УДК 34.096
DOI https://doi.org/10.32837/pyuv.v0i3(32).607

О. В. Шепета
orcid.org/0000-0002-8485-0349
кандидат юридичних наук, доцент,
доцент кафедри організації захисту інформації з обмеженим доступом
Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України

О. К. Тугарова
orcid.org/0000-0003-1346-8342
кандидат юридичних наук, доцент,
доцент кафедри організації захисту інформації з обмеженим доступом
Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України

ОСНОВНІ ВИМОГИ ДО СТВОРЕННЯ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Усе більше і більше Україна входить у світовий інформаційний простір, а у зв'язку з пандемією коронавірусу COVID-19 багато підприємств у себе впроваджують новітні досягнення інтернет-технологій. Розвивають інформаційні та комп'ютерні технології, розширюють межі обробки, зберігання і передачі інформації (віртуальні кабінети тощо), а також ведення онлайн-бізнесу. Цінність інформації в разі введення новаторських методів набагато збільшується. Тому зростає активність інформаційно-аналітичних структур різного роду порушників. Створення відділу захисту інформації дає гарантію забезпечення комплексного захисту інформації та контролю за її функціонуванням.

Як не дивно, але й нині не всі керівники підприємств усвідомлюють нагальну потребу в організації на їхньому підприємстві служби захисту інформації.

Питанням організації захисту інформації на підприємстві присвячено значну кількість праць А.І. Марущака, А.К. Гриня, В.Б. Дудкевича, В.О. Хорошка.

Аналіз наукових публікацій дає підстави стверджувати, що у зв'язку зі збільшенням інформаційних потоків на підприємстві обов'язково треба створювати службу захисту інформації. Служба захисту інформації підприємства повинна регулюватися нормативно-правовими актами, які створюються керівництвом підприємства, в основі яких доцільно використовувати такі рекомендації міжнародних стандартів і чинного законодавства України.

Такими міжнародними стандартами є: ISO/IEC 27002 «Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою»; ISO/IEC 27003 «Інформаційні технології. Методи захисту. Посібник із застосування системи менеджменту захисту інформації»; ISO/IEC 27004 «Інформаційні технології. Методи захисту. Вимірювання»; ISO/IEC 27005 «Інформаційні технології. Методи гарантування безпеки. Управління ризиками інформаційної безпеки»; ISO/IEC 27006 «Інформаційні технології. Методи гарантування безпеки. Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою»; ISO/IEC 27011 «Інформаційні технології. Посібник з управління інформаційною безпекою для телекомунікацій». Серед вітчизняних нормативно-правових актів є: Типове положення про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4-001-2000) [4]; Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (НД ТЗІ 3.7-003-05) [5]; Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (НД ТЗІ 3.7-001-99) [6] та інші.

Дотримання принципів міжнародних стандартів серії ISO 27000 забезпечує керування і контроль за доступом, розробкою й обслуговуванням апаратно-програмних систем [7].

Відповідність вимогам міжнародних стандартів і дотримання національних правових норм з інформаційної безпеки необхідні для сталого розвитку бізнесу.

Мета статті – розкрити мету та завдання служби захисту інформації на підприємстві.

Виклад основного матеріалу. Служба захисту інформації є структурною одиницею підприємства. Структура служби захисту інформації, її склад і чисельність визначаються фактичними потребами інформаційно-телекомунікаційних систем для виконання вимог політики безпеки інформації та затверджуються керівництвом підприємства. Чисельність і склад служби захисту інформації мають бути достатніми для виконання

всіх завдань із захисту інформації в інформаційно-телекомунікаційних системах.

Метою створення служби захисту інформації є організаційне забезпечення завдань керування комплексною системою захисту інформації в інформаційно-телекомунікаційних системах та здійснення контролю за її функціонуванням. На службу захисту інформації покладається виконання робіт із визначення вимог щодо захисту інформації в інформаційно-телекомунікаційних системах, проєктування, розроблення і модернізації комплексної системи захисту інформації, а також з експлуатації, обслуговування, підтримки працездатності комплексної системи захисту інформації, контролю за станом захищеності інформації в інформаційно-телекомунікаційних системах.

Регулятивно-правову основу у вирішенні проблем захисту інформації в інформаційно-телекомунікаційних системах підприємств України різної форм власності становлять: Конституція України [1], відповідні закони України, нормативно-правові акти Президента України і Кабінету Міністрів України, інші нормативно-правові акти з питань захисту інформації, державні та галузеві стандарти, розпорядчі й інші документи організації [2; 3].

Служба захисту інформації повинна здійснювати свою діяльність відповідно до «Плану захисту інформації в інформаційно-телекомунікаційних системах», календарних, перспективних та інших планів робіт, затверджених керівником (заступником керівника) підприємства [9].

На підприємствах, де штатним розкладом не передбачено створення служби захисту інформації, заходи щодо забезпечення захисту інформації в інформаційно-телекомунікаційних системах можуть здійснювати призначені наказом керівника підприємства працівники.

Так, до завдань служби захисту інформації належать:

– захист законних прав щодо безпеки інформації підприємства, окремих її структурних підрозділів, персоналу у процесі інформаційної діяльності та взаємодії один з одним, а також у взаєминах із зовнішніми вітчизняними і закордонними організаціями;

– дослідження технології обробки інформації в інформаційно-телекомунікаційних системах із метою виявлення можливих каналів витоку й інших загроз безпеці інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;

– організація та координація робіт, пов'язаних із захистом інформації в інформаційно-телекомунікаційних системах, необхідність захисту якої визначається її власником або чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

– розроблення проєктів нормативних і розпорядчих документів, чинних у межах підприємства, згідно з якими повинен забезпечуватися захист інформації в інформаційно-телекомунікаційних систем;

– організація робіт зі створення і використання комплексної системи захисту інформації на всіх етапах життєвого циклу інформаційно-телекомунікаційних систем;

– участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів інформаційно-телекомунікаційних систем із питань захисту інформації;

– формування в персоналу і користувачів розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;

– організація забезпечення дотримання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації в інформаційно-телекомунікаційних системах, проведення контрольних перевірок їх дотримання;

– своєчасне виявлення загроз інформації, яка підлягає захисту, причин і умов їх виникнення й реалізації;

– виявлення й максимальне перекриття потенційно можливих каналів і методів несанкціонованого доступу до інформації;

– відпрацьовування механізмів оперативного реагування на загрози, використання юридичних, економічних, організаційних, соціально-психологічних, інженерно-технічних засобів і методів виявлення й нейтралізації джерел загроз безпеці підприємства;

– організація спеціального діловодства, що унеможливлює несанкціоноване одержання конфіденційної інформації [8].

Висновки. Процедура проєктування служби захисту інформації та вибору засобів захисту інформації в інформаційно-телекомунікаційних системах є складним комплексним завданням, у вирішенні якого потрібно врахувати різні типи ймовірних загроз для функціонування інформаційно-телекомунікаційної системи.

У забезпеченні захисту інформації основним елементом є процедура аналізу можливих загроз функціонуванню інформаційно-телекомунікаційних систем, тобто загроз, що підвищують уразливість інформації, яка обробляється інформаційно-телекомунікаційною системою, призводять до її неконтрольованого витоку, випадкового або цілеспрямованого модифікування, знищення.

Засоби системи захисту інформації не варто проєктувати, закуповувати або встановлювати

доти, поки не буде виконаний аналіз ризиків та імовірних загроз. Тільки ґрунтовний аналіз ризиків і загроз надасть можливість об'єктивної оцінки наслідків реалізації загроз, збитків від комерційних втрат, зниження коефіцієнта готовності системи захисту інформації, правових проблем, інформації для визначення найпридатніших методів і засобів гарантування належного рівня безпеки інформаційно-телекомунікаційних систем підприємств.

Служба інформаційної безпеки повинна бути самостійним підрозділом, підкорятися лише першій особі підприємства, здійснювати захист інформації, проєктування, розробки та модернізацію систем захисту інформації, а також забезпечувати контроль над експлуатацією й обслуговуванням підтримки працездатності комплексного захисту інформації.

Проте ніколи не потрібно забувати, що не бізнес існує заради безпеки, а безпека існує заради бізнесу!

Література

1. Конституція України : офіційний текст. Київ : КМ, 2013. 96 с.

2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. № 81/94-ВР. Дата оновлення: 04.07.2017. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 19.08.2020).

3. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657–XII. Дата оновлення: 16.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 19.08.2020).

4. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі (чинне від 4 грудня 2000 р., зі змінами від 28 грудня 2012 р. № 806).

5. НД ТЗІ 3.7-003-05 Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (чинний від 8 листопада 2005 р., № 125).

6. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації (чинний від 2015 р.).

7. ISO/IEC 17799:2000 Information technology – Code of practice for information security management (IDT). URL: https://www.iso.org/standard/39612.html (дата звернення: 19.08.2020).

8. Бондарчук Ю.В., Марущак А.І. Безпека бізнесу: організаційно-правові основи : науково-практичний посібник. Київ : Видавничий дім «Скіф», 2008. 369 с.

9. Гринь А.К. Управління та організація служби захисту інформації : навчальний посібник. Київ : НА СБ України, 2010. 75 с.

Анотація

Шепета О. В., Тугарова О. К. **Основні вимоги до створення служби захисту інформації на підприємстві.** – Стаття.

Перед сучасним приватним підприємством гостро стоїть питання забезпечення захисту інформації, яка циркулює на підприємстві. Це пов'язано з розвитком інформатизації підприємства, з постійним зростанням вартості інформації, з одного боку, і активністю інформаційно-аналітичних структур і різного роду порушників, з іншого. Аналіз наукових публікацій дає підстави стверджувати, що у зв'язку зі збільшенням інформаційних потоків на підприємстві обов'язково треба створювати службу захисту інформації. Натепер захист інформації дедалі більше стосується саме суб'єктів підприємницької діяльності, яким потрібно захищатися від витоку своєї інформації. За результатами негативного впливу на основні властивості інформації (конфіденційність, цілісність, доступність) вирізняють фактори дестабілізації техногенного, антропогенного, природного характеру. Тому діяльність служби захисту інформації підприємства повинна регулюватися нормативно-правовими актами, які створюються керівництвом підприємства, в основі яких доцільно використовувати рекомендації міжнародних стандартів серії ISO 2700 і дотримуватись національних правових норм інформаційної безпеки.

Метою створення служби захисту інформації є організаційне забезпечення завдань керування комплексною системою захисту інформації в інформаційно-телекомунікаційних системах, здійснення контролю за її функціонуванням. На службу захисту інформації покладається виконання робіт із визначення вимог із захисту інформації в інформаційно-телекомунікаційних системах, проєктування, розроблення і модернізації комплексної системи захисту інформації, а також з експлуатації, обслуговування, підтримки працездатності комплексної системи захисту інформації, контролю за станом захищеності інформації в інформаційно-телекомунікаційних системах.

Комплексний захист інформації в інформаційно-телекомунікаційних системах передбачає використання спеціальних правових, фізичних, організаційних, технічних і програмно-апаратних засобів захисту інформації. Контроль за вищевказаними заходами, відповідальність за їх виконання і реалізацію покладається на службу захисту інформації підприємства.

Ключові слова: служба захисту інформації, автоматизована система, комплексна система захисту інформації, персонал, користувач.

Summary

Shepeta O. V., Tuharova O. K. **Basic requirements for creation an information protection service at the enterprise.** – Article.

A modern private enterprise is urgently faced with the information protection ensuring question that is circulating in the enterprise. This is due to the informatization development in the enterprise, with the ever-increasing value of information, on the one hand, and the activity of information-analytical structures of various kinds of violators, on the other.

The scientific publications' analysis gives reason to argue that in connection with the increase in information flows in the enterprise, there is an urgent necessity to create an information protection service. Today, the protection of information is increasingly concerned with business entities that need to protect themselves from the outflow of their information. According to the results of the negative impact on the basic characteristics of information (confidentiality, integrity, accessibility) there are destabilizing factors of man-made, anthropogenic, natural nature. So the enterprise information protection service activity should be regulated by legal acts, created by the enterprise

management. They have to become that foundation on which it is advisable to use the requirements of the international standards of the ISO 27000 series, while the compliance with national legal information security standards is urgently need as well.

The creating an information security service purpose is to organize the management of an integrated information security system in information and telecommunication systems and to monitor its functioning. The information protection service is entrusted with the functions of performing work using information protection requirements in information and telecommunication systems, designing, developing and modernizing an information protection system, as well as operating and maintaining the ability to work, comprehensive information protection, as well as monitoring the state of information security in information and communication systems.

Integrated information protection in information and telecommunication systems is used on the basis of special physical, organizational technical and information protection software-hardware methods. Control over these methods, responsibility for their execution and implementation is in the area of authority of the enterprise information protection service.

Key words: information security service, automated system, comprehensive information security system, personnel, user.