Кавин Ольга Миколаївна
аспірантка кафедри фінансово-економічної безпеки
Українська академія друкарства, Україна

Кавин Святослав Ярославович
ORCID ID: 0000-0002-6189-3848
аспірант кафедри міжнародних відносин і дипломатичної служби
Львівський національний університет імені Івана Франка, Україна

Кавин Богдан Ярославович
магістрант факультету компютерної поліграфічної інженерії
Українська академія друкарства, Україна

Кавин Ярослав Михайлович
кандидат технічних наук, доцент кафедри автоматизації та компютерно-інтегрованих технологій, Начальник управління міжнародних зв'язків
Українська академія друкарства, Україна

СУТНІСТЬ ІНФОРМАЦІЙНО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Анотація. *Стаття присвячена розкриттю сутності поняття "інформаційно-економічної безпеки" в межах об'єктів дослідження, а саме соціально-економічних систем на мікрорівні (підприємств). У статті розглянуто питання забезпечення інформаційної безпеки суб'єктів економічних відносин, зміст елементів, методів і засобів захисту інформаційних ресурсів. Крім того виділені проблеми, що перешкоджають досягненню інформаційної безпеки в сфері економіки, а також представлено методи ліквідації інформаційних загроз і їх класифікація.*

Ключові слова: *інформаційно-економічна безпека, диджиталізація, інформаційний простір, економічна система, захист інформації, економічні відносини.*

У зв'язку із стрімким розвитком інформаційних технологій і глобальною диджиталізацією соціально-економічних відносин, сутєво зросло значення

інформації для економіки. У сучасних умовах процес успішного функціонування і економічного розвитку підприємства залежить від прийняття якісних і своєчасних управлінських рішень, які формуються на основі ретельного і всебічного аналізу інформації, що надходить як з внутрішнього, так і з зовнішнього середовища. По суті, інформація стала одним з важливих управлінських ресурсів. [1],[2],[3]. Її накопичення і споживання закладено в основу ефективного функціонування і розвитку як економіки в цілому, так і підприємництва загалом.

Разом з тим із зростанням ролі інформації, сформувався інформаційний простір, який вимагає захисту від несанкціонованого або ненавмисного впливу як на рівні держави, так і на рівні окремих підприємств. А з розвитком інформаційного суспільства, в якому здійснюють свою діяльність більшість суб'єктів ринкової економіки, інформація і всі основні складові процесу інформатизації набувають все більшої значущості. В економічній діяльності максимальний і ефективний захист інформації дає можливість отримувати високі доходи, укладати вигідні контракти з контрагентами, істотно підвищує рівень конкурентоспроможності підприємства, а також дозволяє значно підвищити ефективність діяльності організації в цілому. [4].

Загрози збереження, цілісності і конфіденційності інформаційних ресурсів обмеженого доступу практично реалізуються через ризик утворення каналу несанкціонованого отримання (добування) кимось цінної інформації і документів. Відповідно забезпечення інформаційної безпеки має починатися з виявлення суб'єктів економічних відносин, пов'язаних з використанням інформаційних систем. Спектр їхніх інтересів може бути розділений на наступні основні категорії: доступність (можливість за прийнятний час отримати необхідну інформаційну послугу), цілісність (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованого зміни), конфіденційність (захист від несанкціонованого ознайомлення).

У зв'язку з цим інформаційна безпека є невід'ємним елементом системи економічної безпеки. Відповідно комплексна інформаційна безпека виступає

запорукою забезпечення економічної безпеки підприємства.

Інформаційна безпека з точки зору економічної безпеки є стан захищеності діяльності організації та її інформаційного середовища від негативного впливу дестабілізуючих факторів, яке забезпечує збереження основних властивостей інформації та досягнення соціально-економічних цілей створення організації [5],

До об'єктів інформаційної безпеки в організації відносять [7]:

– інформаційні ресурси, що містять відомості, віднесені до комерційної таємниці, та конфіденційну інформацію, представлену у вигляді інформаційних масивів і баз даних;

– засоби та системи інформатизації - засоби обчислювальної та організаційної техніки, мережі та системи, загальносистемное і прикладне програмне забезпечення, автоматизовані системи управління, системи зв'язку і передачі даних, технічні засоби збору, реєстрації, передачі, обробки та відображення інформації.

До основних загроз безпеки відносять [8]:

– розкриття конфіденційної інформації;

– несанкціоноване використання інформаційних ресурсів;

– помилкове використання ресурсів;

– несанкціонований обмін інформацією;

– злом системи;

Система захисту інформації являє собою організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз. [9] З позицій системного підходу до захисту інформації пред'являються певні вимоги:

– забезпечення безпеки інформації - це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення та розвитку системи захисту, безперервному контролі її стану, виявлення її вузьких і слабких місць і протиправних дій;

– планування безпеки інформації здійснюється шляхом розробки кожною службою детальних планів захисту інформації в сфері її компетенції;

– захисту підлягають конкретні дані, об'єктивно що підлягають охороні, втрата яких може заподіяти організації певної шкоди;

– методи і засоби захисту повинні надійно перекривати можливі шляхи неправомірного доступу до інформації;

– ефективність захисту інформації означає, що витрати на її здійснення не повинні бути більше можливих втрат від реалізації інформаційних загроз;

– чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;

– забезпечення контролю цілісності засобів захисту і негайне реагування на їх вихід з ладу.

Система захисту інформації, як будь-яка система, повинна мати певні види власного забезпечення, спираючись на які вона буде виконувати свою цільову функцію. [10] З огляду на це система захисту інформації може мати:

– правове забезпечення. Сюди входять нормативні документи, положення, інструкції, керівництва, вимоги яких є обов'язковими в рамках сфери дії;

– організаційне забезпечення. Мається на увазі, що реалізація захисту інформації здійснюється певними структурними одиницями, такими як: служба безпеки, служба режиму, служба захисту інформації технічними засобами та ін .;

– апаратне забезпечення. Передбачається широке використання технічних засобів, як для захисту інформації, так і для забезпечення діяльності власне системи захисту інформації;

– інформаційне забезпечення. Воно включає в себе документовані відомості (показники, файли), що лежать в основі рішення задач, що забезпечують функціонування системи;

– програмне забезпечення. До нього відносяться антивірусні програми, а також програми (або частини програм регулярного застосування), що реалізують контрольні функції при вирішенні облікових, статистичних, фінансових, кредитних та інших задач;

– математичне забезпечення. Передбачає використання математичних методів для різних розрахунків, пов'язаних з оцінкою небезпеки технічних

засобів зловмисників, зон і норм необхідного захисту;

– нормативно-методичне забезпечення. Сюди входять норми і регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації;

– ергономічне забезпечення. Сукупність засобів, що забезпечують зручності роботи користувачів апаратних засобів захисту інформації.

Беручи до уваги той факт, що досягнення певного рівня інформаційної безпеки гарантує відповідний рівень економічної безпеки, можна зробити висновок про те, що поняття "інформаційна-економічна безпека" об'єднує тісно пов'язані між собою різні стани діяльності організації, які гарантують її стабільний і прогресивний розвиток. Відповідно можна зазначити, що інформаційно-економічна безпека - це стан захищеності діяльності організації та її інформаційного середовища від негативного впливу дестабілізуючих факторів, який забезпечує збереження основних властивостей інформації і дозволяє досягти соціально-економічні цілі створення організації.

Список джерел:

1. Гомалеев А.О. Информационная безопасность как составляющая экономической безопасности организации/ Научно-практический электронный журнал Аллея Науки» № 10 (26) 2018
2. Горбунова О.Н., Обидина Н.В. Роль и значение информационной безопасности в экономике/ Научные труды КубГТУ, № 6, 2018
3. Тахтаева Р.Ш., Аргынбеков И.Б., Самыжан К.Н. Экономические аспекты информационной безопасности на мировой арене/ Фундаментальные исследования № 5, 2018
4. Тимаев Р.А. Понятие информационно-экономической безопасности предприятия // Культура народов Причерноморья. – 2014. – № 278, Т. 1. – С. 64 - 69.
5. Ясенев В.Н. Информационная безопасность в экономических системах: Учебное пособие – Н. Новгород: Изд-во ННГУ, 2016. - 253 с
6. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К. : ООО ТИД Диа Софт, 2004. – 992 с.
7. Казанцев С. В. Экономическая безопасность. Определение понятий / С. В. Казанцев // Мир новой экономики. – 2014. – № 2. – Р. 48–53.

8. Козаченко А. В. Экономическая безопасность предприятия : сущность и механизм обеспечения : монография / А. В. Козаченко, В. П. Пономарев, А. Н. Ляшенко. – К. : Либра, 2003. – 280 с.
9. Кузьмина Н. В. Экономическая безопасность в системе оценки функционирования предприятия / Н. В. Кузьмина // Экономика и управление. – 2013. – № 1. – С. 55–58.
10. Information technology – Security techniques – Information security management systems. – Overview and vocabulary : ISO/IEC 27000:2009. –2009.