octave.

Предположим, что:

- арендатор монетизирует каждые сто арендованных компьютеров на 3 доллара США (например, как было упомянуто ранее, находя на них данные кредитных карт и продавая их, или рассылая спам);
- заражение 100000 зомби-машин обходится злоумышленнику в 500 долларов;
- злоумышленник поддерживает два канала связи, каждый из которых обходится ему в 10 долларов;
- затраты арендатора на поддержку инфраструктуры составляют 10 долларов США.

В качестве стоимости аренды бот-нетов используются данные корпорации DELL за 2014 год [184], предоставленные ранее, в таблице 2.1.

Таким образом, можно получить данные, представленные в приложении 1.

Очевидно, что для достижения прибыльности злоумышленникам нужно преодолеть порог стоимости аренды ботнета, в то время, как хозяину ботнета необходимо окупить затраты на создание и поддержание ботнета, как показано на рисунках 3.3 и 3.4.

Рисунок 3.3. Порог прибыльности ботнета, разработано автором на основе модели доходности ботнета.

Теперь предпримем попытку сопоставить прибыльность аренды ботнета с доходом бот-мастера.

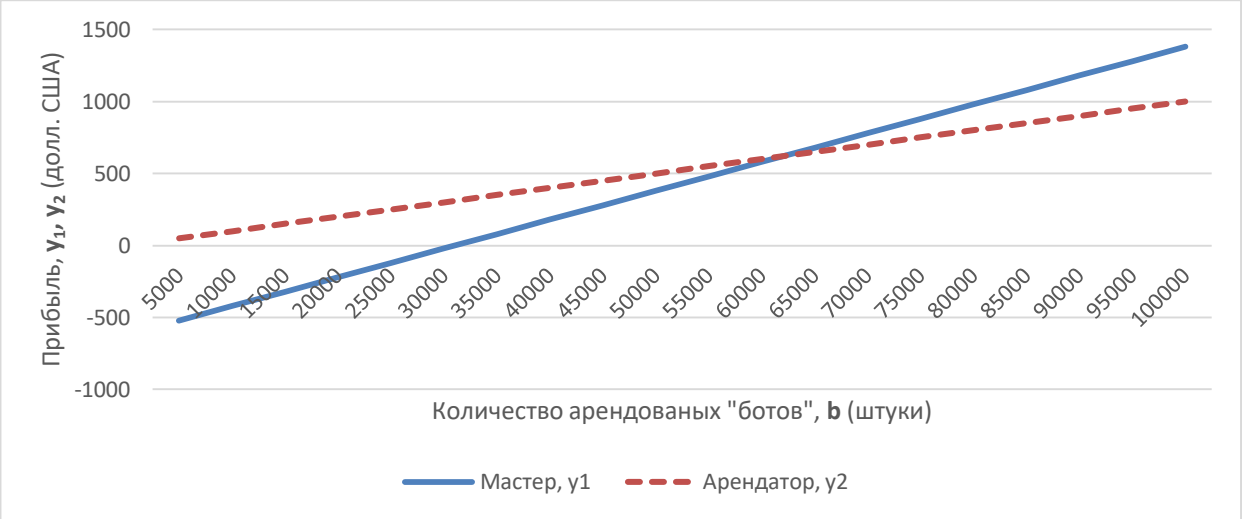

Рисунок 3.4. Сопоставление прибыльности аренды ботнета с доходом бот-мастера, разработано автором на основе модели доходности ботнета.

Необходимо учитывать тот факт, что чем больше времени ботнет арендуют и используют, тем больше шанс быть обнаруженным и возрастает шанс потери арендованной части ботнета.

Ещё одним важным фактором, который необходимо учитывать бот-мастеру и арендатору, является репутация бот-мастера. Данный показатель складывается из отзывов предыдущих клиентов бот-мастера и является решающим при выборе поставщика услуг бот-сети.

Таким образом, может показаться, что прибыльность ботнета для мастера никак не зависит от дохода арендатора, хотя очевиден тот факт, что в случае отсутствия экономической эффективности аренды ботнета для конечного арендатора, он не будет прибегать к подобным услугам.

Рассмотрим факторы, понижающие прибыльность ботнета, а значит, повышающие цену для конечного потребителя:

1) Поддержание каналов связи. Допустим, цена сдачи в аренду ботнета будет оставаться неизменной. Из рисунка 3.5 очевидно, что чем выше стоимость поддержания каналов связи, тем меньший доход получит бот-мастер. К данной категории затрат относятся оплата за услуги Internet, оплата электричества и т.д. Однако, очевидно, что эти затраты в общем случае не так высоки и влияют на конечную прибыль незначительно.

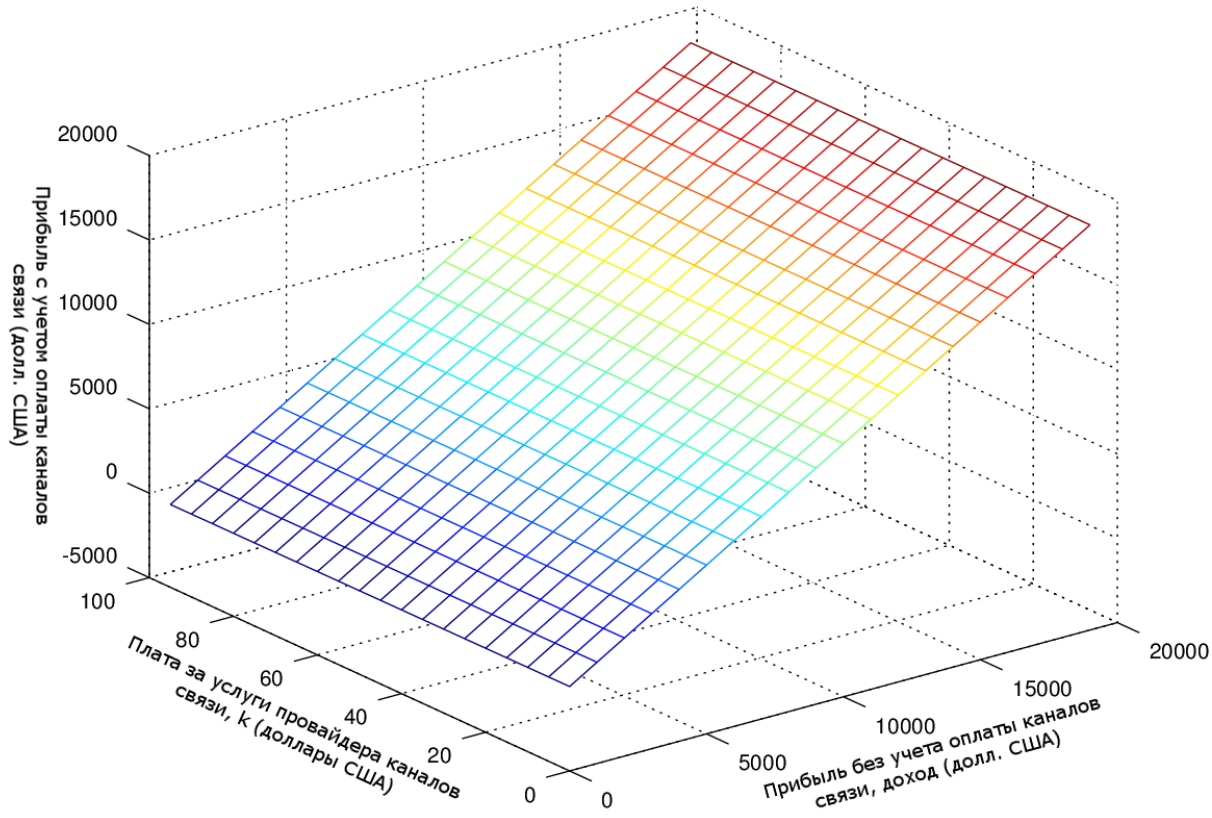

Рисунок 3.5. Зависимость прибыльности ботнета от стоимости поддержания каналов связи, разработано автором на основе модели доходности ботнета.

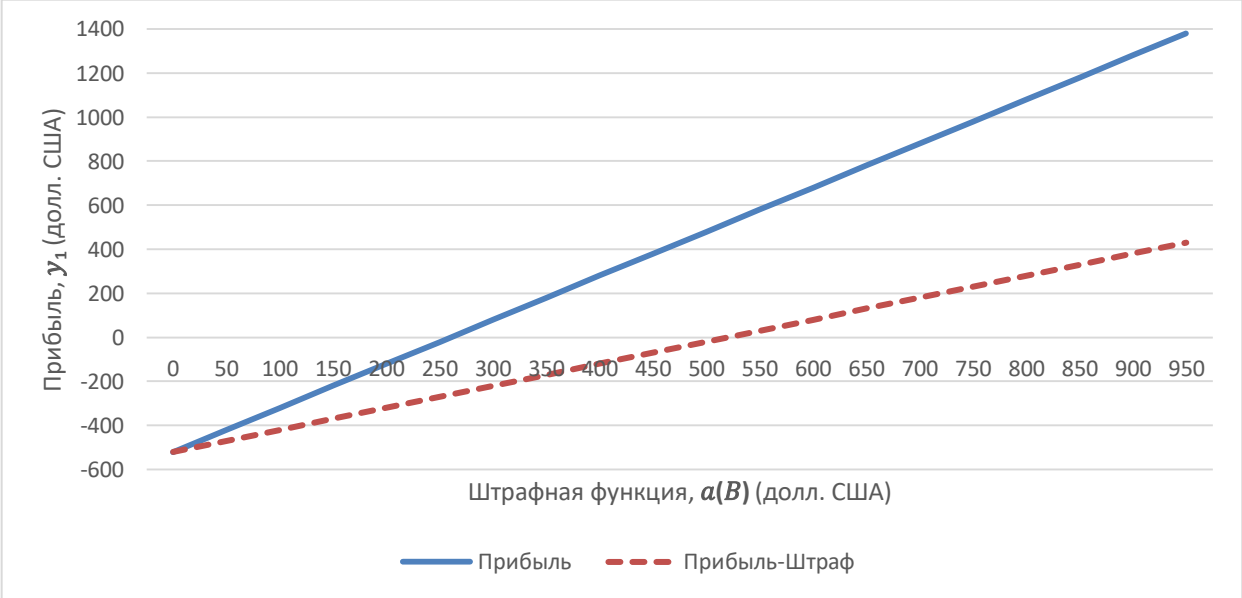

Рисунок 3.6. Зависимость прибыльности ботнета от штрафной функции, разработано автором на основе модели доходности ботнета.

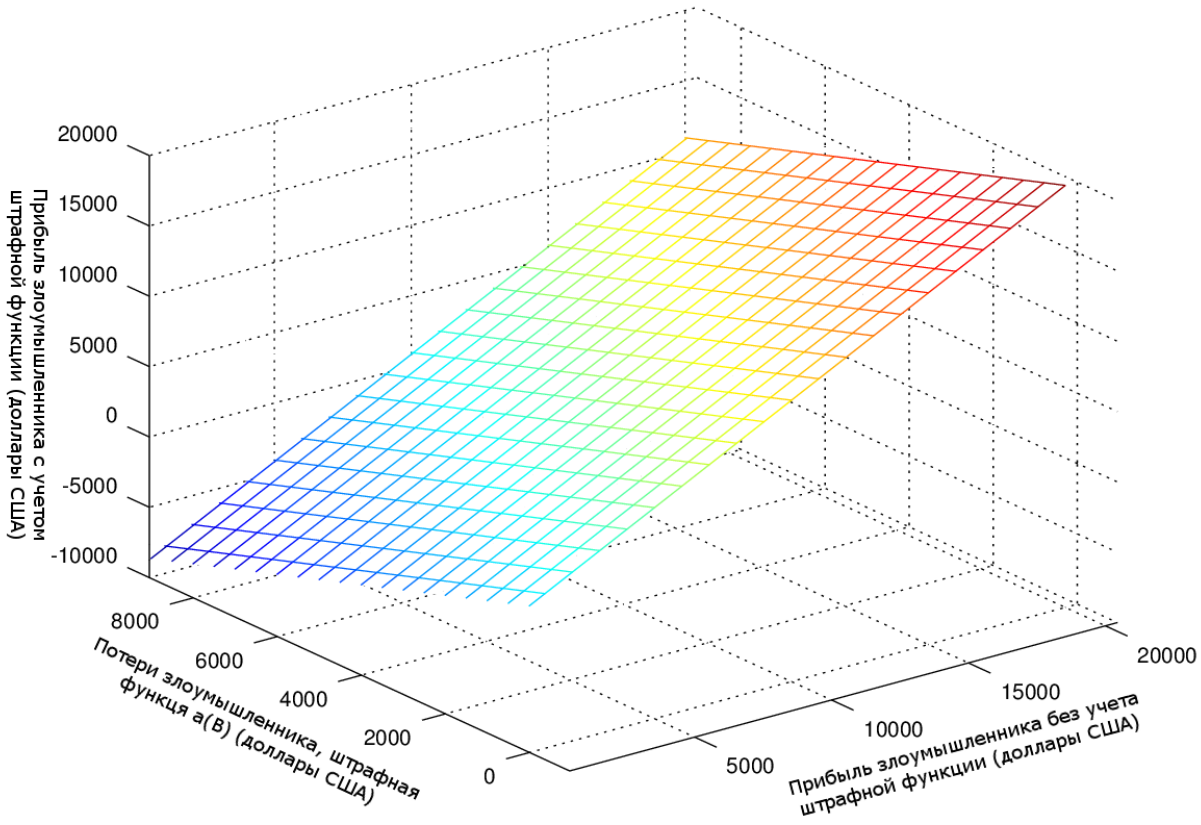

Рисунок 3.7. Зависимость конечной прибыли бот-мастера от штрафной функции и дохода, разработано автором на основе модели доходности ботнета.

2) Штрафная функция. Из рисунка 3.6 очевидно, что чем больше риск и потери в случае обнаружения и потери созданного ботнета, тем меньше желание злоумышленника заниматься подобным видом деятельности. Из рисунка 3.6 также очевидно, что чем выше штрафная функция, тем меньше конечная прибыль бот-мастера. Таким образом, для поддержания прибыльности бот-мастеру придется повышать стоимость аренды ботнета, что приведет к понижению показателя экономической эффективности.

На рисунке 3.7 рассмотрена зависимость конечной прибыли бот-мастера от штрафной функции и дохода.

3) Стоимость заражения компьютера. На рисунке 3.8 отображено изначальное вложение, на которое злоумышленник должен потратить определенное количество времени и ресурсов, прежде чем ботнет возможно будет использовать для получения прибыли.

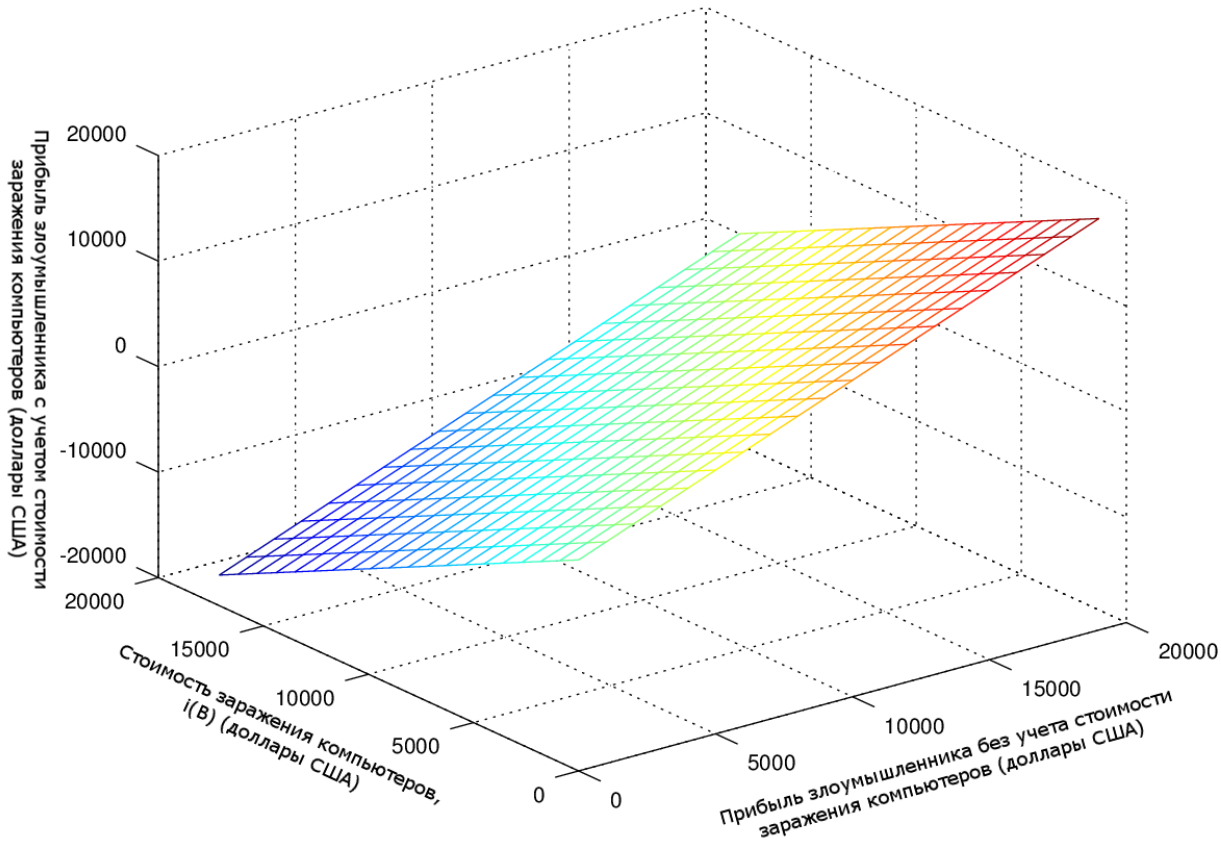

Рисунок 3.8. Зависимость прибыльности и доходности ботнета от стоимости заражения каждого компьютера, разработано автором на основе модели доходности ботнета.

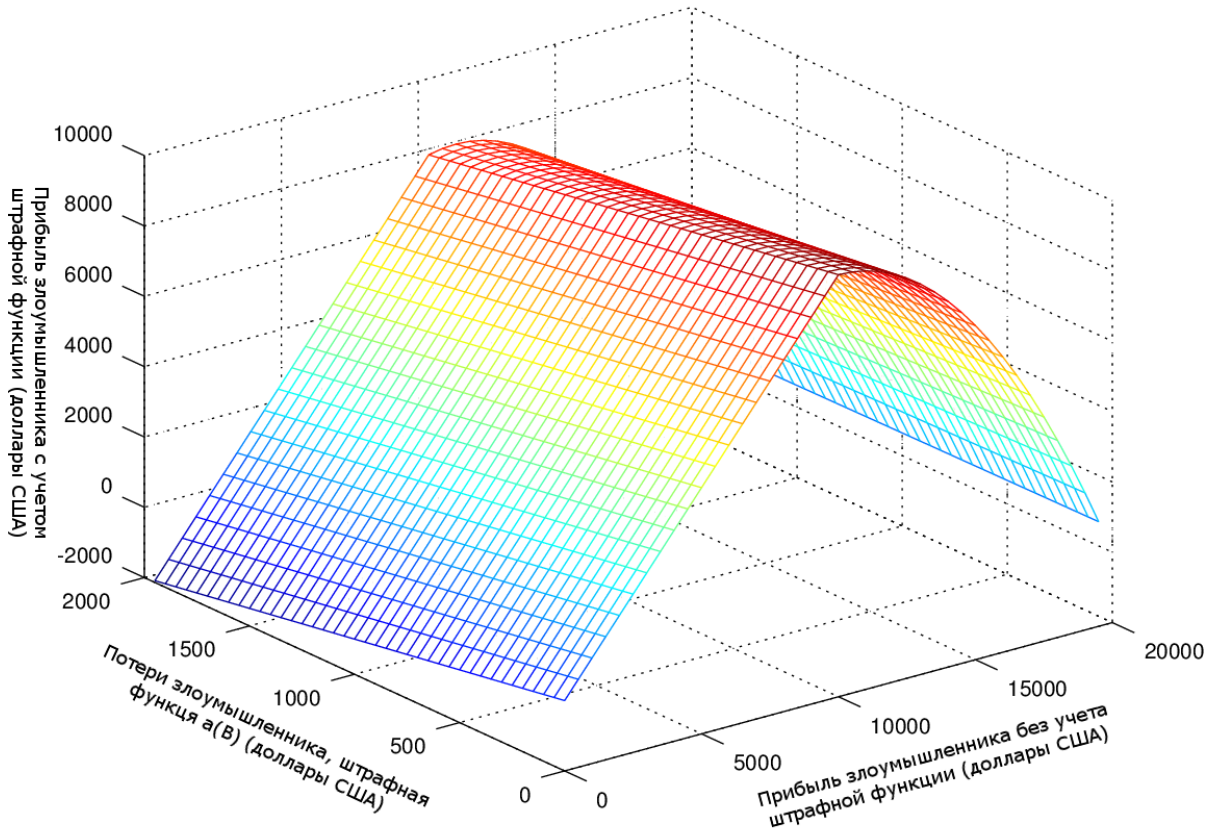

Рисунок 3.9. Убывающая предельная полезность заражения каждого дополнительного компьютера, разработано автором на основе модели доходности ботнета.

Кроме того, как видно из рисунка 3.9, слишком большим количеством ботов может быть затруднительно управлять и увеличивается риск обнаружения зомби-машин, а значит, возникает вопрос об убывающей предельной полезности заражения дополнительных компьютеров.

Построенная модель позволяет предложить следующие возможные векторы противодействия злоупотреблениям в сфере информационных технологий, связанных с ботнетами:

1. Максимизация штрафной функции a(B) посредством ужесточения уголовного кодекса в части противодействия злоупотреблениям в информационной сфере.

2. Увеличение стоимости заражения компьютеров i(B) путем повышения осведомленности конечных пользователей, использования более совершенного системного и прикладного программного обеспечения.

3. Снижение эффективности взятия в аренду зараженных зомби-машин, посредством совершенствования спам-фильтров, а также средств противостояния DoS и DDoS атакам.

4. Разработка комплекса мер, в том числе технических и программных для исключения создания инфраструктуры бот-нетов и каналов связи.

5. Создание условий, затрудняющих коммуникацию между возможными поставщиками и покупателями подобных услуг.

3.2. Построение модели денежных потоков в теневой информационной экономике

На данный момент, цели злоумышленников в сфере информационных технологий направлены на получение прибыли. Таким образом, по мнению автора, необходимо понимание источников доходов и расходов злоумышленников для эффективного противостояния преступлениям в сфере информационных технологий. В результате анализа, проведенного во второй главе, стала возможной характеристика наиболее значимых источников доходов злоумышленников, а также категорий расходов и препятствий на пути к получению прибыли, которые, в свою очередь позволили сформулировать модель денежных потоков в ТИЭ, основные элементы которой рассмотрены далее:

- Противодействие (противостояние/закон) – к данной категории относятся расходы на предотвращение обнаружения, а также потенциальные расходы в случае раскрытия ботнета, поимки злоумышленника. В качестве основных источников противодействия выступают законодательство и органы официальной власти, а также программные и аппаратные меры противостояния компьютерным злоупотреблениям, такие как брандмауэры, антивирусы и т.д.

- Анализ и исследование (рынок идей) – к данной категории относятся исследования в области уязвимостей и распространенности программного и аппаратного обеспечения, исследования в области законодательства, исследования рынка. Злоумышленники приобретают результаты подобных исследований, зачастую тратя на это значительные суммы денег, либо же занимаются подобными исследованиями самостоятельно, тратя на это значительные объемы времени.

- Разработка – на данном этапе происходит реализация найденных уязвимостей в программный код, который в дальнейшем будет распространен на устройства жертв с целью получения прибыли. Источниками прибыли могут служить персональные данные жертв, вычислительные мощности их аппаратного обеспечения и т.д.

- Отмывание – услуга, заключающаяся в легализации доходов, полученных в теневой области информационных технологий. Важно подчеркнуть, что отмывание денег может происходить как в информационной сфере, так и за её пределами. Чаще всего, подобная услуга оказывается в обмен на определенную долю дохода.

- Pay-per-Install – услуга, заключающаяся в установке исполнителем злонамеренного программного обеспечения, предоставленного заказчиком, на устройство жертвы. Данный метод эффективен благодаря своей гибкости: нет необходимости встраивать в каждую вредоносную программу средства заражения, сократив тем самым затраты на исследование, тестирование и разработку.

- Command and Control – к данной группе расходов относятся расходы на аппаратное обеспечение, поддержание каналов связи, оплату услуг провайдера, электричества, поиск или создание и поддержание прокси-серверов.

- Жертвы – к данной категории могут относиться как физические, так и юридические лица и даже государственные структуры, устройства которых оказались заражены, их конфиденциальные данные оказались доступны злоумышленникам, или иным образом пострадавшие от компьютерных злоупотреблений, описанных во второй главе данного исследования.

Предлагаемая модель носит концептуальный и гипотетический характер, а наглядное представление изображено на рисунке 3.10. Основным источником дохода злоумышленников служат зараженные компьютеры жертв, в то время, как затраты состоят из противостояния, анализа и исследования, заражения, Command and Control и отмывания. Таким образом получаем формулу 3.5, в которой злоумышленник стремится максимизировать y.

$$y = (\mathrm{V} - \mathrm{PPI} - \mathrm{C} - \mathrm{R}) \times \mathrm{Ls} \times \mathrm{L} \quad (3.5)$$

Где:

- V – доходы злоумышленников. Доходы могут складываться из монетизации персональных данных, украденных у жертв, платежей злоумышленникам, как результат вымогательства, использования вычислительных мощностей зараженных компьютеров, для, например, рассылки спама, проведения DDoS атак, добычи криптовалют и т.д. Данный параметр является частично управляемым для злоумышленников и единственным управляемым с точки зрения жертв в данной модели.

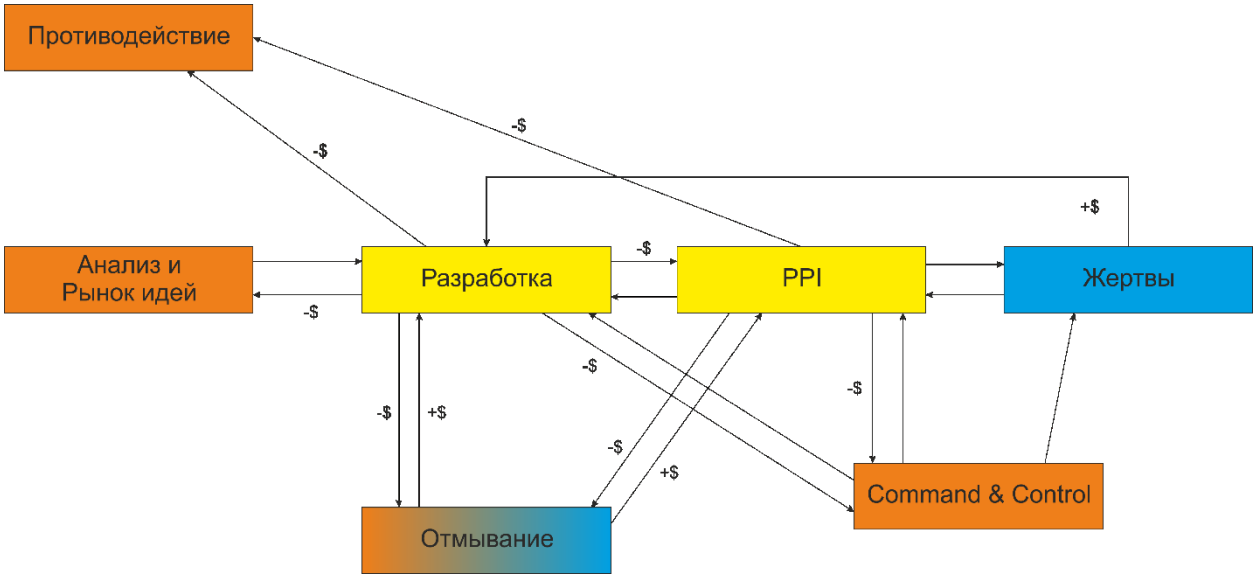

Рисунок 3.10. Модель денежных потоков в ТИЭ, разработка автора.

- PPI – оплата услуги заражения жертв вредоносным программным обеспечением. Эта схема, её преимущества и особенности рассмотрены подробно в параграфе 2.3. Данный параметр является контролируемым для злоумышленников, поскольку на рынке существует множество поставщиков подобных услуг. Кроме того, злоумышленники могут не покупать данную услугу, а самостоятельно заниматься заражением компьютеров жертв, в таком случае затраты выражаются в затраченном на это времени, возможном приобретении уязвимостей, исследовании рынка и т.д. и может сливаться с параметром R.
- C – затраты за поддержание каналов связи. Данный параметр складывается из затрат на услуги связи, покупку аппаратного обеспечения, а также является контролируемым, поскольку на рынке существует множество поставщиков услуг интернета и поставщиков необходимого аппаратного обеспечения.
- R – затраты на покупку результатов исследований, багов и уязвимостей. Кроме покупки злоумышленники могут самостоятельно провести исследование рынка, а также программного и аппаратного обеспечения с целью поиска уязвимостей. Данный параметр является контролируемым, поскольку на рынке существует множество продавцов уязвимостей, исследователей, а также существует возможность самостоятельно заняться исследованиями, в таком случае затраты будут выражаться в потраченном на исследования времени.
- Ls – коэффициент оплаты услуги отмывания денег. Данная категория затрат выражается в процентном отношении к финальной сумме, заработанной злоумышленниками. Данный параметр является контролируемым с точки зрения

злоумышленника, поскольку существует несколько возможных способов отмывания денег, а также ряд потенциальных поставщиков подобных услуг.

- L – коэффициент потерь в случае обнаружения ботнета. Данный коэффициент может носить как бинарный характер, так и любое промежуточное значение. Бинарный параметр может использоваться в том случае, когда ботнет был обнаружен полностью и его существование было прекращено, и, соответственно, все предыдущие затраты, связанные с его созданием и поддержкой, не окупились, либо же не был обнаружен совсем, или обнаружение не повлияло на его существование. Промежуточные значения, соответственно отражают ситуации, когда ботнет был обнаружен или его существование было прекращено лишь частично. Данный параметр может быть контролируемым для злоумышленника с той точки зрения, что он может предпринять все возможные меры для сокрытия ботнета, однако не все факторы, влияющие на возможности его обнаружения и прекращения существования подвластны непосредственно злоумышленнику. Данный коэффициент модели представляет собой элемент противостояния злоумышленникам со стороны органов правопорядка.

Исходя из построенной модели, можно выделить несколько векторов потенциального противодействия получению дохода злоумышленниками, создания условий, в которых функционирование потеряет свою экономическую эффективность:

- Минимизация непосредственно доходов злоумышленников, например, при помощи более эффективной защиты персональных данных, которые могут быть в последствии монетизированы.
- Создание условий, в которых будет максимально затруднительно заражать новые компьютеры. По мнению автора, это может быть достигнуто, в первую очередь, за счет повышения уровня осведомленности среди пользователей информационных технологий, поскольку многие заражения компьютеров происходят из-за незнания или по неосторожности.
- Создание условий, затрудняющих отмывание денег. В том случае, когда отмывание денег будет отбирать достаточно значимую часть полученных доходов, злоумышленники не смогут ими воспользоваться, не привлекая к этому внимание соответствующих органов.
- Создание условий, в которых избежание обнаружения и поддержание функционирования ботнетов будут затруднительны настолько, что доходы, получаемые от их существования, будут превышать получаемую прибыль.

По мнению автора, несмотря на то, что реализация лишь одного из упомянутых векторов противодействия на уровне, который будет достаточным для того, чтобы предотвратить появление злоупотреблений в сфере информационных технологий не представляется возможной, может быть достигнут достаточно высокий для предотвращения злоупотреблений уровень в сочетании упомянутых векторов противодействия.

3.3. Роль государства в регулировании уровня теневой информационной экономики

Роль государства в области информационной безопасности можно разделить на две основных составных части:

1. Во-первых, государство должно заботиться о безопасности своих граждан.
2. Во-вторых, государство должно заботиться о безопасности своих критически важных данных.

Несомненно, обеспечение безопасности является сложной задачей с точки зрения государства, особенно если принимать в расчёт всю сложность и комплексность структуры его информационной системы.

Согласно национальной стратегии развития информационного общества «Цифровая Молдова 2020», информационно-коммуникационные технологии являются неотъемлемой частью политики развития как государства в целом, так и предпринимательской среды, и правительственных организаций. Подобная стратегия необходима для повышения качества услуг, оказываемых населению. Стратегия, утвержденная в Республике Молдова, опирается на три основных напавления:

- развитие инфраструктуры и доступа,
- цифровой контент и электронные услуги,
- повышение уровня компьютерной грамотности.

Ожидается, что эти направления окажут благоприятное воздействие на общество, предоставляя более комфортные условия для социальной и деловой среды, а также правительственных структур.

Среди существующих на данный момент проблем, выделяются:

- недостаточно развитая инфраструктура за пределами городов, а также ограниченный доступ к ней,
- неготовность потенциальных пользователей к подобным услугам,
- низкую развитость национальных информационных ресурсов,

- недоступность национального культурного и научного достояния в цифровом формате,
- неготовность нормативно-правовой базы.

Отмечаются и проблемы в сфере информационной безопасности. Так, например, большое количество данных хранится в дата-центрах, не соответствующих требованиям безопасности, а также отмечается нехватка квалифицированного персонала. Отмечается и сильная разбросанность центров, в которых эта информация хранится, что значительно повышает расходы на их содержание.

В документе отмечается, что 37,7% пользователей сети Интернет осуществляют покупки онлайн, однако, подавляющее большинство этих покупок совершены на зарубежных сайтах. Важно подчеркнуть, что отсутствие покупок в молдавских магазинах свидетельствует о слабой развитости национальных интернет порталов. В Молдове отмечается и низкое количество создаваемого цифрового контента на душу населения. Данный показатель измеряется количеством статей на языке страны в Википедии, количеством блогов на душу населения и количеством зарегистрированных доменных имен первого уровня. Одним из объяснений данной ситуации может служить низкая образованность населения. Так, в документе утверждается, что лишь 14% населения в возрасте от 35 до 44 лет являются пользователями сети Интернет. В возрасте от 45 до 54-х лет пользователей интернета всего лишь 10%. Решить эту проблему предлагается посредством:

- введения соответствующих учебных программ,
- подготовки преподавательских кадров,
- интегрированием информационных технологий в учебный процесс,
- созданием цифрового образовательного контента.

В документе подчеркивается, что чем выше уровень информатизации общества, тем больше оно подвержено киберугрозам. Также уточняется, что обеспечение безопасности должно являться основной задачей всех участвующих в данном процессе лиц, особенно учреждений, ответственных за политики в данном секторе. В документе предлагается следующее определение: «под кибернетической безопасностью понимается состояние нормальности, установившееся в результате принятия проактивных и реактивных мер, направленных на обеспечение конфиденциальности, целостности, доступности, достоверности и безотказности информации в электронном виде, государственных и частных ресурсов и услуг в кибернетическом пространстве».

Предлагается классификация уязвимостей на три категории в зависимости от характера:

- Человеческие;
- Технические;
- Процедурные.

Кроме того, перечисляются основные формы угроз:

- Кибернетические атаки;
- Неавторизированный доступ;
- Неавторизированное изменение;
- Кибернетический шпионаж;
- Причинение вреда имуществу.

Подобное внимание, уделяемое данной проблеме, явно демонстрирует необходимость оповещения пользователей о возможных рисках при совершении интернет-платежей и работе с личными данными и мерах по их предотвращению, а также о важности продвижения подобных услуг на молдавских ресурсах.

В Европейском Союзе была утверждена и в данный момент реализуется стратегия «Цифровая повестка Европы», направления которой были откорректированы в соответствии с современными реалиями. Цифровая экономика растёт намного быстрей всех остальных отраслей экономики, однако считается, что её потенциал не реализуется в полной мере из-за отсутствия соответствующей политики общеевропейского уровня. Ожидается, что этот потенциал будет раскрыт в рамках новой цифровой стратегии. За счёт роста инвестиций в информационные и коммуникационные технологии прогнозируется рост ВВП на 5%, т.е. 1500 евро на душу населения в последующие 8 лет. Основными приоритетами данной политики выступают:

- создание нормативно-правовой базы в области широкополосных услуг,
- улучшение инфраструктуры государственных цифровых услуг,
- создание рабочих мест в области информационной индустрии,
- актуализация законодательства в области авторских прав,
- стимулирование развития облачных технологий,
- разработка производственной стратегии в данной области.

Одним из важных пунктов данной стратегии является разработка стратегии информационной безопасности на уровне ЕС.

В США в январе 2008 года была запущена Комплексная Национальная Инициатива по Кибербезопасности (Comprehensive National Cybersecurity Initiative). Даная инициатива базируется на трёх основных целях:

1. Установка передовой защиты от непосредственных угроз путем информирования правительства, а также всех уровней управления на государственном и частном уровнях о существующих уязвимостях, угрозах и возможных событиях, а также быстрое реагирование с целью устранения существующих уязвимостей и предотвращения вторжений.

2. Защита от всех возможных угроз путем улучшения возможностей контрразведки и улучшением безопасности линий поставки ключевых информационных технологий.

3. Укрепление будущего климата информационной безопасности путем улучшения образования в данной области, координирования исследований, а также работой над созданием и совершенствованием стратегии по предотвращению вредоносных действий в киберпространстве.

Важным шагом для Республики Молдова выступило подписание Соглашения об ассоциации Республики Молдова с Европейским Союзом [2], одним из наиболее важных элементов которого выступает статья, направленная на предупреждение организованной преступности, коррупции и прочей незаконной деятельности и борьба с этими явлениями, в которой, среди прочего, упоминается и двухстороннее сотрудничество, направленное на борьбу с международными организованными и неорганизованными кибер-преступлениями.

Данное соглашение будет внедряться в соответствии с национальным планом [3], который включает в себя:

1. Анализ текущей ситуации в области расследования и применения наказаний в случаях информационных преступлений.

2. Инструктаж судей и прокуроров в области расследования, уголовного преследования и наказания информационных преступлений.

3. Консолидация возможностей в области предупреждения и борьбы с информационными преступлениями.

4. Обеспечение эффективного взаимодействия с отделом EC3, входящего в состав Europol.

5. Внедрение международного проекта «Child Sexual Exploitation Database Connectivity and Awareness Raising Enhancement I-CARE».

6. Улучшение возможностей предотвращения сексуальной эксплуатации и домогательств в сети Internet.

7. Создание партнерства по обмену информацией в области кибернетической безопасности в Республике Молдова.

Также, одним из пунктов данной программы выступала разработка и утверждение Постановления Правительства Республики Молдова Nr. 201 от 28.03.2017 об утверждении Минимальных обязательных требований кибернетической безопасности, в котором определяются меры, необходимые для обеспечения кибернетической безопасности [37].

Другим важным документом является «Национальная программа кибербезопасности Республики Молдова на 2016-2020 годы» [37], целью которой является создание системы менеджмента кибербезопасности Республики Молдова путем обеспечения безопасности услуг информационного общества, способствуя, таким образом, развитию экономики, основанной на знаниях, что в свою очередь будет стимулировать рост уровня экономической конкурентоспособности, социального единства, а также обеспечит создание новых рабочих мест. В программе определяются базовые термины, такие как: киберугроза, киберзащита, кибератака, аудит кибербезопасности, кибернетический инцидент, событие, произошедшее в киберпространстве, кибернетические инфраструктуры, кибернетические инфраструктуры национального значения, менеджмент идентичности, управление рисками, операции в компьютерных сетях, устойчивость кибернетических инфраструктур, риск безопасности в киберпространстве, кибербезопасность, киберпространство, уязвимость в киберпространстве. Программа основа на следующих принципах: защита прав и основных свобод человека, общедоступность, кибернетическая устойчивость, совместное управление, совместная ответственность и персональная ответственность за обеспечение кибербезопасности. Кроме того, в программе анализируется текущая ситуация в области ТИЭ: количество преступлений в Республике Молдова, а также ущерб, нанесенный ими. Наконец, в программе очерчиваются её цель, задачи и действия, которые необходимо предпринять для достижения этой цели. В качестве главной цели программы выдвигается создание и внедрение системы менеджмента кибербезопасности Республики Молдова, обеспечивающей соответствующим структурам публичной и частной сферы планирование и использование доступных ресурсов, определение вмешательств, необходимых для понижения пагубного воздействия кибернетических преступлений, атак и инцидентов на устойчивое развитие информационного общества.

Несмотря на то, что определенные шаги в борьбе с теневым сектором информационной экономики были предприняты, по мнению автора, их недостаточно. Необходим пересмотр существующих законов и стратегий, существенная их доработка и совершенствование в соответствии с аналогичными законами и стратегиями Европейского Союза и США. Кроме того, нет единой структуры, в обязанности которой входило бы исследование и противостояние исследуемому феномену. Подобная структура необходима как на государственном, так и на международном уровнях. Помимо вышеперечисленного, важным шагом в противостоянии теневой экономике было бы создание реестра или базы данных всех случаев правонарушений в информационной сфере на территории Республики Молдова, на европейском и мировом уровнях.

3.4. Анализ тенденций в теневом секторе информационной экономики

В направлении исследования перспектив теневого сектора информационной экономики проводятся работы по всему миру, в частности, компания RAND в своём исследовании [40] прогнозирует следующие течения на ближайшее время:

1. Увеличится активность на хакерских форумах, но отбор участников будет ужесточен; увеличение популярности криптовалют; большая анонимность в злонамеренном программном обеспечении; улучшение анонимности и более криптоустойчивое программное обеспечение, используемое для общения и совершения платежей и денежных переводов.

2. Учитывая развитие теневого сектора, технологии атаки существенно опередят технологии защиты.

3. Повсеместная доступность информационных технологий и интернета открывает множество новых возможностей для атак, создавая новые горизонты для теневого информационного рынка.

4. Атаки на мобильные устройства и социальные сети участятся.

5. Будет расширяться рынок оказания услуг, брокерства.

В то же время невозможно прийти к единому мнению по поводу того, на каком секторе данный рост скажется больше (малый или крупный бизнес, физические или юридические лица), спрос на какие продукты будет наибольшим (интеллектуальная собственность или персональные данные), а также какой тип атак будет преобладать (направленные атаки, оппортунистические или массовые).

В прогнозе корпорации RSA [142] предполагается, что наиболее подвержены угрозам будут такие области предпринимательства, как:

- денежные переводы (19%),
- туризм (15%),
- корпоративные услуги (13%),
- магазины электроники (10%).

Кроме того, в прогнозе подчеркивается перспективность мобильных устройств как в качестве целей, так и источника атаки. В подтверждение этому прогнозу приводится статистика, в которой утверждается, что около 45% денежных транзакций и 60% случаев мошенничества совершаются благодаря мобильным устройствам. Предполагается, что количество денежных транзакций, совершенное при помощи мобильных устройств, перегонит количество транзакций через «классический веб», соответственно будет расти и количество мошенничеств, совершенных в данной области, в частности в мобильных приложениях, поскольку проявляется тенденция поставлять услуги конечным пользователям с использованием данного канала. Подчеркивается и тенденция внедрения биометрических технологий для аутентификации пользователей, основным двигателем которой является не обеспечение безопасности, а лишь повышение удобства использования технологий.

Ещё одной важной тенденцией, отмеченной в прогнозе, является вредоносное ПО ransomware, на которое приходится каждая 20ая атака с использованием вредоносного ПО, наносящая при этом средний урон жертвам в размере 300 долларов США.

Наконец, последней тенденцией, отмеченной в прогнозе, являются атаки типа фишинг. Утверждается, что атаки подобного типа запускаются каждые 30 секунд, и наносят ущерб организациям, подвергшимся им в 9.1 миллиардов долларов США каждый год. Предполагается, что злоумышленники продолжат привносить инновации в данную сферу, совершенствуя существующие методы, фокусируясь в первую очередь на повышении срока их жизнеспособности.

В прогнозе «Scenarios for the Future of Cybercrime» [169] помимо уже упомянутых, предполагаются следующие возможные тенденции развития технологий и преступлений, связанных с ними:

- Инвазивность технологий, в том числе сбор огромного числа персональных пользовательских данных, таких как данные о привычках, покупках. Использование электронных имплантов, собирающих данные о пользователе и предоставляющих доступ

к определенным технологиям, дополненная реальность, биометрические данные. Неоспоримое удобство подобных технологий, тем не менее, компенсируется их потенциальными многочисленными уязвимостями, предоставляющими доступ к подобным данным злоумышленникам и недобросовестным лицам.

- Осложненный доступ к совершенствующимся технологиям для более пожилых лиц. С одной стороны, более совершенные технологии помогают диагностировать болезни, следить за общим состоянием здоровья, облегчать выполнение многих задач, с другой пользователи подобных технологий могут становиться более легкими жертвами как мошенничеств и злоупотреблений, так и системных недоработок, вызванных человеческим фактором в процессе проектирования и разработки подобных устройств.
- С точки зрения корпоративных компаний, большая зависимость от автоматизированных технологий управления процессами, с одной стороны упрощает выполнение многих задач, а с другой, повышает риск и объемы потенциального ущерба в случае отказа определенной технологической составляющей или их комплекса. В том числе, возрастает зависимость от коммуникации как между отделениями внутри самой корпорации, так и с бизнес партнерами, перебои в коммуникации могут приводить к существенным простоям и ущербу для корпорации.
- Будут увеличиваться и объёмы данных, которые необходимо хранить, соответственно, будет и увеличиваться зависимость от надежности носителей информации и резервного копирования и восстановления.
- С точки зрения глобализации и государств, может стираться грань между международной дипломатией и интернет-дипломатией. Страны с более отсталым уровнем информационной безопасности могут стать «изгоями» в плане туризма и дипломатии, а также раем для преступников в области информационных технологий.
- Граждане государств могут требовать повышения прозрачности органов управления, могут появиться такие элементы, как система репутации в органах администрации. Зависимость от технологий также может открыть новые векторы атаки для хактивистов.
- Атаки на критические элементы информационной инфраструктуры могут выливаться в физические катастрофы и насилие. Например, атаки на транспортные сети и энергетическую инфраструктуру.

По мнению автора, упомянутые прогнозы достаточно хорошо обоснованы и учитывают тенденции последнего времени, проанализированные в данном

диссертационном исследовании, согласовываясь с ними. Спрогнозированные тенденции применимы как для глобального уровня в целом, так и для Республики Молдова, в частности.

Автор считает, основываясь на тенденциях и материалах, проанализированных в данном диссертационном исследовании, что наибольшее распространение в ближайшем будущем в Республике Молдова получат атаки вредоносного программного обеспечения типа ransomware. Кроме того, тенденция перехода на мобильные устройства также окажет заметное влияние. Оцифровка административных функций несмотря на то, что значительно упрощает многие процессы и повышает удобство в их использовании, тем не менее, несет в себе значительные технологические риски, предоставляя новые потенциальные векторы для возможных атак. Кроме того, отсутствие синхронизации и разобщенность между отдельными государственными органами и структурами в процессе внедрения подобных технологий и процессов может привести к наличию дополнительных уязвимостей и неудобствам в их использовании, и как следствие, негативному опыту и недовольству пользователей.

Противостояние теневой информационной экономике.

Согласно исследованию [118] уровень теневой экономики напрямую зависит от количества электронных платежей: чем больше их совершается в стране, тем ниже уровень теневой экономики. Например, в таких странах, как Великобритания и Финляндия, где количество электронных платежей достаточно высоко, уровень теневой экономики ниже, чем в странах с небольшим количеством электронных платежей, таких как Болгария, Греция и Румыния. Этому способствует прозрачность подобных платежей, а также большие сложности в их сокрытии. Согласно исследованию, увеличение электронных платежей на 10% в год на как минимум 4 последовательных года, может уменьшить объем теневой экономики на 5%. Подобные изменения повлияют на привычки и поведение особенно среди тех, кто является несознательным участником теневой экономики, способствуя продавцам, не декларирующим продажи.

Кроме того, одним из важнейших факторов существования теневого сектора является низшая стоимость ведения бизнеса в теневом сегменте экономики по сравнению с легальным сегментом. Таким образом, переходя в теневой сектор, субъект стремится максимизировать свою прибыль [34]. Формирование теневого ресурса происходит на основе легальных ресурсов, однако, они используются уже лишь в интересах владельца, а не на благо всего общества. Одним из главных условий ведения бизнеса в теневом секторе является менее низкая стоимость функционирования. Исходя из вышеперечисленных

условий, можно утверждать, что борьба с теневым сектором информационной экономики может осуществляться путем снижения экономической эффективности от функционирования в данной сфере деятельности: увеличивать издержки функционирования в теневом секторе и уменьшать издержки функционирования в легальном.

В своей работе Эрнандо де Сото [18] выделяет в качестве одноразовых издержек затраты на получение права функционирования, а в качестве постоянных – налоги, социальные платежи, затраты на персонал, юридические аспекты бизнеса и бюрократические нормы. Если же рассматривать теневую сферу бизнеса, то их издержки формируются из затрат на отмывание денег, затрат на нивелирование рисков, связанных с поимкой. Кроме того, существуют препятствия в виде невозможности участия в определенных областях производства, отсутствие гарантий надежности контрагентов и прочие. Примечательно, что, несмотря на то, что данные методы могут быть эффективны для противостояния “классической” теневой экономике, совершенно необязательна их эффективность при противостоянии информационной её части, поскольку факторы, влияющие на её существование, зачастую отличаются.

3.5. Выводы по третьей главе

В результате проведенной работы, стало возможным:

1. Построить и предложить многофакторную модель доходности ботнета на основании отчётов и публикаций, раскрывающих стоимость услуг в данной области.

2. Построить и предложить модель денежных потоков в теневой информационной экономике, охватывающей все сферы производства и воспроизводства продуктов и услуг в данной сфере, основываясь на модели монетизации, предложенной во второй главе.

3. На основе построенных моделей предложить векторы противодействия злоумышленникам в сфере ТИЭ, заключающиеся в необходимости снижения возможных источников доходов злоумышленников и в повышении эффективности штрафной функции.

4. Выделить роль государства в качестве главного участника в процессе снижения уровня теневой информационной экономики. А также выдвинуть организационные и правовые предложения в контексте необходимости дальнейших шагов по борьбе с теневой информационной экономикой.

5. Спрогнозировать пути дальнейшего развития теневой информационной экономики, выражающиеся, среди прочего, в увеличении количества инцидентов в данной сфере.

Построенные модели позволяют выделить следующие возможные рычаги противодействия злоумышленникам в сфере теневой информационной экономики:

1. Максимизация штрафной функции за счёт совершенствования законодательной базы, совершенствования средств обнаружения и борьбы с ботнетами и злоупотреблениями в области ТИЭ, а также затруднения поддержки и создания новых ботнетов.

2. Снижение эффективности и качества продуктов и услуг, предоставляемых в сфере ТИЭЮ и, как следствие, минимизация эффективности пользования подобными продуктами и услугами.

3. Повышение осведомленности среди пользователей ИКТ в области возможных угроз в области информационной безопасности, что, по мнению автора, значительно снизит количество инцидентов в данной сфере.

4. Создание условий, в которых отмывание денег будет затруднено, а цена услуги высока настолько, что нивелирует значительную часть доходов злоумышленников.

5. Создание препятствий в коммуникации между поставщиками и покупателями услуг в сфере ТИЭ.

6. Минимизация доходов злоумышленников, посредством более эффективной защиты данных, которые могут быть в последствии монетизированы. К подобным данным могут относиться данные кредитных карт, пароли доступа к почтовым ящикам, социальным сетям и т.д.

ОБЩИЕ ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

Противостояние информационной стороне теневой экономической деятельности приобретает всё большую актуальность в контексте постоянного роста количества и масштабов преступлений, совершенных в данной сфере.

Рассмотрены существующие подходы к определению теневой экономики и предложены три новых определения, охватывающих непосредственно теневую сторону информационных технологий. Впервые предложены концептуальные и методологические основы исследования теневой информационной экономики, базирующиеся на анализе фундамента её формирования, сущности и особенностей, основных черт, факторов формирования и методик оценок её уровня [7, 32, 45].

В рамках исследования генезиса теневой информационной экономики охарактеризованы три основных этапа её становления: докомпьютерный, ранний и современный. Предложены временные рамки для каждого из этапов, проанализированы основополагающие для каждого из этих этапов события и предложена их визуализация в виде временных шкал [7].

Разработана, смоделирована и обоснована структура теневой информационной экономики, охватывающая все этапы производства и воспроизводства продуктов и услуг в области теневой информационной экономики. В частности, подробно изучены все составные элементы, предложены и уточнены определения категориям, составляющим данную структуру, таким как монетизация, adware, crimeware, scareware, черви, троянские программы, криптолокер, кибероружие, фишинг, фарминг, саботаж, терроризм, пиратство и так далее. Изучены методы и способы монетизации продуктов и услуг в сфере теневой информационной экономики. Это исследование может послужить фундаментом для понимания процессов, протекающих на теневой стороне информационных технологий и стать основой для дальнейших разработок [7, 32, 108].

Кроме того, разработаны и предложены модели доходности ботнета и денежных потоков в области теневой информационной экономики, описывающие ротацию денежных средств между злоумышленниками, источники прибыли и затраты. Данные модели являются основополагающими в борьбе с теневыми информационными технологиями, поскольку, лишив данный сектор экономики доходности, количество правонарушений значительно уменьшится [105, 109].

Проанализированы события, послужившие ключевыми на этапах формирования современного состояния теневой информационной экономики, и на их основе предложен генезис, который позволяет понять историю данного феномена. Данное исследование

может послужить отправной точкой для дальнейших прогнозов и эффективной дальнейшей борьбы и противостояния теневой информационной экономике [7].

Выявлено, что становление и развитие теневой информационной экономики имело свои специфические особенности, продиктованные уровнем развития технологий, глобализацией мировой экономики [7].

Необходимо совершенствование законодательной базы Республики Молдова в виду создания предпосылок невозможности существования элементов ТИЭ с учетом международного опыта в данной сфере, в том числе опыта ЕС и США.

Построенные модели позволили предложить ряд возможностей противостояния теневому сектору информационной экономики [105, 109], заключающиеся, главным образом, в применении экономических рычагов, понижающих эффективность существующих схем получения прибыли в данной сфере деятельности, таких как:

1. Максимизация штрафных функций посредством совершенствования законодательной базы, а также средств борьбы со сформировавшимися и формирующимися бот-нетами.

2. Минимизация доходов злоумышленников, посредством более эффективной защиты данных, предоставляющих возможности монетизации.

3. Снижение эффективности монетизации услуг, предоставляемых в области теневой информационной экономики.

4. Создание препятствий на пути легализации доходов, полученных в сфере ТИЭ, а также создание препятствий на пути отмывания доходов с использованием информационных технологий.

Кроме того, возможны и технико-технологические способы препятствования теневым информационным технологиям, такие как: создание препятствий на пути заражения компьютеров вредоносным программным обеспечением, в том числе в целях создания бот-нетов, совершенствование средств противостояния вредоносному программному обеспечению, создание препятствий на пути коммуникации между возможными покупателями и поставщиками услуг в сфере ТИЭ. Однако самым важным, по мнению автора, средством противостояния ТИЭ должно выступать информирование пользователей о возможных угрозах в сфере информационных технологий, а также способов противостояния подобным угрозам [7, 105].

Особое внимание следует уделить анализу новых заказных услуг, которые представляются в анонимной 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. Отдельного внимания заслуживают криптовалютная экономика, рынки криптовалют.

По мнению автора, необходимо регулирование статей уголовного кодекса с точки зрения защиты информации и пресечения информационных преступлений [10, 109]. Кроме того, необходимы дальнейшие исследования, направленные на поиск эффективных рычагов противодействия ТИЭ в целом, и отдельным её элементам в частности, как посредством снижения их экономической эффективности, так и с точки зрения повышения рисков, связанных с уголовной и административной ответственностью для лиц, принимающих участие в данной сфере деятельности.

БИБЛИОГРАФИЯ

1. **Dragan A.** Frauda informatică: analiza juridico-penală a infracțiunii. 12 05 2017 г., 10 08 2017 г., http://www.cnaa.md:8080/thesis/51769/.
2. Acord de asociere între Republica Moldova, pe de o parte, și Uniunea Europeană și comunitatea europeană a energiei atomice și statele membre ale acestora, pe de altă parte. http://www.mfa.gov.md/img/docs/Acordul-de-Asociere-RM-UE.pdf.
3. Planul naţional de acţiuni pentru implementarea Acordului de Asociere Republica Moldova–Uniunea Europeană în perioada 2017–2019. http://mf.gov.md/sites/default/files/documente%20relevante/pnaaa_2017-2019.pdf.

* * *

4. **Безмалый В.** Расследование Компьютерных Происшествий. bezmaly.wordpress.com, 19 09 2012 г., 27 09 2015 г., https://bezmaly.wordpress.com/2012/09/19/sec-2/.
5. **Блэк Д.** Экономика. Толковый словарь. под ред. И.М. Осадчая, Москва, Издательство "Весь Мир", 2000.
6. **Борисов А.** Большой экономический словарь. Москва, Книжный мир, 2003, стр. 895.
7. **Бортэ Г.** Теневая Информационная Экономика. Годишен Алманах. Научни Изследвания на Докторанти, Книга 5, 2012 стр. 485-495. Болгария.
8. **Бортэ Г.** Критерии Оценки Стоимости Уязвимостей Программного Обеспечения. Проблеми и Перспективи на Развитието на Сотрудничеството Между Страните от Югоиточна Европа в Рамките на Черноморското Икономическо Сътрудничество, Том II, Албена, Болгария, 18-19 09 2012, стр. 278-281.
9. **Бортэ Г.** Исторические предпосылки развития теневой информационной экономики, Системи Обробкі Інформації, Випуск 4(102), том 2, Харьков, Украина, ISSN-1681-7710, 2012.
10. **Бортэ Г.** Исследование жизненного цикла вредоносного программного обеспечения. Международна Научна Конференция Информационните Технологии - Стратегически Приоритет В Икономика На Знанието, Болгария. 2011.

11. **Бортэ Г., Склифос К., Спынаки В.** Проблемы информационной безопасности в электронной коммерции, Съвременни измерения на търговския бизнес – комуникация между наука и практика. Volume II, 12-13 05 2011.

12. **Бортэ Г.** Теневая Информационная Экономика. Securitatea Informationala 2011, Молдавская Экономическая Академия, 04 05 2011, ISBN 978-9975-75-558-0.

13. **Бортэ Г.** Природа уязвимостей программного обеспечения. In: Хоризонт 2020 пред икономическото знание и бизнеса, volume 2, 7-8 10 2010, Издательство Ценов, Свиштов, Болгария, ISBN 987-954-23-0481-4.

14. **Бортэ Г.** Природа инсайдерства. Системи за управление на бизнеса в малки и средни предприятия, 23-24 04 2010, Издательство Ценов, Свиштов, Болгария, ISBN 978-954-23-0455-5.

15. **Бортэ Г.** Методы классификации инсайдеров. In: Securitatea Informationala 2010, Молдавская Экономическая Академия, Chisinau, 2010, ISBN 978-9975-75-509-2.

16. **Бортэ Г.** Система предотвращения утечки конфиденциальной информации. In: Securitatea Informationala 2009, published by ASEM, Chisinau, 2009, ISBN 978-9975-75-459-0.

17. **Буров В.** Исследование Теневой Экономики. Известия, Иркутская Государственная Экономическая Академия, 06 2010 г., 05 09 2014 г., http://eizvestia.isea.ru/pdf.aspx?id=13936.

18. **Де Сото Э.** Иной путь. Невидимая революция в третьем мире. Москва, Gatallaxy, 1995.

19. **Дорохов Р., Никольский А.** Вирус под арестом, Ведомости, 09 10 2013 г., 20 03 2015 г., http://www.vedomosti.ru/newspaper/articles/2013/10/09/virus-pod-arestom.

20. **Зиновьева Е.** Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы. Диссертация на соискание ученой степени доктора наук. Московский Государственный Институт Международных Отношений, Москва, 2017 г.

21. **Катасонов В.** Международный наркобизнес и отмывание грязных денег. Военное обозрение, 30 01 2014 г., 31 01 2014 г., http://topwar.ru/39060-mezhdunarodnyy-narkobiznes-i-otmyvanie-gryaznyh-deneg.html.

22. **Колесников С.** Теневая экономика: как ее считать. Экономика России XXI век, Январь 2001 г., http://www.ruseconomy.ru/nomer1_200101/ec27.html.

23. **Коркин И.** Руткиты: проблемы безопасности и тенденции развития. Москва, Издательство GameLand, 2013 г.

24. **Латов В.** Социальные функции теневой экономики в институциональном развитии постсоветской России. Диссертация доктора социологических наук. Высшая Школа Экономики, Тюмень, 2008.

25. **Райзберг Б., Лозовский Л., Стародубцева Е.** Современный экономический словарь. Москва, ИНФРА-М, 1999, 2ое издание, стр. 479.

26. **Родионов И., Гиляревский Р., Цветкова В., Залаев З.** Рынок информационных услуг и продуктов. МК-Пародика, Москва 2002, ISBN 5-94697-001-1.

27. **Сачков И.** ОТЧЕТ GROUP-IB: Тенденции Развития Преступности В Области Высоких Технологий 2014. Group-IB.ru, 2014 г., 19 09 2015 г., http://report2014.group-ib.ru/.

28. **Мануков С.** 4-я промышленная революция в Давосе. Expert Online, Москва, 02 06 2017, 15 06 2017, http://expert.ru/2016/01/21/chetvertaya-promyishlennaya-revolyutsiya/

29. **Моторин Р., Моторина Т.** Система национальных счетов. Киевский национальный экономический университет имени Вадима Гетьмана, 2001.

30. **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. ISBN 978-966-484-233-1, стр. 138-150, Киев, Украина.

31. **Охрименко С., Саркисян А., Бортэ Г.** Противостояние в информационной сфере (Confrontation in the Domain of Information Technologies). Revista Militara Nr.1(9)/2013, Министерство Обороны Республики Молдова.

32. **Охрименко С., Бортэ Г.** Теневая Информационная Экономика. (Shadow Information Economics). Формирование Современного Информационного Общества – Проблемы, Перспективы, Инновационные Подходы, Saint Petersburg, 05-10 09 2012, стр. 137-145.

33. **Охрименко С., Хырбу Э., Бортэ Г., Склифос К., Солоненко О., Левандовский В., Сторож О., Павлова Л**. Информационная Безопасность Предпринимательской

Деятелности (Infromation Security in Etrepreneurship). Международна Научна Конференция Информационните Технологии - Стратегически Приоритет В Икономика На Знанието (International Information Technologie Conference – Strategical Priorities of Knowledge Economics), 2011 г., стр. 38-43.

34. **Панасенко А.** Киберпреступники заработали в 2016 году на вымогателях $1 млрд. https://www.anti-malware.ru/news/2017-06-07/23111
35. **Филиппова Т.** Деактивация теневой экономики в России. Томск, STT, 2013, ISBN 978-5-93629-508-9.
36. История сценера и крупнейшего релизёра EliteTorrents, который «отделался» условным сроком. Хабрахабр, 16 07 2013 г., 26 01 2014 г., http://habrahabr.ru/post/186840/.
37. Постановление о Национальной программе кибербезопасности Республики Молдова на 2016-2020 годы № 811 от 29.10.2015. http://www.mtic.gov.md/ru/postanovlenie-o-nacionalnoy-programme-kiberbezopasnosti-respubliki-moldova-na-2016-2020-gody.
38. Постановление об утверждении Минимальных обязательных требований кибернетической безопасности Nr. 201 от 28.03.2017. http://lex.justice.md/viewdoc.php?action=view&view=doc&id=369772&lang=2.
39. Предъявлено обвинение хакерам организаторам ограбления века. Аналитика и новости компьютерной преступности, 10 11 2009 г., 26 01 2014 г., http://carderplanet.blogspot.com/2009/11/blog-post_6568.html.

* * *

40. **Ablon L., Libicki M., Golay A.** Markets for Cybercrime Tools and Stolen Data. RAND, 2014 г., 02 09 2014 г., http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
41. **Appelbaum J., Horchert J., Stöcker C.** Shopping for Spy Gear: Catalog Advertises NSA Toolbox. Spiegel Online, Spiegel, 29 12 2013 г., 01 07 2014 г., http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

42. **Berr J.** "WannaCry" ransomware attack losses could reach $4 billion. CBS MoneyWatch, CBS News, 16 05 2017 г., 16 06 2017 г., http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

43. **Bilton N.** How Credit Card Data Is Stolen and Sold. The New York Times, 03 05 2011 г., 21 05 2014 г., http://bits.blogs.nytimes.com/2011/05/03/card-data-is-stolen-and-sold/?_php=true&_type=blogs&_r=1.

44. **Boehme R**. Vulnerability Markets. What is the economic value of a zero-day exploit?. Technische Universitat Dresden, Institute for System Architecture, Берлин, Германия, 27–30 12 2005 г., 18 09 2015 г., https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3 _VulnerabilityMarkets.pdf

45. **Borta G.** The Dark Side of Information Economics. Economica. An. XXIII, nr2. (92), iunie 2015, ISSN 1810-9136, Academia De Studii Economice A Moldovei, Chisinau, Moldova, стр. 97-102.

46. **Borta G.** The Issues of Personal Data Protection. Standards in and Challenges to Public Administration in XXI Century. May 10-11, 2013 стр. 608-614, Svishtov, Bulgaria.

47. **Borta G.** Vulnerability Life Cycle Analysis. ITSEC-2012, International Conference on Information Technologies and Security. Chisinau, Republic of Moldova, 15-16 October, 2012. ISBN 978-9975-4172-3-5

48. **Borta G.** Small and Medium Enterprise Information Security Risk Assessment. Обліково-аналітичне забезпечення системи менеджменту підприэмства, Львів, April 2012, ББК У9(4Укр)212я43+У052(4Укр)я43, УДК 657.1:658.012:330.14, стр. 385-387.

49. **Borta G.** Vulnerability Researchers Role in Malware Lifecycle. International Conference on Application of Information and Communication Technology and Statistics in Economy and Education, ICAICTSEE-2011, December 2-3, 2011, University of National and World Economy, Sofia, Bulgaria, ISBN: 978-954-92247-3-3, стр. 656-660.

50. **Bradley T.** DroidDream Becomes Android Market Nightmare. PCWorld, 02 03 2011 г., 11 06 2014 г., http://www.pcworld.com/article/221247/droiddream_becomes_android _market_nightmare.html.

51. **Brewster T.** Confirmed: Alleged Blackhole Exploit Kit Author Arrested In Russia. TechWeek Europe, 08 10 2013 г., 20 03 2015 г., http://www.techweekeurope.co.uk/workspace/blackhole-exploit-kit-author-arrested-in-russia-128978?PageSpeed=noscript.

52. **Brinson A., Robinson A., Rogers M.** A cyber forensics ontology: Creating a new approach to studying cyber forensics. DFRWS, Elsevier, 08 2006 г., 20 03 2015 г., http://www.dfrws.org/2006/proceedings/5-Brinson.pdf.

53. **Broadhurst R., Grabosky P., Alazab M., Chon S.** Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. www.cybercrimejournal.com, Cybercrime Journal, 2014 г., 2015 10 21 г., http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf.

54. **Burghouwt P.** Detection of Botnet Command and Control Traffic in Enterprise Networks. Technische Universiteit Delft, 2015 г., https://repository.tudelft.nl/islandora/object/uuid:1640ad86-fc07-4e54-9f05-1629296738c7/datastream/OBJ/download.

55. **Caballero J., Grier C., Kreibich C., Paxson V.** Measuring Pay-per-Install: The Commoditization of Malware Distribution. Usenix, UC Berkeley, 20 03 2015 г., https://www.usenix.org/legacy/event/sec11/tech/full_papers/Caballero.pdf.

56. **Choo Kim-Kwang R.** The cyber threat landscape: Challenges and future research directions [В Интернете]. - University of South Australia, 11 2011 г., 21 09 2015 г., http://www.sciencedirect.com/science/article/pii/S0167404811001040.

57. **Ciza T.** Performance Enhancement of Intrusion Detection Systems using Advances in Sensor Fusion. Supercomputer Education and Research Centre, Indian Institute of Science, 04 2009 г., http://www.serc.iisc.ernet.in/graduation-theses/CizaThomas-PhD-Thesis.pdf.

58. **Cluley G.** First iPhone worm discovered - ikee changes wallpaper to Rick Astley photo. Naked Security, Sophos, 08 11 2009 г., 04 06 2014 г., http://nakedsecurity.sophos.com/2009/11/08/iphone-worm-discovered-wallpaper-rick-astley-photo/.

59. **Dagon D., Zou C., Lee W.** Modelling Botnet Propagation Using Time Zones. College of Computing, Georgia Institute of Technology, https://www.cc.gatech.edu/classes/AY2007/cs7260_spring/papers/botnet.pdf.

60. **Danchev D.** DDoS for hire services offering to ‘take down your competitor’s web sites’ going mainstream. Webroot Threat Blog, 06 06 2012 г., 28 05 2014 г., http://www.webroot.com/blog/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-sites-going-mainstream/.

61. **Danchev D.** Modern banker malware undermines two-factor authentication. ZDnet, 23 09 2009 г., 26 01 2014 г., http://www.zdnet.com/blog/security/modern-banker-malware-undermines-two-factor-authentication/4402.

62. **Danchev D.** New E-shop selling stolen credit cards data spotted in the wild. Webroot, Threat Blog, 24 09 2012 г., 20 03 2015 г., http://www.webroot.com/blog/2012/09/24/new-e-shop-selling-stolen-credit-cards-data-spotted-in-the-wild/.

63. **Davis J.** The Crypto-Currency. The Newyorker, 10 10 2011 г., 12 08 2017 г., http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency.

64. **Dikaiakos M., Pallis G., Katsaros D., Mehra P., Vakali A.** Distributed Internet Computing for IT and Scientific Research. 28 07 2014 г., http://linc.ucy.ac.cy/publications/pdfs/mic2009050010.pdf.

65. **Ducklin P.** Android "Master Key" vulnerability - more malware exploits code verification bypass. Naked Security, Sophos, 09 08 2013 г., 17 06 2014 г., http://nakedsecurity.sophos.com/2013/08/09/android-master-key-vulnerability-more-malware-found-exploiting-code-verification-bypass/.

66. **Dunn J.** Real Viagra sales power global spam flood. TechWorld, 13 07 2009 г., 20 03 2015 г., http://www.techworld.com/news/security/real-viagra-sales-power-global-spam-flood-119086/.

67. **Ellison C.** Symbian Skulls: A Virus by Any Other Name?. eWeek, 24 11 2004 г., 27 03 2014 г., http://www.eweek.com/c/a/Mobile-and-Wireless/Symbian-Skulls-A-Virus-by-Any-Other-Name/.

68. **Etalle S.** The New Cyber Weapons. www.w-i-c.org. - TU Eindhoven & U of Twente, 23 09 2010 г., 28 09 2015 г., http://www.w-i-c.org/MWM2013/Etalle_cyberweapons.pdf.

69. **Fekolkin R.** Botnet-originated DDoS attacks: Overview and Mitigation. Luleå University of Technology, 07 01 2015 г., 01 10 2015 г., http://www.academia.edu/10139036/Botnet-originated_DDoS_attacks_Overview_and_Mitigation.

70. **Foster I., Zhao Y., Raicu I., Lu S.** Cloud Computing and Grid Computing 360-Degree Compared. 28 07 2014 г., http://arxiv.org/ftp/arxiv/papers/0901/0901.0131.pdf.

71. **Gareth O.** Tor: Hidden Services and Deanonymisation. media.ccc.de., 01 01 2015 г., 09 10 2015 г., http://media.ccc.de/browse/congress/2014/31c3_-_6112_-_en_-_saal_2_-_201412301715_-_tor_hidden_services_and_deanonymisation_-_dr_gareth_owen.html.

72. **Garza G.** Top 10 worst computer viruses. 18 09 2015 г., http://www.catalogs.com/info/travel-vacations/top-10-worst-computer-viruses.html.

73. **Gaspareniene L., Remeikiene R.** Digital Shadow Economy: a Critical Review of the Literature. 6th International Conference on Social Sciences, Volume III, Istanbul, 11-12 September 2015, ISBN 9788890916335, http://lib.euser.org/res/prc/6/6th_ICSS_2015_Proceedings_Book_Vol_3_ISBN_9788890916335.pdf.

74. **Gaspareniene L., Remeikiene R., Schneider F.** The factors of digital shadow consumption. Intellectual Economics 9 (2015) 108–119, http://www.econ.jku.at/members/Schneider/files/publications/2016/DigitalShadowConsumption.pdf.

75. **Geist M.** BSA Admits Canadian Software Piracy Rates Estimated; Canada Viewed as Low Piracy Country. Michael Geist, 27 05 2009 г., 26 01 2014 г., http://www.michaelgeist.ca/content/view/4005/125/.

76. **Goodin D.** TJX suspect indicted in Heartland, Hannaford breaches. The Register. - The Register, 14 08 2009 г., 26 01 2014 г., http://www.theregister.co.uk/2009/08/17/heartland_payment_suspect/.

77. **Grobauer B., Walloschek T., Stöcker E.** Understanding Cloud Computing Vulnerabilities. InfoQueue, 15 08 2011 г., 28 07 2014 г., http://www.infoq.com/articles/ieee-cloud-computing-vulnerabilities.

78. **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.

79. **Holm E.** Responding to Identity Crime on the Internet. The Business School, University of Ballarat, 2012 г., 27 09 2015 г., http://sdiwc.us/digitlib/journal_paper.php?paper=00000289.pdf.

80. **Jacobsson S.** BSA Piracy Study: Quantifying Piracy Data Easier Than We Thought. PCWorld, 11 05 2011 г., 26 01 2014 г., http://www.pcworld.com/article/196110/BSA_Piracy_Study.html.

81. **Jacobsson S.** Government Says Data Estimating Piracy Losses is Unsubstantiated. PCWorld, 14 04 2010 г., 26 01 2014 г., http://www.pcworld.com/article/194203/Government_Piracy.html.

82. **Jason M.** Russian Anti-Spam Chief Caught Spamming. DailyTech, 19 05 2010 г., 14 05 2014 г., http://www.dailytech.com/Russian+AntiSpam+Chief+Caught+Spamming/article18423.htm.

83. **Jiang X.** GingerMaster: First Android Malware Utilizing a Root Exploit on Android 2.3 (Gingerbread). NC State University, 17 08 2011 г., 13 06 2014 г., http://www.csc.ncsu.edu/faculty/jiang/GingerMaster/.

84. **Jiang X.** Security Alert: New Sophisticated Android Malware DroidKungFu Found in Alternative Chinese App Markets. NC State University, 31 05 2011 г., 13 06 2014 г., http://www.csc.ncsu.edu/faculty/jiang/DroidKungFu.html.

85. **Kalakota R.** Market Sizing – Analytics and Big Data. Amberoon, 5 11 2013 г., 6 11 2013 г., http://www.amberoon.com/CarpeDatumRx/bid/323448/market-sizing-analytics-and-big-data?source=Blog_Email_[Market%20Sizing%20%E2%80%93%20Anal].

86. **Kantouris C.** Russian Wanted by U.S. Over $4 Billion Bitcoin Crime Caught in Greece. Bloomberg, The Associated Press, 26 07 2017 г., 12 08 2017 г., https://www.bloomberg.com/news/articles/2017-07-26/russian-wanted-in-us-caught-in-greece-for-money-laundering.

87. **Kerr D.** NSA reportedly installing spyware on US-made hardware. CNet, 12 05 2014 г., 26 06 2014 г., http://www.cnet.com/news/nsa-reportedly-installing-spyware-on-us-made-hardware/.

88. **Krebs B.** ‘Blackshades’ Trojan Users Had It Coming. Krebs on Security, 14 05 2014 г., 27 05 2014 г., http://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/.

89. **Krebs B.** ‘Booter Shells’ Turn Web Sites into Weapons. Krebs on Security, 10 08 2012 г., 28 05 2014 г., http://krebsonsecurity.com/2012/08/booter-shells-turn-web-sites-into-weapons/.

90. **Krebs B.** Buying Battles in the War on Twitter Spam. Krebs on Security, 14 08 2013 г., 20 03 2015 г., http://krebsonsecurity.com/.

91. **Krebs B.** Crimeware Author Funds Exploit Buying Spree. Krebs on Security, 07 01 2013 г., 20 03 2015 г., http://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/.

92. **Krebs B.** How Carders Can Use eBay as a Virtual ATM. Krebs on Security, 03 11 2015 г., 06 11 2015 г., http://krebsonsecurity.com/2015/11/how-carders-can-use-ebay-as-a-virtual-atm/.

93. **Krebs B.** SpyEye vs. ZeuS Rivalry. Krebs on Security, 01 04 2010 г., 20 03 2015 г., https://krebsonsecurity.com/2010/04/spyeye-vs-zeus-rivalry/.

94. **Kshetri N.** The Simple Economics of Cybercrimes. IEEE Security and Privacy, 2006 г., http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.947.3671&rep=rep1&type=pdf

95. **Leyden J.** Russian bookmaker hackers jailed for eight years. The Register, 4 10 2006 г., 5 11 2013 г., http://www.theregister.co.uk/2006/10/04/russian_bookmaker _hackers_jailed/.

96. **Li Z., Liao Q., Blaich A., Striegel A.** Fighting botnets with economic uncertainty. Albion College, University of Notre Dame, 15 07 2010 г., http://onlinelibrary.wiley.com/doi/10.1002/sec.235/abstract.

97. **Li Z., Liao Q., Striegel A.** Botnet Economics: Uncertainty Matters. Albion College, University of Notre Dame, 22 12 2008 г., http://www.econinfosec.org/archive/ weis2008/papers/Liao.pdf.

98. **Macdonald D.** Zeus: God of DIY Botnets. FortiGuard Center, 26 01 2014 г., http://www.fortiguard.com/legacy/analysis/zeusanalysis.html.

99. **Maiberg E.** Hacks! An investigation into aimbot dealers, wallhack users, and the million-dollar business of video game cheating. PC Gamer, 30 04 2014 г., 26 05 2014 г., http://www.pcgamer.com/2014/04/30/hacks-an-investigation-into-aimbot-dealers-wallhack-users-and-the-million-dollar-business-of-video-game-cheating/3/.

100. **Majoras D.** Spyware Workshop: Monitoring Software On Your Personal Computer: Spyware, Adware and other Software, Federal Trade Comission, 2005 г.

101. **Maslennikov D.** New ZitMo for Android and Blackberry. SecureList, Kaspersky Lab, 08 2007 г., 13 06 2014 г., http://www.securelist.com/en/blog/208193760/New_ZitMo_for_Android_and_Blackberry.

102. **Maslennikov D.** ZeuS-in-the-Mobile – Facts and Theories. SecureList, Kaspersky Lab, 2005 г., 13 06 2014 г., http://www.securelist.com/en/analysis/204792194/ZeuS_in_the_Mobile_Facts_and_Theories.

103. **Menta R.** Movie and Record Industry Piracy Figures Incendiary, But Not Fact. 15 06 2006 г., 26 01 2014 г., http://www.mp3newswire.net/stories/6002/250billion.html.

104. **Mills E.** First SMS-sending Android Trojan reported. Cnet, 10 08 2010 г., 10 06 2014 г., http://www.cnet.com/news/first-sms-sending-android-trojan-reported/.

105. **Ohrimenco S., Borta G.** Rental Relationships in Shadow Information Economics. 5th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education, University of National and World Economy, November 2015, Sofia, Bulgaria.

106. **Ohrimenco S., Borta G.** Social Aspects of Shadow Information Economics. 4th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education, University of National and World Economy, October 2014, Sofia, Bulgaria.

107. **Ohrimenco S., Borta G.** Informal Economics of Information Threats. 3rd International Conference on Application of Information and Communication Technology and Statistics in Economy and Education, ICAICTSEE-2013, December 6-7th, 2013, University of National and World Economy, Sofia, Bulgaria, ISBN 978-954-644-586-5, pp. 27-34.

108. **Ohrimenco S., Borta G.** The Structure of Shadow Information Economics. ITSEC-2012, International Conference on Information Technologies and Security. Chisinau, Republic of Moldova, 15-16 October, 2012. ISBN 978-9975-4172-3-5

109. **Ohrimenco S., Sarkisian A., Borta G.** Price policy model at the modern shadow market of information technologies. International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE-2012). October 5 – 6th, 2012 University of National and World Economy. Sofia, Bulgaria.

110. **Ohrimenco S., Harbu E., Borta G., Sclifos C., Solonenco O., Levandovsky V., Storoj O., Pavlova L.** Information Security in SMB (Информационная безопаспость среднего и малого бизнеса), Management and Production Engineering, University of Bielsko-Biala, Bielsko-Biala, Poland, 2012, pp. 203-220.

111. **Orfila A., Carbo J., Ribagorda A.** Decision Model Analysis for Spam. Connections, the Quarterly Journal, 2004 г., 27 09 2015 г., http://connections-qj.org/system/files/15.10_Orfila_Carbo_Ribagorda.pdf?download=1.

112. **Passeri P.** 2013 Cyber Attacks Statistics (Summary). Hackmageddon, 19 01 2014 г., 06 02 2014 г., http://hackmageddon.com/2014/01/19/2013-cyber-attacks-statistics-summary/.

113. **Perlroth N., Sanger D.** Nations Buying as Hackers Sell Flaws in Computer Code. The New York Times, 13 07 2013 г., 26 01 2014 г., http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?_r=0.

114. **Peterson A.** Why stolen European credit card numbers cost 5 times as much as U.S. ones. The Washington Post, 2013 г., http://www.washingtonpost.com/.

115. **Prescott S.** Blizzard to sue creators of 'ValiantChaos' StarCraft 2 hack. PC Gamer, 26 05 2014 г., 26 05 2014 г., http://www.pcgamer.com/2014/05/26/blizzard-to-sue-creators-of-valiantchaos-mappack-starcraft-2-hack/.

116. **Rentrop C., Zimmermann S.** Shadow IT Evaluation Model. FedCSIS, 2012 г., 27 09 2015 г., https://fedcsis.org/proceedings/2012/pliks/394.pdf. - ISBN 978-83-60810-51-4.

117. **Rosenberg E.** U.S. Internet fraud at all-time high / 'Nigerian' scam and other crimes cost $198.4 million. SFGate, Hearst Newspapers, 31 03 2007 г., 29 07 2014 г., http://www.sfgate.com/crime/article/U-S-Internet-fraud-at-all-time-high-Nigerian-2576989.php.

118. **Rossow C.** Using Malware Analysis to Evaluate Botnet Resilience. Vrije Universiteit, 23 04 2013 г., https://www.cs.vu.nl/en/Images/PhD-thesis-CRossow_ tcm210-342357.pdf.

119. **Ruitenbeek E., Sanders W.** Modelling Peer-to-Peer Botnets. Electrical and Computer Engineering Department, Information Trust Institute, and Coordinated Science Laboratory University of Illinois at Urbana-Champaign, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.218.6101&rep=rep1&type=pdf.

120. **Ryba M., Sulwiński J., Poniewierski A.** The Methodology For Detecting And Managing The Abuse Of IT Systems. AGH University of Science and Technology, 2008 г., 27 09 2015 г., http://journals.agh.edu.pl/ csci/article/view/193/114.

121. **Schneider F.** Implausible Large Differences in the Sizes of Underground Economies in Highly Developed European Countries? A Comparison of Different Estimation Methods. 06 2017 г., 08 10 2017 г. ISSN 2364-1428 https://www.cesifo-group.de/ifoHome/publications/docbase/DocBase_Content/WP/WP-CESifo_Working_Papers/wp-cesifo-2017/wp-cesifo-2017-06/12012017006522

122. **Schneider F., Buehn A., Montenegro C.** Shadow Economies All over the World. World Bank, 07 2010 г., 06 10 2015 г., https://openknowledge.worldbank.org/ bitstream/handle/10986/3928/WPS5356.pdf?sequence=1.

123. **Schneider F., Kepler J.** The Shadow Economy in Europe 2013. VISA, 2013 г., 03 02 2014 г., http://www.protisiviekonomiji.si/fileadmin/dokumenti/si/projekti/2013/ siva_ekonomija/The_Shadow_Economy_in_Europe_2013.pdf.

124. **Schwabach A.** Internet and the Law: Technology, Society, and Compromises. Santa Barbara, California, 2006 г., ISBN 1-85109-731-7.

125. **Sennholz H. F.** The Underground Economy. Auburn, Ludwig von Mises Institute, 20 07 1984 г., https://mises.org/library/underground-economy.

126. **Smith P.** Assessing the Size of the Underground Economy: the Statistics Canada Perspective. Canadian Economic Observer, 05 1994 г., http://www.statcan.gc.ca/pub/13-604-m/13-604-m1994028-eng.pdf.

127. **Steigerwald D.** The Underground Economy of Fake Antivirus Software. eScholarship, 06 01 2011 г., 26 01 2014 г., http://escholarship.org/uc/item/ 7p07k0zr#page-1.

128. **Stoneburner G., Goguen A., Feringa A.** Information Security. Guide for Conducting Risk Assessments - NIST Special Publication 800-30 Revision 1. National Institute of Standards and Technology, 09 2012 г., 08 02 2014 г., http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

129. **Svajcer V.** Aftermath of the Droid Dream Android Market malware attack. Sophos, 02 03 2011 г., 11 06 2014 г., http://nakedsecurity.sophos.com/2011/03/03/droid-dream-android-market-malware-attack-aftermath/.

130. **Tanase S.** Satellite Turla: APT Command and Control in the Sky. Securelist, Kaspersky Lab, 09 09 2015 г., 09 09 2015 г., https://securelist.com/blog/research/ 72081/satellite-turla-apt-command-and-control-in-the-sky/.

131. **Van Der Meulen R., Rivera J.** Gartner Says Every Employee Is a Digital Employee. Gartner, 20 08 2015 г., https://www.gartner.com/newsroom/id/3115717.

132. **Wang R.** Malware B-Z: Inside the Threat From Blackhole to ZeroAccess. Sophos, 29 09 2015 г., https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophos_from_blackhole_to_zeroaccess_wpna.pdf.

133. **Woda K.** Money Laundering Techniques With Electronic Payment Systems. procon.bg, Procon Ltd., 20 12 2003 г., 27 09 2015 г., http://procon.bg/system/files/18.02_Woda.pdf.

134. **Zaslavsky V., Strizhak A.** Credit Card Fraud Detection Using Self-Organizing Maps. Connections, the Quarterly Journal, 2006 г., 27 09 2015 г., http://connections-qj.org/ru/system/files/18.03_Zaslavsky_Strizhak.pdf.

135. 2012 Cost of Cyber Crime Study: United States. Ponemon, 2012 г., 27 09 2015 г., http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

136. 2012 Payment Security Practices Survey: United States. Ponemon, 07 2012 г., 27 09 2015 г., http://www.ponemon.org/local/upload/file/US_Cybersource_WPFinal.pdf.

137. 2013 Cyber Security Study. Bit9, 2013 г., 30 09 2015 г., https://www.bit9.com/resources/research-reports/2013-cyber-security-study/.

138. 2013 Online Fraud Report. CyberSource, 04 2013 г., 27 09 2015 г., http://www.cybersource.com/content/dam/cybersource/CyberSource_2013_Online_Fraud_Report.pdf.

139. 2013/2014 Global Fraud Report. Kroll, 2014 г., 19 09 2015 г., http://fraud.kroll.com/wp-content/uploads/2013/10/GlobalFraudReport_2013-14_WEB.pdf.

140. 2014 Cost of Cyber Crime Study: United States. Ponemon, 2014 г., 27 09 2015 г., http://resources.idgenterprise.com/original/AST-0130677_2014_US_Cost_of_Cyber_Crime_Study_FINAL_2.pdf.

141. 2016 Internet Crime Report. 22 10 2017 г., https://pdf.ic3.gov/ 2016_IC3Report.pdf.

142. 2017 Global Fraud & Cybercrime Forecast. RSA, 22 10 2017 г., https://www.rsa.com/content/dam/pdfs/5-2017/3956-infographic-fri-2017-global-fraud-forecast.pdf

143. Analysis of a Cybercrime Infrastructure. Proofpoint, 23 09 2015 г., https://www.proofpoint.com/.

144. Blue Coat Systems 2013 Mobile Malware Report. Blue Coat, 2013 г., 29 09 2015 г., https://www.bluecoat.com/sites/default/files/documents/files/BC_2013_Mobile _Malware_Report-v1d.pdf.

145. Blue Coat Systems 2014 Mobile Malware Report. Blue Coat, 2014 г., 29 09 2015 г., https://www.bluecoat.com/documents/download/aaa09ef6-f5a6-4c0b-a247-b0ff6bf8abe4.

146. Botnet DDoS Attacks. Incapsula, 20 03 2015 г., https://www.incapsula.com/ddos/ddos-attacks/botnet-ddos.html.

147. BSA's Canadian Piracy Numbers Based On Hunches, Not Actual Surveys. Techdirt, 26 01 2014 г., http://www.techdirt.com/articles/20090527/1125035034.shtml.

148. Crimeware. Panda Security, 26 01 2014 г., http://www.pandasecurity.com/ homeusers/security-info/types-malware/crimeware/.

149. CryptoLocker's crimewave: A trail of millions in laundered Bitcoin. ZDNet, Zero Day, 22 12 2013 г., 18 09 2015 г., http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/.

150. Cybercrime. Kaspersky Lab, 26 01 2014 г., http://www.kaspersky.com/internet-security-center/threats/cybercrime.

151. Emerging Tyber Threats Report 2013. Georgia Institute of Technology, 2012 г., 07 07 2014 г., http://www.gtsecuritysummit.com/pdf/2013ThreatsReport.pdf.

152. Get ahead of cybercrime EY’s Global Information Security Survey 2014. Ernst & Young, 2014 г., 27 09 2015 г., http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf.

153. Hacker Intelligence Initiative, Monthly Trend Report #13. Imperva, 10 2012 г., 07 07 2014 г., http://www.imperva.com/docs/HII_Monitoring_Hacker_Forums _2012.pdf.

154. Hacker Intelligence Summary Report. Imperva, 29 09 2015 г., http://www.imperva.com/docs/hii_the_anatomy_of_an_anonymous_attack.pdf.

155. Hope Is Not A Strategy: 2012 Annual DDoS Attack and Impact Survey: A Year-to-Year Analysis. Neustar, 2012 г., 27 09 2015 г., https://www.neustar.biz/enterprise/docs/whitepapers/ddos-protection/2012-ddos-attacks-report.pdf.

156. IBM X-Force Threat Intelligence Quarterly, 2Q 2014. IBM, 06 2014 г., 18 09 2014 г., http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=WGL03050USEN#loaded.

157. If It's May It's Time For The Press To Parrot Bogus Stats Announcement From The BSA. Techdirt, 26 01 2016 г., http://www.techdirt.com/articles/20100511/1516059386.shtml.

158. Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management. - British Standard Institute, 22 03 2010 г.

159. Intellectual Property Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods. United States Government Accountability Office, 04 2010 г., 26 01 2014 г., http://www.gao.gov/new.items/d10423.pdf.

160. International Blackshades Malware Takedown. Federal Bureau of Investigation, 19 05 2014 г., 27 05 2014 г., http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown.

161. Internet Security Threat Report 2013. Symantec, 2013 г., 29 09 2015 г., http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

162. Internet Security Threat Report 2014. Symantec, 2014 г., 29 09 2015 г., http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

163. IT Market Statistics and Trends. Ironpaper, 21 09 2016 г., 12 08 2017 г., http://www.ironpaper.com/webintel/articles/it-market-statistics-and-trends/.

164. McAfee Looks Back on a Decade of Cybercrime. McAfee, 25 01 2011 г., 26 11 2016 г., http://www.mcafee.com/us/about/news/2011/q1/20110125-01.aspx.

165. Ninth Annual BSA Global Software 2011 Piracy Study. BSA The Software Alliance, 2011 г., 26 01 2014 г., http://globalstudy.bsa.org/2011/.

166. NSA’s ANT Division Catalog of Exploits for Nearly Every Major Software/Hardware/Firmware. LeakSource, 30 12 2013 г., 07 01 2014 г., http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/.

167. NY Times: правительства заинтересованы в 0day. Хабрахабр, Eset, 14 07 2013 г., 26 01 2014 г., http://habrahabr.ru/company/eset/blog/186580/.

168. Potentially Unwanted Programs. McAfee, 09 2005 г., 13 05 2014 г., http://www.mcafee.com/tw/resources/white-papers/wp-potentially-unwanted-programs-spyware-adware.pdf.

169. Project 2020. Scenarios for the Future of Cybercrime. ICSPA, Europol, Trendmicro, 27 09 2015 г., http://2020.trendmicro.com/Project2020.pdf.

170. Ransomware Past, Present, and Future. Technical Marketing Team. https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf

171. Report To The Nations On Occupational Fraud And Abuse. 2012 Global Fraud Study. Association of Certified Fraud Examiners, 2012 г., 27 09 2015 г., https://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf.

172. Russian hackers given stiff prison sentences. Риа Новости, 3 October 2006, 5 November 2013, http://en.ria.ru/russia/20061003/54474373.html.

173. Second Annual Cost of Cyber Crime Study. Ponemon, 10 08 2011 г., 27 09 2015 г., http://www.ponemon.org/local/upload/file/2011_2nd_Annual_Cost_of_Cyber_Crime_Study%20.pdf.

174. Security Threat Report 2014. Sophos, 2014 г., 29 09 2015 г., https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf.

175. Serious and Organised Crime Threat Assessment (SOCTA). Europol, 2017 г., https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment.

176. Shadow IT in the Enterprise. Nasuni, 22 09 2015 г., http://www6.nasuni.com/rs/nasuni/images/White_Paper-Shadow_IT_in_the_Enterprise.pdf.

177. Skulls Mobile Virus. Computer Virus, 17 06 2009 г., 27 03 2014 г., http://creatingcomputervirus.blogspot.com/2009/06/skulls-mobile-virus.html.

178. Spyware, Adware and Malware. RM Education, 12 08 2004 г., 26 01 2014 г., http://www.rm.com/Support/TechnicalArticle.asp?cref=TEC276510.

179. The Cost of Cybercrime. Detica, 17 02 2011 г., 21 09 2015 г., https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

180. The Cyber-Crime Black Market Uncovered. Panda Security, 2010 г., 15 06 2017 г., http://globalinitiative.net/wp-content/uploads/2017/01/panda-the-cyber-crime-black-market-uncovered.pdf.

181. The Evolving Threat Landscape Anatomy of an Attack Securing Tomorrow's Perimeter. Radware, 01 10 2015 г., http://www.cio.gov.bc.ca/local/cio/informationsecurity/PS2013_pdfs/CarlHerberger_vendor.pdf.

182. The Internet Organised Crime Threat Assessment (IOCTA) 2016. Europol, 2016 г., https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

183. The Leaking Vault 2011 Six Years of Data Breaches. Digital Forensics Association, 08 2011 г., 21 09 2015 г., http://static1.1.sqspcdn.com/static/f/305562/13944683/1314851775340/The_Leaking_Vault_2011-Six_Years_of_Data_Breaches.pdf

184. The Underground Hacker Markets are Booming with Counterfeit Documents, Premiere Credit Cards, Hacker Tutorials and 100% Satisfaction Guarantees. DELL Secureworks, 12 2014 г., 02 11 2015 г., http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf.

185. Threat Report 2012. www.websense.com, Websense, 16 04 2012 г., 27 09 2015 г., https://www.websense.com/assets/reports/report-2012-threat-report-en.pdf.

186. Timofonica Virus: Questions and Answers. Kaspersky Lab, 12 06 2000 г., 27 03 2014 г., http://www.kaspersky.com/news?id=68.

187. Timofonica Virus Targets Mobile Phones. Telecompaper, 7 06 2000 г., 27 03 2014 г., http://www.telecompaper.com/news/timofonica-virus-targets-mobile-phones--219755.

188. Trustwave 2013 Global Security Report. Trustwave, 21 02 2013 г., 27 09 2015 г., https://www.trustwave.com/Resources/Library/Documents/2013-Trustwave-Global-Security-Report/.

189. Under cyber attack EY's Global Information Security Survey 2013. Ernst & Young, 2013 г., 27 09 2015 г., http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf.

190. Verizon 2015 Data Breach Investigations Report. verizonenterprise.com, Verizon, 13 04 2015 г., 15 04 2015 г., http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/.

191. Websense 2014 Threat Report. Websense, 03 04 2014 г., 27 09 2015 г., http://www.websense.com/assets/reports/report-2014-threat-report-en.pdf.

192. Websense 2015 Threat Report. Websense, 08 04 2015 г., 27 09 2015 г., https://www.websense.com/assets/reports/report-2015-threat-report-en.pdf.

* * *

193. **Гюров Р.** Модел За Изграждане На Система За Киберсигурност. studia-analytica.blogspot.md. - 03 11 2014 г., 27 09 2015 г., http://studia-analytica.blogspot.md/2014/11/blog-post.html.

Приложение 1. Расчётные данные для модели доходности ботнета

M(b) – суммарные доходы арендатора ботнета (долл. США)	**P** – стоимость аренды зараженного компьютера (долл. США)	**b** – количество арендованных зараженных компьютеров (штуки)	**k** – оплата услуг поддержания каналов связи (долл. США)	**B** – размер ботнета (штуки)	**a(B)** – потери злоумышленника в случае обнаружения ботнета (долл. США)	**i(B)** – стоимость заражения компьютеров (долл. США)	**O** – затраты на поддержание структуры арендатором(долл. США)	y_1 – прибыль бот-мастера (долл. США)	y_2 – прибыль арендатора (долл. США)
150	0.02	5000	20	100000	100	500	10	-520	50
300	0.02	10000	20	100000	100	500	10	-420	100
450	0.02	15000	20	100000	100	500	10	-320	150
600	0.02	20000	20	100000	100	500	10	-220	200
750	0.02	25000	20	100000	100	500	10	-120	250
900	0.02	30000	20	100000	100	500	10	-20	300
1050	0.02	35000	20	100000	100	500	10	80	350
1200	0.02	40000	20	100000	100	500	10	180	400
1350	0.02	45000	20	100000	100	500	10	280	450
1500	0.02	50000	20	100000	100	500	10	380	500
1650	0.02	55000	20	100000	100	500	10	480	550
1800	0.02	60000	20	100000	100	500	10	580	600

1950	0.02	65000	20	100000	100	500	10	680	650
2100	0.02	70000	20	100000	100	500	10	780	700
2250	0.02	75000	20	100000	100	500	10	880	750
2400	0.02	80000	20	100000	100	500	10	980	800
2550	0.02	85000	20	100000	100	500	10	1080	850
2700	0.02	90000	20	100000	100	500	10	1180	900
2850	0.02	95000	20	100000	100	500	10	1280	950
3000	0.02	100000	20	100000	100	500	10	1380	1000

Источник: рассчитано автором на основе данных, приведенных в параграфе 3.1.

Приложение 2. Перечень законов и постановлений Правительства Республики Молдова, касательно информационной безопасности

1. Закон о Службе информации и безопасности Республики Молдова Nr. 753 от 23.12.1999.

2. Закон о защите персональных данных Nr. 133 от 08.07.2011.

3. Постановление о Национальной стратегии развития информационного общества «Цифровая Молдова 2020» Nr. 857 от 31.10.2013.

4. Постановление о национальной программе кибербезопасности Республики Молдова на 2016-2020 годы № 811 от 29.10.2015.

5. Постановление об утверждении Минимальных обязательных требований кибернетической безопасности Nr. 201 от 28.03.2017.

Приложение 3. Перечень государственных органов, отвечающих за обеспечение информационной безопасности Республики Молдова

1. **Служба информации и безопасности Республики Молдова** (Serviciul de Informaţii şi Securitate al Republicii Moldova) – государственный орган, специализированный в области обеспечения государственной безопасности. Служба представляет собой единый централизованный орган, в который входят подразделения центрального аппарата Службы и его территориальные органы.

2. **Центр специальных телекоммуникаций** (Centrul de Telecomunicaţii Speciale) – Государственное предприятие Центр специальных телекоммуникаций создано в соответствии с Постановлением Правительства № 735 от 11 июня 2002 года "О специальных телекоммуникационных системах Республики Молдова" для решения задач в области информационной безопасности, обеспечения функционирования и развития государственных защищенных информационных и телекоммуникационных систем.

3. **Министерство информационных технологий и связи** (Ministerul Tehnologiei Informației și Comunicațiilor) – орган государственного управления, в функции которого входит разработка, продвижение и применение государственной политики в области информационных технологий, информационного общества и связи.

4. **Министерство внутренних дел** (Ministerul Afacerilor Interne).

Приложение 4. Справка о внедрении результатов исследования в Национальном Банке Республики Молдова

Banca Națională a Moldovei

Nr. 13-004/96 "01" iulie 2016

Справка о внедрении

Научно-практические предложения диссертационного исследования Бортэ Григория актуальны и своевременны для эффективной работы Департамента информационных технологий и Управления менеджмента непрерывности деятельности, безопасности информации и надзора в области информационных технологий Национального Банка Республики Молдова.

Исследование рынка продуктов и услуг в области информационной безопасности, представленное в работе, нашло свое применение в разработке проектов развития отрасли информационной безопасности.

Методология, представленная в исследовании, была принята на вооружение и оказала существенное влияние на формирование политики Национального банка Республики Молдова в области информационной безопасности.

Полученные результаты будут положены в основу новой методологии формирования стратегии развития и защиты информационных ресурсов банка.

С точки зрения учебной деятельности, результаты данного диссертационного исследования используются для повышения квалификации молодых сотрудников, их информированности в области информационной безопасности.

Чуботару Виктор,
Директор управления менеджмента непрерывности деятельности, безопасности информации и надзора в области информационных технологий

Adresa: Bulevardul Grigore Vieru nr. 1, MD-2005, Chişinău, Republica Moldova
Tel: (+373) 22 226 374, Fax: (+373) 22 220 591, email: official@bnm.md, web: www.bnm.md

Приложение 5. Справка о внедрении результатов исследования в Молдавской Экономической Академии

APROB
Prorector cu activitate ştiinţifică şi relaţii externe
al Academiei de Studii Economice a Moldovei
prof. univ., dr. Vadim Cojocaru
„ ” mai 2017

Certificat
privind implementarea rezultatelor cercetării obținute în teza de doctorat a dlui Bortă Grigori pe tema “Economia tenebră în domeniul tehnologiei informației.”

Rezultatele cercetării au fost utilizate pentru dezvoltarea activității cursului universitar și al programului “Economia informațională tenebră”

Pentru pregătirea prelegerilor, a seminarelor și a lucrărilor de laborator au fost folosite momentele cheie al cercetării, inclusiv:

1. Contextul de actualitate al problemei de Economie informațională tenebră (Introducere, p. 10 și capitolul 1, pp. 15-21).
2. Definițiile propuse a economiei informaționale tenebre, inclusiv generală, economică și tehnologică (Capitolul 1, pp. 21-25).
3. Elaborarea complex a modelelor de Economie informațională tenebră, inclusiv:
   - Modelul structurii pieței produselor și serviciilor în domeniul economiei informaționale tenebre (Capitolul 2, pp 46-77.);
   - Modelul de monetizare a produselor și serviciilor în domeniul economiei informaționale tenebre (capitolul 2, pp 78-89.);
   - Modelul elementelor de profitabilitate botnet (Capitolul 3, pp 90-99.);
   - Modelul fluxului de numerar în economia informațională tenebră (Capitolul 3, pp. 99-102).
4. Analiză detaliată a bunurilor și serviciilor incriminată, în domeniul tehnologiilor informaționale, precum și compararea acestora cu omologii „ușoare“ (Capitolul 2, pp. 78-89).
5. Structura sectorială propusă a economiei informaționale tenebre (Capitolul 2, pp. 78-89).
6. Geneza economiei informaționale tenebre (Capitolul 2, pp. 34-46).
7. Clasificarea produselor și serviciilor pe piața economiei informaționale tenebre (Capitolul 2, pp. 78-89).
8. Rezultatele analizei datelor, caracteristicile proceselor individuale ce au loc în economia informațională tenebră (capitolele 1, 2, 3, pp. 15-28, pp. 34-89, pp. 90-102).
9. Metode economice și matematice folosite pentru a determina profitabilitatea produselor și serviciilor cu impact negativ în domeniul economiei informaționale tenebre (Capitolul 3, pp. 90-102).

Cursul “Economie informațională tenebră” a fost predat în perioada anilor universitari 2014-2015 și 2016-2017.

Anatolie PRISĂCARU
conferențiar universitar,
doctor în științe fizico-matematice,
șef-catedră "Tehnologii Informaționale"

ДЕКЛАРАЦИЯ ОБ ОТВЕТСТВЕННОСТИ

Нижеподписавшийся, заявляю под личную ответственность, что материалы, представленные в докторской диссертации, являются результатом личных научных исследований и разработок. Осознаю, что в противном случае, буду нести ответственность в соответствии с действующим законодательством.

Бортэ Григорий

CV АВТОРА

Фамилия, имя: Бортэ Григорий

Гражданство: Республика Молдова

Образование:

Июль, 2011 American Institute on Political and Economic Systems (AIPES), Georgetown University, Charles University, Prague.

2010-н.м. Ph.D. по специальности Информационные Системы, Академия Экономических Знаний Молдовы.

2008-2010 M.Sc. по специальности Информационный Менеджмент, Академия Экономических Знаний Молдовы. Название дипломной работы: “Improvement of Data Leak Prevention System” (на примере Национального Банка Республики Молдова с успешным внедрением).

2005-2008 B.Sc. по специальности Кибернетика, Статистика и Экономическая Информатика, Академия Экономических Знаний Молдовы. Название дипломной работы: “Проектирование системы предотвращения утечки информации” (на примере Национального Банка Республики Молдова с успешным внедрением).

Опыт работы:

Август 2016 – н.м. Офицер информационной безопасности, 13 Elements A.G.

Сентябрь 2008 – Июль 2016 Офицер информационной безопасности, Национальный Банк Республики Молдова.

Ноябрь 2007 – Август 2008 “BestJobs” SRL. Разработка и поддержка веб-страниц (PHP, MySQL, Javascript). http://faces.md http://neogen.ro

Июнь 2005 – Ноябрь 2007 “RBB International” S.A. Разработка и поддержка веб-страниц (PHP, MySQL, Javascript). http://rbbinternational.com

Области научного интереса:

Информационная безопасность, теневая экономика, экономика информационных технологий, экономика информационной безопасности.

Языки:

Русский – родной

Английский – отлично (Internet Based TOEFL test score: 103/120)

Румынский – отлично

Немецкий – B11

Французский – со словарем.