ISSN 2522-9087 (Print)
ISSN 2523-434X (Online)

UDC 004.6:339.138 **JEL Classification L 86, M 31**

Nataliya Kosar
Ph.D in Economics, Associate Professor
Department of Marketing and Logistics
Lviv Polytechnic National University
(Lviv, Ukraine)
Nataliia Kuzo
Senior Teacher
Department of Marketing and Logistics
Lviv Polytechnic National University (Lviv, Ukraine)
Anastasiia Kyrylenko
Student
Department of Marketing and Logistics
Lviv Polytechnic National University
(Lviv, Ukraine)

PROBLEMS OF PROTECTION CONSUMERS' PERSONAL DATA BY DOMESTIC ENTERPRISES: ASPECTS OF SOCIAL AND ETHICAL MARKETING

In modern conditions society pays more and more attention to the ethical problems of marketing activities of enterprises. Among these problems the important role belongs to the protection of personal information about consumers and the adequate using of this information. Researches show that people do not pay enough attention to these issues in Ukraine. It can negatively affect the image of enterprises and the attractiveness of their cooperation with foreign partners. Cases of leakage of consumers' personal data at domestic enterprises have been analyzed (with the help of) using secondary marketing information. Most of them are related to the human factor - the actions of their employees. The level of interest of Ukrainian citizens about safety of their personal data has been determined on the basis of collecting primary marketing information using Google Forms. The analysis was the basis for justification of the measures in the field of increasing the level of personal data protection at the enterprise level and the level of individual consumers.

Keywords: customer personal data, data protection, social-ethical conception of marketing, privacy policy, social networks.

DOI: 10.15276/mdt.3.1.2019.6

Statement of the problem in general form and it's connection with important scientific or practical tasks. Nowadays it is known about the great role of the marketing in the activities of domestic enterprises. The successful using of marketing can lead to enterprises` market share increase, improvement of financial results, attraction of new and retaining of current customers. Nevertheless, at the same time society's attention to ethical marketing issues is increasing. Among these problems the important role belongs to the protection of personal information about consumers and the adequate using of this information. The urgency of this problem is compounded by the increaseing of users' number and the intensity of using of the Internet, which allows tracking the behavior of consumers.

Analysis of the latest research and publications, which initiated the solution of this problem and on which the author relies. The ethical aspects of marketing activity of domestic enterprises are not analyzed enough in the scientific publications on marketing. In particular, in publication of Reshetnikova I.L. [1] the essence of ethical marketing and its main directions are defined. The issues of social and ethical marketing are analyzed in publications of Sokoly I.I., Katashinskaya M.O. [2], which state that marketing is aimed at building respect for people, the environment for their staying now and in the future. The basic principles of the implementation by enterprises of business ethics are given in [3].

Highlighting the previously unresolved parts of the general problem to which the article is devoted. The analysis of literary sources on marketing shows that these sourses do not pay enough attention to the issues of safety of consumers' personal data in marketing activity of enterprises, and to the conviction of consumers that information which they provided will be used only purposefully. The issues of protection of information from a technical point of view are widely researched in scientific publications in the field of computer sciences and information systems and networks [4].

Formulation of the purposes of the article (statement of the problem). The purpose of this article is to develop recommendations for strengthening the protection of consumers' personal data by domestic enterprises in the direction of their implementing of the concept of social and ethical marketing.

Statement of the main material of the research with full justification of the scientific results obtained. Personal data includes information or a set of information about a particular individual that is identified or can be specifically identified [5]. These data includes passport data, bank account data, e-mail addresses, and different physiological, genetic, intellectual, economic, and socio-cultural indicators [6]. Everyone aspires the access to this information was private and could be provided only with the knowledge and consent of the owner. Social networks open up significant opportunities for obtaining consumers' personal data. In exchange for free using of Skype and Facebook services consumers provide a wealth of information about themselves. This information can be used for forming a sample in marketing researches or in development of new marketing campaigns in the field of product promotion, or in determining the target audience [7].

On May 25, 2018, the General Data Protection Regulation (GDPR) began to operate in the countries of the European Union. The Regulation is a set of rules; in accordance with them the EU has strengthened and unified the protection of personal information about individuals in the EU. By this time, Directive 95/46/EU of the European Parliament and of the Council "Protection of individuals with regard to the processing of personal data and free movement of such data" was the main document which governed the right of EU citizens to protect their personal data [8].

The main principles of the functioning of the Regulations are presented in Table 1.

Exceptions to the Regulation includes the conducting of actions with information used in law enforcement, the fight against crime or terrorism and in the area of ensuring national security.

The difference between the GDPR and the previously developed legal regulation is the imposition of significant penalties. For non-compliance with the existing GDPR rules, the company must pay up to 2-4% of the company's total annual revenue income or 10 million euros [10].

ISSN 2522-9087 (Print)
ISSN 2523-434X (Online)

Table 1 – The main principles of functioning of the GDPR

Principles	Characteristic
The principle of lawfulness, fairness and transparency	It demands to provide a clear and understandable definition of the purpose of data collection and directions for their further using
The principle of limiting the purpose and minimizing the collection of data	Actions with personal data should always provide for a legitimate purpose. Actions on personal data must always have a legitimate aim. Also, enterprises must guarantee that the information they store and process is relevant and limited
The principle of accurate and relevant processing of data	It requires constantly checking by the controllers that the processed information is still accurate, relevant and suitable for the purposes
The principle of limiting the storage of personal information in a form that allows its identification	It restricts the movement and duration of the accumulation and preservation of information
The principle of confidentiality and safety of information storage	It demands the protection of the integrity and confidentiality of the collected data through the further maintenance of their storage reliability
The principle of accountability and responsibility	At any time enterprises must provide confirmation to public authorities regarding the compliance of conducted operations with the specified requirements of the GDPR

Formed on the basis [9]

Ukraine also operates GDPR, which, although not directly related to the legislation of Ukraine but relates to the activities of many domestic enterprises. This is explained by the fact that according to Art. 3 The regulation has an extraterritorial effect, that is also extended to companies located outside the EU and receive information from the source in the EU member states [6]. The principle under which Ukrainian enterprises will be held liable is applied in case of failure non-fulfillment of the Regulation requirements. A company located in the territory of the EU, which entrusted with the processing of personal information to an enterprise in the territory of Ukraine should be aware that in case of a breach of the Regulation requirements European company will be the first one that falls under its penalty. That's why it is primarily unprofitable for European company to cooperate with those Ukrainian enterprises that do not comply with the main provisions of the Regulation.

Despite the fact that the technology in the field of information security is progressing rapidly, even leading specialists can't always guarantee the absolute safety of clients' personal data. The larger, more influential and more profitable the company is, the more attempts and ways of stealing important data by outsiders and competing companies exist.

Frequently there are cases when the transfer of personal data is carried out for the personal benefit of enterprises' employees. The result of such case is the enforcement of the judgment of the Moscow District Court of Kharkiv on February 16, 2018, under Art. 361 and art. 361-2 (computer network hacking and illegal sale of restricted information) regarding the employee of "Nova Poshta", who accessed the company's database and tried to sell clients' personal data [11].

Information about clients of the bank can be stolen not only by "reading" cards: on June 6, 2018, it became known about a collective lawsuit against "PrivatBank". It is noted that the bank has unauthorized transfers of their clients` personal data to the third parties. The lawsuit is directed from 750 clients of the bank, whose representative is the lawyer association "ISU LAWYERS" [12].

Three months later, on September 27, 2018, by the court decision found guilty the manager of the branch of "PrivatBank", who deliberately unauthorizedly copied the information with limited access to the clients' personal data, after which provided them to the unidentified person by using the messenger Telegram, which specify on the leak of such information. It is

also determined that in February the manager transferred data of the client of "PrivatBank" to an outsider and he had received 400 UAH to his bank account for it. [13].

A progressive way to receive an access to personal data is social engineering, which involves the wrecking of a private account through the preliminary legitimate collection of the personal information. Exactly by this way the famous service Moneyveo provided a large number of fake online loans, having issued them to Ukrainians, as it became known on November 12, 2018, on the news site Segodnya.UA. The Security Service of Ukraine reported that the number of deceivers exceeds 1,000 people [14]. The same day, officers of the cyber police during the monitoring of the Internet revealed an intruder who tried to sell personal data of Ukrainian citizens. A man previously held a managing position in one of the Ukrainian banks. He was trying to sell the database which contained the information about 500 thousand people [15].

One more example of leakage of data through deliberate actions of the employees of the enterprises is that on November 14, 2018, the Kyiv Prosecutor's Office sent a prosecution of an employee of the State Fiscal Service in the Kyiv region, who in May 2018 copied the information about legal entities, which are taxpayers, and transferred the information to the third party for the corresponding monetary compensation [16].

The above analysis allows to conclude that most cases of data leakage in Ukraine arise precisely because of the human factor: individuals who have an access to the confidential information, wish to receive additional funds, self-assert, or influence other persons with the help of this information. According to the existing data, 25% of the employees of the enterprises are ready to betray the interests of their own enterprise immediately, 50% are ready to do so under certain conditions, and only 25% are patriots of their enterprise [17]. Employees may provide information to third parties as a result of bribery, intimidation or prosecution. That's why domestic enterprises should pay much attention to working with employees in order to create a loyalty to the company through the implementation of internal marketing measures. They should also increase responsibility for disclosing confidential information about the enterprise and its employees through the using of administrative methods.

Non-compliance with established requirements of the legislation on the protection of consumers' personal data, which resulted in unauthorized access to them by third parties (outsiders) or in violations of the rights of the subjects' personal data, may lead to the imposition of fines on citizens in the amount of 100 to 500 non-taxable minimum incomes of citizens, and on business entities - in the amount from 300 to 1000 non-taxable minimum incomes (according to Art. 188 of the Code of Ukraine on Administrative Offenses) [18]. Illegal collection, as well as storage, use or dissemination of confidential personal information about a person may result in the imposition of fines in the amount of 500 to 1,000 non-taxable minimum incomes of citizens or involvement in correctional proceedings for a term up to two years or until the term of arrest up to six months, or until the restraint of liberty for a term of up to three years (according to Art. 182 of the Criminal Code of Ukraine) [19].

The losing of money by an enterprise due to the payment of fines for violating the Law "On Protection of Personal Data" is not the worst thing that happens to an enterprise. In addition to administrative and criminal responsibility for the admittance of leakage of data, there are a many others also important consequences for the enterprise. Among them:

- temporary violations in work schedules, schedules of certain events, etc.;
- system can't be accessible for users;
- damage of hardware devices;
- damage of company's software;
- losing of important resources (monetary, investment, labor, intellectual, etc.);
- losing of monopolistic using the information;

ISSN 2522-9087 (Print)
ISSN 2523-434X (Online)

- violation of rights (copyright, adjacent, patent, inventive);
- complete or partial failure of the company's security system;
- reduction of client base.

It is clear that each of the listed consequences is undesirable for the enterprise, but the most serious one is a significant decrease of the level of consumers' confidence.

Enterprises should use methods for providing the safety of information in order to establish a high level of personal data protection during the development and implementation of information processing systems. These methods are conventionally divided into legal, software, technical and organizational-economic – Figure 1.

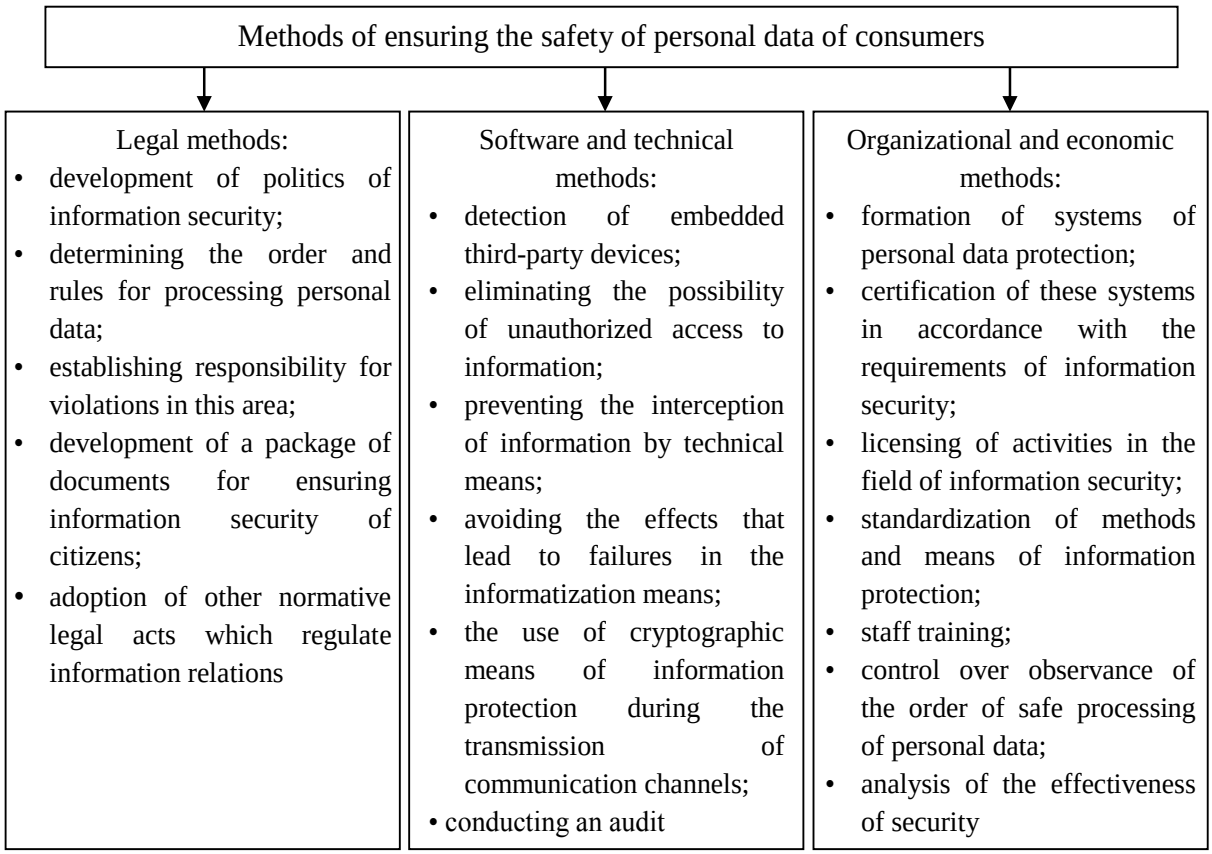

Figure 1 – Methods of protecting personal data
Developed by the authors on the basis of [20]

All methods for protecting of personal data at enterprise level will be more effective if they are integrated into an algorithm to provide reliable protection of personal data [21]. This algorithm contains a series of stages – Figure 2.

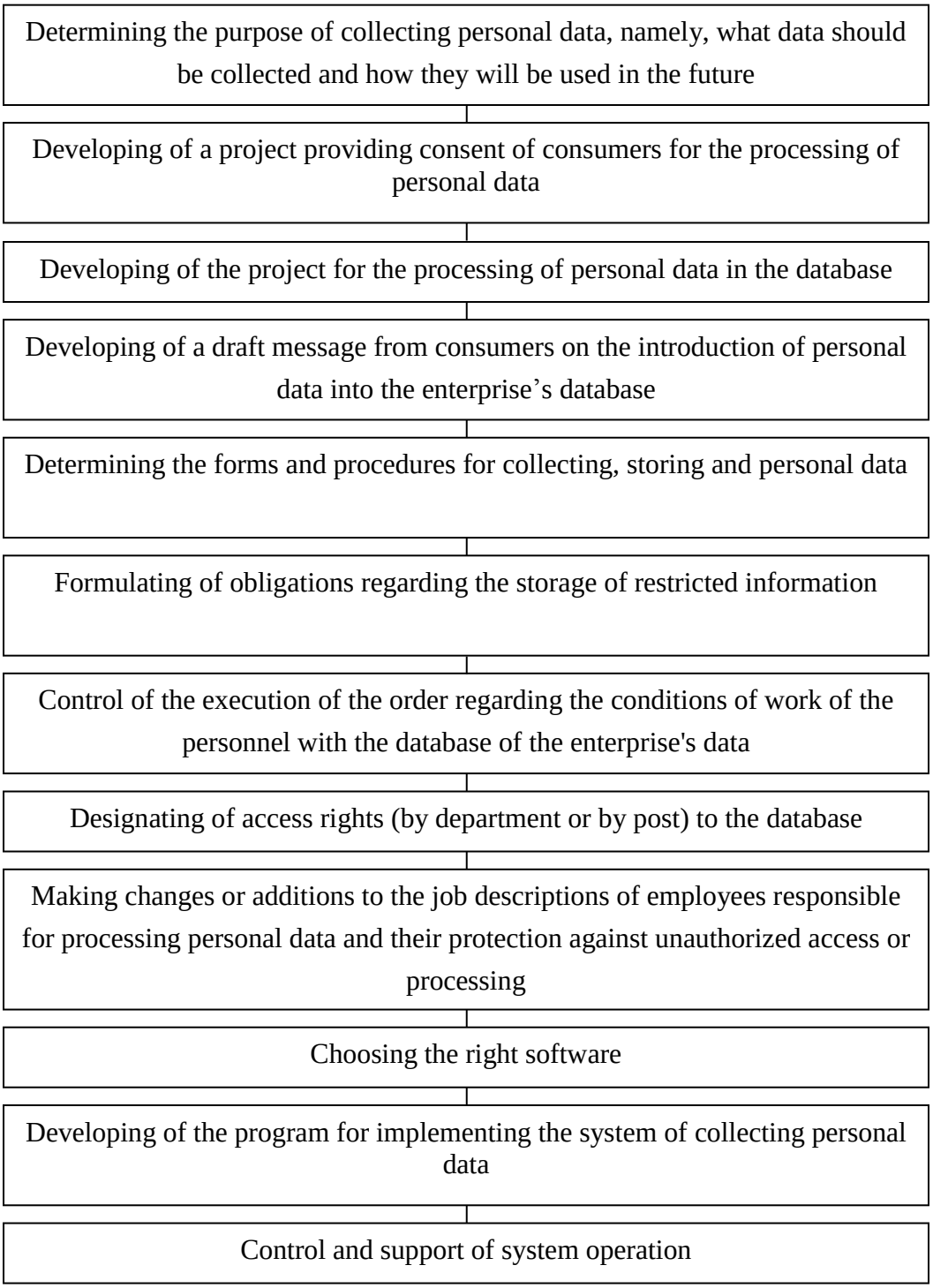

Figure 2 – Algorithm for providing protection of personal data
Developed by the authors on the basis of [21]

The main condition for the successful using of the algorithm is that all of the above actions should be executed in accordance with the Law of Ukraine "On Protection of Personal Data".

The active using of the Internet by domestic enterprises in different directions makes this algorithm relevant for most domestic enterprises – Table 2.

ISSN 2522-9087 (Print)
ISSN 2523-434X (Online)

Table 2 – Directions of use of websites by domestic enterprises

Directions of using	Amount of enterprises	The share of the total amount of companies which have a website
Customer service	7442	45,83
Supply of products and services on-line	2774	17,08
Possibility for visitors to create order of goods and services on-line	4457	27,44
Observation of the status of placed orders	4003	24,65
Personalized information content for regular or recurring clients	4018	24,74
Link to the company's website in social media	6847	42,16
Announcement of open vacancies or filing an application for filling vacant positions online	4575	28,17
Staff training	1598	9,84

Developed on the basis of [22]

The poll was conducted in order to develop recommendations for strengthening the protection of personal data of consumers. The sample size was determined by the formula given in [23]. During forming of the sample, the error in the results was 4%. In this case, the maximum value of the coefficient of variation which is taken into consideration is 0.25. Intended sample size is 150 people.

The survey was conducted within two weeks – from January 15 to January 28, 2019, using the Google Forms service. During this time, 222 people were interviewed.

During analyzing of the answers to the question about public wi-fi connection, it's possible to differ three large groups. The respondents from the first group (27%) connect to the public network every time they come into the area of "free wi-fi" coverage; interviewed from the second group (34.2%) use the public network only when they want to save the resource of mobile Internet and the respondents of the third group (28.8%) do not use public wi-fi at all (Figure 3).

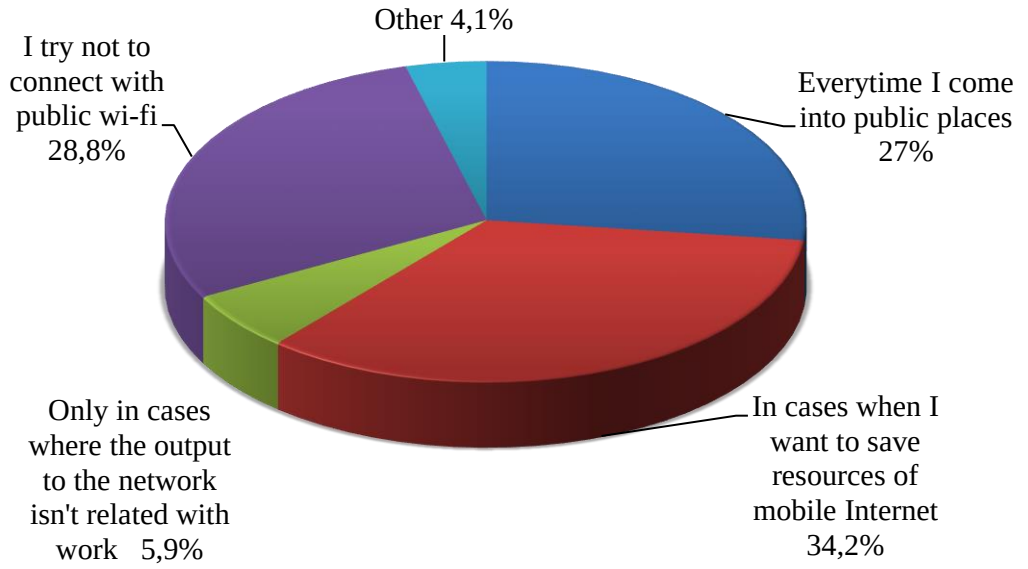

Figure 3 – Using of public wi-fi connection by respondents

While analyzing answers to the question about the amount, complexity and way of storing passwords for accounts, it has been discovered that the most common (every second one) is the choice of creating several simple passwords that "protect" all the accounts of a person. Every fifth respondent has created only one reliable password that is used for all his user pages, every tenth person store his passwords on paper. Only 7.2% of respondents use a special application for generating and storing passwords (Figure 4).

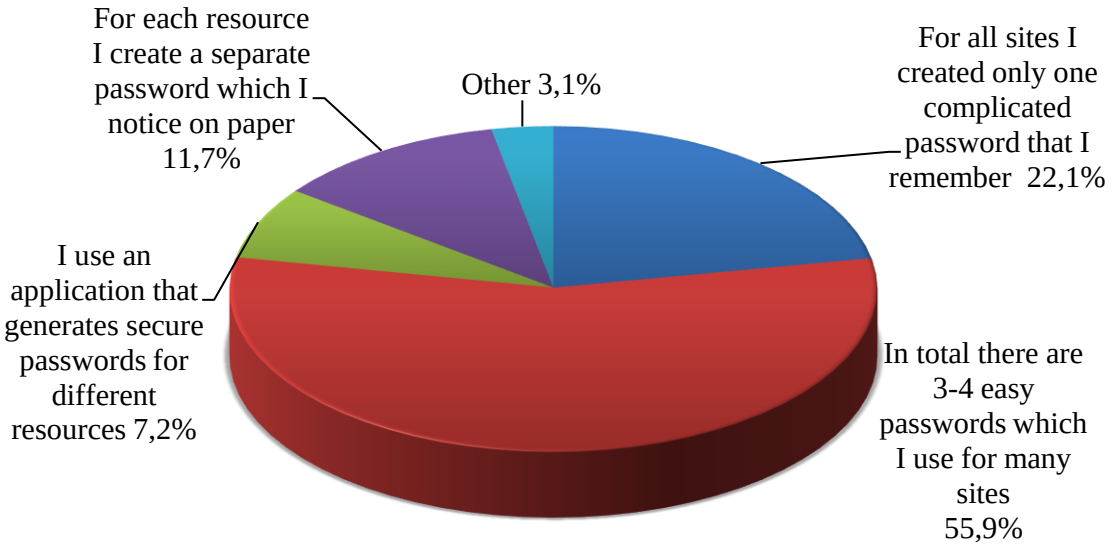

Figure 4 – Using different options for setting the password by respondents

Survey results showed that more than 50% of respondents do not publish their mobile phone number on social networks. Another third do it, "protecting" it from strangers by using point "only for friends". Every tenth of the respondents publishes the work telephone number on the page, and only 5.9% of respondents set free access to their phone number on social networks (Figure 5).

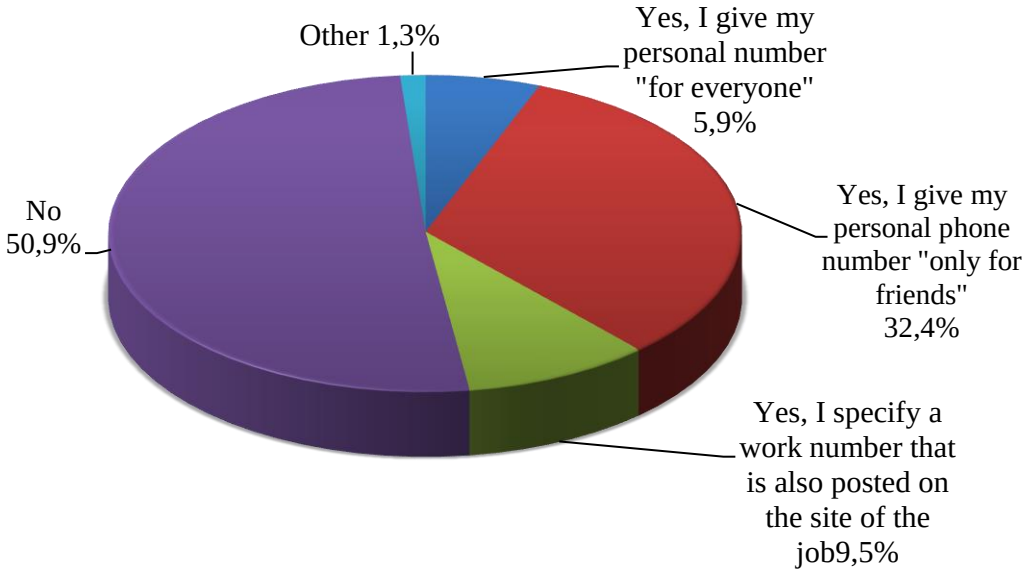

Figure 5 – Accessibility of the telephone number of the respondents

ISSN 2522-9087 (Print)
ISSN 2523-434X (Online)

On the question about "sign in via Facebook / Google" feature, which is available on almost every web-resource, the most respondents (47.3%) answered that they often use it, as it saves time on registration. One third of the respondents (30.6%) use this function only when they trust the site where the registration takes place. A fifth of the respondents answered that they favored a separate registration on each site (Figure 6).

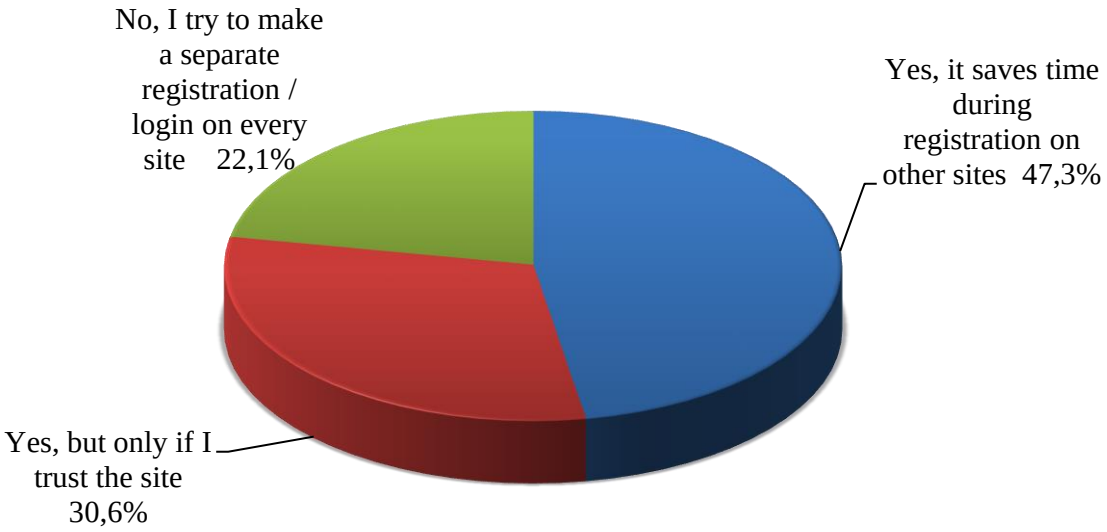

Figure 6 – Using of "log in via Facebook / Google" by respondents

In one of the questions, respondents were asked to indicate a protocol indicating that the data transmission on this site is protected. Every second (49,5%) respondent marked the right answer "https://", and 40,1 % answered, that they don't know the answer for this question. The rest of respondents gave incorrect answers (Figure 7).

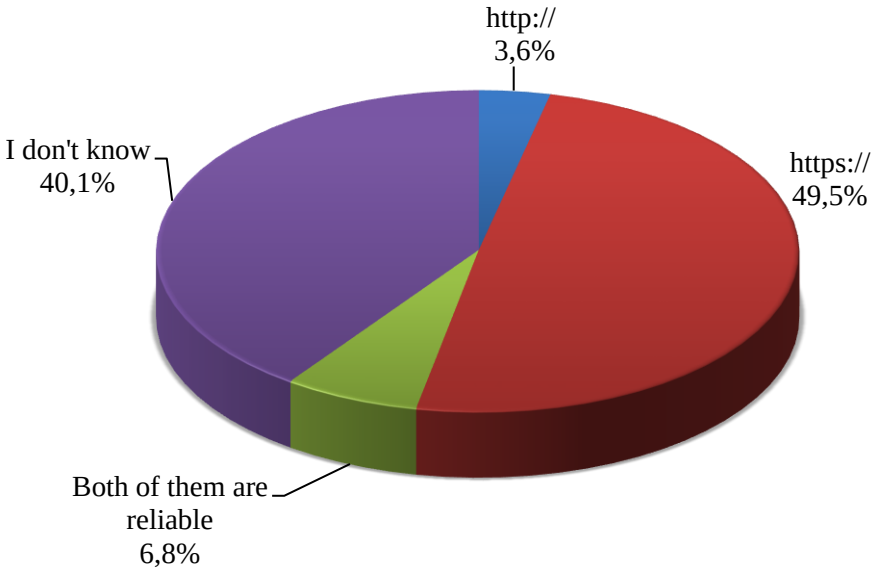

Figure 7 – Awareness of the respondents regarding the availability of secure data transmission protocol in the network

Based on the analysis of the collected primary marketing information, it was found that only 12.6% of users are thoroughly familiarizing with the privacy policy on the sites before agreeing with it. More than half of the respondents (52.7%) believe that the rules of privacy on all resources are the same, therefore refamiliarization does not make sense, and another 34.2% of respondents do not attach importance to this document at all (Figure 8).

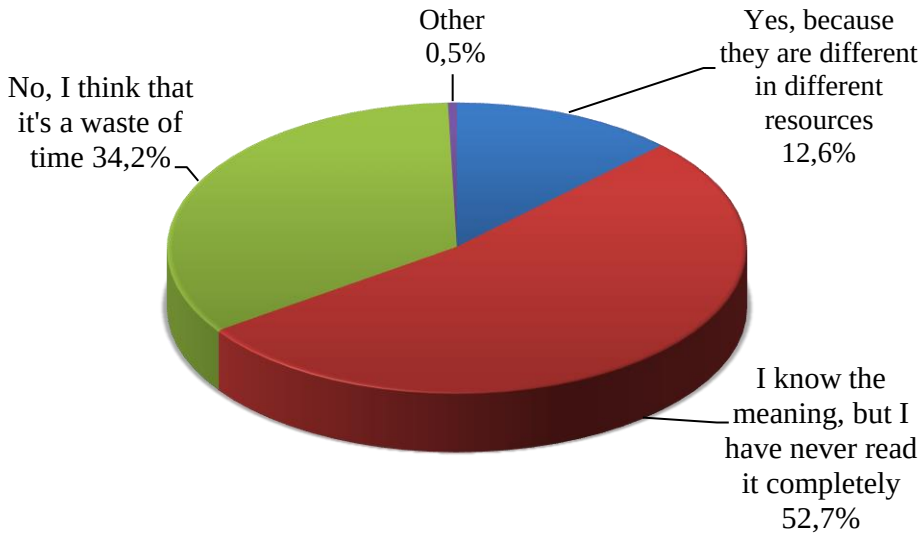

Figure 8 – Relation of respondents to the privacy policy on the sites

In order to determine whether consumers are interested in the purpose of using their data, respondents were offered a situation in which the store consultant offers to fill out a questionnaire for obtaining a customer's card. One in three answered that in this situation he would not ask the consultant about the purpose of obtaining personal data, because of "all shops are asking for the same standard data"; next 24.3% of respondents will be interested only if the questionnaire contains questions that are not related to the seller-buyer relationship; almost 30% will answer only those questions which they consider necessary, and only 10.4% of consumers in any case will be interested in the purpose of collecting and processing their personal data (Figure 9).

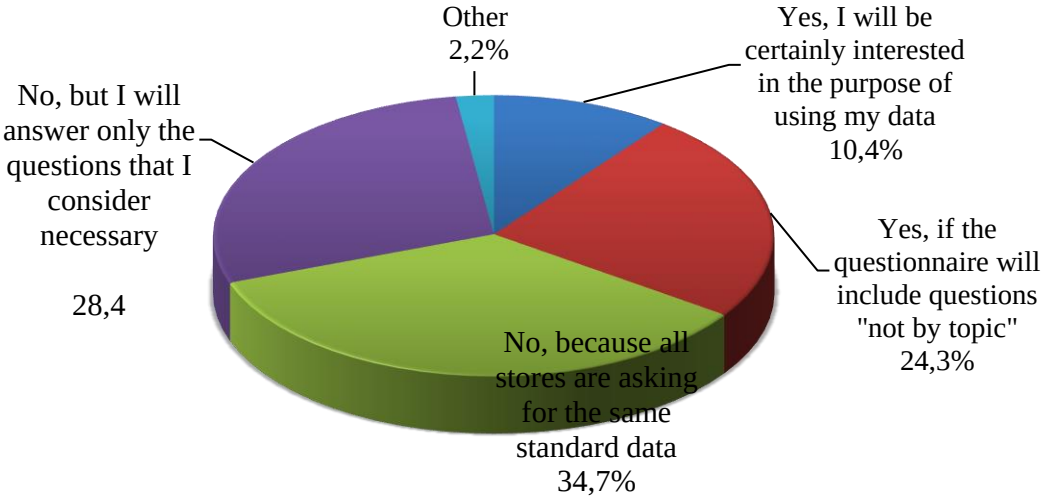

Figure 9 – The importance of the purpose of using the personal data of the respondent while providing information about him for obtaining the Customer's card

ISSN 2522-9087 (Print)
ISSN 2523-434X (Online)

It has been established that the most popular correspondence channels are messengers that use message encryption (Figure 10). The second place in popularity is the standard (without encryption) correspondence in social networks, on the third - e-mail. The last place is the SMS correspondence channel (only 16.2%), which is also considered the most vulnerable channel for data transmission.

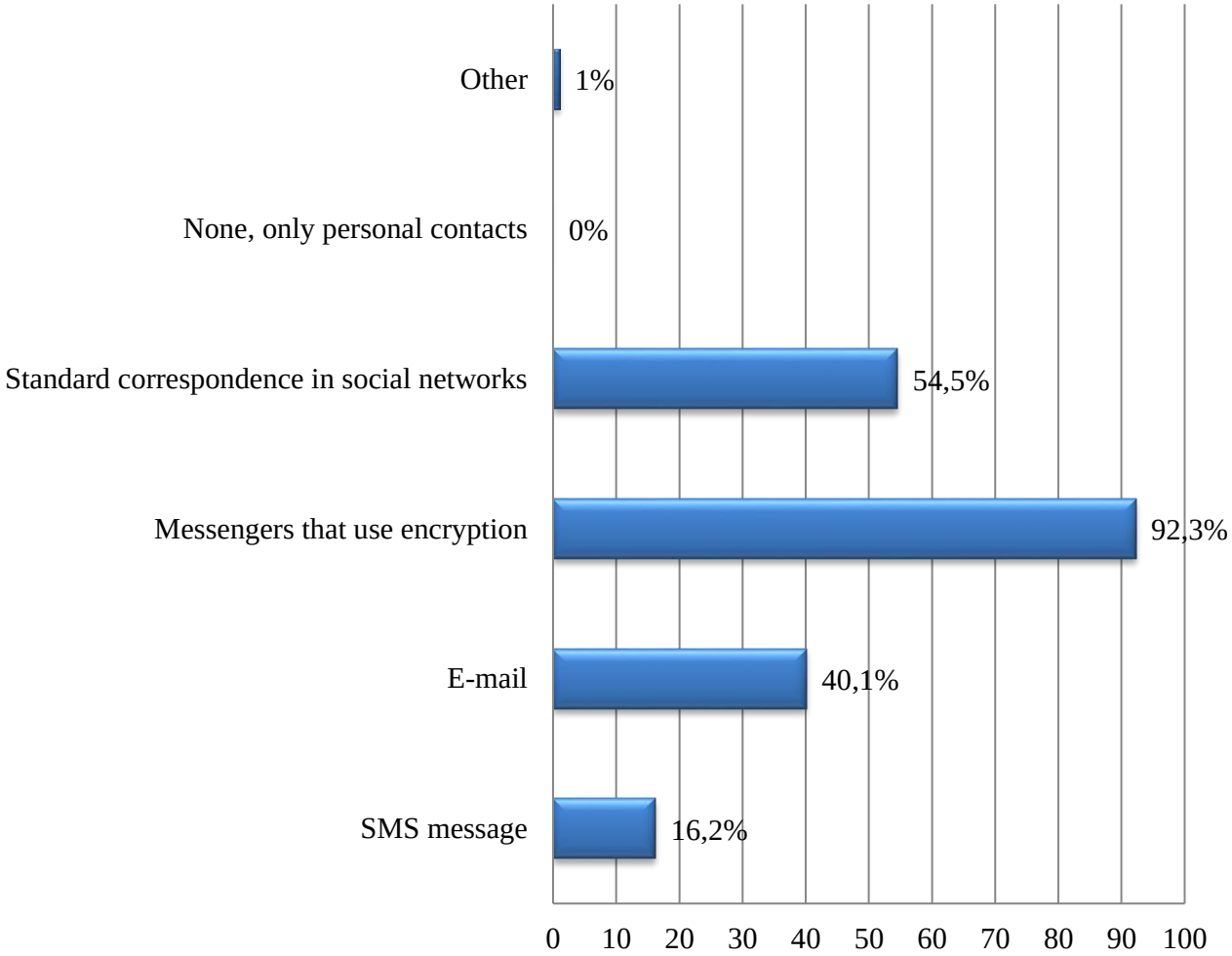

Figure 10 – Benefits of respondents regarding the using of different channels of correspondence

The last question was not required for the answer, so only 49.1% of respondents answered it. The respondents were asked to imagine a situation in which the "unknown" company had illegally gained their data, and now it imposes its' goods / services by using this data. The vast majority of respondents (86.7%) answered that they would immediately block this contact and hope that this company will no longer care for them. Only 13.3% answered that they would solve this problem by filing complaints and involving law enforcement officers.

Therefore, effective protection of personal data of consumers in Ukraine requires efforts of state bodies, enterprises and, of course, consumers. Taking into account the foregoing, it is possible to provide certain recommendations for the protection of personal information by enterprises and consumers – Table 3.

Compliance with these recommendations by businesses and consumers will not provide one-hundred percent guarantee against the leakage of personal data, but will facilitate their effective control and better protection.

Table 3 – Recommendations for the effective protection of personal information

Protection of personal data by consumers	Protection of personal data by enterprises
1. Do not use public wi-fi, or minimize its use. 2. Set up secure passwords for your accounts using mobile add-ons of complex password generators. 3. Use reliable communication channels. 4. Avoid using the "sign in with Facebook / Google" feature. 5. Check the address bar of the visited sites. Data sharing is secure if it starts with the "https" protocol. 6. Pay attention on the purpose of collecting consumers' personal data and how they will be processed. 7. In case of data leakage, customer should file the complaints, and require the removal of his data.	1. Collect only the information necessary for the operation of the enterprise and / or agree to provide the consumer with a detailed explanation of the purpose for which they will be used. 2. Delete consumers' data at the first requirement, if the consumer breaks the relationship with the enterprise. 3. Provide instructions for creating a secure password for access to your personal cabinet. 4. Provide reasonable answers to all questions of consumers about ways of collecting personal data and methods of their processing. 5. Use secure communication channels for conversations. 6. Carefully select employees who will work with consumer databases and warn them about administrative and criminal liability in case of leaking information.

Developed by authors

Conclusions from this research and prospects for further developments n this area. Nowadays Ukraine is on the list of countries with a low level of protection of personal data, that reduces not only the attractiveness of business and possible cooperation with other states, but also the reputation of Ukraine in general. It has been established that the majority of leaksages of personal data are caused by a human factor - deliberate or unintentional actions of employees of enterprises and inadequate attention to this issue at the enterprise level.

The survey provided an opportunity to define the level of interest of Ukrainian citizens in the security of their personal data. According to the results of the study, it was found that people in many cases behave carelessly when providing their data to third parties, and in the case of theft of these data often choose to ignore the situation, measures for protection of personal data by consumers were developed on the basis of the results of the analysis of secondary and primary information. These recommendations include creation of complex passwords for accounts, checking the address line of sites, avoiding of using of public wi-fi connection and the "log in through Facebook" function, active protection of law to privacy on their own or with the help of law enforcement agencies.

The article also claimed the recommended measures to ensure a high level of protection of personal data at the enterprise level, in particular: to collect only the necessary information for the enterprise; to delete consumers' data at their request; to provide instructions and advice for creating reliable passwords; to select employees to work with databases carefully; to use secure communication channels. For minimizing the threat of massive leakages of consumers' personal data, first of all the following measures are needed: a legislative base, an effective control system and, most importantly, a high level of legal literacy among the population. In case of a successful combination of these three factors it becomes possible to make reliable protection of personal data of Ukrainian citizens and to reduce the amount and complexity of thefts and fraud related to them.

Prospects for further development are related to the analysis of trends in the use of personal data of consumers in the marketing activities of domestic enterprises.

1. Reshetnikova, I.L. (2012). Etychnyi marketynh yak kontseptsiia marketynhovoi diialnosti [Ethical marketing as a marketing concept]. *Marketynh i menedzhment innovatsii – Marketing and Management of Innovations, 4, 91–96* [in Ukrainian].
2. Sokoly, I.I., & Katashynska, M.O. (2014). Sutnist i znachennia sotsialno-etychnoi kontseptsii marketynhu v upravlinni natsionalnym hospodarstvom Ukrainy [Nature and significance of social and ethical marketing concept in the management of national economy Ukraine]. *Ekonomichnyi prostir – Economic area, 91, 84–93* [in Ukrainian].
3. Beliavtseva, M.I., & Vorobiova, V.N. (2006). *Marketynhovyi menedzhment* [*Marketing management]*. Kyiv: Tsentr navchalnoi literatury [in Ukrainian].
4. Richer, J. & Sanso, A. (2017). OAuth 2 in Action. Manning Publications. *books.google.de*. Retrieved from https://books.google.de/books?id=QNLEjwEACAAJ.
5. Zakon Ukrainy "Pro zakhyst personalnykh danykh" # 2297-VI z podalshymy zminamy [Law of Ukraine "On Protection of Personal Data" No. 2297-VI with further changes] *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17 [in Ukrainian].
6. Shuliakivska, M.O. (2018). GDPR i personalni dani za General Data Protection Regulation [GDPR and the personal data according to the General Data Protection Regulation]. Zakhidna konsaltynhova hrupa. Retrieved from https://zkg.ua/gdpr-personalni-dani-za-general-data-protection-regulation-scho-tse-take [in Ukrainian].
7. Johnson, K. (2018). What is consumer data privacy, and where is it headed? Forbes Media LLC. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/07/09/what-is-consumer-data-privacy-and-where-is-it-headed/#54634f3a1bc1.
8. Dyrektyva 95/46/YeS Yevropeiskoho Parlamentu i Rady "Pro zakhyst fizychnykh osib pry obrobtsi personalnykh danykh i pro vilne peremishchennia takykh danykh" [Directive 95/46/EU of the European Parliament and the Council "Protection of individuals with regard to the processing of personal data and free movement of such data"] (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/994_242 [in Ukrainian].
9. Sharov, D. (2018). GDPR: sutnist, pryntsypy, vidpovidalnist za novymy pravylamy obihu personalnykh danykh u YeS [GDPR: the essence, principles, responsibility for the new rules for the processing of personal data in the EU]. *Ukrainske pravo.* Retrieved from http://ukrainepravo.com/scientific-thought/legal_analyst/gdpr-sutnist-pryntsypy-vidpovidalnist-za-novymy-pravylamy-obigu-personalnykh-danykh-u-yes [in Ukrainian].
10. Kozak, A. (2018). Zakhyst personalnykh danykh v YeS: shcho potribno znaty ukrainskym kompaniiam [Protection of personal data in the EU: what Ukrainian companies need to know]. *delo.ua*. Retrieved from https://delo.ua/business/zahist-personalnih-danih-v-jes-scho-potribno-znati-ukrajinskim-k-341115 [in Ukrainian].
11. Spivrobitnyka "Novoi poshty" zasudyly za kradizhku danykh kliientiv [The employee of "Nova Poshta" was convicted of theft the data of clients]. *ua.news*. Retrieved from https://ua.news/ua/spivrobitnyka-novoyi-poshty-zasudyly-za-kradizhku-danyh-kliyentiv [in Ukrainian].
12. Proty "Pryvatbanku" podano kolektyvnyi pozov za vytik personalnykh danykh [A collective lawsuit is filed against "PrivatBank" for the leakage of personal data]. *dt.ua.* Retrieved from https://dt.ua/ECONOMICS/proti-privatbanku-podano-kolektivniy-pozov-za-vitok-personalnih-danih-279921_.html [in Ukrainian].
13. Menedzher filii "PryvatBanku" u Lutsku ziznavsia u prodazhu danykh kliientiv [The manager of the "PrivatBank" branch in Lutsk confessed to the sale of customers' data]. *RBK-Ukraina.* Retrieved from https://www.rbc.ua/ukr/news/menedzher-filiala-privatbanka-lutske-priznalsya-1538058718.html [in Ukrainian].
14. V Ukraini nabyraie populiarnist nova kredytna skhema [A new credit scheme is gaining in popularity in Ukraine]. *Sohodni.* Retrieved from https://ukr.segodnya.ua/economics/finance/v-ukraine-nabiraet-populyarnost-novaya-kreditnaya-shema-1187896.html [in Ukrainian].
15. Kiberpolitsiia vykryla cholovika u prodazhi personalnykh danykh kliientiv ukrainskykh bankiv [Cyber police disclosed a man selling personal data of clients of Ukrainian banks]. *Ofitsiinyi sait*

Natsionalnoi politsii. Retrieved from https://www.npu.gov.ua/ news/kiberzlochini/kiberpolicziya-vikrila-cholovika-u-prodazhi-personalnix-danix-klijentiv-ukrajinskix-bankiv [in Ukrainian].
16. Sudytymut kolyshnoho podatkivtsia, yakyi nezakonno prodavav informatsiiu z bazy danykh DFS [A former taxman will be convicted of illegaly selling information from the database of State Fiscal Service]. *Ofitsiinyi sait prokuratury m. Kyieva.* Retrieved from https://kyiv.gp.gov.ua/ ua/news.html?_m=publications&_c=view&_t=rec&id=240354 [in Ukrainian].
17. Krykavskyi, Ye.V., Deineha, O.V., Deineha, I.O., Sheliuk, L.O., Kratt, O.A., & Patora, R. (2014). *Marketynhova informatsiia [Marketing information]*. Lviv: Vydavnytstvo Lvivskoi politekhniky [in Ukrainian].
18. Kodeks Ukrainy pro administratyvni pravoporushennia [Code of Ukraine on Administrative Offenses] (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/ show/80731-10 [in Ukrainian].
19. Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine] (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14 [in Ukrainian].
20. Ortynskyi, V.L., Kernytskyi, I.S., & Zhyvko, Z.B. (2009). *Ekonomichna bezpeka pidpryiemstv, orhanizatsii ta ustanov [Economic security of enterprises, organizations and institutions]*. Kyiv: Pravova yednist [in Ukrainian].
21. Los, V., & Pankiv, Ya. (2012). Zakhyst personalnykh danykh: z choho pochaty i yaki dokumenty neobkhidno rozrobyty [Protection of personal data: where to start from and which documents should be developed]. *Kadrovyk.UA.* Retrieved from https://www.kadrovik.ua/content/zahist-personalnih-danih-z-chogo-pochati-i-yaki-dokumenti-treba-rozrobiti [in Ukrainian].
22. Sait Derzhavnoi sluzhby statystyky Ukrainy [Site of the state statistics service of Ukraine]. *ukrstat.gov.ua.* Retrieved from http://www.ukrstat.gov.ua [in Ukrainian].
23. Kosar, N.S., Mnykh, O.B., Krykavskyi, Ye.V., & Leonova, S.V. (2018). *Marketynhovi doslidzhennia [Market Research]*. Lviv: Vydavnytstvo Lvivskoi politekhniky [in Ukrainian].

Косар Н.С., *канд. екон. наук, доцент, доцент кафедри маркетингу і логістики, Національний університет "Львівська політехніка"(Львів, Україна).*

Кузьо Н.Є., *старший викладач кафедри маркетингу і логістики, Національний університет "Львівська політехніка" (Львів, Україна).*

Кириленко А.А., *студентка кафедри маркетингу і логістики, Національний університет "Львівська політехніка"(Львів, Україна).*

Проблеми захисту персональних даних споживачів вітчизняними підприємствами: аспекти соціально-етичного маркетингу.

У сучасних умовах зростає увага суспільства до етичних проблем маркетингової діяльності підприємств, серед яких важлива роль належить захисту інформації особистого характеру про споживачів та її адекватному використанню. Дослідження свідчать, що в Україні недостатньо уваги приділяється цим питанням, що негативно може позначитися на іміджі підприємств та привабливості їх співпраці з іноземними партнерами. З використанням вторинної маркетингової інформації проаналізовано випадки витоку персональних даних споживачів на вітчизняних підприємствах, більшість яких пов'язана з людським чинником – діями їх працівників. На підставі збирання первинної маркетингової інформації за допомогою сервісу Google Forms визначено рівень зацікавленості громадян України безпекою своїх персональних даних. Проведений аналіз був підставою для обґрунтування заходів у сфері підвищення рівня захищеності персональних даних на рівні підприємства та окремих споживачів.

Ключові слова: персональні дані споживачів, безпека даних, концепція соціально-етичного маркетингу, політика конфіденційності, соціальні мережі.

Received to the editor February 15, 2019.