УДК 004.73056.5(045)
DOI: 10.31891/2307-5740-2020-286-5-44

ЯРЕМКО С.МА., КУЗЬМІНА О. М.
Вінницький торговельно-економічний інститут

АКТУАЛЬНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ БІЗНЕС-СТРУКТУР

У статті розглянуто основні поняття інформаційної безпеки; досліджено джерела загроз інформаційним ресурсам підприємства, зокрема антропогенних, техногенних та стихійних; висвітлено особливості комплексної системи інформаційної безпеки; здійснено аналітичний огляд найбільш поширених у світі платформ для захисту корпоративної інформації. Це дозволило виявити переваги і недоліки сучасних засобів захисту інформаційних ресурсів та розробити ряд рекомендацій щодо удосконалення організації захисту підприємницької інформації.

В цілому, можна відзначити, що розроблення та впровадження методів та засобів захисту інформаційних ресурсів є безумовно одним із важливих питань для бізнес-структур, оскільки вони є сучасним та ефективним засобом забезпечення цілісності, доступності та конфіденційності інформаційних потоків підприємства.

Ключові слова: інформаційна безпека, суб'єкт безпеки, бізнес-структура, джерело загрози, комплексна система інформаційної безпеки підприємства, платформи засобів захисту інформації.

YAREMKO S., KUZMINA O.
Vinnytsia Institute of Trade and Economics

CURRENT ASPECTS OF PROTECTION INFORMATION RESOURCES OF BUSINESS STRUCTURES

The article considers the basic concepts of information security; the sources of threats to the information resources of the enterprise, in particular anthropogenic, technogenic and natural; features of complex information security system are covered; an analytical review of the world's most common platforms for the protection of corporate information.

This allowed to identify the advantages and disadvantages of modern means of protection information resources and to develop a number of recommendations for improving the organization of protection business information.

It was found that information protection measures at the enterprise are mainly related to counteracting unauthorized receipt of information by technical means.

It is established that at present in business structures the information is protected in various ways. These include protection of programs from reading and copying, protection of copyright on information, protection against unauthorized access and launch of programs, self-testing and self-recovery of running program code and other means capable of ensuring the integrity, accessibility and confidentiality of information. However, the advantage is a comprehensive information security system that comprehensively covers vulnerabilities and provides protection both externally and internally. This provides a flexible combination of the necessary software and hardware and organizational measures. The construction of such a system involves not only its assembly from specialized tools from different manufacturers, as a designer, but also the implementation of a single concept of information security. It is a comprehensive conceptual analysis of the information system then allows you to develop an optimal policy to ensure this security.

In general, it can be noted that the development and implementation of methods and means of protection information resources is certainly one of the important issues for business structures, as they are a modern and effective means of ensuring the integrity, accessibility and confidentiality of information flows.

Keywords: information security, security entity, business structure, threat source, complex information security system of the enterprise, information security platforms.

Вступ. У сучасному світі інформація стає найдорожчим активом у житті людини та суспільства загалом. В епоху інформаційних технологій стає можливим майже миттєво отримувати інформацію, яка з'являється кожну секунду в різних куточках світу, зокрема щодо укладених торговельних угод, коливання валют і цінних паперів, запуску нових бізнес-проектів та багато іншого. У зв'язку із цим, все більшої актуальності набуває питання захисту інформаційних ресурсів бізнес-структур засобами сучасних інформаційних технологій і систем. При цьому основною метою створення системи захисту інформації стає забезпечення надійного зберігання та ефективного використання інформації в діяльності бізнес-структур.

Аналіз останніх досліджень і публікацій. Проблемам розробки та впровадження систем захисту інформаційних ресурсів присвячені праці таких вітчизняних та зарубіжних вчених, як Р. Калюжний, Г. Почепцов, Б. Кормич, П. Жарков. І. Панарів, А. Тер-Акопов, В. Ярчкин та ін. Проте питання безпеки інформаційних ресурсів, технологій, методів і засобів, що застосовуються для захисту інформації залишаються актуальними і потребують подальших досліджень.

Постановка завдання. Метою статті є проведення аналітичного огляду сучасних аспектів захисту інформаційних ресурсів бізнес-структур та визначення напрямків оптимізації існуючих методів та засобів забезпечення цілісності, доступності та конфіденційності інформації.

Результати дослідження. На початку розгляду суті та основних понять інформаційної безпеки варто зазначити, що вони з'явилося в кінці 80-х років. В працях німецького вченого Г. Одермана комплексно розглядалися проблеми безпеки, пов'язані з інформаційними загрозами. А у вітчизняній і

зарубіжній пресі з кінця 1991 – початку 1992 року спостерігалась тенденція до відкритого дослідження проблеми інформаційної безпеки як окремого питання [2].

Цікавий погляд на поняття «інформаційна безпека» навів у своїх працях відомий український дослідник Калюжний Р.А., який вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані зі створенням, зберіганням, поширенням і використанням інформації [5, с. 18].

Інформаційна безпека (ІБ) – це стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема, власникам і користувачам інформації та інфраструктури [4].

В Українській законодавчій базі термін «інформаційна безпека» наведено у Концепції національної програми інформатизації, затвердженій Законом України від 4 лютого 1998 року № 75/98, де «інформаційна безпека» – невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, телекомунікації, канали інформаційного обміну, функціонування телекомунікаційних мереж і систем та інші елементи інформаційної інфраструктури країни» [4]. З інформаційної точки зору суб'єкт бізнесу являє собою комплекс компонентів, пов'язаних між собою єдиною метою, структурними відносинами, технологіями інформаційного обміну. Зазначені компоненти в процесі функціонування суб'єкта можуть змінюватися, на них можуть впливати різного роду внутрішні і зовнішні чинники, які складно прогнозувати і оцінювати. Всі компоненти можна сформувати в чотири групи:

– персонал;
– технічні засоби інформатизації;
– програмне забезпечення;
– документи і вважати як об'єкти захисту інформації [3].

З цією метою суб'єкти, що мають потребу в підтвердженні юридичної вагомості переданого повідомлення, домовляються про прийняття деяких атрибутів інформації, що описують і здатність бути юридично значимою. Дана властивість інформації особливо актуальна в системах електронних платежів, де здійснюється операція з пересилання коштів.

Актуальність даної вимоги виникла завдяки появі таких понять, як електронні гроші та Internet-banking. Так, для авторизації доступу до електронної платіжної системи користувач повинен надати деякі відомості, що однозначно його ідентифікують. У процесі розвитку даних систем може з'явитися реальна небезпека, що, наприклад, усі платіжні операції будуть контролюватися, тим самим виникнуть умови для тотального стеження за користувачами ІС.

Використання всесвітньої мережі та нових технологій супроводжується такими явищами, як низький рівень культури безпеки, збільшення онлайн-користувачів і залежності від цифрової інфраструктури, поширення небажаного контенту, розвиток кібер-шахрайства, витоки інформації, втрата даних, несанкціонований доступ до інформації. Кібервійни та кібертероризм набувають глобального характеру та вираженої динаміки, що ускладнює їх виявлення та можливості протидії [8].

По суті, сучасна корпоративна безпека мало чим відрізняється від давньої. Змінюються лише реалії, в яких бізнесмени повинні вести свою справу. Будь-яка компанія хоче бути надійно захищена не тільки від зовнішніх загроз, а й від внутрішніх. Цю проблему і вирішують фахівці з корпоративної та інформаційної безпеки. Перед ними стоїть завдання проводити цілий комплекс заходів, що включають в себе практично всі сфери життя компанії: захист комерційної таємниці; внутрішня робота із співробітниками; внутрішня контррозвідка; службові розслідування; економічна безпека; технічна підтримка та фізичний захист.

Захист інформації на підприємстві є дуже важливим і цей аспект повинен бути обов'язковим при укладенні контракту компанією з її працівником, особливо якщо цей працівник займає керуючу посаду в компанії. Небезпека, в першу чергу, загрожує інформації, що зберігається в інформаційних системах підприємства. У цю систему входять програмне забезпечення автоматизованої системи, програми для виконання конкретних завдань компанії, програмні оболонки, текстові редактори, пакети програм, бази даних. Інформація може надходити по локальній мережі з пристрою введення, а саме з клавіатури, з зовнішнього середовища, а саме з мережі Інтернет, за системою SWIFT, від інших компаній. Щоб гарантувати безпеку інформаційної системи підприємства, необхідно наділення повноважень зареєстрованим користувачам, серед яких можуть бути як певні особи, так і організації. Ці користувачі можуть здійснювати тільки зумовлені дії з використанням інформаційних технологій [9].

Небезпека інформації на підприємстві виникає з певних джерел (див. рис. 1).

Деякі керівники компаній уявляють собі систему захисту інформації як якийсь пристрій або програму, яка, будучи одного разу встановлена, вирішить всі їхні проблеми на багато років вперед. Хотілося б застерегти від подібної омани, так як, слідуючи таким принципам і встановлюючи «комплекс захисту» з коробки, компанія, безумовно, отримує ряд захисних функцій, але далеко не завжди адекватних, необхідних і достатніх в конкретній ситуації. При цьому тим більш неприємним є отримання на тлі часом значних витрат хибного відчуття безпеки.

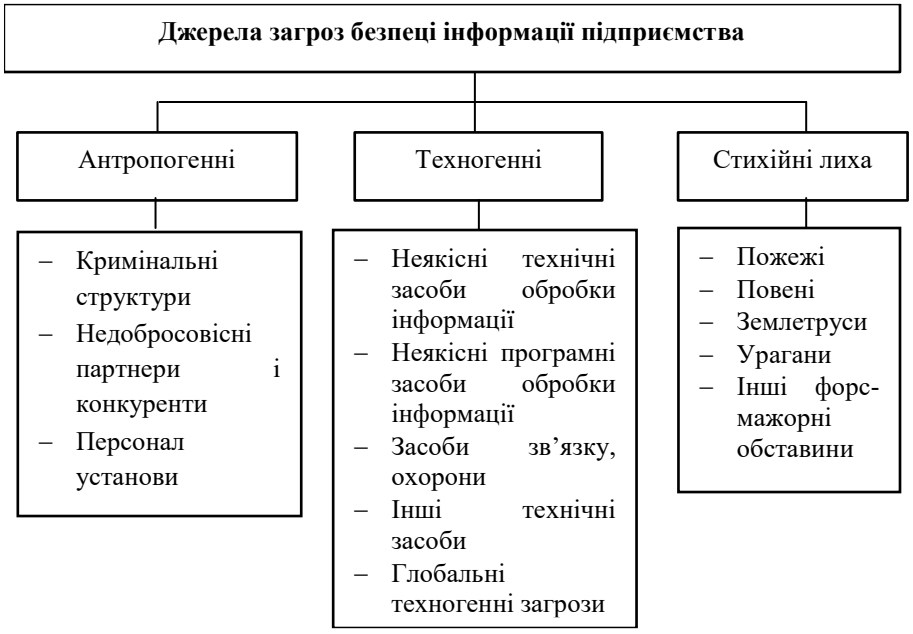

Рис. 1. Джерела небезпеки для інформації на підприємстві

Основні переваги комплексної системи інформаційної безпеки – це всебічне охоплення слабких місць, захист як зовні, так і зсередини, гнучке поєднання необхідних програмно-технічних і організаційних заходів. Побудова такої системи передбачає не просто її складання зі спеціалізованих засобів від різних виробників, як з конструктора, а й реалізацію єдиної концепції інформаційної безпеки. Саме всебічний концептуальний аналіз ІС дозволяє потім виробити оптимальну політику забезпечення цієї безпеки.

Малий бізнес часто використовує в якості захисту безкоштовні антивіруси або рішення, призначені для домашніх користувачів, але коли компанія доростає до певного масштабу, їй потрібні інші, спеціалізовані рішення, щоб грамотно управляти захистом свого підприємства.

Однією з головних турбот керівників, власників підприємств або фірм різних форм власності є забезпечення стабільної діяльності своїх виробничих об'єктів – підприємств, офісів, банків, магазинів тощо. Але стабільна робота будь-якої фірми чи підприємства неможлива без надійного захисту від дій, збитки від яких можуть бути дуже великі.

Таблиця 1

Платформи засобів захисту інформації

Найменування платформи	Коротка характеристика
InfoWatch ARMA, комплексної системи забезпечення кібербезпеки АСУ ТП	InfoWatch ARMA захищає критичну інформаційну інфраструктуру від загроз, що створюються зовнішніми і внутрішніми порушниками і виникають при поєднанні різних систем захисту. До складу рішення включені три продукти (Industrial Firewall, Industrial Endpoint і Management Console), що дозволяють побудувати захист для промислових сегментів на рівні як мережі, так і кінцевих пристроїв. Розслідування інцидентів відбувається в єдиному інтерфейсі, процес реагування автоматизований
Group-IB Fraud Hunting Platform, системи для боротьби з шахрайством	Group-IB Fraud Hunting Platform здатна працювати в високонавантаженому режимі, обробляючи десятки мільйонів запитів до Інтернет-ресурсів і мобільних додатків і одночасно блокуючи на них шкідливу активність. Система не тільки дозволяє виявляти шахрайство на ранній стадії, але і виступає в якості технології для скорочення витрат на Cool-центр, SMS-оповіщення, розширення операційних лімітів
«Паспорти ПО», системи контролю конфігурацій робочих місць	Система «Паспорт ПО» від ОКБ САПР призначена для контролю змін конфігурацій АРМ співробітників підприємств. Через можливість випадкового або навмисного втручання в програмну конфігурацію пристроїв, як з боку зовнішніх, так і внутрішніх зловмисників, може бути порушена безпека інформаційної інфраструктури. Даний програмний модуль призначений для протидії цьому вектору атак
Мережева пісочниця PT Sandbox	PT Sandbox - пісочниця від компанії Positive Technologies - відрізняється можливістю гнучко налаштовувати віртуальні середовища таким чином, щоб вони відповідали реальним робочим станціям: завантажувати в них крім стандартного офісного пакету спеціалізований «софт» і певні версії ПЗ, що використовуються в організації. Ця особливість поряд з глибоким комплексним аналізом файлів дозволяє продукту забезпечувати захист від цільових і масових атак, що супроводжуються застосуванням невідомих шкідливих програм і загроз
SafeNet Authentication Service, системи для впровадження корпоративного сервісу двофакторної аутентифікації	SafeNet Authentication Service - програмний комплекс, що дозволяє реалізувати двофакторну аутентифікацію для доступу до корпоративних ресурсів за допомогою одноразових паролів, що доставляються користувачеві великою кількістю способів. Поряд з цим він підтримує легку масштабованість, управління ризиками та повноцінний аудит. Також система забезпечує повністю автоматизовану аутентифікацію з гнучкими можливостями для налаштувань, адаптованих до потреб конкретної організації, що істотно знижує загальну вартість експлуатації. Програмний комплекс призначений для локальної установки, тоді як ті ж функції в хмарі надає сервіс SafeNet Trusted Access

На даний час на ринку програмних продуктів є ціла низка програм для безпеки. При цьому ринок програмних продуктів постійно поповнюються і видозмінюються, а також з'являються абсолютно нові, що враховують досвід раніше створених. Доречно також зазначити, що такого роду програми наповнюються великою кількістю окремих функціональних можливостей. Перелік найбільш відомих платформ наведені в таблиці 1. Потрібно також враховувати, що функції підсистеми захисту інформації є допоміжними по відношенню до основних функцій ІС. Робота усіх компонентів системи захисту не повинна негативно позначатися ні на продуктивності самої системи, ні на зручності роботи в ній.

Щоб система захисту відповідала таким умовам, вимоги до неї повинні формуватися на основі аналізу завдань, покладених на інформаційно-обчислювальну систему в цілому.

Зрозуміло, що застосування технічних засобів захисту інформації в жодному разі не замінює собою спеціаліста, який контролює сигнали, отримані за допомогою відповідних пристроїв, у разі порушення рубежів захисту. В останні роки з'явилася можливість підійти до вивчення проблеми захисту підприємницької інформації комплексно, оскільки переважна більшість опублікованих робіт присвячена або конкретним системам захисту інформації, або її окремим аспектам [7].

Уявлення про інформаційну безпеку дедалі поглиблюються. Однак принципове значення має правильне розуміння меж захищеності підприємницької інформації та фізико-технічних основ, спеціально розроблених технічних засобів і винайдених тактичних прийомів.

Заходи щодо захисту інформації на підприємстві головним чином повинні бути пов'язані з протидією несанкціонованого отримання інформації за допомогою технічних засобів.

Одну з головних ролей у забезпеченні інформаційної безпеки підприємств різних організаційно-правових форм (малих підприємств, науково-виробничих об'єднань, фінансово кредитних установ і т. д.) відіграють принципи організації системи захисту комерційної таємниці, методики комплексного контролю і перевірки захищеності інформації, якісний аналіз основних завдань захисту інформації [1].

Загалом захист інформації здійснюється різними способами. До них відносяться захист програм від читання і копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу та запуску програм, самотестування і самовідновлення коду програм, що виконуються та інші засоби, що здатні забезпечити цілісність, доступність та конфіденційність інформації.

На основі усього наведеного можна виділити ряд рекомендацій щодо організації заходів стосовно захисту підприємницької інформації:

– забезпечення розмежування доступу до інформації, що використовується в системі підприємства;

– обмеження доступу до інформації, що вважається комерційною таємницею;

– використання багаторівневої ідентифікації для доступу до засекреченої інформації її власником або уповноваженим ним органом;

– застосування комплексних заходів для контролю захищеності інформації, що є власністю підприємства.

Висновки. Отже, забезпечення інформаційної безпеки бізнес-структур полягає у здійсненні постійного контролю за джерелами виникнення потенційних загроз (антропогенні, технологічні та стихійні джерела) та необхідності здійснювати захист інформації різними способами (захист програм від читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу і запуску програм). Захист інформації на основі системи інформаційної безпеки є найбільш поширеним варіантом організації останньої, інколи навіть тотожним самій безпеці. На даний час заходи захисту інформації поширюються на економічну, правову, кадрову, організаційно-управлінську, технічну сфери діяльності суб'єктів підприємництва. Тобто, існує певний комплекс, об'єднаний в досить розвинену систему заходів захисту інформації. Разом з тим, як показує аналіз ефективності функціонування такої системи тут досить багато проблем, насамперед в організації захисту інформації. Сучасні системи захисту інформації досить складні, дорогі і не зовсім надійні, що потребує подальших заходів щодо їх удосконалення.

Література

1. Грушо А.А. Теоретические основы защиты информации / Грушо А.А., Тимонина Е.Е. – М. : Издательство агентства «Яхтсмен», 2001. – 76 с.

2. Про концепцію національної програми інформатизації : закон України // Відомості Верховної Ради України. – 1998. – № 27-28.

3. Зубок М.І. Інформаційна безпека в підприємницькій діяльності : навч. посібник / Зубок М.І. – К. : КНТЕУ, 2006. – 115 с.

4. Лужецький В.А. Основи інформаційної безпеки : навч. посібник / Лужецький В.А., Кожухівський А.Д., Войтович О.П. – Вінниця : ВНТУ, 2006. – 115 с.

5. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / Ліпкан В.А. Максименко Ю.Є., Желіховський В.М. – К. : КНТ, 2006. – 280 с.

6. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности / Щербаков А.Ю. – М. : Нолидж, 2001. – 150 с.

7. Соснін А.С. Менеджмент безпеки підприємництва / Соснін А.С., Пригунов П.Я. – К. : Європейський ун-т, 2002. – 128 с.

References

1. Grusho A.A. Teoreticheskie osnovy zashity informacii / Grusho A.A., Timonina E.E. – M. : Izdatelstvo agentstva «Yahtsmen», 2001. – 76 s.

2. Pro kontseptsiiu natsionalnoi prohramy informatyzatsii : zakon Ukrainy // Vidomosti Verkhovnoi Rady Ukrainy. – 1998. – № 27-28.

3. Zubok M.I. Informatsiina bezpeka v pidpryiemnytskii diialnosti : navch. posibnyk / Zubok M.I. – K. : KNTEU, 2006. – 115 s.

4. Luzhetskyi V.A. Osnovy informatsiinoi bezpeky : navch. posibnyk / Luzhetskyi V.A., Kozhukhivskyi A.D., Voitovych O.P. – Vinnytsia : VNTU, 2006. – 115 s.

5. Lipkan V.A. Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii : navchalnyi posibnyk / Lipkan V.A. Maksymenko Yu.Ie., Zhelikhovskyi V.M. – K. : KNT, 2006. – 280 s.

6. Sherbakov A.Yu. Vvedenie v teoriyu i praktiku kompyuternoj bezopasnosti / Sherbakov A.Yu. – M. : Nolidzh, 2001. – 150 s.

7. Sosnin A.S. Menedzhment bezpeky pidpryiemnytstva / Sosnin A.S., Pryhunov P.Ia. – K. : Yevropeiskyi un-t, 2002. – 128 s.

Надійшла / Paper received: 20.09.2020 Надрукована / Paper Printed : 05.11.2020