DOI: https://doi.org/10.36059/978-966-397-259-6-23

ЗНАЧЕННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ

Янчук Т.В.
кандидат економічний наук, доцент,
доцент кафедри маркетингу та бізнес-аналітики
Донецького національного університету імені Василя Стуса
м. Вінниця, Україна

Проблема процесу захисту інформації не є новою. Реалії сьогодення підвищують актуальність даного питання для сучасного підприємства.

Економічні та юридичні питання, приватна та комерційна таємниця, національна безпека – усе це зумовлює необхідність захисту інформації. Згідно із Законом України «Про захист інформації в автоматизованих системах» захист інформації – це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації та осіб, які користуються інформацією. У літературі вживаються також споріднені терміни «безпека інформації» та «безпека інформаційних технологій». Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації під час війни [1].

Розуміння поняття «захист інформації» є важливим завданням сьогодення. Враховуючи, що відбувається сьогодні в Україні та в світі – інформаціє стає ще більш значущою. Для того, що б розуміти та використовувати достовірну інформацію, актуальну, перевірену та глибинну – необхідно знати та вміти нею користуватися. При цьому захищати свою інформацію від несанкціонованого доступу та витоку з підприємств. Сутність самого поняття проявляється у вираженні процесу управління загрозами та небезпеками. Тобто, процес управління загрозами та небезпеками в інформаційному полі [4]. Найважливіша мета інформаційної безпеки – це надання безпеки системи в цілому, її захист і гарантія точності. Якщо вона модифікується або руйнується, то ці руйнування треба мінімізувати [3].

Питання захисту інформації на сучасних підприємствах розглядається як науковцями, так і практиками. Найбільш відомими є праці Н. Задорожнюка, О. Бурячка, Р. Калюжного, К. Коваленко,

Г. Почепцова, Л. Пашнюк, Б. Кормича, І. Панаріва, А. Тер-Акопова, В. Ярчкина тощо [1–6].

Ефективний розвиток інформаційного суспільства можливий лише завдяки тому, що кожен суб'єкт інформаційних відносин чи то на підприємстві, чи на державному рівні, має усвідомити наскільки важливим є забезпечення інформаційної безпеки, також мають бути створенні передумови для запровадження сучасного технічного та програмного забезпечення, здатного швидко реагувати на «непідконтрольні» атаки.

Слід зазначити, що у науковій літературі поки бракує єдиного визначення захисту інформації. Для одних науковців поняття «Захист інформації» відображається стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію. Для інших враховують різницю між інформаційною безпекою та безпекою інформації.

Розглянемо класифікацію можливих загроз для інформації (табл. 1).

Таблиця 1

Класифікація загроз для інформації

№	Загрози	Методи боротьби
1	Наслідки стихійних лих і техногенних катастроф	Резервування апаратного забезпечення (дзеркальні файлові та web-сервери, географічно рознесені); резервні копії інформації
2	Відмови обладнання	Резервування апаратного забезпечення; резервні копії інформації; вибір надійного постачальника апаратного забезпечення; вчасна профілактика та ремонт апаратного забезпечення
3	Наслідки помилок проектування системи захисту	Залучення ліцензованих спеціалістів для побудови та експертизи системи захисту; обов'язкова експертиза проекту; періодичний аудит системи захисту
4	Наслідки помилок персоналу	Ретельне підбирання персоналу; навчання персоналу; створення системи адміністративних стягнень за порушення; створення позитивного мікроклімату в колективі
5	Навмисні дії порушників	Залежно від способу дій

Джерело: [1–6]

Основне завдання захисту інформації полягає в тому, щоб злам системи відбувся якомога пізніше та/або не мав суттєвих наслідків для її функціонування й використання інформації, що нею циркулює. Це правило існує роками і має універсальний характер. Деякі з завдань захисту інформації на підприємстві розглянемо у вигляді рисунку 1.

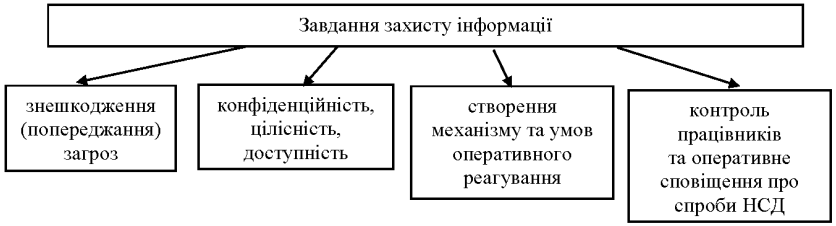

Рис. 1. Завдання захисту інформації

Джерело: [6]

Маючи обґрунтовані надії на стійкість системи захисту інформації, краще, все ж таки, пам’ятати основне правило захисту інформації: жодна система захисту не може довгий час протистояти цілеспрямованим діям озброєного сучасними технологіями кваліфікованого порушника.

Щодо видів захисту, то їх об'єднують у групи [4–6]: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні (рис. 2).

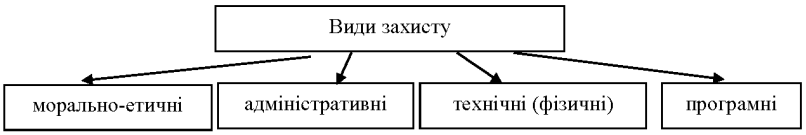

Рис. 2. Види захисту

Сучасний ринок програмних продуктів містить різні програми для забезпечення інформаційної безпеки. Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, криптографічний захист інформації, захист від комп'ютерних вірусів тощо. Такі програми можна поділити на системні та прикладні програми.

Всі розуміють, що основні переваги комплексної системи інформаційної безпеки полягає в всебічному охопленні слабких місць.

Захист має здійснюватися враховуючи зовнішні та внутрішні небезпеки, тому вважається необхідним поєднувати і програмні, і технічні, і різного роду організаційні засоби і заходи. Важливість побудова такої системи передбачає реалізацію єдиної концепції інформаційної безпеки. Саме всебічний аналіз даних та інформаційного забезпечення дозволяє виробити оптимальну політику забезпечення цієї безпеки.

Захист інформації не обмежується лише завдяки використанню технічних засобів. Треба враховувати людський фактор. Можна сказати, що на надійність системи безпеки впливає багато чинників, в тому числі і відношення персоналу до безпеки інформації. Звичайно, і відношення і намагання використовувати досконалу систему безпеки складають основу ефективного використання комп'ютерних систем.

Підсумовуючи викладене, можна сказати, що кожен підхід і засіб захисту інформації по різному впливають на захист та безпеку інформації і відповідно на діяльність підприємства чи організації. Не можна недооцінювати тих, хто бажає заподіяти шкоду підприємству завдяки недосконалій системі захисту інформації. Тому важливо здійснювати управління інформацією на підприємстві з врахуванням всіх новітніх досягнень програмного, технічного та іншого напрямку забезпечення інформаційної безпеки.

Список використаних джерел:

1. Задорожнюк Н.О. Сучасні технології бізнес-аналітики. *Економічна аналітика: сучасні реалії та прогностичні можливості : збірник матеріалів міжнар. наук.-прак. конф. (*Київ, 19 квітня 2019 р.). Київ, 2019. С. 105–107.

2. Коваленко В.В. Ризики в системі економічної безпеки підприємства та засоби їх нейтралізації. *Вчені записки Університету «КРОК».* 2018. № 3(51). С. 175–180.

3. Найгучніші хакерські атаки, які сколихнули всю Україну: вражаючі деталі. 24 канал. 2018. URL: https://24tv.ua/nayguchnishi_hakerski_ataki_yaki_skolihnuli_vsyu_ukrayinu_vrazha yuchi_detali_n1079849 (дата звернення: 17.03.2022).

4. Пашнюк Л. Загрози економічній безпеці підприємства та засоби їх нейтралізації *Вісник Київського національного університету імені Тараса Шевченка. Серія : Економіка*. 2013. Вип. 10(151). С. 93–97.

5. Поняття, сутність, значення захисту інформації. URL: http://www.infobezpeka.com/publications/?id=102 (дата звернення: 15.03.2022).

6. Рівні захисту інформації: поняття, основні принципи, аналіз ризиків та їх усунення. URL: http://hi-news.pp.ua/kompyuteri/16972-rvn-zahistu-nformacyi-ponyattya-osnovn-principi-analz-rizikv-ta-yih-usunennya.html (дата звернення: 23.08.2022).