УДК 338.55

ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Смачило Т.В., Кахній М.І.
Тернопільський національний економічний університет

Досліджено теоретичні аспекти інформаційної безпеки підприємства. Обґрунтовано важливість впливу інформаційної безпеки підприємства на його конкурентоспроможність на ринку виробництва, збуту товарів і послуг. Охарактеризовано важливість системи інформаційної безпеки для мінімізації можливості нанесення шкоди інформаційній інфраструктурі підприємства. Виокремлено основні принципи системи інформаційної безпеки. Розглянуто етапи управління інформаційною безпекою підприємства.
Ключові слова: підприємство, інформація, інформаційна безпека, система інформаційної безпеки, управління, конфіденційність, цілісність, доступність.

Постановка проблеми. Забезпечення сталого розвитку вітчизняних підприємств в умовах нестабільності та кризи ускладнюється чинниками, серед яких все більшого значення набувають загрози інформаційного характеру. Інформація – це найбільший щодо обсягу та один із найважливіших ресурсів підприємства. За її допомогою досягається, з одного боку, як забезпечення безпеки, конкурентоспроможності, сталого розвитку підприємства, а з іншого – вона може бути загрозою для його функціонування.

В сучасних умовах інформаційної доби XXI ст. інформаційна безпека підприємства набуває все вагомішого значення, а питання її забезпечення стають все більше гострішими. Підприємства, які не можуть забезпечити власну інформаційну безпеку, стають неконкурентоспроможними на ринку виробництва, збуту товарів і послуг. Можна стверджувати, що банкрутство підприємств відбувається в тому числі і через неспроможність ефективного управління та невідповідність інформаційної структури новим умовам господарювання. Незаперечним є те, що будь-яке підприємство повинне мати систему інформаційної безпеки, яка б попереджала втрату або розголошення інформації про його діяльність. А тому, виникає необхідність постійного управління системою інформаційної безпеки підприємства для забезпечення стабільного та ефективного функціонування, починаючи з моменту його створення. Крім того, у зв'язку зі зростанням динаміки злиттів і поглинань підприємств, розвитком інформаційного суспільства, вимогами бізнесу проблема інформаційної безпеки потребує постійної уваги.

Аналіз останніх досліджень і публікацій. Ученим вдалося досягти значних успіхів в царині інформаційної безпеки підприємства. Серед найвагоміших досліджень, які висвітлюють різні аспекти інформаційної безпеки, слід виокремити розробки науковців, серед яких О. Гладківська, М. Гуцалюк, О. Зінченко, А. Марущак, Д. Ольшанський, А. Новицький, О. Сороківська, В. Хахановський, Л.Дж. Хоффман, В. Цимбалюк, М. Швець та інші.

Виділення не вирішених раніше частини загальної проблеми. Незважаючи на наявність важливих рекомендацій та настанов провідних науковців щодо забезпечення інформаційної безпеки підприємства, проблема управління системою інформаційної безпеки підприємства залишається недостатньо дослідженою. Зміна умов зовнішнього середовища, вплив внутрішніх та зовнішніх факторів посилюють необхідність удосконалення методів управління інформаційною безпекою підприємства, формування ефективної системи інформаційної безпеки, оцінки рівня інформаційної безпеки підприємства.

З огляду на зазначене, **мета статті** полягає у теоретичному обґрунтуванні найбільш актуальних проблем управління системою інформаційної безпеки підприємства в сучасних умовах.

Виклад основного матеріалу. У науковій літературі відсутній єдиний підхід до визначення понять «інформаційна безпека» та «інформаційна безпека підприємства».

Відповідно до Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Найбільш поширене серед країн-членів Європейського Союзу є визначення поняття «інформаційна безпека» під яким розуміють захист особистої інформації про відправників та одержувачів; захист інформації від несанкціонованого доступу; створення надійного джерела постачання інформації, інформаційних послуг та необхідного обладнання; захист інформації, що безпосередньо стосується національної безпеки [1].

Інформаційна безпека – стан захищеності основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну та телекомунікаційну інфраструктуру, власне інформацію та її параметри: повноту, об'єктивність, доступність і конфіденційність [6, с. 88].

Раціональним на наш погляд є визначення поняття «інформаційна безпека», як стану захищеності інформаційних відносин та пов'язаних із ними інформаційних процесів, за якого досягається стабільний інформаційний розвиток, унеможливлюється негативний інформаційний вплив та негативні наслідки незаконного застосування інформаційних технологій в усіх сферах суспільного життя, у результаті чого можна до-

сягти створення та ефективного функціонування інформаційного суспільства [2].

Виходячи з вище наведеного можна стверджувати, що інформаційну безпеку досліджують за такими основними характеристиками: стан захищеності інформаційного середовища та установлених законом правил, суспільні відносини.

Розглянемо головні підходи до визначення поняття «інформаційна безпека підприємства», що існують сьогодні:

1) інформаційна безпека підприємства – це суспільні відносини щодо створення та підтримання на належному рівні життєдіяльності відповідної інформаційної системи [12];

2) інформаційна безпека підприємства – це суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [10];

3) інформаційна безпека підприємства – це відношення рівня інформаційного захисту до рівня інформаційних загроз; сукупність засобів та дій уповноважених осіб, спрямованих на захист інформаційних ресурсів та інформаційної інфраструктури даного підприємства в процесі обміну, обробки та зберігання інформації на всіх рівнях інформаційної системи підприємства [11, с. 5];

4) інформаційна безпека підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [7, с. 94].

Узагальнюючи перелічені та інші формулювання, на нашу думку, слід погодитись з визначенням Чередниченко А.О., що інформаційна безпека підприємства – це стан внутрішнього та зовнішнього інформаційно-комунікаційного середовища і процесів управління його складовими й діяльністю із забезпечення безпеки, що формує відповідний цілям функціонування підприємства рівень інформатизації і забезпечує попередження виникнення загроз інформаційній безпеці й нейтралізацію їх впливу [13, с. 7]. Оскільки об'єктом інформаційної безпеки підприємства є не окремий безпечний стан інформації, інформаційних ресурсів, інформаційної системи, інформаційного середовища, а його інформаційно-комунікаційне середовище.

Система інформаційної безпеки – це взаємопов'язана сукупність напрямів, методів, засобів, заходів, які спрямовані на захист інформаційної інфраструктури підприємства від будь-яких випадкових або навмисних, зовнішніх або внутрішніх загроз, що можуть привести до крадіжки, пошкодження або несанкціонованій зміні та використання інформації, розголошення або її витоку. Тому, все те, що орієнтоване на побудову, підтримку та розвиток системи має основну мету – мінімізувати можливість нанесення шкоди інформаційній інфраструктурі підприємства, а у випадку форс-мажорних обставин звести її до мінімуму.

Головною метою системи інформаційної безпеки є забезпечення сталого розвитку підприємства, запобігання загроз його безпеки, захист законних інтересів від протиправних посягань, недопущення розголошення, втрати, витоку, спотворення і знищення інформації, забезпечення ефективної виробничої діяльності всіх структурних підрозділів.

Структура системи інформаційної безпеки залежить від цілей, завдань, методів і засобів діяльності підприємства, особливостей самої інформації (обсягу, цінності), характеру можливих загроз, необхідного ступеня надійності захисту, вартості системи та інших характеристик. А її ефективність – від дотримання інформаційними ресурсами відповідного рівня конфіденційності (англ. Confidentiality, privacy), цілісності (англ. Integrity) та доступності (англ. Availability) – тріади CIA.

Для забезпечення максимально можливого ступеню захисту необхідне використання системного (врахування всіх умов діяльності підприємства) та комплексного підходів – взаємопов'язане використання спеціальних технічних та програмних засобів (контролю доступу, моніторингу витоків, антивірусного захисту, міжмережевого екранування, захисту від електромагнітних випромінювань), організаційних заходів (документовані процедури і правила роботи з різними видами інформації, IT-сервісами, засобами захисту), нормативно-правових актів (нормативні документи, положення, інструкції), математичних методів для оцінки та аналізу інформаційної безпеки, морально-етичних заходів протидії та інших.

Виходячи з вище наведеного, систему інформаційної безпеки підприємства можна представити як сукупність підсистем управління елементами інформаційно-комунікаційного середовища та підсистем забезпечення інформаційної безпеки.

Одним з базових, основних елементів будь-якої системи в тому числі інформаційної безпеки виступають принципи. Для підприємств основними принципами системи інформаційної безпеки є наступні: простота використання, повний контроль (організація безперервного контролю за станом інформаційної безпеки та моніторинг всіх подій), загальна заборона (виконання тільки відомих безпечних дій), відкритої архітектури (забезпечення безпеки через неясність, ускладнення, заплутування і приховування слабких місць), розмежування доступу (призначення права на виконання дій), мінімальні привілеї (виділення найменших прав і доступу до мінімуму необхідних функціональних можливостей програм), достатня стійкість (перешкоди у вигляді досить складних обчислювальних завдань), мінімізація дублювання (мінімізація ідентичних процедур) [3, с. 56-57].

Одним із фундаментальних чинників успішності управління системою інформаційної безпеки підприємства є її побудова на основі міжнародних стандартів [9].

Проведені дослідження дозволяють виокремити головні етапи управління системою інформаційної безпеки підприємства:

1. Діагностика загроз інформаційній безпеці.

2. Оцінка рівня захищеності системи інформаційної безпеки (на основі системи показників) та надійності управлінського персоналу.

3. Планування стратегічних та оперативних заходів забезпечення інформаційної безпеки.

4. Організація та впровадження заходів забезпечення інформаційної безпеки, оцінка їх результативності та коригувальні дії [13].

Необхідною умовою підтримання належної інформаційної безпеки підприємства є оцінка та аналіз її рівня через розрахунок системи показників [4], а також використання економіко-математичних моделей (кластерний аналіз, стохастичний факторний аналіз та інші).

Отже, на сьогодні питання інформаційної безпеки підприємства повинно розглядатись як комплекс взаємопов'язаних заходів, які повинні розширюватись і удосконалюватись.

Висновки і пропозиції. Отже, управління системою інформаційної безпеки потребує врахування всіх компонентів інформаційно-комунікаційного середовища і організації ефективної діяльності із забезпечення інформаційної безпеки. Теоретичним базисом управління системою інформаційної безпеки підприємства є цілі, завдання, методи, принципи, засоби забезпечення інформаційної безпеки. Дотримання конфіденційності, цілісності та доступності інформації дозволить підвищити результативність інформаційної безпеки підприємства – забезпечить захист інформації від внутрішніх і зовнішніх загроз, створить сприятливі умови для ефективного функціонування підприємства і підвищить його конкурентоспроможність. Тому управління системою інформаційної безпеки слід розглядати як невід'ємний елемент процесу управління підприємством.

Перспективи подальших досліджень полягають у детальній розробці кожного із розглянутих нами аспектів в рамках системного дослідження теоретичних засад управління системою інформаційної безпеки підприємства.

Список літератури:

1. Developments in the field of information and telecommunications in the context of international security / Report of the Secretary General. Fifty-six session. 3 July, 2001. United Nations. A/56/164.
2. Абакумов В.М. Інформаційна безпека підприємництва як об'єкт адміністративно-правової охорони / В.М. Абакумов // Форум права. – 2012. – № 4. – С. 10-16. – [Електронний ресурс]. – Режим доступу: http://arhive.nbuv.gov.ua/e-journals/FP/2012-4/12avmapo.pdf
3. Верескун М.В. Методичне забезпечення системи інформаційної безпеки промислових підприємств / М.В. Верескун // Економіка і організація управління. – 2014. – № 1 (17). – С. 54-60.
4. Журавель М.Ю. Формування системи показників оцінки рівня інформаційної безпеки підприємства / М.Ю. Журавель, Т.В. Полозова, О.В. Стороженко // Вісник економіки транспорту і промисловості. – 2011. – № 33. – С. 171-177.
5. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»: від 09.01.2007 р., № 537.
6. Легомінова С.В. Теоретичні засади інформаційної безпеки підприємства / С.В. Легомінова // Економіка. Менеджмент. Бізнес. – 2015. – № 3 (13). – С. 87-92.
7. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки // Державна безпека України / А.І. Марущак. – 2011. – № 21. – С. 92-95.
8. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Джабраил Матиев. – Електронний ресурс. – Режим доступу:http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161
9. Мацків О.І. Аналіз перспективних стандартів забезпечення інформаційної безпеки / О.І. Мацків, К.Б. Айвазова // Проблеми технічного регулювання та якості: IV Всеукр. наук.-практ. конф. (9-10 жовтня 2014 р.). – Одеса: ОДАТРЯ, 2014. – С. 39-42.
10. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи [Текст] / О.А. Сороківська, В.Л. Гевко // Вісн. Хмельниц. нац. ун-ту. Сер.: Екон. науки. – 2010. – № 2. – Т. 2. – С. 32-35.
11. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим): автореф. дис. на здобуття наук. ступеня канд. екон. наук: спец. 08.00.04 / М.Ю. Танцюра. – Сімферополь, 2012. – 21 с.
12. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) / В. Цимбалюк // Підприємництво, господарство і право. – 2004. – № 3. – С. 88-91.
13. Чередниченко А.О. Організаційно-економічне забезпечення управління інформаційною безпекою підприємств будівельної галузі: автореф. дис. на здобуття наук. ступеня канд. екон. наук: спец. 21.04.02 «Економічна безпека суб'єктів господарської діяльності» / А.О. Чередниченко. – Харків, 2016. – 21 с.

Смачило Т.В., Кахний М.И.
Тернопольский национальный экономический университет

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ УПРАВЛЕНИЯ СИСТЕМОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Аннотация
Исследованы теоретические аспекты информационной безопасности предприятия. Обоснована важность влияния информационной безопасности предприятия на его конкурентоспособность на рынке производства, сбыта товаров и услуг. Охарактеризована важность системы информационной безопасности для минимизации возможности нанесения вреда информационной инфраструктуре предприятия. Выделены основные принципы системы информационной безопасности. Рассмотрены этапы управления информационной безопасностью предприятия.

Ключевые слова: предприятие, информация, информационная безопасность, система информационной безопасности, управление, конфиденциальность, целостность, доступность.

Smachylo T.V., Kahniy M.I.
Ternopil National Economic University

THEORETICAL FOUNDATIONS MANAGEMENT OF THE ENTERPRISE'S INFORMATION SECURITY SYSTEM

Summary
Theoretical aspects of information security are investigated. The importance of enterprise information security influence on its competitiveness in the market of production, sales of goods and services is proved. The importance of information security system to minimize the possibility to cause damage of enterprise information infrastructure are given. The basic principles of information security system is determined. The stages of enterprise information security management are presented.
Keywords: enterprise, information, information security, information security system, management, confidentiality, integrity, accessibility.