Теневая информационная экономика

Бортэ Григорий, аспирант Академии Экономических Знаний Молдовы.
Национальный Банк Республики Молдова.

Ключевые слова: теневая информационная экономика, информационная безопасность.

Вступление

Предмет теневой информационной экономики в рамках сегодняшнего рынка информационных технологий, а также проблемы «классической» теневой экономики, по нашему мнению, недостаточно хорошо изучен, даже, несмотря на то, что эта тема важна как для специалистов в области информационных технологий, так и для экономистов.

Определение теневой информационной экономики

Теневая экономика во многих странах является важным направлением экономического исследования. Многие ученые и исследователи пытались предложить достойное определение для данного феномена, определить его границы. Наряду с термином теневая экономика, очень часто используются и другие, такие как подпольная, неосязаемая, параллельная, серая, черная, криминальная экономика. Мы считаем важным отметить, что каждый из этих терминов ссылается на определенную область теневой экономики, покрывает, определенный из её сегментов. Некоторые из этих терминов охватывают явление целиком, например, термины серая, подпольная, теневая, параллельная, чаще всего охватывают явление целиком, в то время, как такие термины, как черная и криминальная ссылаются лишь на отдельные, более узкие её участки.

Далее, мы предпримем попытку предложить своё определение этому феномену.

Мы считаем, что под понятием теневая экономика следует понимать всю индивидуальную и коллективную деятельность, являющуюся незаконной, связанную с проектированием, разработкой, распространением, поддержкой и использованием компонент информационных и коммуникационных технологий, скрываемой от общества. Другими словами, теневая информационная экономика это все незаконные и скрываемые продукты и услуги, использующие и основывающиеся на информационных технологиях. Основные экономические элементы данной сферы это – незаконные экономические взаимоотношения, незаконная деятельность,

связанная с производством, распространением, и использованием запрещенных продуктов и услуг. Таким образом, главной причиной существования теневой экономики вообще, и теневой информационной экономики в частности выступают такие условия, при которых выгодно скрывать определенную деятельность, либо её элементы, а также осуществлять противоправную и противозаконную деятельность.

Генезис теневой информационной экономики.

В истории возникновения теневой информационной экономики мы выделяем три основных этапа, которые будут рассмотрены далее.

Рисунок 1. Генезис теневой информационной экономики.

Докомпьютерный этап

На данном этапе развиваются первые предпосылки появления теневой информационной экономики. Эта стадия начинается примерно с третьего тысячелетия до нашей эры и длится вплоть до середины двадцатого столетия нашей эры. В этот период начинают развиваться первые законодательные системы, появляются первые вычислительные устройства, развиваются рычаги экономического регулирования. На этом этапе уже почти все государства столкнулись с негативным эффектом существования теневой экономики. Наиболее важными событиями данной эпохи являются следующие:

- Первые денежные единицы – наряду с первыми деньгами начали появляться и подделки, например, одними из древнейших считаются варварские подделки монет Римской империи.
- Абак – одно из первых вычислительных устройств, когда-либо использованных человеком.
- Калькулятор – следующий революционный скачек в развитии вычислительной техники. Считается, что первый калькулятор был представлен в 1820м году.

- Римское право – основа почти всех законодательных систем, существующих в наши дни. Обычно, их появление связывают с двенадцатью таблицами, датируемыми 439 годом до н.э. Как уже упоминалось, причиной существования теневой экономики являются условия, при которых выгодно скрывать деятельность, либо заниматься запрещенной деятельностью, что, в свою очередь, говорит о неэффективности законодательного и исполнительного аппаратов.
- Двойной учёт – важная веха в истории развития теневой экономики, двойной учёт послужил основой современной бухгалтерии. Первые упоминания датируются 13м веком нашей эры.
- Charga Plate – прообраз современных кредитных карт. Мы считаем данное событие значимым потому, что значительная часть мошеннических операций в сфере информационных технологий сегодня сводятся к краже данных кредитных карт, будучи очень прибыльной. Появление Charga Plate датируется 1928м годом н.э.
- Пиратство – значение, которое наиболее часто приходит на ум современному человеку, связанное с кражей интеллектуальной собственности, данный термин получил в Великобритании в 17м веке нашей эры.
- Программируемые устройства – первым программируемым устройством, в какой-то мере послужившим прародителем современной вычислительной техники, считается антикитерский механизм, датируемый 100м годом до н.э., который, скорее всего, был предназначен для расчета движения небесных тел.

Ранний этап

ПО нашему мнению, начало данного этапа относится к середине двадцатого столетия нашей эры. Наиболее важной тенденцией данного периода является значительное ускорение темпов развития вычислительной техники, появление первых вредоносных программ, написание многих фундаментальных трудов в области информационных технологий. Наиболее значимыми событиями этого периода, по нашему мнению, являются следующие:

- Программируемый компьютер – первым представителем данной категории является британский Колосс (the Colossus), предназначением которого была расшифровка немецких сообщений.
- Теория самовоспроизводящихся автоматов – данный труд венгеро-американского ученого Джона фон Неймана считается одной из фундаментальных работ в области вычислительной техники,

послужившей основой для развития вредоносного программного обеспечения.

- ARPANET – один из важнейших этапов в развитии современных компьютерных сетей, также, наряду со следующей упомянутой вехой, послужил одним из важных шагов на пути становления глобальной сети Internet.
- TCP/IP – стек протоколов, ещё один важный этап в развитии сети Internet.
- Internet – следствие событий, упомянутых в двух предыдущих вехах данного этапа развития теневой информационной экономики, при этом является, по нашему мнению, одной из наиболее важных вех. Internet в наши дни является одной из самых распространенных сред общения, обмена данными, распространения программного обеспечения (в том числе и вредоносного), а также отмывания денег.
- Процессоры Intel 80386 – очень важная, по нашему мнению, веха в истории развития теневой информационной экономики в связи с тем, что компьютеры на базе данного процессора в значительной мере поспособствовали продвижению компьютеров в широкую публику.
- Червь Морриса (Morris Worm) – один из первых экземпляров вредоносного программного обеспечения. Считается одним из первых компьютерных червей, а так же одной из первых вредоносных программ, использующих уязвимости программного обеспечения.
- MS DOS – операционная система, также внесшая значительный вклад в дело популяризации компьютеров, а также один из первых программных продуктов, подвергшихся пиратству.

Современный этап

На данном этапе хакеры начинают объединяться в группировки, структура их организации напоминает «классическую» криминальную древовидную структуру. Более того, информационные преступления, совершаемые на данном этапе, всё больше и больше напоминают «классические» преступления: кражи, шантаж, шпионаж, вымогательство. Почти все члены группировки выполняют узкоспециализированные задачи, возможно, даже не подозревая о возможностях дальнейшего использования результата своей работы. Они могут заниматься как исследованием рынка, так и исследованием законодательства, изучением возможностей отмывания денег и непосредственно проектированием, написанием, разработкой, распространением программного обеспечения. На данном этапе вредоносное программное обеспечение всё реже и реже несет шутливый или

деструктивный характер, стремясь приносить непосредственно доход, например, при помощи кражи личных данных, рассылки спама, DDoS атак и т.д. На данном этапе выделяется такой термин, как кибервойна (англ. Cyberwarfare). На современном этапе учащаются вирусные эпидемии, а также, благодаря растущему быстрыми темпами количеству вычислительной техники, существенно увеличивается и их масштаб. Важной, по нашему мнению, тенденцией на данном этапе является рост количества мобильных устройств, а также существенное увеличение их вычислительных мощностей. Наравне с усложнением защиты программного обеспечения от незаконного копирования увеличиваются и масштабы пиратства интеллектуальной собственности. На данном этапе появляется такое понятие, как хактивизм: люди стремятся выразить своё отношение к событиям реального мира посредством атак на информационные ресурсы. Наиболее значимыми событиями этого периода, по нашему мнению, являются следующие:

- Zeus – эпидемия троянской программы, поразившая, по некоторым данным, порядка 3.6 миллиона компьютеров в 196ти странах мира в 2007 году. Данное вредоносное программное обеспечение объединяет зараженные компьютеры в ботнет. В 2010 году автор опубликовал исходный код вредоносной программы.
- Conficker – ещё одна существенная эпидемия вредоносного программного обеспечения, поразившая, по некоторым данным, от 9ти до 15ти миллионов компьютеров. Данная программа использовала для заражения уязвимости операционной системы, и даже несмотря на то, что патч для уязвимости был достаточно быстро выпущен, он не внедрялся месяцами, что и привело к такой существенной эпидемии. От данного вируса пострадали Национальные военно-морские силы Франции, Министерство обороны Великобритании и Бундесвер.
- Stuxnet, Duqu, Flame – данные вирусы считаются наиболее яркими представителями, так называемого кибероружия.
- Проявления хактивизма – успешные DDoS атаки на PayPal, Visa, MasterCard – одни из наиболее ярких проявлений. Благодаря своему значительному количеству, протестующие смогли замедлить работу сайтов этих гигантов. Люди выражали свой протест в деле о проекте WikiLeaks, а также его основателе, Джулиане Ассанже.

Структура рынка теневой информационной экономики

Рынок теневой информационной экономики состоит из продуктов и услуг. По нашему мнению, ключевая особенность информационного мира диктует и основную особенность данного рынка: продукты и услуги очень

тесно переплетены и взаимосвязаны настолько, что между ними часто крайне сложно провести четкую границу.

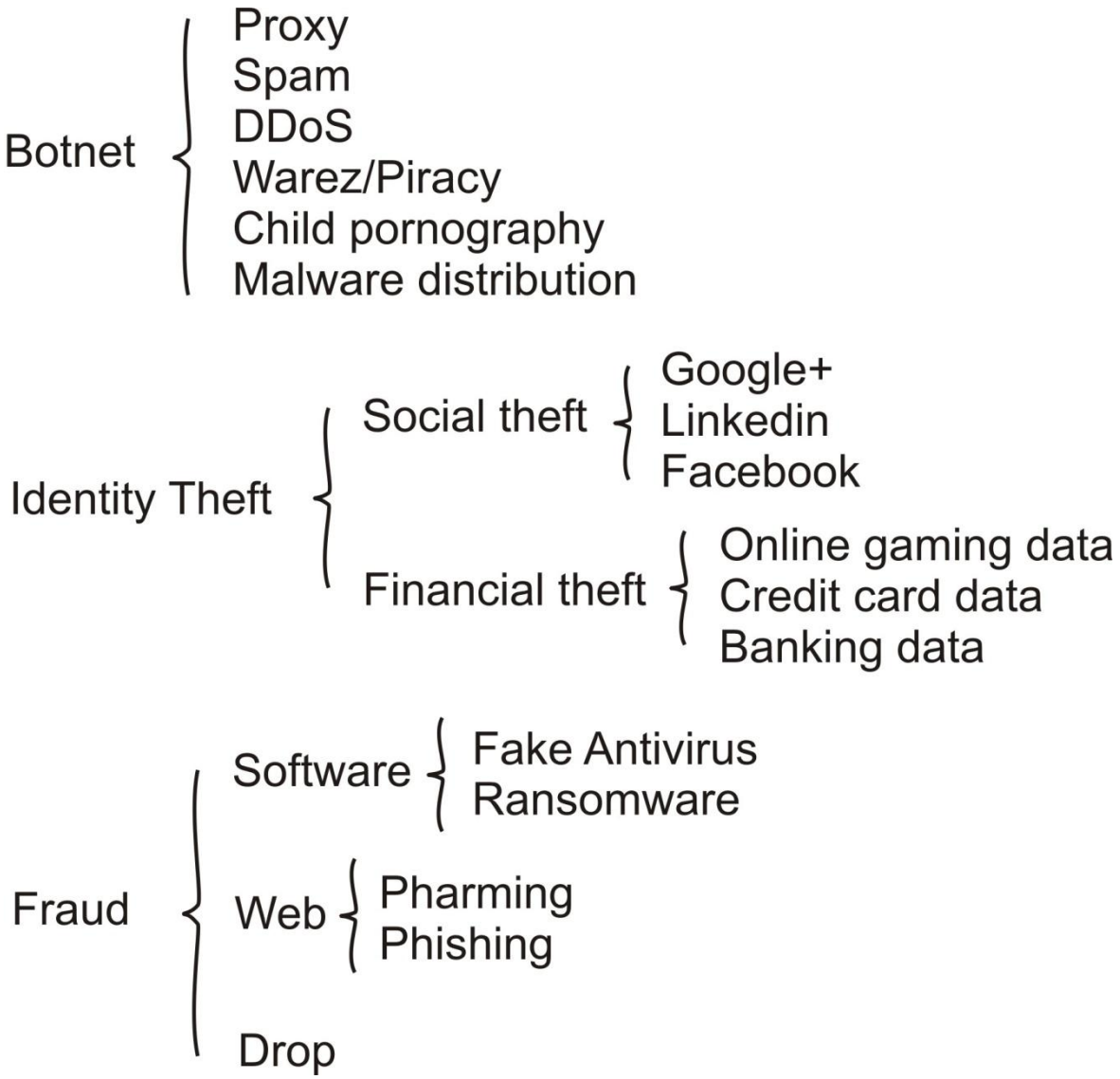

Рисунок 2. Структура теневых информационных доходов

Продукты

Далее мы попытаемся выделить наиболее значимые по нашему мнению категории продуктов, представленных на теневом информационном рынке:

- Специализированное программное обеспечение. Как уже упоминалось, одной из важных, по нашему мнению, тенденций последнего времени является значительное увеличение количества мобильных устройств на рынке, в связи с этим, всё чаще и чаще объектом атак и целью вредоносного программного обеспечения становятся именно мобильные устройства.
    - Вирусы
    - Шпионские программы

- Троянские программы
- Лже-антивирусы
- Черви
- Adware
- Crimeware
- Хакерские утилиты
- Эксплойты

- Подслушивающие устройства, такие как клавиатурные шпионы, устройства для считывания электромагнитных импульсов, скиммеры для банкоматов, сетевые (проводные и беспроводные) шпионы.
- Технологии и аппаратура для фальсификации пластиковых карт.
- Пиратское программное обеспечение, а также программы для обхода определенных видов защиты

Рисунок 3. Продукты на рынке теневой информационной экономики

Услуги

Наиболее значимыми, по нашему мнению, услугами на теневом рынке информационных технологий являются следующие:

- Аналитика, в том числе исследование рынка, законодательства, программного обеспечения;
- Кража личной информации, а также продажа подобных данных.
- Рассылка спама – относительно малоприбыльное занятие, которое, тем не менее, продолжает оставаться актуальным и приносить доход злоумышленникам.
- Фишинг – попытка выдать мошеннический сайт за известный пользователю сайт с целью кражи личных данных.
- Фарминг – атака, целью которой является перенаправление трафика с одного сайта на другой, мошеннический.
- Вымогательство – в том числе и посредством, например, лже-антивирусов и программ, блокирующих работу компьютера, обещающих за вознаграждение исправить неполадки.
- Терроризм – злонамеренные действия, поводом для которых служат убеждения злоумышленника.
- Аренда прокси-серверов – как для управления обширными бот-сетями, так и для распространения вредоносного программного обеспечения и отмывания денег.
- Отмывание денег при помощи информационных технологий. Притом, мы считаем важным отметить, что в данном случае могут отмываться как деньги заработанные в рамках теневого рынка информационных технологий, так и за его пределами
- Создание и аренда ботнетов. Мы считаем необходимым отметить, что современная структура ботнетов построена таким образом, что уничтожение целых ботнетов обычно не приводит к желаемым результатам в связи с тем, что у злоумышленников в резерве есть достаточное количество запасных ресурсов, которые он может относительно быстро ввести в эксплуатацию. Вышесказанное наталкивает на вывод о малой эффективности современных методов противодействия данному виду правонарушений и злоупотреблений.
- DoS-атаки, в том числе, посредством арендованных ботнетов.
- Саботаж – как грубые DDoS атаки «в лоб», так и более изощренные и узкоспециализированные атаки.

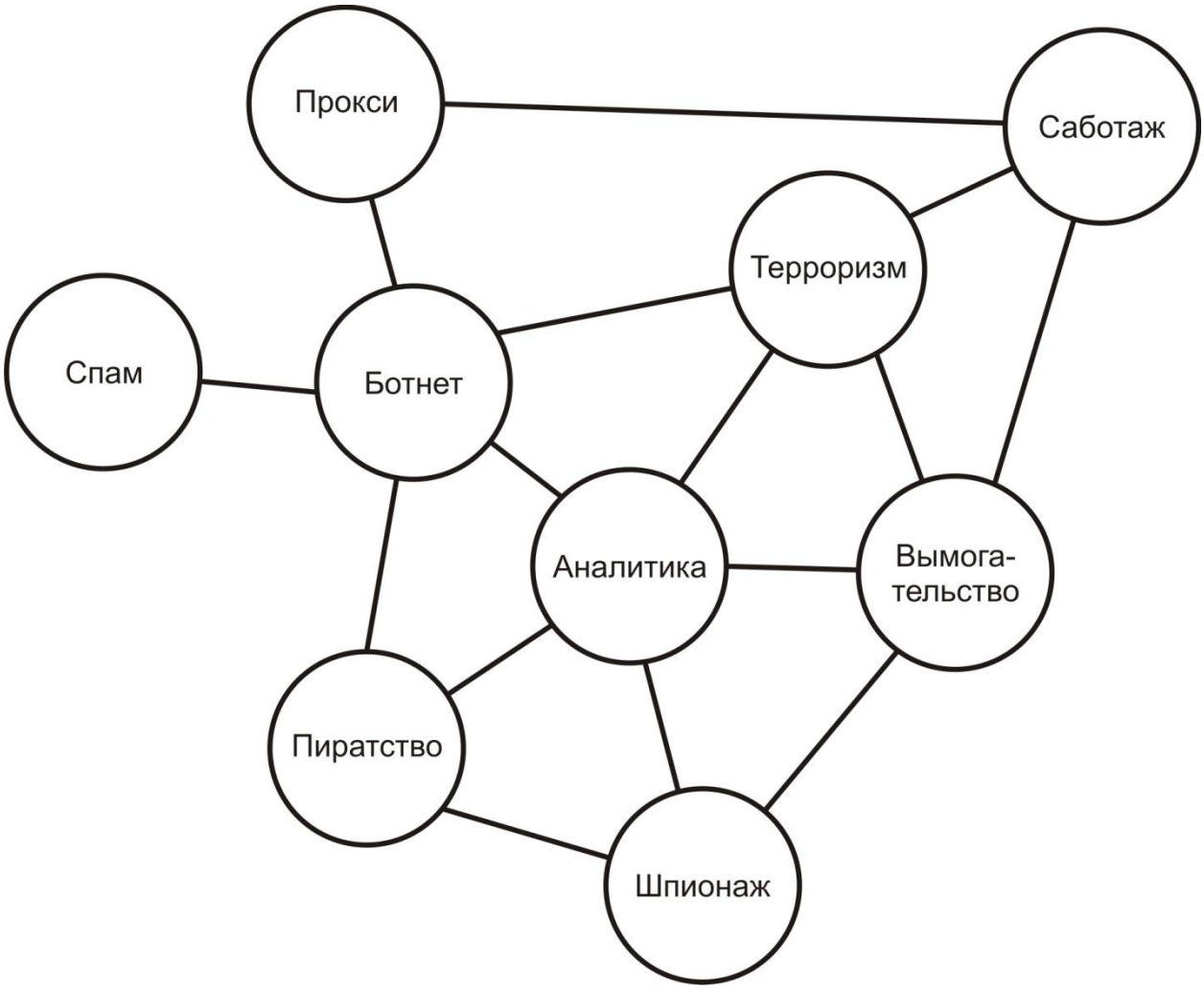

Рисунок 4. Услуги на рынке теневой информационной экономики

Заключение

По нашему мнению, главным выводом из данной работы должна служить необходимость разработки целостной стратегии противодействия теневой информационной экономике. Мы считаем данные принципы основополагающими для этой стратегии:

- Совершенствование законодательной базы экономического регулирования, нацеленного на создание условий, при которых сокрытие определенных видов деятельности или их элементов, как и любая незаконная деятельность станут невыгодными.
- Развитие сотрудничества на государственном, региональном и международном уровнях с целью понижения уровня теневой информационной экономики.
- Создание рабочих мест, реформация системы налогообложения, с целью ужесточения мер борьбы с отмыванием денег, а также ожесточение борьбы с коррупцией.

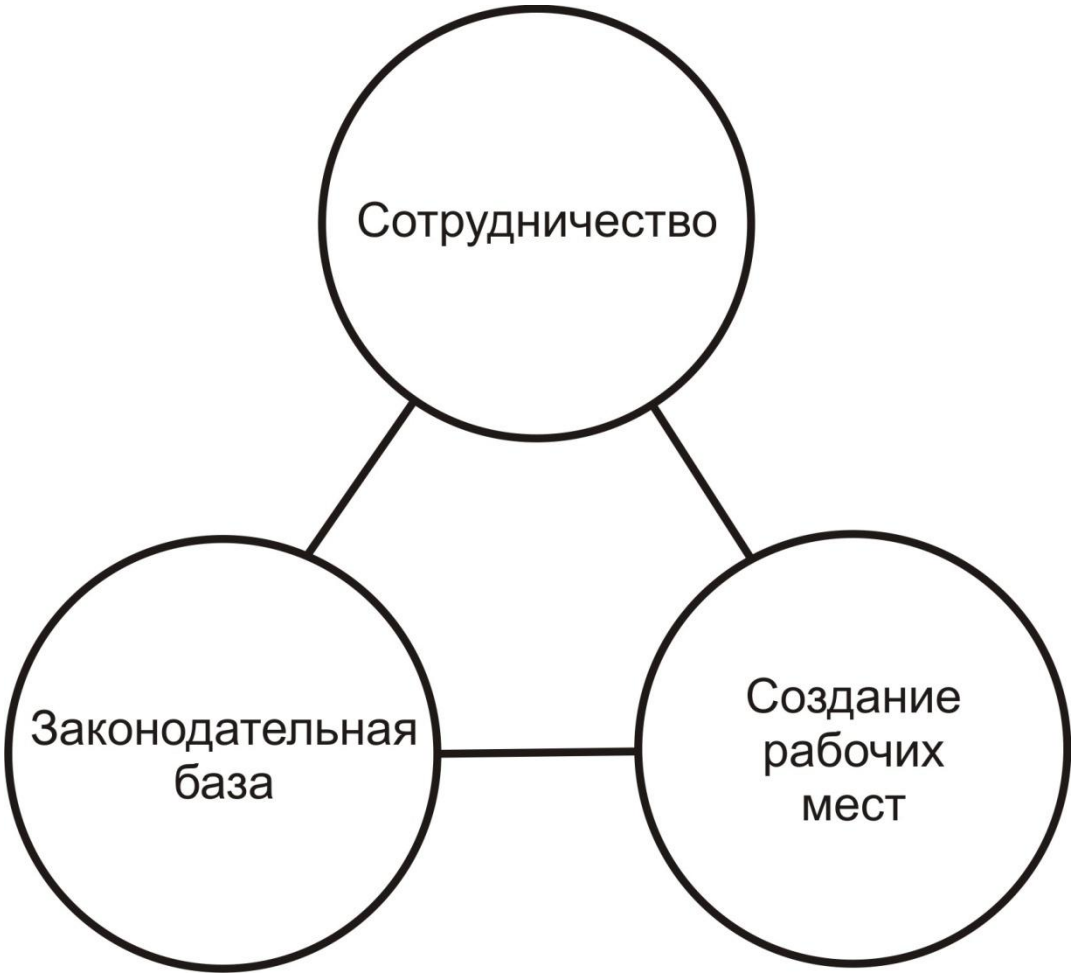

Рисунок 5. Основополагающие принципы противодействия теневой информационной экономике

Библиография

1. **Boehme R.** Vulnerability Markets. What is the economic value of a zero-day exploit? [Online] http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf
2. **Chiesa R.** Cybercrime & underground economy: operating and business model. *Flare Network.* [Online] July 1, 2010. [Cited: July 22, 2012.] http://www.flarenetwork.org/report/enquiries/article/cybercrime_and_underground_economy_operating_and_business_model.htm.
3. **Chiesa R**. Cybercrime: reasons, evolution of the players and an analysis of their modus operandi. *Bright.* [Online] July 1, 2010. http://flarenetwork.org/report/enquiries/article/cybercrime_reasons_evolution_of_the_players_and_an_analysis_of_their_modus_operandi.htm.
4. **Curry S., Williams A.** The Economics of Cybercrime and the “Law of Malware Probability”. *RSA.* [Online] [Cited: September 10, 2012.] http://www.rsa.com/blog/pdfs/economics_cybercrime.pdf.

5. **Greenberg A.** Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees). *Forbes.* [Online] March 21, 2012. [Cited: June 21, 2012.] http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/.
6. **Greenberg A**. Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. *Forbes.* [Online] March 23, 2012. [Cited: July 20, 2012.] http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.
7. **Ohrimenco S., Hârbu E., Bortă G., Sclifos C., Solonenco O., Levandovsky V., Storoj O., Pavlova L.** Information security in SMB. *Management and Production Engineering.* Bielsko-Biala : 2012.pp 203-220.
8. **Richardson R.J.** Monitoring Sale Transactions for Illegal Activity. *IIMA online* . [Online] 2006. http://www.iima.org/CIIMA/13%20CIIMA%206-1%20105-114%20Richardson.pdf.
9. **Sarkisyan A., Ohrimenco S.** Training Higher Education Degrees Specialists in the Field of Information Security. *Laboratory of Information Security.* [Online] [Cited: September 10, 2012.] http://security.ase.md/materials/publications/index.html?artNr=15.
10. **Valentino-Devries J., Sonne, P., Malas N.** U.S. Firm Acknowledges Syria Uses Its Gear to Block Web . *The Wall Street Journal.* [Online] October 29, 2011. [Cited: July 20, 2012.] http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html.
11. **Zorz Z.** How much does a 0-day vulnerability cost? *Help Net Security.* [Online] March 26, 2012. [Cited: July 20, 2012.] http://www.net-security.org/secworld.php?id=12652.
12. **Бортэ Г.** Исследование жизненного цикла вредоносного программного обеспечения. *laboratory of Information Security.* [Online] [Cited: September 10, 2012.] http://security.ase.md/materials/publications/index.html?artNr=6.
13. **Бортэ Г.** Теневая Информационная Экономика. *Laboratory of Information Security.* [Online] [Cited: September 10, 2012.] http://www.security.ase.md/materials/si2011/Security_inform_2011_Pages_94_-_96.pdf.
14. **Охрименко С., Саркисян А.** Подпольная информационная индустрия. *The Bulletin of Transport and Industry Economics.* Харків : N 29, 2010, p.19-22.

15. **Охрименко С., Саркисян А.** Сенчестият Пазар на Инфомационни Технологии. Приложна информатика и статистика -съвременни подходи и методи. Международна научна конференция. 25-26 септември 2009, Равда, с.131-138.
16. **Охрименко С., Саркисян А.** Экосистема Информационной Безопасности. //Съвременни измерения на търговския бизнес. Комуникация между наука и практика. Юбилейна научнопрактическа конференция с международно участие. 12-13 май 2011 г. , Свищов, с.31-36.
17. **Синцов А.** Стоимость эксплойта... *SecurityLab.* [Online] June 21, 2012. [Cited: September 10, 2012.] http://www.securitylab.ru/blog/personal/asintsov/23097.php.
18. **Федотов Н.** Ботнеты процветают. *SecurityLab.* [Online] August 26, 2012. [Cited: September 10, 2012.] http://www.securitylab.ru/blog/company/infowatch/23945.php.