DOI: 10.18522/2073-6606-2016-14-4-156-172

CRITICAL ATTITUDE TOWARDS THE THEORY OF DIGITAL SHADOW ECONOMY: LITERATURE REVIEW AND NEW FOUNDATIONS

Ligita GASPARĖNIENĖ
Mykolas Romeris University,
Address: Ateities str. 20, LT 08303,
Vilnius, Lithuania
e-mail: ligitagaspareniene@mruni.eu

Rita REMEIKIENĖ
Mykolas Romeris University,
Address: Ateities str. 20, LT 08303,
Vilnius, Lithuania
e-mail: rita.remeikiene@mruni.eu

Romualdas GINEVIČIUS
Vilnius Gediminas Technical University,
Address: Saulėtekio al. 11, LT-10223
Vilnius, Lithuania
e-mail: romualdas.ginevicius@vgtu.lt

Arjan SKUKA
SS. Cyril and Methodius University,
Address: Goce Delcev 9, 1000 Skopje, R.
Macedonia
e-mail: arjan.skuka@gmail.com

This article is aimed at the complement of the theory of traditional shadow economy with the definition, features and channels of digital shadow economy. The issue of digital shadow economy is indeed new and, considering it as a branch of traditional shadow economy, very young. According to the results of the national scientific project "Digital Shadow Economy" the definition of digital shadow economy has been developed; the distinctive features and the main channels of digital shadow economy have been identified. The position of consumers' towards the phenomenon of digital shadow economy and consumers' motives to buy products/services in digital shadow markets has been found out as well.

Keywords: *digital shadow economy, concept and features of digital shadow economy, theory of digital shadow economy*

Acknowledgements: *This work was supported by the Research Council of Lithuania [grant number MIP-15642]*

JEL classifications: *E26, 017*

КРИТИКА ТЕОРИИ ЦИФРОВОЙ ТЕНЕВОЙ ЭКОНОМИКИ: ОБЗОР ЛИТЕРАТУРЫ И НОВЫЕ ОСНОВЫ

Лигита ГАСПАРЕНЕНЕ,
университет Миколаса Ромериса,
Вильнюс, Литва,
e-mail: ligitagaspareniene@mruni.eu;

Рита РЕМЕКЕНЕ,
университет Миколаса Ромериса,
Вильнюс, Литва,
e-mail: rita.remeikiene@mruni.eu;

Ромуальдас ЖИНЕВИЧЮС,
Вильнюсский технический университет им. Гедиминаса,
Вильнюс, Литва,
e-mail: romualdas.ginevicius@vgtu.lt;

Аржан СКУКА,
Университет Святого Кирилла и Мефодия,
Македония,
e-mail: arjan.skuka@gmail.com

Цель статьи – дополнение теории традиционной теневой экономики определением, представлениями об особенностях и каналах цифровой теневой экономики. Цифровая теневая экономика – действительно новое проблемное поле, рассматриваемое как очень молодое ответвление традиционной теневой экономики. Согласно результатам национального научного проекта «Цифровая теневая экономика», разработано определение цифровой теневой экономики, а также обозначены отличительные особенности и основные каналы цифровой теневой экономики. Кроме того, выявлено отношение потребителей к феномену цифровой теневой экономики и потребительские мотивы покупать товары и услуги на цифровых теневых рынках.

Ключевые слова: *цифровая теневая экономика; понятие и особенности цифровой теневой экономики; теории цифровой теневой экономики*

Благодарность: *Данная статья подготовлена при поддержке Исследовательского совета Литовской Республики (грант номер MIP-15642)*

Introduction

Although the advancement of IT and the Internet has greatly expanded business opportunities, it also provided the environment for the performance of illegal activities online, and gave birth to a new category of entrepreneurs who operate outside law or at the boundaries of law (*Dobson et al. 2015; Fuschi, Tvaronavičienė 2014; Teivāns-Treinovskis, Amosova 2016; Allabouche et al. 2016; Rezk et al. 2016; Samašonok et al. 2016; Belás et al. 2016; Tvaronavičienė 2016*), which, in turn, leads to wide scopes of digital shadow economy.

With reference to *Amasiatu and Shah* (*2014*), the success of online business transactions to a large extent depends on mutual trust and identity confirmation/authenticity because many agents operating in e-space aim at the gain of dishonest financial benefits.

Growing scopes of economic activities, which are difficult to define, as well as an increasing number of unidentified subjects and objects operating in e-space have become the most urgent economic issues of the recent decade. Via remote platforms like social networks, e-commerce and e-business systems, e-game sites, etc., real money circulates. However, in most cases, the revenue earned in these platforms is not accounted, and the taxes to a state budget are not paid. Although the scopes of digital shadow economy have not been accurately estimated so far, following the figures announced by *Europol* (2011), the losses incurred due to unreported activities online may reach nearly 750 billion EUR per year. Growing volumes of digital activities have been confirmed by different bodies responsible for the conduction of economic analysis. For instance, U.S. Government Accountability Office (GAO) estimated that the value of the losses incurred as a consequence of different types of cybercrime make nearly 117.5 billion US dollars per year (*GAO, 2007*).

Due to the reasons explicated above, both developed and developing countries are trying to find the ways to reduce the scopes of digital shadow economy without violation of individual and business rights to privacy (*Astrauskaitė, Paškevičius 2016; Dobrovič et al. 2016; Lavrinenko et al. 2016; Pauceanu 2016*).

At the same time, they face the emerging need to estimate the real value the revenue earned by agents in e-space. Lack of the official statistics on the real scopes of digital shadow economy in both local and global terms causes major difficulties to develop the measures of digital shadow economy prevention. Indeterminancy of the phenomenon of digital shadow economy exacerbates the problem even further.

Thus far, the research on the issues of digital shadow economy has covered the analysis of the single forms and manifestations of this phenomenon, in particular, cybercrimes like hacking into online banking systems, cracking of PIN codes or steal of credentials (*Yip, et al. 2012; Holz et al. 2012; Bossler, Holt 2012; Thomas & Martin, 2006; Mello, 2013; Vlachos, et al. 2011; Amasiatu & Shah, 2014; Zorz, 2015*), e-fraud (*Mello, 2013; Vlachos et al., 2011; Amasiatu & Shah 2014*), and digital piracy (*Sirkeci, Magnusdottir, 2011; Camarero, Anton, & Rodriguez, 2014; Camarero et al. 2014; Taylor 2012; Arli, Tjiptono, & Porto, 2015; Yu, et al. 2015*). Some authors also analysed the motives of subjects' involvement into illegal activities online (*Williams, Nicholas, & Rowlands, 2010; Sirkeci & Magnusdottir, 2011; Amasiatu & Shah, 2014; Vida, et. al., 2012; Taylor, 2012; Arli, et. al., 2015; Yu, et. al., 2015*). Nevertheless, the phenomenon of digital shadow economy has not been analysed in complex. Moreover, the definition of digital shadow economy has not been developed either in national or intenational levels, which would be truly purposeful minding the rapid penetration of e-communications and the expansion of e-business. In addition, although scientific literature is rich in different interpretations of illegal (underground) activities online, such illegal acitivities as cybercrimes, digital piracy or e-fraud should not be included in a definition of digital shadow economy since they refer to crimes and criminal responsibility rather than to performace of shadow economic activities. Hence, an exact and clear definition of digital shadow economy as well as identification of the features and channels typical of this phenomenon could help to form a clear notion of what this phenomenon refers to, and would contribute to the improvement of the methodologies of shadow economy estimation.

This article is aimed at the complement of the theory of traditional shadow economy with the definition, features and channels of digital shadow economy. In order to fulfil the defined aim, the following objectives have been raised: 1) to analyse the scientific literature on the issues of digital shadow economy focusing on theoretical interpretations, features and channels of this phenomenon; 2) with reference to the results of the empirical surveys conducted over the period of the last two years, to complement the theory of traditional shadow economy with the definition, features and channels of digital shadow economy.

The concept of digital shadow economy and its theoretical interpretations: a literature review

According to *Bossler and Holt* (*2012),* a substantial share of shadow economy revenue is generated in e-space. This attitude is supported by *Holz et. al.* (*2012*), who note that growing scopes of digital economy make conditions favourable to illegal digital business, which, in turn, leads to the increase in digital shadow economy. Rapid advancement and changeability of IT make observation and perception of the phenomenon of digital shadow economy a truly challenging task. Without any clear definition of digital shadow economy, its accurate scopes cannot be estimated because it remains vague which illegal (non-recorded) digital activities should be considered as digital shadow activities and included in statistical estimations, and which of them should be left for criminal consideration.

Minding an agressive nature of digital shadow economy, the concept of digital shadow economy can be aligned with the term of "digital underground economy", which refers to conduct of repeated illegal activities online in a global scale. According to *Yip, et al. (2012),* such activities are aimed at the achievement of incredibly complex wide-scale objectives *(Yip, et al. 2012)*. As it was noted by *Moore, Clayton and Anderson (2009),* digital underground economy refers to trade in the Internet, when the agents act openly, without any need to hide, although their actions are treated as illegal. *Herley and Florencio (2010)* interpret digital shadow economy as an online crime, which is committed aiming at particular gains (e.g. benefits or profits). The authors also note that the scopes of such crimes commonly exceed the capacities of a closed group of agents.

Considering illegality of activities as the main feature of digital shadow economy, the concept of digital shadow economy can be linked to the term of "cybercrime". In the scientific literature, a cybercrime refers to a strong underground economy that provides and produces tools and channels for crimes online *(Mello, 2013)*. On the other hand, a cybercrime may refer to technologically advanced criminal activities that cover employment of malware causing serious threats to consumers, organisations and business enterprises as well as to the entire public sector *(Vlachos et al., 2011; Ferreira et al. 2015)*.

According to *Smith* (*2015*), cybercrimes are remote crimes, which are committed by the Internet, when an illegally acting agent embezzles somebody else's assets or resources. Resources can also be embezzled by violating intellectual property rights, and in many other ways. Illegality of an action is recognised following jurisdiction of a state's government, i.e. it is recognized in the crime scene, but not in the place of origin of the crime.

Hence, the analysis of the scientific literature has revealed that the nature and different interpretations of digital shadow economy are closely related to the concept of cybercrime, proposing that digital shadow economy can be interpreted as an illegal online activity, which is conducted aiming at misappropriation of somebody else's assets and/or resources (*Smith, 2015*). *Amasiatu and Shah* (*2014*) call cybercrimes "faceless crimes", which, actually, are referred to as illegal activities that are performed in Internet networks or via information technologies. According to the authors (*Amasiatu, Shah, 2014*), illegal business activities are commonly linked to retail.

The above-introduced concepts of cybercrimes mainly refer to the operations of illegal sellers or service providers. Indeed, the link between the notions of a cybercrime and digital shadow economy seems logical because both of the notions refer to generation of illegal flows of money in digital shadow economy. Nevertheless, the definition of digital shadow economy should not be interepreted only as illegal flows of money. Illegal consumer activities (or deviant behaviour) in e-space (e.g. downloading of particular products/services from the Internet without any payment or with a partial payment only) should also be considered as a part of digital shadow economy because such behaviour deprives legally operating agents (natural or juridical persons) from a share of their potential revenues, which could be legally earned and declared. Scientific literature often links illegal or deviant consumer behaviour online with the term "e-fraud". E-fraud may

refer to consumption of illegal copies of particular products or services (*Ho & Weinberg, 2011; Taylor, 2012; Arli et al., 2015*), violation of the terms of a contract establish online (Hjort & Lantz, 2012) or breach of trust between the contract parties (*Amasiatu & Shah, 2014*). With referenfce to *Amasiatu and Shah (2014),* trust is breached when one contract party refuses to compy with the contract terms. On one hand, a consumer is a party that may act unfairly and fail to compy with contract terms in order to get benefits from unfairness. Such unfair consumer behaviour is called a first party *fraud* (*Amasiatu & Shah, 2014*). *Vlachos et al.* (*2011*) note that the largest number of e-fraud cases are related to fraudulent transactions, when consumers are looking for opportunities to purchase goods (e.g. luxurious clothes, computers, software, music records, entertainment devices, etc.) at a discount or obtain them for free.

It should not be overlooked that interpretations of digital shadow economy found in the scientific literature go beyond the concepts of illegal trade or service provision online. The notion of digital shadow economy also covers the agents who participate in shadow activities in e-space. Illegal activities of e-consumers are often aligned with such terms as "e-piracy" and "e-crime". E-piracy (in other words, digital piracy) is described as an illegal copying/downloading of an object, which is protected by copyrights (*Castro et al. 2009; Cronan, Al-Rafee 2008; Camarero et al. 2014*). Other authors (*Jacobs et al. 2001; Ho, Weinberg, 2011*) use such terms as forgery, product thefts or piracy. The key aim of digital piracy is benefit gained from genuine, authentic brands/trademarks. In legal terms, it is violation of intellectual property rights (*Camarero et al. 2014*), when a legal owner of the rights is deprived from potential cash flows and potential revenue. With reference to *Ho and Weinberg* (*2011*) currently prevailing types of digital piracy cover downloading of films, music records or other digital products as well as acquisition of paper or digital pirated goods.

Leaning on the results of the literature analysis, the authors of this article support the opinion that digital shadow economy is related to illegal activities in e-space that generate illegal flows of money for illegally operating traders/service providers (supplier's attitude) and deprive legally operating entrepreneurs from the revenues that could be officially earned and reported (consumer's attitude). If digital shadow economy was treated as a system, it would combine the elements of classical and digital crimes (*Holz et al., 2012*).

With reference to the concepts and interpretations of digital shadow economy found in the scientific literature, the following definitions of digital shadow economy can be proposed:

- Digital shadow economy is a part of shadow economy, when illegal profit-driven online trade or service provision is performed. The activities of digital shadow economy tend to be of repeated or non-repeated nature, with or without changing IP addresses/computer networks;
- Digital shadow economy refers to global networks emerging in closed Internet forums and promoting chains of e-crimes, including bank attacks, payment card crimes, identity steals and other Internet intrusions;
- (Un)interrupted, financial-gain-driven provision of particular commodities or services in the remote space, performed without activity registration and causing damage to an officially registered subject, who provides similar commodities or services;
- Digital shadow economy is an illegal operation in the Internet space, which generates illegal money flows for commodity/service providers or purchasers, and deprives legal traders/service providers from the revenue that could be officially accounted, calculated and declared;
- Digital shadow economy refers to the trade in e-space, performed without paying any taxes to the state budget, excluding purely criminal activities such as drug trafficking, prostitution, etc.).

In general sense, digital shadow economy refers to unregistered and/or illegal profit-driven activities (usually trade or service provision) in e-space. Nevertheless, it is important to note that such illegal profit-driven offences as cybercrimes, digital piracy or e-fraud, should be separated from the definition of digital shadow economy and left for consideration of criminal law since these offences refer to crime rather than to illegal economic activities. Minding different nature of crime and shadow economy, the authors of this article are convinced that **criminal activities and illegal economic activities should be distinguished.**

The features of digital shadow economy

As previously mentioned, rapid technological advancement as well as fast changes in IT communications burden perception and detection of the cases of digital shadow economy. Due to this reason, scientific literature is rich in explanations of the nature, general aims and forms of this phenomenon. The literature also introduces different attitudes towards unregistered profit-driven online activities (*Herley, Florencio 2010*) and illegal revenues generated as a result of online trade or service provision (*Zorz, 2015*).

The analysis of the scientific literature has enabled to identify and systematise the main features of digital shadow economy (see Table 1).

Table 1

Theoretical features of digital shadow economy

Feature	Description
Subjects	Traders, service providers, consumers (buyers), natural and juridical persons, MNEs, business networks
Forms	E-business, e-commerce, online service provision, cybercrimes, digital piracy, e-fraud
Aim	Financial aims - profits, revenues, cash flows
Registration	Unregistered, illegal activities
Repeatedness	Repeated, non-repeated
Equipment	Sophisticated, advanced technologies
Abilities of participants	Advanced abilities, high level of coordination
Losses	Deprivation of officially registered subjects from potential revenues/profits, tax losses for state budgets
Nature/character	Deceptive, non-deceptive

First of all, traders and services providers (natural or juridical persons) are treated as the most active participants of digital shadow economy *(Zorz, 2015; Moore et al. 2009; Vlachos et al. 2011),* although *Herley and Florencio (2010)* note that the nature of this phenomenon may exceed the capacities of a single agent group (e.g. an enterprise, an institution, a community, etc.), and suggest to consider the probability that the subjects of digital shadow economy may also include MNEs or even large business networks.

The assertions that the activities of digital shadow economy are profit-driven disclose the key aim of this phenomenon – financial benefit *(Holz et al. 2012; Herley, Florencio 2010; Zorz, 2015; Moore et al. 2009; Delina, Tkač 2015)*. Employment of sophisticated equipment, technical expertise as well as engagement of high-level coordination between the contract parties are also attributable to the main features of digital shadow *economy (Dittrich 2009; Provos et al. 2009; Vlachos, et al. 2011)*. The losses generated by digital shadow economy consist of the damages incurred by officially registered subjects (deprivation of these subjects from potential benefits – profits or revenue) and losses to state budgets *(Vlachos, et al. 2011; Holz et al. 2012; Dobson et al. 2015)*. Finally,

although some forms of digital shadow economy (e.g. e-fraud, cybercrime) may be hard to detect due to their fraudulent or criminal nature, in particular cases (e.g. in the case of e-fraud) consumers must be aware that getting involved in shadow transactions (e.g. digital piracy) they also commit a crime *(Ho, Weinberg 2011)*. This leads to the conclusion that subjects' participation in digital shadow economy can have a deceptive or non-deceptive (voluntary) background.

The analysis of the scientific literature has also disclosed that acting in e-space basically means employment and usage of a remote space (e.g. online shops, online service provision websites, social networks, etc.) *(Hafezieh et al. 2011; Levi, Williams 2013; Amasiatu, Shah 2014)*. What is more, e-advertisment and e-auctions *(Vlachos, et al. 2011; Dion 2011; Smith, 2015),* e-games and e-gambling sites *(Vlachos, et al. 2011; Smith, 2015),* online broadcasts *(Dion 2011; Dobson et al. 2015)*, bitcoins and other cryptocurrencies *(Haines, Johnstone 1999; Holz et al. 2012; Zorz, 2015)* may be considered as the channels of digital shadow economy, minding the flows of unreported revenues generated via them. According to *Smith (2015),* the channels of digital shadow economy may cover the Internet access, data on hard discs, remote financial resources, intellectual capital, etc. In other words, the channels of digital shadow economy are the remote platforms that ensure anonymity of users, this way allowing both a customer and a supplier/service provider to hide their geographical location, which, in turn, ensures that their identities and transactions will not be detected *(Zorz, 2015)*.

The forms of digital shadow economy in black digital markets

Thomas and Martin (2006), who provided a deeper insight in the problems of digital shadow economy, analysed such forms of this phenomenon as trade in stolen credit card credentials via online chats. This form of digital shadow economy was later recognised by other scientists *(Herley & Florencio, 2010; Yip, et al. 2012)*. Over the last few years, the interest in the forms of digital shadow economy has been gradually increasing. The forms of digital shadow economy are more and more often selected as an object of scientific research.

Mello (2013) introduces five forms of cybercrimes:

- data security violations – stolen credentials employed for wide scopes of industrial frauds via social networks, such as Twitter, Linkedln, LivingSocial's, etc.;
- malware – malicious software that is employed in order to get an access to various authorisations; to prevent malware attacks, anti-malware is developed to protect computer systems from viruses and detect illegal users;
- telephone threats – smart phones and mobile malware applications;
- industrialisation – covers online and mobile interactions "a machine-to-a machine", i.e. a user's device (a computer or a mobile phone) is linked to a business server, and such electronic connection generates automatic authorization; this way, an agent has an access to a potential victim's accounts, and the process of money transfer can be started;
- distributed denial of service attacks – interruptions of regular functioning of a website, leading to a dramatical incease in a website manager's operational costs and lost trust from consumers' position.

The study of the climate of cybercrime in Greece, conducted by *Vlachos et al. (2011),* disclosed such forms of cybercrime as financial frauds (i.e. frauds driven by financial gain starting from simple fraudulent attacks and ending with money "pumping" schemes), children's issues (i.e. any cases of children's abuse from pedophilia to pornography), spams (i.e. unwanted huge quantities of e-mails, which negatively affect the efficiency of the Internet users and are linked to promotion of fraudulent products/services), violations of personal data and privacy (i.e. all the incidents related to privacy issues and abuse of the private data that was transmitted or received via electronic communications),

technologically advanced activities (i.e. network usage for the spread of malware and attacts), e-games (i.e. administration of the accounts to which illegaly earned virtual money flows), and technical issues (i.e. deliberately caused technical problems that are directly linked to the protection of a computer or computer system).

Yip, et al. (2012) provided a detailed analysis of online social networks, known as online forums *(Holt & Lampke, 2010; Poulsen, 2011)*. The authors *(Yip, et al., 2012)* found that online social networks were previously used as a black online market for the trade in stolen credentials. It was also established that the current usage of online social networks has slightly changed by its nature: at present it covers sharing of criminal values and trade in goods and services that promote criminal co-operation *(Thomas & Martin, 2006; Holt & Lampke, 2010; Yip, et el., 2012),* money laundering, bank data steals, identity steals, exchange of virtual currency, decoding systems, etc. *(Holt & Lampke, 2010)*. In their study on digital underground economy (in particular, the study on the trade in stolen digital credentials), *Holz et al. (2012)* researched keylogger-based steals of credentials via dropzones (publicly writable directories on a server in the Internet) and anonymous collection points of illicitly collected data. With reference to the authors, keylogger-based stealing is a newly emerging form of digital underground economy. What is more, the results of the study revealed that this technique can be applied in e-banking to extract information from protected databases (a computer memory).

The above-introduced forms of digital shadow economy are initiated by a supplier, whose basic aim is to generate illegal money flows. Nevertheless, digital shadow economy is also linked to fraudulent consumer activities, which deprive legal service providers from the revenues that could be officially earned, reported and declared. For this reason, it is purposeful to have an insight into the forms of digital shadow economy initiated by a consumer.

Digital piracy is one of the general forms of e-fraud indicated in the scientific literature. With reference to *Ho and Weinberg (2011),* digital piracy is a type of piracy that emerges from the need to copy, produce or illegally consume genuine products. In other words, digital piracy refers to buying, copying, downloading and/or sharing of illegal CDs or software *(Arli et al., 2015)*. In fact, the volumes of digital piracy all over world stun legal producers of such easily copied digital products as music *(International Federation of Phonographic Industry, 2009),* films *(Castro, Bennett, & Andes, 2009),* software *(Business Software Alliance, 2009),* etc. That is why general cases of digital piracy are based on the presumption that individuals involved in it make a profit from the abuse of legally registered brands/trademarks *(Ho & Weinberg, 2011)*.

Amasiatu and Shah (2014) focused on the research of the forms of fraudulent (deviant) consumer behaviour online. Their study enabled to indentify the following forms of e-fraud:

1. Deshopping – buying a product online with the intentions to return it by the defined term and take the money back;
2. Return of payment – fraudulent or illegal claim to return the money with the intentions to gain particular financial benefits;
3. Bust out - taking off a credit with no intentions to pay in back;
4. Submission of false information – applicants submit falsified information about themselves because otherwise they could not get an access to particular services (for example, to a credit).

Scientific literature analysis has revealed that deshopping is the most common form of consumers' deviant behavior online (*Hjort & Lantz, 2012; Amasiatu & Shah, 2014*). It is often considered to be the result of unreasonably liberal return policies in e-commerce. As it was noted by *Hjort and Lantz (2012),* deshopping is reinforced by offering a free return of a product; it is driven by lower consumer general expenditure and low delivery costs.

The methods of payment return, analysed in the scientific literature, are based on the understanding that a consumer should not be willing to return the goods which he/she orders, although in practice consumers are often inclined to do so or they are inclined to submit a claim that not all goods on order were delivered even in case they were *(Greek, 2010; Amasiatu & Shah, 2014)*. With reference to the report of Cybersource Corporation *(2012),* the affair of payment return emerges when a consumer makes a purchase with his/her card, and later impugns the purchase. According to *Amasiatu and Shah (2014),* a payment return fraud is beneficial in its general sense because particular legal obligations ensure protection of the rights of consumers when they are shopping online; for instance, consumers are ensured the protection from card payment frauds, when a supplier assumes full responsibility for any possible losses incurred before a purchase is delivered to a consumer. In accordance with *Fair Isaak Corporation (2008*), the cases of e-frauds often emerge in financial institutions since they possess a wide variety of credit issuance equipment. *Amasiatu and Shah (2014)* note that, in exceptional cases, e-frauds are based on masking of real consumer intentions or on the principle of a "slight lie", which may help to get a bigger credit before avoidance of regular payments or complete disapperance. According to *CIFAS (2012*), submission of falsified infomation is widely-spread while making mail orders, when individuals hide their real addresses, which, in turn, has a negative impact on the credit information. Submission of falsified data is also popular in the field of insurance, where consumers artificially "inflate" their capacities to match the insurance requirements. Benefit hunters lie about their income to gain from insurance systems *(Amasiatu & Shah, 2014)*.

The analysis of the scientific literature has enabled to systematise the forms of digital shadow economy. The data in Figure 1 show that digital shadow economy can be initiated by either a supplier/service provider or a consumer. Supplier-initiated forms of digital shadow economy cover financial crimes, children's issues, spam, violations of private data and privacy, e-games, technologically advances activities, technical issues and social forums. All these forms of digital shadow economy commonly emerge as steals of credentials, money laudering, exchange of virtual currencies, illegal transactions in virtual currencies, and codification of systems with malicious and deceptive software. Consumer-initiated forms of digital shadow economy cover digital piracy, deshopping, returns of payment, bust out, taking credits without any intentions to pay them back, and submission of falsified data. Consumers get involved in digital shadow economy in order to reduce their general consumer expenditure and/or have an access to credits, funds, insurance and social benefits.

According to *Zorz (2015),* different forms of digital shadow economy emerge in digital black markets depending on a type of target products or services. Considering an object of an activity (i.e. minding whether a product or service is digital or non-digital), the author *(Zorz, 2015)* distinguishes two basic types of digital black market: physical (or material) black market (i.e. online trade in material products, such as drugs, guns, etc.) and fraudulent data market (i.e. performance of digital activities, such as codification, data violations, system iterruptions, etc.). The author *(Zorz, 2015)* notes that the first market - physical black market – functions via online platforms (e.g. TOR network), which allow anonymous customers and suppliers hide their locations and be sure that their identities cannot be tracked. The second market – fraudulent data market – functions via traditional *http* websites, which can be accessed from any computer by employing a browser; these websites are created to trade in stolen credentials (e.g. credit card credentials, users' names and passwords, etc.), which have become the most prevalent type of the stolen data on sale. Digital shadow activities are mostly performed via such channels as online chat sites, formus, social network and dropzones.

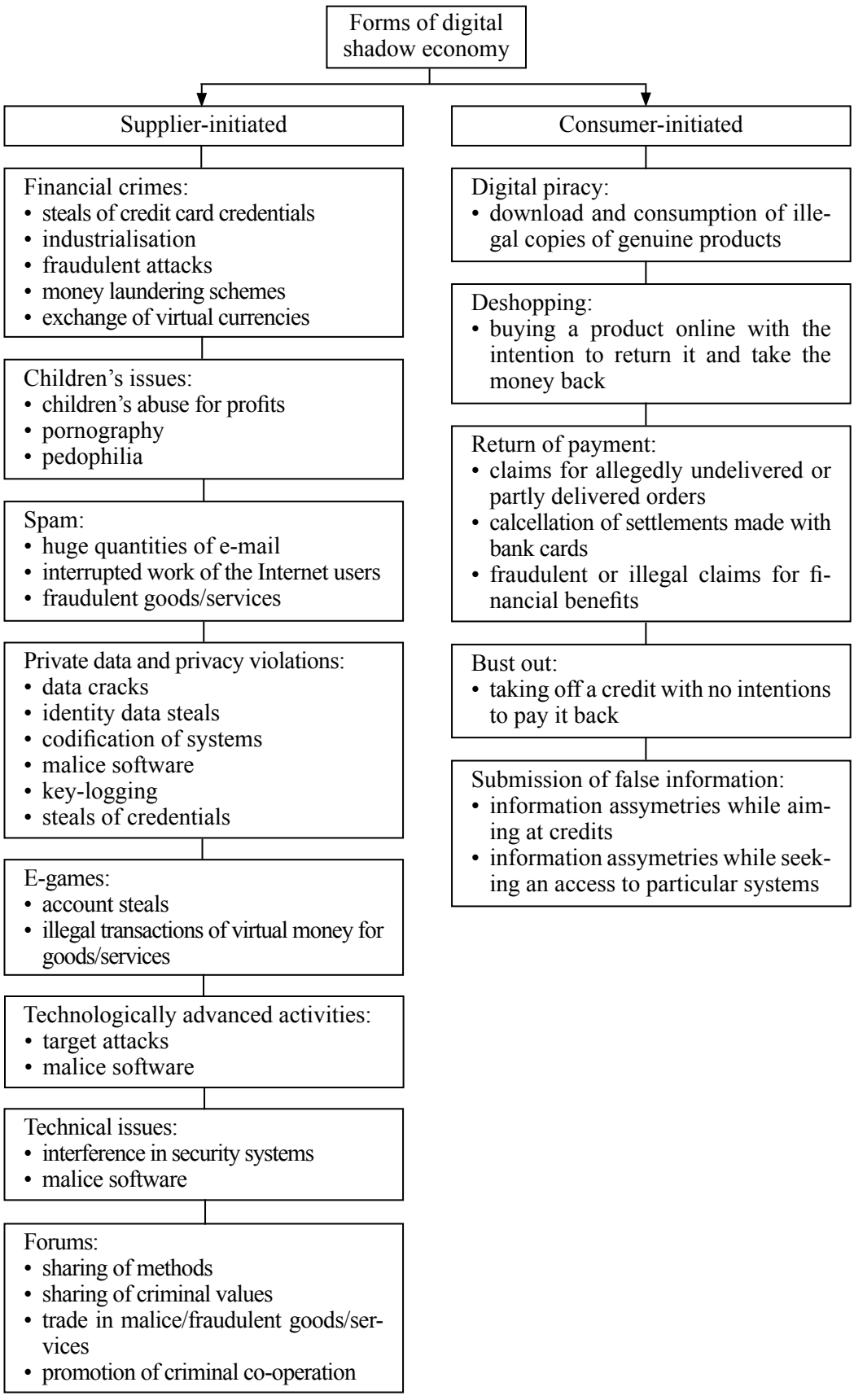

Fig. 1. *Classification of the forms of digital shadow economy (Gaspareniene, Remeikiene, 2015, p. 409)*

The newest results of the research on the issues of digital shadow economy

Scientific literature is comparatively rich in the methodologies of shadow economy estimation that are employed for clarification of the scopes of this phenomenon in both Europe and all over the world. Different methodologies are based on subjective evaluations (direct methods), inclusion of particular indicators (indirect methods) or variable models (for instance, MIMIC model). Direct methods provide an opportunity to obtain the data from natural and/or juridical persons on plausible scopes of shadow economy. Indirect methods lean on a comparative analysis of various statistical data and reveal the discrepancies that are explained by employing the relevant monetary, economic and social factors. Finally, the models with different variables can reveal the impact of production, labour, money markets and other relevant indicators on the overall scopes of shadow economy. The results of the newest research *(Gaspareniene, Remeikiene, 2016)* have shown that direct methods of shadow economy estimation mainly include such participants as households and business subjects, and are based on the analysis of general economic variables; indirect methods lean on the variables of general economics, monetary policy, money turnover, electric energy consumption, and labour market; the models include the indicators of general economics, taxes, and legal, social, labor and monetary environment. The scopes of unrecorded economy are reflected in the estimations of GDP and GNP. Nevertheless, the indicators of digital shadow economy are not included the methods of traditional shadow economy estimations, which not only burdens grasping the true volumes of this phenomenon, but also impedes the development of digital shadow economy detection and prevention measures. In addition, it should be noted that estimations of shadow economy are usually funded by public institutions because the costs of the estimation process are relatively high, especially in the cases when direct methods are employed. Another way to estimate the scopes of shadow economy is to find the difference between total reported revenues and the revenues detected during a selective audit. In this case, tax audit, which enables to estimate the scopes of unreported revenues, is extremely effective. Hence, this method could be employed for estimations of the share of digital shadow economy in the total scope of shadow economy in a particular sector or country. However, it should not be overlooked that selection of the subjects for audit is typically based only on tax delarations submitted to state tax inspectorates by tax payers. This way, the sample of the research is not random and can not accurately reflect the real situation. Furthermore, the estimations based only on the data of tax audit, reflect the share of shadow economy revenue that was disclosed by the authorised officials, while the rest part of shadow economy revenue remains undisclosed. On balance, a significant disadvantage of both direct and indirect methods of shadow economy estimation is that they fail to reflect all types of shadow activities (including the ones performed in e-space). What is more, these methods represent only annual data, and this practice impedes estimation of the real scopes of shadow economy in the long run. Some widely-spread methods like surveys of tax auditors or comprehensive analysis of employment data (comparison of employment data obtained from different sources of information – administrative reports, media, etc.) can be helpful for identification of the in-depth causes of shadow economy, but they can hardly reveal the numerical scopes of this phenonenon. Macro models (e.g. money demand model, MIMIC, DGE, etc.) are not recommended for statisticians since these models do not provide any opportunities to detect the causes of unrecorded economy, and the presumptions of the models are not firmly substantiated. Thus, the probability to double estimations of shadow economy is relatively high.

Summarising, it can be stated that the theory of shadow economy cannot provide the methodologies of shadow economy estimation which would include the indicators that reflect the features of digital shadow economy. What is more, no generally accepted definition of the phenomenon of digital shadow economy has been developed. The results of this research (that have not been publically announced thus far) have enabled to complement the theory of traditional shadow economy:

1. The definition of digital shadow economy has been developed. The authors propose that digital shadow economy should be referred to as illegal online activities, such as digital services and/or trade in products/services online, performing which economic agents violate applicable regulatory norms while aiming at illegal mutual material benefits.

2. The distinctive features of digital shadow economy have been identified: digital shadow economy is defined by promptness of transactions, hardly identified geographical location, communication exceptionally in e-space/the Internet, and absence of physical contact betwen the agents. The other features that can be attributed not only to digital shadow economy, but also to traditional shadow economy include anonymity, settlement exceptionally in electronic tenders, and high competence of the agents in the fields of IT and the English language.

3. It has been found that consumers clearly perceive that digital shadow economy is not the same as cybercrime, and treat it as illegal acting in e-space that allows to generate illegal money flows for traders/service providers or consumers and deprives legal traders/service providers from the revenues that could be oficially earned, accounted and declared. Digital shadow economy causes huge losses of tax revenue in the budgets of states.

4. Consumers' motives to buy products/services in digital shadow markets have been identified: it has been found that consumers are driven by lower prices, unfavourable economic situation in the country, favourable economic opportunities, advantages of the IT age, absence of a desirable product/service in domestic markets, and time cost saving. Legal factors, such as low probability of detection of the fact that a person has acquired a product/service from a formally non-existant or illegally operating supplier without paying VAT to the state budget, weak legal framework of a country (especially concerning regulation of e-commerce), weakly regulated IT industry, and lack of professional officials with the competence to detect cybercrimes, have not been recognized as critical ones. Hence, acquisition of products/services from illegally operating suppliers is mostly based on such determinants as lower prices and advantages of the IT age (access to the Internet, relatively low prices of computers, smart phones, mobile applications, etc.).

5. It has been established that the issues of digital shadow economy as well as the difficulties to estimate the real scopes of this phenomenon burden the problems of poor tax collection not only in Lithuania, but also in other countries of Eastern Europe. Unfortunately, no clear strategies to solve the problems of this type have been developed yet. The authors of this article make this conclusion following the results of the expert survey (with participation of the officials from the Department of Control, Lithuanian State Tax Inspectorate, directly responsible for inspection of economic agents): more than a half of the experts (52.6 percent) declared that they had never inspected illegal agents operating in e-space or had never detected operation of such agents during the term of 2015; 53.9 percent of the experts indicated that they had never detected any cases when agents ran a traditional business, but at the same time were involved in unregistered e-business. Hence, the results lead to the conclusion that the Department of Control under Lithuanian State Tax Inspectorate either does not possess sufficient financial and human resources for the detection of the cases of digital shadow economy, or does not follow any effective strategies purposefully developed for detection of such cases. It is obvious that timely detection of the cases of digital shadow economy calls for additional staff competences and skills in the fields of IT and law; extra funds are necessary for acquisition of the advanced software that could help to track illegal acitivities in e-space.

6. With reference to the results of the expert survey (as already mentioned at point 5), it has been found that 2 percent of the cases of digital shadow economy were detected while dealing with the cases of traditional shadow economy over 2015. The main areas of manifestation of digital shadow economy covered wholesale and retail, and repair of motor vehicles (with average ranks equal to 3.55). The general industries were tiered to some smaller groups of products/services: in the industry of construction, the cases of digital shadow

economy mostly appear in the form of rent of real estate; in the industry of sales – in the form of trade in clothes, automobiles and electronics; in the industry of services – in the form of provision of educational and catering services. Variation of the plausible scopes of digital shadow economy in a relatively wide interval from 15 thousand EUR to 1.5 million EUR proposes that the estimations are not accurate.

7. It has been found that e-shops are the objects in e-space most frequently inspected by assigned officials, while websites and social networks hardly fall under inspection, which makes them a favourable enviroment for digital shadow transactions.

8. Thus far, the scopes of digital shadow economy have been estimated neither in Europe, nor in any other continents. Officials from the Department of Control under Lithuanian State Tax Inspectorate attribute the random cases of digital shadow economy to the general statistics of traditional shadow economy. Due to this reason, the real scopes and tendencies of digital shadow economy remain undiscovered, which, in turn, determines the neccessity to complement the methodologies of shadow economy estimation with the indicators of digital shadow economy. Employment of comprehensive methodologies would allow to have a deeper insight in the nature of the phenomenon of digital shadow economy, and at the same time could contribute to the development of efficient detection mechanisms.

Conclusions

The issue of digital shadow economy is indeed new and, considering it as a branch of traditional shadow economy, very young. The research, conducted on the basis of the national scientific project "Digital Shadow Economy", has enabled to collect the original and valuable data on the issues of digital shadow economy and achieve the following results:

1. The definition of digital shadow economy has been developed: digital shadow economy should be referred to as illegal online activities, such as digital services and/or trade in products/services online, performing which economic agents violate applicable regulatory norms while aiming at illegal mutual material benefits.

2. The distinctive features of digital shadow economy have been identified: digital shadow economy is defined by promptness of transactions, hardly identified geographical location, communication exceptionally in e-space/the Internet, and absence of physical contact betwen the agents. The other features that can be attributed not only to digital shadow economy, but also to traditional shadow economy include anonymity, settlement exceptionally in electronic tenders, and high competence of the agents in the fields of IT and the English language.

3. The main channels of digital shadow economy have been identified. They cover e-shops with electronic tenders of settlement, poker/casino/bingo sites, e-game sites, social networks, settlements in bitcoins and other cryptocurrencies, and advertisement portals.

4. The position of consumers' towards the phenomenon of digital shadow economy has been found out: consumers clearly perceive that digital shadow economy is not the same as cybercrime, and are inclined to treat it as *illegal acting in e-space that allows to generate illegal money flows for traders/service providers or consumers and deprives legal traders/service providers from the revenues that could be oficially earned, accounted and declared*. Consumers are of the opinion that digital shadow economy causes huge losses of tax revenue in the budgets of states.

5. Consumers' motives to buy products/services in digital shadow markets have been identified: it has been found that consumers are driven by lower prices, unfavourable economic situation in the country, favourable economic opportunities, advantages of the IT age, absence of a desirable product/service in domestic markets, and time cost saving. Legal factors, such as low probability of detection of the fact that a person has acquired a product/service from a formally non-existant or illegally operating supplier without

paying VAT to the state budget, weak legal framework of a country (especially concerning regulation of e-commerce), weakly regulated IT industry, and lack of professional officials with the competence to detect cybercrimes, have not been recognized as critical ones. Hence, acquisition of products/services from illegally operating suppliers is primarily based on such determinants as lower prices and advantages of the IT age (access to the Internet, relatively low prices of computers, smart phones, mobile applications, etc.).

6. The channels to acquire products/services from digital shadow markets have been identified: they cover e-shops, social networks and internet sites; the above-mentioned channels are commonly employed for acquisition of clothes and footwear, trips, entertainment, perfume and cosmetics.

7. It has been established that the majority of consumers are not inlined to verify the status of a supplier/service provider in e-space; they are also not inclined to ask for bills or other types of documents for confirmation of a purchase. The latter factors serves as an extra motive for suppliers/service providers not to register their activities.

ЛИТЕРАТУРА/REFERENCES

Allabouche K., Diouri O., Gaga A. and *El Amrani El Idrissi N.* (2016). Mobile phones' social impacts on sustainable human development: case studies, Morocco and Italy // *Entrepreneurship and Sustainability Issues*, no. 4(1), pp. 64–73.

Amasiatu C.V. and *Shah M.H.* (2014). First party fraud: A review of the forms and motives of fraudulent consumer behaviours in e-tailing // *International Journal of Retail & Distribution Management*, no. 42(9), pp. 805–17.

Arli D., Tjiptono F. and *Porto R.* (2015). The impact of moral equity, relativism and attitude on individuals' digital piracy behaviour in a developing country // *Marketing Intelligence & Planning*, no. 33(3), pp. 348–365.

Astrauskaitė I. and *Paškevičius A.* (2016). Assessing the optimal taxation of the capital income: a case of corporate bond market // *Journal of Security and Sustainability Issues*, no. 5(4), pp. 519–532.

Belás J., Korauš M., Kombo F. and *Korauš A.* (2016). Electronic banking security and customer satisfaction and in commercial banks //*Journal of Security and Sustainability Issues*, no. 5(3), pp. 411–422.

Bossler A.M. and *Holt T.J.* (2012). Patrol officers' perceived role in responding to cybercrime, *Policing An International Journal of Police Strategies & Management*, no. 35(1), pp. 165–181.

Business Software Alliance (2009). *Software piracy on the internet: A threat to your security* (A report) (http://global.bsa.org/internetreport2009/2009internetpiracyreport.pdf).

Camarero C., Anton C. and *Rodriguez J.* (2014). Technological and ethical antecedents of e-book piracy and price acceptance: Evidence from the Spanish case // *The Electronic Library*, no. 32(4), pp. 542–566.

Castro D., Bennett R. and *Andes S.* (2009). Steal these policies: Strategies for reducing digital piracy. *The Information Technology & Innovation Foundation, 12* (www.itif.org/files/2009-12-15.DigitalPiracy.pdf).

CIFAS (2012). *Fraudscape: depicting the UK's fraud landscape* (Research and Reports) (https://www.cifas.org.uk/secure/contentPORT/uploads/documents/Cifas%20Reports/External-Fraudscape_2013_Cifas.pdf).

Cronan T.P. and *Al-Rafee S.* (2008). Factors that influence the intention to pirate software and media // *Journal of Business Ethics*, no. 78(4), pp. 527–545.

Cybersource Corporation (2012). *13th annual online fraud report* (www.jpmorgan. com/cm/BlobServer/13th_Annual_2012_Online_Fraud_Report.pdf?blobkey¼id&blobwhere¼1320571432216&blobheader¼application/pdf&blobheadername1¼Cache-Control&blobheadervalue1¼private&blobcol¼urldata&blobtable¼MungoBlobs).

Delina R. and *Tkač M.* (2015). Role of e-business in the perception of ICT impact on revenue growth // *Journal of Business Economics and Management*, no. 16(6), pp. 1140–1153.

Dittrich D. (2009). Malware to crimeware: how far have they gone, and how do we catch up? // *Login*, no. 34(4), pp. 35–44.

Dion M. (2011). Corruption, fraud and cybercrime as dehumanizing phenomena // *International Journal of Social Economics*, no. 38(5), pp. 466–476.

Dobrovič J., Korauš A. and *Dančišinová L.* (2016). Sustainable economic development of Slovakia: factors determining optimal tax collection // *Journal of Security and Sustainability Issues*, no. 5(4), pp. 533–544.

Dobson S., Sukumar A. and *Tipi L.* (2015). Dark Matters: The Institutional Entrepreneurship of Illicit and Illegal Cyberspace / In: *Mcelwee G.* and *Smith R. (eds.)* // *Exploring Criminal and Illegal Enterprise: New Perspectives on Research, Policy & Practice (Contemporary Issues in Entrepreneurship Research)*, no. 5, pp. 179–201.

Europol (2011). *Cybercrime as a business: The digital underground economy* (Press Releases) (https://www.europol.europa.eu/content/press/cybercrime-business-digital-underground-economy-517).

Fair Isaak Corporation (2008). *Reducing bad debt levels by addressing first party fraud and credit abuse* (white paper) (http://brblog.typepad.com/files/first_party_fraud_2486wp_en.pdf).

Ferreira N.C.M.Q., Ferreira F.A.F., Marques C.S.E., Perez-Bustamante Ilander G.O. and *Cipi A.* (2015). Challenges in the implementation of public electronic services: Leassons from a regional-based study, *Journal of Business Economics and Management*, no. 16(5), pp. 962–979 (http://dx.doi.org/10.3846/16111699.2014.920718).

Fuschi D. and *Tvaronavičienė M.* (2014). Sustainable development, Big Data and supervisory control: service quality in banking sector // *Journal of Security and Sustainability*, issue 3(3), pp. 5–14.

Gaspareniene L. and *Remeikiene R.* (2015). Digital Shadow Economy: a Critical Review of the Literature // *Mediterranean Journal of Social Sciences*, vol. 6, no. 6, S5: 402–409.

Gasparėnienė L. and *Remeikienė R.* (2016). Shadow economy estimation methods: Digital shadow economy assessment aspect // *9th International Scientific Conference "Business and Management 2016"* Vilnius, Lithuania (http://dx.doi.org/10.3846/bm.2016.34).

Government Accounting Office (2007). *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats* [online] [cited 10 October 2015]. United States Government Accountability Office Report to Congressional Requesters (www.gao.gov/new.items/d07705.pdf).

Greek D. (2010). *Who is responsible when goods go missing in transit?* (www.computeractive.co.uk/ca/consumerrights/1931458/missing-transit).

Hafezieh N., Akhavan P. and *Eshraghian F.* (2011). Exploration of process and competitive factors of entrepreneurship in digital space: a multiple case study in Iran, Education, Business and Society // *Contemporary Middle Eastern Issues*, no. 4(4), pp. 267–279.

Haines J. and *Johnstone P.* (1999). Global cybercrime: new toys for the money launderers // *Journal of Money Laundering Control*, no. 2(4), pp. 317–325.

Herley C. and *Florencio D.* (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy // *Economics of Information Security and Privacy, 10* (http://link.springer.com/chapter/10.1007%2F978-1-4419-6967-5_3#page-1).

Hjort K. and *Lantz B.* (2012). (R)e-tail borrowing of party dresses: An experimental study // *International Journal of Retail & Distribution Management*, no. 40(12), pp. 997–1012.

Ho J. and *Weinberg C.B.* (2011). Segmenting consumers of pirated movies // *Journal of Consumer Marketing*, no. 28(4), pp. 252–260.

Holt T.J. and *Lampke E.* (2010). Exploring stolen data markets online: Products and market forces // *Criminal Justice Studies*, no. 23(1), pp. 33–50.

Holz T., Engelberth M. and *Freiling F.* (2012). Learning more about the underground economy: A case-study of keyloggers and dropzones // *ESORICS Proceedings*, no. 9, pp. 1–18.

Jacobs L., Samli A.C. and *Jedlik T.* (2001). The nightmare of international product piracy // *Industrial Marketing Management*, no. 30(6), pp. 499–509.

International Federation of the Phonographic Industry (2009). *New business models for a changing environment* (Digital music report) (www.ifpi.org/content/ section_ resources/ dmr2009.html).

Kalyugina S., Strielkowski W., Ushvitsky L. and *Astachova E.* (2015). Sustainable and secure development: facet of personal financial issues // *Journal of Security and Sustainability Issues*, no. 5(2), pp. 297–304 (http://dx.doi.org/10.9770/jssi.2015.5.2(14)).

Lavrinenko O., Ohotina A., Tumalavičius V. and *Pidlisna O.V.* (2016). Assessment of partnership development in cross-border regions' innovation systems (Latvia-Lithuania-Belarus) // *Journal of Security and Sustainability Issues*, no. 6(1), pp. 155–166 (http://dx.doi.org/10.9770/jssi.2016.6.1(12)).

Levi M. and *Williams M.L.* (2013). Multi-agency partnerships in cybercrime reduction // *Information Management & Computer Security*, no. 21(5), pp. 420-443

Mello J.P. (2013). *Cybercrime fueled by mature digital underground* (Identity & Access) (http://www.csoonline.com/article/2133649/identity-access/cybercrime-fueled-by-mature-digital-underground.html).

Moore T., Clayton R. and *Anderson R.* (2009). The economics of online crime // *Journal of Economic Perspectives*, no. 23(3), pp. 3–20.

Pauceanu A.M. (2016). Innovation and entrepreneurship in Sultanate of Oman – an empirical study // *Entrepreneurship and Sustainability Issues*, no. 4(1), pp. 83–99 (http://dx.doi.org/10.9770/jesi.2016.4.1(8)).

Poulsen K. (2011). *Kingpin: How one hacker took over the billion-dollar cybercrime underground*. New York: Crown Publishing.

Provos N., Rajab M.A. and *Mavrommatis P.* (2009). Cybercrime 2.0: when the cloud turns dark // *Commun ACM*, no. 52(4), pp. 42–7.

R*ezk M.A., Ibrahim H.H., Radwan A., Sakr M.M., Tvaronavičienė M.* and *Piccinetti L.* (2016). Innovation magnitude of manufacturing industry in Egypt with particular focus on SMEs // *Entrepreneurship and Sustainability Issues*, no. 3(4), pp. 306–318 (http://dx.doi.org/10.9770/jesi.2016.3.4(1)).

S*amašonok K., Išoraitė M.* and *Leškienė-Hussey B.* (2016). The internet entrepreneurship: opportunities and problems // *Entrepreneurship and Sustainability Issues*, no. 3(4), pp. 329–349.

Sirkeci I. and *Magnusdottir L.B.* (2011). Understanding illegal music downloading in the UK: A multi attribute model // *Journal of Research in Interactive Marketing*, no. 5(1), pp. 90–110.

Smith G.S. (2015). Management models for international cybercrime // *Journal of Financial Crime*, no. 22(1), pp. 104–125.

Taylor S.A. (2012). Evaluating digital piracy intentions on behaviors // *Journal of Services Marketing*, no. 26(7), pp. 472–483.

Thomas R. and *Martin J.* (2006). The underground economy: Priceless // *The USENIX Magazine*, no. 31(6), pp. 7–16.

Teivāns-Treinovskis J. and *Amosova J.* (2016). Some aspects of criminal environment impact on sustainable entrepreneurship activities // *Entrepreneurship and Sustainability Issues*, no. 4(1), pp. 17–27.

Tvaronavičienė M. (2016). Start-ups across the EU: if particular tendencies could be trace // *Entrepreneurship and Sustainability Issues*, no. 3(3), pp. 290–298.

Vida I., Koklic M.K., Kukar-Kinney M. and *Penz E.* (2012). Predicting consumer digital piracy behavior: The role of rationalization and perceived consequences // *Journal of Research in Interactive* Marketing, no. 6(4), pp. 298–313.

Vlachos V., Minou M., Assimakopouos V. and *Toska A.* (2011). The landscape of cybercrime in Greece // *Information Management & Computer Security*, no. 19(2), pp. 113–123.

Williams P., Nicholas D. and *Rowlands I.* (2010). The attitudes and behaviours of illegal downloaders // *Aslib Proceedings*, no. 62(3), pp. 283–301.

Yip M., Shadbolt N., Tiropanis N. and *Webber C.* (2012). The digital underground economy: A social network approach to understanding cybercrime. In *Digital Futures 2012: The Third Annual Digital Economy All Hands Conference* (2012) (http://eprints.soton.ac.uk/343351/1/yip_de2012_submission.pdf).

Yu C.P., Young M.L. and *Ju B.C.* (2015). Consumer software piracy in virtual communities: An integrative model of heroism and social exchange // *Internet Research*, no. 25(2), pp. 317–334.

Zorz M. (2015). *Global black markets and the underground economy* (Featured News) (http://www.netsecurity.org/article.php?id=2288).