DOI: 10.14529/ctcr170409

INFORMATION SECURITY OF SMALL BUSINESS: MODERN CONDITION, PROBLEMS AND THE WAYS OF THEIR SOLUTIONS

L.Yu. Ovsyanitskaya[1], *larovs@rambler.ru,*
Yu.V. Podpovetnaya[1,2], *y-u-l-i-a-v-a-l@mail.ru,*
A.D. Podpovetnyy[2], *ruter98@mail.ru*
[1] *Financial University under the Government of the Russian Federation (Chelyabinsk branch), Chelyabinsk, Russian Federation,*
[2] *South Ural State University, Chelyabinsk, Russian Federation*

The actuality of the investigated problem is caused by the fact that information is the most valuable resource of business. It is substantiated that the peculiarity of small business is the limited financial possibilities allocated for means and methods of information protection. Therefore, the decisions should allow to realize the optimal protection of the information system and data – to ensure the maximum possible result with the limited investment of funds. It is presented the author's approach to the problems of choosing means and methods for protecting information in the conditions of a limited budget and in justifying a set of measures aimed at ensuring information security for small business. The materials of the article can be useful for managers and owners of small business, students of higher and secondary educational institutions of technical and economic direction.

Keywords: information security, small business, information threats, information systems.

Introduction

At present, it is impossible to imagine the direction of small businesses that do not use information technology to conduct financial settlements, organize document circulation, advertise their activities, search for suppliers and buyers, implement online services and use information as an object of commodity-money relations.

However, there are factors that can not only disrupt the work of any enterprise or organization, but also stop the activity for a while. Cybercriminals have recently paid a lot of attention to small business as the easiest way to acquire information that allows to steal personal data of employees and funds from bank accounts of employees and businesses. The reason is that the large companies pay great attention to information security issues: they have highly skilled IT staff, use licensed software, store data on their own reliable servers and are able to invest in information security. In the small business segment, these problems are dealt with much less. There are three reasons for this behavior:

1. Incompetence of employees.
2. Lack of awareness of leaders in the current state of information protection.
3. Reluctance or inability to allocate financial resources to ensure information security, to train employees, to purchase modern software and hardware.
4. Use of free services, software and cloud-based data storage.

There are four actions performed with information that may contain a threat: collection, modification, leakage and destruction. Sources of threats are divided into external and internal ones. The sources of internal threats are:

– employees of the organization;
– software;
– hardware.

The internal threats can be manifested in the following forms:

– errors of users and system administrators;
– violations by employees of the company of established regulations for the collection, processing, transfer and destruction of information;
– errors in the operation of the software;
– failures and malfunctions in the operation of computer equipment.

The maximum damage to business, according to Kaspersky Lab's [1], causes vulnerabilities in the software. This issue is especially acute when using free software, public cloud data warehouses and using password protection for access to information resources.

With the installed licensed information systems, the use of their own servers to store information and provide multifactor protection of access to information resources, the probability of information loss is significantly reduced. However, these measures require investments.

At the same time, there are actions that are equally probable and dangerous both in the segment of large and small business, for example, leakage of information on the intentional or accidental fault of employees, loss of mobile devices by employees, employee fraud, etc. The reasons for irresponsible attitude to the fulfillment of information security requirements are the lack of knowledge in the field of IT security and, accordingly, understanding the importance of exact compliance with rules and requirements.

External sources of threats include:

– computer viruses and malware;

– organizations and individuals;

– natural disasters.

Forms of external threats are:

– infection of computers with viruses or malicious programs;

– unauthorized access to corporate information;

– information monitoring by competing structures, intelligence and special services;

– accidents, fires, man-made disasters.

External threats occur in the absence of installed licensed software products that protect the computer and the information system as a whole from malicious programs. The offered free or shareware software will never support the full functionality of the security tools available in commercial versions: blocking viruses and spyware, securing online purchases, blocking spam and phishing messages, protecting data privacy, having a firewall, preventing hacker attacks, the protection of money transactions, a warning about the substitution of domain names for fraudulent and other.

Ignoring existing internal and external cyber threats, a low level of investment in information security tools and training employees can lead to significant financial and reputational losses.

Losses from incidents occur from the costs of external professional services, from missed business opportunities, as well as damage from forced downtime due to the blocking of the company's IT processes and stopping activities during the recovery of information processes and data.

Ways to solve the problems of information security for small businesses

According to the Federal Law “On Information, Information Technologies and Information Protection” [2], the protection of information is understood as the adoption of legal, organizational and technical measures aimed at:

– to ensure the protection of information from unauthorized access, destruction, modification, blocking, copying, provision, distribution, as well as from other unlawful actions with respect to such information;

– to respect the confidentiality of restricted access information;

– on the realization of the right to access to information.

Let’s consider the components of the information security of small business.

1. Protection of information from unauthorized access, destruction, modification, blocking, copying, provision and distribution.

The choice of methods and means of protecting information at the enterprise depend on its type.

Fig. 1 presents a classification of information based on the restriction of access to it.

Information existing in the enterprises is divided into public information and information with limited access.

The public information includes:

– information signed by the management to transfer to the outside (for example, for conferences, presentations, etc.);

– information obtained from external open sources;

– information from the company's external website.

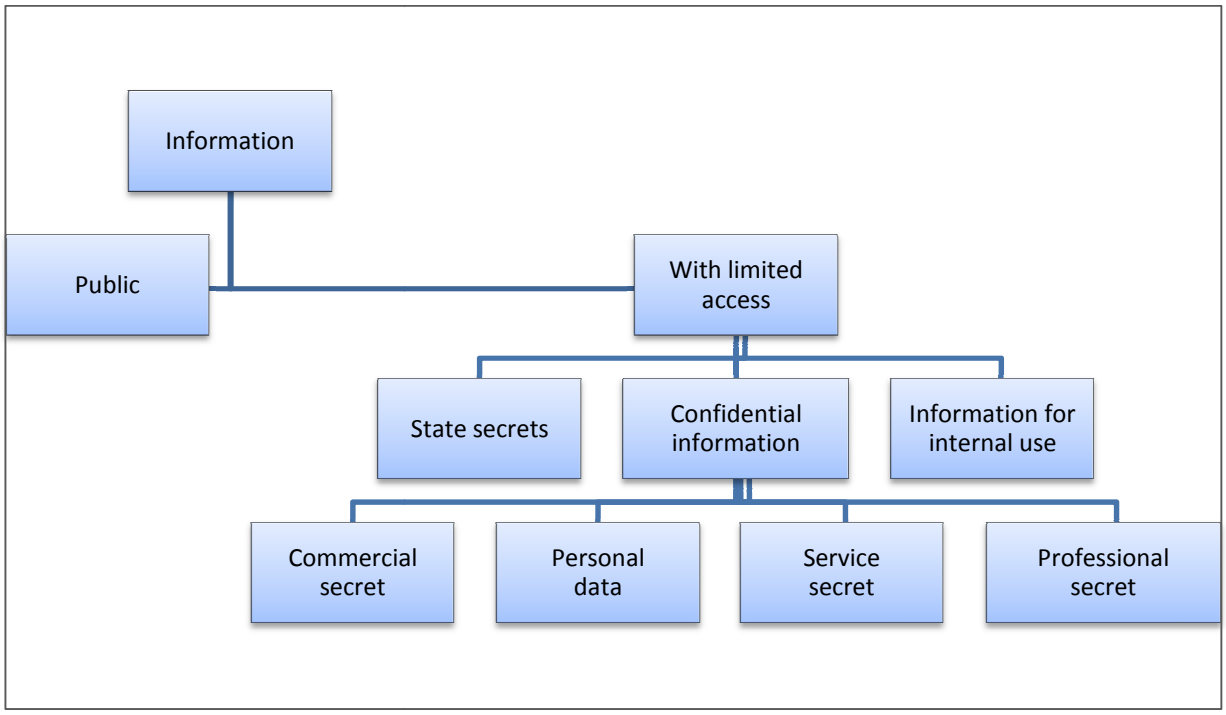

Fig. 1. The classification of information on the basis of access restriction

Many people believe that protecting open information does not make sense. However, this is not so: for example, the substitution of information on the company's website, depending on what it is replaced, can lead to some undesirable consequences of varying severity.

To protect public information, it is sufficient to use minimal means and methods of information security: password protection of files and folders, use of built-in data protection mechanisms in MS Office. These tools allow to protect with the help of password files from review or modification, prohibit editing, formatting or making any changes to the document, organize protection of macros, hide certain parts of the document from viewing, distribute restrictions for users and add an electronic signature.

Information containing state secrets

According to the Law of the Russian Federation "On State Secrets" [3], state secrets mean information protected by the state in the field of its military, foreign policy, economic, intelligence activities, the proliferation of which may damage the security of the Russian Federation.

The protection of this information is implemented in the information system in the framework of its information security system, depending on the class of security of the information system, information security threats, the structural and functional characteristics of the information system, the information technologies used and the features of the information system [4].

We note the main feature of the protection of information containing state secrets: all methods and means of information security must have a certificate of compliance of FSTEC (Federal Service for Technical and Export Control) - a document issued by the federal FSTEC structure that confirms compliance of the certified object with the requirements of regulatory Russian acts.

Information for internal use

Information for internal use includes any information used by employees within their divisions, thematic groups, which:

– circulates between departments and is necessary for their normal functioning;

– is the result of work with information from open sources (for example, a review of the market of manufactured products);

– does not refer to confidential information;

– does not apply to public information.

To protect information for internal use, it is necessary to apply all of the above protection mechanisms for open information, but with a much greater responsibility: when passwords are created, use passwords with an increased bit space, use not only letters and numbers, but special symbols and distin-

guish registers. For convenience and speed of access, password protection can be replaced by biometric-based protection and e-Token or ru-Token keys, using an electronic signature that is officially received in certifying centers.

Confidential information

Confidential information is documented information, access to which is limited in accordance with the legislation of the Russian Federation. Confidential information is not publicly available information and, in the event of disclosure, may damage the rights and legally protected interests of the person provided it.

Let us consider in detail the types of confidential information [5–8].

Personal information

According to the Federal Law "On Personal Data" [9], any information pertaining to a certain individual (subject of personal data) refers to personal data.

Personal data is information that allows to uniquely determine which person is talking about. Law No. 152-FL divides personal data into three types:

– general;

– special;

– biometric.

The common personal data are the surname, name, place of residence, passport data, information on education and qualifications, salary, work activity, etc. This information is always available at the enterprise.

Special data are information about race, nationality, political views, religious or philosophical beliefs, health status and others. These data can be contained in questionnaires filled out by employees in hiring, medical certificates, etc.

Biometric data refer to information that reflects the physiological and behavioral characteristics, allowing to determine his personality. For example, fingerprints, the figure of the iris, the data of measurements of the facial parameters, the shape of the hand, the picture of the retina of the eye, handwriting, voice, and others. Also biometric data includes photographs of a person, with the exception of photographs and video recordings made during mass and public events.

The enterprise is liable to employees for violation of the protection regime, processing and use of this information.

For the protection of personal data, all methods and means listed in the description of the protection of information for official use are used. If there is an illegality in the collection or dissemination of information and if there is no consent of its carrier to collect or disclose information, criminal liability arises. If the disclosure of confidential personal information occurred during the performance of official duties, the punishment becomes tougher. Even more severe consequences are provided for the disclosure of data on minors.

Commercial secret

Commercial secret is information related to production, technical, technological information, management of financial and other activities of an enterprise, the disclosure of which may damage its interests.

Trade secrets may include scientific and technical, technological, production information, including secrets of production (know-how), financial and economic and other information that has real or potential commercial value due to its unknown to third parties.

The signs of a commercial secret, manifested when it is disclosed, are:

– causing economic damage to the company;

– occurrence in the company of losses in the form of lost profits;

– reduction of economic, technical efficiency of the company's activities, including foreign economic activity;

– damaging the image of the company and discrediting it as a bona fide, reliable partner in foreign economic and other activities;

– damage to the prestige and reputation of the partner with whom a commercial transaction is made.

The decision to apply methods and means to ensure the safety of commercial information is taken by the information owner. If the information does not contain state secrets and personal data of employees, methods and means are not regulated by law, there are no requirements for the existence of a FSTEC certificate.

Professional secret

Professional secrecy refers to information related to professional activities, access to which is limited in accordance with the Constitution of the Russian Federation and federal laws, the violation of which entails criminal liability.

According to the Law of the Russian Federation "On Information, Information Technologies and Information Protection" [2], professional secrets are information received by citizens in the performance of their professional duties or organizations in the performance of certain activities.

The following types of professional secrets stand out:

– the secret of insurance and information about the insured;

– communication secret;

– medical secret;

– information about the donor and the recipient;

– the secret of confession;

– the secret of the lawyer, information communicated by the principal in connection with the provision of legal assistance;

– information that has become known in connection with the performance of notarial acts;

– the secret of notarial acts.

The components of information security systems in small business

Having defined the peculiarities of each type of information, we formulate the main provisions concerning its optimal protection within the framework of use in small business, taking into account small financial costs. This will be possible when creating a security system that performs only the required mandatory functions.

1. Antivirus and firewall.

The largest security systems offer software applications designed specifically for companies belonging to the small business segment, with the number of employees and, accordingly, computers, up to 25. These offers provide comprehensive protection for computers, file servers and mobile devices from malicious programs, Internet attacks and online fraud taking into account all the requirements of the law.

2. Authentication, authorization and administration (AAA) system.

The work of a small business enterprise is impossible without providing a system that has the abbreviation AAA or 3A (authentication, authorization, administration). In some cases, the fourth component is added and the fourth «A» is audit. These systems are designed to provide protection against unauthorized access to information systems and resources.

The specific composition and content of organizational and technical measures to ensure the information security of personal data are specified in the FSTEC Order No. 21 on February 18, 2013 "On the Approval of the Composition and the Content of Organizational and Technical Measures to Ensure the Safety of Personal Data when Processing them in Personal Data Information Systems".

3. Information storage systems.

For enterprises of any size the problem of storage, management and recovery in case of loss is actual.

The system of backup and data recovery allows to create a copy of the data at a specified interval with the purpose of their possible recovery in the future. They also help to ensure the continuous operation of the enterprise or organization in the event of damage to the operating system through its rapid recovery without loss of information.

We note an important feature that must be taken into account when using cloud storage information [10]. In case where the company uses to process personal data cloud data warehouse located outside the territory of the Russian Federation, it must have a copy of the database located in our country, to carry out all the necessary changes and additions to the database, and then transmit the information to cloud storage. That is, on the territory of the Russian Federation there must always be an updated database containing processed personal information.

4. Protection against leaks of confidential information.

Information systems to protect against confidential information leaks (Data Loss Prevention, DLP) allow to track and block the transfer of information outside the corporate network. These systems are able to monitor the actions of employees of the organization, record and analyze their messages sent during work via e-mail, social networks, FTP, Skype, ICQ and other applications and protocols that are

printed on the printer or stored on external storage media. The main objective of DLP systems is to ensure the implementation of the privacy policy adopted by the particular organization.

The result is the prevention of unauthorized transmission of confidential and personal information, minimizing the risks of reputational damage and increasing the discipline of employees of the organization.

Conclusion

Information is a valuable resource of business. Protection of data containing state secrets and personal information of people is regulated by the laws of the Russian Federation, and is mandatory for execution. Algorithms for the protection of commercial secrets must be set independently, depending on the specifics and size of each enterprise or organization.

A feature of small business is the limited financial resources allocated to the means and methods of protecting information. Therefore, the decisions should allow to realize the optimal protection of the information system and data – to ensure the maximum possible result with limited investment of funds.

References

1. *Informatsionnaya bezopasnost' biznesa: issledovanie tekushchikh tendentsiy v oblasti informatsionnoy bezopasnosti biznesa* [Business Information Security: a Survey of Current Trends in Information Security of Business]. Available at: http: // www.kaspersky.com (accessed 03.11.2016).

2. *Ob informatsii, informatsionnykh tehnologiyah i o zashchite informatsii*. *Federal'nyy zakon ot 27.07.2006 No. 149-ФЗ* [About Information, Information Technologies and Information Protection]. Federal Law No. 149-FZ on July 27, 2006.

3. *O gosudarstvennoy tayne*. *Zakon Rossiyskoy Federatsii ot 21.07.1993 No. 5485-I (s izmeneniyami i dopolneniyami* [On State Secrets]. Law of the Russian Federation on July 21, 1993 No. 5485-I (with amendments and additions).

4. *Mery zashhity informacii v gosudarstvennyh informacionnyh sistemah: Metodicheskiy dokument* [Measures to Protect Information in Public Information Systems: the Methodical Document]. Available at: http://fstec.ru/component/attachments/download/675.

5. *O perechne svedeniy, kotorye ne mogut sostavlyat' kommercheskuyu taynu. Postanovlenie pravitel'stva RSFSR ot 05.12.1991 No. 3* [On the List of Information that Can not Constitute a Trade Secret: the Decree of the Government of the RSFSR on 05.12.1991 No. 3]. Available at: http://www.consultant. ru/document/cons_doc_LAW_158/.

6. *Ob utverzhdenii Perechnya svedeniy konfidentsial'nogo kharaktera: Ukaz prezidenta RF ot 06.03.1997 No. 188* [On approval of the List of Confidential Information: the Decree of the President of the Russian Federation on 06.03.1997 No. 188]. Available at: http://base.garant.ru/10200083/.

7. Ovsyanitskaya L.Yu. [Actual Issues of Information Protection (on the Example of Industrial Enterprises and Public Health Institutions in Chelyabinsk City)]. *National Interests: Priorities and Security*, 2013, no. 21 (210), pp. 54–59 (in Russ.)

8. Prokhorova I.A., Ovsyanitskaya L.Yu. [Practical Aspects of Teaching Students to Work with Data in the Context of Economic, Medical and Engineering Education]. *Nauka YuUrGU: sbornik trudov 67-y nauchnoy konferentsii* [Science of the South Ural State University: Proc. of the 67th Scientific Conference]. Chelyabinsk: South Ural St. Univ. Publ., 2015, pp. 475–481.

9. *O personal'nyh dannyh: Federalnyy zakon ot 27.07.2006 N 152-FZ* [On personal data: the Federal Law No. 152-FL on July 27, 2006]. Available at: http://www.consultant.ru/document/cons_doc_LAW_61801/.

10. *O vnesenii izmeneniy v otdel'nye zakonodatel'nye akty Rossiyskoy Federatsii v chasti utochneniya poryadka obrabotki personal'nykh dannykh v informatsionno-telekommunikatsionnykh setyakh: Federalnyy zakon ot 21.07.2014 No. 242-FZ.* [On the Introduction of Amendments to Certain Legislative Acts of the Russian Federation Regarding the Clarification of the Procedure for the Processing of Personal Data in Information and Telecommunication Networks: the Federal Law on July 21, 2014 No. 242-FL]. Available at: http://base.garant.ru/70700506/.

Received 5 September 2017

УДК 004.056 **DOI: 10.14529/ctcr170409**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МАЛОГО БИЗНЕСА: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Л.Ю. Овсяницкая[1], Ю.В. Подповетная[1,2], А.Д. Подповетный[2]

[1] Челябинский филиал Финансового университета при Правительстве РФ, г. Челябинск, Россия
[2] Южно-Уральский государственный университет, г. Челябинск, Россия

Актуальность исследуемой проблемы обусловлена тем, что информация является ценнейшим ресурсом бизнеса. Обосновано, что особенностью малого бизнеса являются ограниченные финансовые возможности, выделяемые на средства и методы защиты информации. Поэтому принимаемые решения должны позволить реализовать оптимальную защиту информационной системы и данных – обеспечить максимально возможный результат при ограниченных вложениях средств. Представлен авторский подход к проблемам выбора средств и методов защиты информации в условиях ограниченного бюджета и к обоснованию комплекса мер, направленных на обеспечение информационной безопасности для малого бизнеса. Материалы статьи могут быть полезными для руководителей и владельцев предприятий малого бизнеса, студентам высших и средних учебных заведений технического и экономического направления.

Ключевые слова: информационная безопасность, малый бизнес, информационные угрозы, информационные системы.

Литература

1. Информационная безопасность бизнеса: исследование текущих тенденций в области информационной безопасности бизнеса. – http://www.www.kaspersky.ru (дата обращения: 03.11.2016).

2. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ.

3. О государственной тайне: закон Российской Федерации от 21 июля 1993 г. № 5485-I (с изменениями и дополнениями).

4. Меры защиты информации в государственных информационных системах: метод. док. (утв. Федерал. службой по техн. и экспорт. контролю 11 февр. 2014 г.).

5. О перечне сведений, которые не могут составлять коммерческую тайну: Постановление Правительства РСФСР от 05.12.1991 № 3.

6. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188.

7. Овсяницкая, Л.Ю. Актуальные вопросы защиты информации (на примере промышленных предприятий и учреждений здравоохранения г. Челябинска) / Л.Ю. Овсяницкая // Нац. интересы: приоритеты и безопасность. – 2013. – № 21(210). – С. 54–59.

8. Прохорова, И.А. Практические аспекты обучения студентов работе с данными в контексте экономического, медицинского и инженерного образования / И.А. Прохорова, Л.Ю. Овсяницкая // Наука ЮУрГУ: сб. тр. 67-й науч. конф. – Челябинск: Издат. центр ЮУрГУ, 2015. – С. 475–481.

9. О персональных данных»: федер. закон от 27.07.2006 № 152-ФЗ.

10. О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях: федер. закон от 21.07.2014 № 242-ФЗ.

Овсяницкая Лариса Юрьевна, канд. техн. наук, доцент кафедры математики и информатики, Финансовый университет при Правительстве РФ (Челябинский филиал), г. Челябинск; larovs@rambler.ru.

Подповетная Юлия Валерьевна, д-р пед. наук, доцент, зав. кафедрой математики и информатики, Финансовый университет при Правительстве РФ (Челябинский филиал); профессор кафедры русского языка как иностранного, Южно-Уральский государственный университет, г. Челябинск; y-u-l-i-a-v-a-l@mail.ru.

Подповетный Артем Дмитриевич, студент Архитектурно-строительного института, Южно-Уральский государственный университет, г. Челябинск; ruter98@mail.ru.

Поступила в редакцию 5 сентября 2017 г.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Ovsyanitskaya, L.Yu. Information Security of Small Business: Modern Condition, Problems and the Ways of Their Solutions / L.Yu. Ovsyanitskaya, Yu.V. Podpovetnaya, A.D. Podpovetnyy // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2017. – Т. 17, № 4. – С. 77–84. DOI: 10.14529/ctcr170409

FOR CITATION

Ovsyanitskaya L.Y., Podpovetnaya Y.V., Podpovetnyy A.D. Information Security of Small Business: Modern Condition, Problems and the Ways of Their Solutions. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2017, vol. 17, no. 4, pp. 77–84. DOI: 10.14529/ctcr170409