DOI: https://doi.org/10.25140/2411-5215-2023-4(36)-86-94
УДК 332.12
JEL Classification: G00

Олександр Храпкін
здобувач PhD
Запорізький національний університет (Запоріжжя, Україна)
E-mail: atomaders98@gmail.com. **ORCID:** https://orcid.org/0000-0002-2281-9581

СТРАТЕГІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА: СУЧАСНІ ПІДХОДИ ТА ВИКЛИКИ

У статті розглянуто особливості забезпечення стратегічного управління інформаційною безпекою сучасних підприємств. Нині системи інформаційної безпеки призначені для забезпечення повноцінного функціонування інформаційної інфраструктури підприємства, використовуючи різні види інформаційних сервісів, автоматизації фінансової та виробничої діяльності, а також його бізнес-процесів.

Розглянуто необхідність формування системи управління інформаційною безпекою, яка зумовлюється існуванням внутрішніх і зовнішніх загроз, їхніми деструктивними наслідками для діяльності та іміджу підприємства. Проаналізовано завдання інформаційної безпеки. Управління інформаційною безпекою передбачає виявлення потенційних ризиків для підприємства, оцінювання потенційного впливу, розробку та впровадження стратегій усунення проблем, розроблених для максимального зменшення ризиків за допомогою наявних ресурсів.

Визначено головні етапи побудови політики інформаційної безпеки. Вказано основні принципи системи управління інформаційної безпеки для підприємства. Йдеться також про зберігання та обробку значних обсягів інформації різного ступеня конфіденційності, тому питання про захищеність важливих інформаційних даних підприємства від різних внутрішніх та зовнішніх загроз є актуальним.

Ключові слова: *підприємство*; *інформаційна безпека підприємства; управління інформаційною безпекою; стратегічне управління; інформаційні ресурси; конфіденційність даних; захист.*

Бібл.: 13.

Постановка проблеми. Поряд із людськими, фінансовими та матеріальними ресурсами інформація виступає також одним із важливих ресурсів стратегічного управління. Для кожного підприємства будь-якої сфери актуально формування ефективної системи безпеки та збереження інформаційного суверенітету. Важливим є вміння розбудови системи інформаційної безпеки – розроблення й ефективне впровадження комплексу заходів із захисту конфіденційних даних та інформаційних процесів, формуючи відповідний комплекс вимог до персоналу, менеджерів та технічних служб.

Сучасні інформаційні системи сприяють успішному збереженню інформаційної інфраструктури підприємства. Надаються різні види інформаційних послуг для автоматизації фінансової та виробничої діяльності, бізнес-процесів. Відповідно різні інформаційні системи зберігають та обробляють великі обсяги інформації (з різним ступенем конфіденційності). Проблема забезпечення інформаційної безпеки підприємства від різноманітних зовнішніх та внутрішніх загроз є вагомою в сучасних умовах.

Аналіз останніх досліджень і публікацій. Основні теоретичні й практичні аспекти питання забезпечення інформаційної безпеки підприємства займаються науковці різних сфер.

В. Панченко визначив основні цілі, завдання, принципи побудови та види загроз, на основні яких сформував методичний підхід до формування системи інформаційної безпеки підприємств, а також запропонував розглядати систему інформаційну безпеку підприємства як модель інформаційного протиборства у внутрішньому та зовнішньому середовищі. А. Босак, В. Вержиковський, І. Калінін, І. Максимів, Д. Приступа, О. Ривак досліджували основні засади формування інформаційної безпеки підприємства, розглядаючи забезпечення безперебійної роботи підприємства, уникнення загроз безпеці (розкривання, зберігання, створення, знищення та доставляти неправдиву інформацію) як основну мету будь-якої інформаційної системи підприємства. І. Маркіна та В. Дячков розглянули передумови формування системи інформаційної безпеки підприємства, визначили особливості управління нею (розвиток інформаційної інфраструктури підприємства, автоматизації фінансової та виробничої діяльності та інше). С. Онищенко та О. Ківшик опрацювали специфіку управління інформаційною безпекою стратегічно важливих підприємств в умовах воєнного стану. Г. Бранденбург вказав детальні кроки впровадження системи управління інформаційною безпекою, яка відповідає довгостроковим бізнес-цілям підприємства.

Виділення недосліджених частин загальної проблеми. Незважаючи на значні наукові напрацювання, є питання, які потребують додаткових досліджень: основні аспекти та кроки застосування культури інформаційної безпеки в підприємстві, ефективні засоби захисту інформаційної системи: своєчасне виявлення та мінімізація негативного впливу загроз.

Мета статті – дослідити сучасні підходи та виклики у сфері стратегічного управління інформаційною безпекою підприємства.

Виклад основного матеріалу дослідження. Сьогодні усім підприємствам слід приділяти увагу питанням захисту інформації, особливо в умовах воєнного стану. Інформація, яка виступає конкурентною перевагою підприємства, має бути захищеною від будь-якої можливої втрати – крадіжки, випадкового знищення тощо. Питання захисту даних у більшості вітчизняних підприємств ще не вирішується на відповідному рівні. Крім того, деякі підприємства не мають достатньо вільних обігових коштів для забезпечення захисту інформації [5, с. 72].

Відповідно до Концепції інформаційної безпеки України (від 30.09.2015 року) «інформаційна безпека» визначається як «стан захищеності життєво важливих інтересів людини та громадянина, суспільства та держави, за якого запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій» [6].

Під інформаційною безпекою підприємства розуміється сукупність усіх елементів системи управління, зокрема і стратегічного, які пов'язані з визначенням, формуванням конфіденційності, цілісністю та доступністю, відповідною підзвітністю, автентичністю та достовірністю інформації або засобів її обробки на підприємстві [3, с. 55].

Система стратегічного управління інформаційною безпекою – це систематичний підхід управління та захисту інформаційних активів підприємства. Вона включає набір процедур і засобів контролю, які допомагають визначити, оцінити та зменшити потенційні ризики підприємства, включаючи їх зберігання, обробку та передачу. Основною метою є забезпечення управління інформаційним ризиком у межах прийнятного для підприємства рівня залишкового ризику [11].

Метою управління інформаційною безпекою є довгостроковий захист даних: *конфіденційність даних* (обмеження доступу, лише авторизованим користувачам; неможливості несанкціонованого отримання будь-яких даних), *цілісність* (здатність гарантувати точність та повноту даних; неможливості навмисного або випадкового модифікування інформації), *доступність* (дані та послуги, які на них покладаються, мають бути доступні авторизованим користувачам як у компанії, так і за її межами; оперативне отримання офіційно запитуваної інформації) [13; 7, с. 91].

Конфіденційність, цілісність і доступність підприємства можуть бути під загрозою різними способами. Управління інформаційною безпекою передбачає виявлення потенційних ризиків для підприємства, оцінку їхньої ймовірності та потенційного впливу, а також розробку та впровадження стратегій усунення проблем, розроблених для максимального зменшення ризиків за допомогою наявних ресурсів [13]. Для даних із підвищеним ризиком можна застосувати додаткові засоби керування конфіденційністю. Для підтримки цілісності даних можна застосувати такі заходи, як контроль версій, контроль доступу користувачів і контрольні суми. Що стосується дійсності, тут типова діяльність включає технічне обслуговування та ремонт апаратного забезпечення, установку виправлень і оновлень, а також впровадження процесів реагування на інциденти та аварійного відновлення, щоб запобігти втраті даних у разі кібератаки [12].

До вказаних завдань інформаційної безпеки відносять також гарантування вірогідності інформації, забезпечення юридичної значущості інформації (електронні документи), організація не відстежуваності дій користувача [10, с. 106].

Інформаційна безпека повинна гарантувати захист від будь-яких порушень функціонування інформаційної системи через вплив на інформаційні канали та сигналізацію, керування та віддаленого завантаження баз даних, комутаційного обладнання, системного й прикладного програмного забезпечення; неправомірних дій користувачів і персоналу; несанкціонованого

доступу до інформаційних даних; витоку даних, впливу на цілісність мережі й інформації, доступності баз даних; руйнування зовнішніх та вбудованих засобів захисту [10, с. 106].

Головними етапами побудови політики інформаційної безпеки є:

1) повна реєстрація усіх ресурсів, які потребують захисту;

2) формування переліку можливих загроз для кожного зі списку ресурсу;

3) оцінка ймовірності появи кожної загрози;

4) застосування дій для ефективного захисту кожного ресурсу [7, с. 90].

Більш детально запровадження системи управління інформаційною безпекою можна продемонструвати у вигляді загального плану (підходи відрізняються залежно від організаційного контексту) з визначеними кроками [11]:

1. Отримання завдання з боку керівництва, його підтримка, наголошуючи на важливості узгодження із бізнес-цілями підприємства. Мається на увазі, виділення необхідних ресурсів і сприяння організаційній культурі безпеки.

2. Створення структури управління, яка окреслює ролі, обов'язки та лінії звітності щодо інформаційної безпеки в підприємстві (призначення керівника інформаційної безпеки або створення керівного комітету з інформаційної безпеки).

3. Визначення сфери застосування та межі діяльності: реєстр інформаційних активів, процесів та системи, які потребують захисту, враховуючи бізнес-цілі та пріоритети підприємства.

4. Розробка політики інформаційної безпеки високого рівня, яка відображає підхід до інформаційної безпеки та бізнес-цілі загалом. Результат повинен бути затверджений вищим керівництвом і доведений до відома всіх співробітників.

5. Запровадження програми моніторингу та обчислення. Визначення ключових показників ефективності для вимірювання ефективності та її узгодження з бізнес-цілями.

6. Визначення методології оцінки ризику, яка відповідає схильності та бізнес-цілям підприємства.

7. Проведення оцінки ризиків: визначення, аналіз та оцінка потенційних ризиків для інформаційних активів організації, беручи до уваги потенційний вплив на поставлені цілі.

8. Розробка та запровадження плану (-ів) обробки ризиків: вибір відповідних заходів зменшення ризику (процедури та технічні засоби контролю) на основі оцінки ризику. Навчання персоналу відповідним процедурам.

9. Визначення чітких ролей та обов'язків щодо інформаційної безпеки, переконавшись, що вони відповідають бізнес-цілям і структурі підприємства.

10. Системне проведення програм навчання та підвищення обізнаності персоналу щодо їх ролі у захисті інформаційних активів.

11. Встановлення процесу управління інцидентами (розробка процесу реагування на інциденти безпеки).

12. Проведення внутрішнього аудиту та перевірки керівництва для оцінки продуктивності та ефективності системи управління інформаційної безпеки, за потреби запроваджувати коригувальні дії.

13. Постійно вдосконалення для адаптації до змін у бізнес-середовищі та загроз.

14. Отримання сертифікації (необов'язково) в акредитованому органі сертифікації, такому як ISO/IEC 27001. Це може забезпечити зовнішню перевірку зобов'язань організації щодо інформаційної безпеки [11].

Дотримання вказаних кроків, підприємства не тільки можуть зменшити інформаційні ризики, але й підтримувати їхні бізнес-стратегії, сприяючи досягненню конкурентної переваги на ринку. Проте обов'язково слід адаптувати ці кроки до контексту конкретного підприємства.

Для підприємства основними принципами системи інформаційної безпеки є простота у використанні, забезпечений повний контроль (стан інформаційної безпеки та моніторинг усіх дій), відкрита архітектура (забезпечення безпеки, приховання неоднозначності, складності, плутанини та вразливі місця), межі доступу (призначення дозволів для виконання робочих завдань), найменші привілеї (доступ до мінімальних необхідних функцій), достатня стабільність (більш-менш складні перешкоди у вигляді арифметичних задач), мінімізація дублювання (уникнення ідентичних процедур) [3, с. 56-57; 2].

Стандартна система стратегічного управління інформаційною безпекою підприємства має всі елементи, які є загальними для систем управління. Серед основних чинників забезпечення інформаційної безпеки на сучасних підприємствах виділяють:

− сформована політика, визначені цілі та заходи інформаційної безпеки, які відповідають бізнес-цілям підприємства;

− цілеспрямований підхід і структура застосування, моніторингу, підтримки та вдосконалення інформаційної безпеки відповідають корпоративній культурі підприємства;

− підтримка та залучення всіх рівнів керівництва;

− розуміння та встановлення вимог до інформаційної безпеки підприємства, оцінка зовнішніх та внутрішніх ризиків, доступність управління ризиками;

− ефективні заходи для належної обізнаності персоналу;

− встановлення головних принципів щодо політики та стандартів інформаційної безпеки;

− сприяння фінансуванню заходів з управління інформаційною безпекою;

− забезпечення ефективного процесу керування всіма інцидентами в системі інформаційної безпеки;

− оцінювання рівня ефективності управління інформаційною безпекою, внесення коректив та пропозицій щодо його покращення [8, с. 84-85].

Для забезпечення найвищого рівня захисту потрібен системний та комплексний підхід, враховуючи усі умови діяльності підприємства. Мається на увазі, спеціальні технології та програмні засоби (контроль доступу, антивірусний захист, моніторинг витоків, міжмережне екранування, захист від електромагнітного випромінювання), організовані заходи (документовані процедури та правила використання різних типів інформації, IT-сервісів та захисних заходів), математичний захист інформації, морально-етичні заходи протидії та інші [8, с. 83].

Більшість заходів щодо оцінки захищеності систем інформаційної безпеки відрізняються великими обсягами. Програми захисту створюють власними силами у підприємстві, проте навіть сучасні методи та засоби інформаційних технологій не можуть повністю забезпечити продуктивну та надійну обробку постійно зростаючих масивів інформаційних даних. У сучасних інформаційних технологіях існує позиційна двійкова система числення, проте має недоліки оскільки чинні методи несанкціонованого доступу, хакерські атаки, віруси та інші види порушення цілісності інформації побудовані саме з використанням двійкового позиційного коду [9, с. 82].

У формуванні зазначеної системи не менш вагому роль відіграє дотримання вимог державних та міжнародних нормативно-правових актів і стандартів в цій сфері. Стандарти виступають еталоном дій, проте носять більш декларативний характер, не враховуючи специфіку інформатизації діяльності кожного підприємства [8, с. 86]. Керівництво повинно зорієнтуватися, оцінити кожен вектор діяльності та прийняти рішення щодо дотримання стандартів і положень інформаційної безпеки. Водночас майже всі міжнародні стандарти управлінської системи методологічно сумісні. Це дозволяє виділити та підтримувати уніфіковані завдання. До прикладу, у частині роботи з персоналом підприємства щодо використання інформації та її захист, реєстрації та збору даних, створення інформаційних систем, застосування автоматизованих засобів тощо.

Висновки та пропозиції. Система інформаційної безпеки є складною частиною загального управління бізнесом підприємства. Стан безпеки підприємства характеризується рівнем зрілості, ефективністю діючих програм та реалізованих засобів контролю безпеки. Важливим є засоби контролю, які впроваджуються на рівні персоналу, робочих процесах та загальної політичної культури підприємства.

Список використаних джерел

1. Атамас О. П. Удосконалення системи управління інформаційною складовою фінансово-економічної безпеки підприємства / О. П. Атамас, Т. М. Майстер // Проблеми сучасних трансформацій. Серія: економіка та управління. – 2023. – № 8. DOI: https://doi.org/10.54929/2786-5738-2023-8-04-02.

2. Босак А. О. Засади формування інформаційної безпеки підприємства / А. О. Босак, В. П. Вержиковський, І. Є. Калінін, І. Д. Максимів, Д. А. Приступа, О. І. Ривак // Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки». – 2023. – № 11. DOI: https://doi.org/10.25313/2520-2294-2023-11-9157.

3. Верескун М. В. Методичне забезпечення системи інформаційної безпеки промислових підприємств / М. В. Верескун // Економіка і організація управління. – 2014. – Вип. 1-2. – С. 54-60.

4. Волот О. Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання / О. Волот // Центральноукраїнський науковий вісник. Економічні науки. –2019. – Вип. 3(36). – С. 238–247. DOI: https://doi.org/10.32515/2663-1636.2018.3(36).238-247.

5. Дейнега О. Інформаційна безпека підприємств в умовах глобалізації / О. Дейнега // Економіка та суспільство. – 2019. – Вип. 20. – С. 70–79.

6. Концепція інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/files/banners/Final%20Проект%20 концепції%20(Текст)%20-%2030.09.15.pdf.

7. Костюченко В. В. Особливості організації інформаційної безпеки сучасної інформаційної системи та її економічна доцільність / В. В. Костюченко, К. О. Шиковець // Економіка і суспільство. – 2017. – № 10. – С. 89-93.

8. Маркіна І. А. Основи формування системи менеджменту інформаційної безпеки підприємства / І. А. Маркіна, Д. В. Дячков // Проблеми і перспективи розвитку підприємництва. – 2016. – № 3(1). – С. 80–88.

9. Онищенко С.В. Управління інформаційною безпекою стратегічно важливих підприємств в умовах викликів й загроз / С.В. Онищенко, О.П. Ківшик // Економіка і регіон. – 2022. – № 3 (86). – С. 80-85. DOI: https://doi.org/10.26906/EiR.2022.3(86).2817.

10. Панченко В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти / В. Панченко // Актуальні проблеми правознавства. – 2020. – № 1 (21). – С. 103-109.

11. Brandenburg G. The Role and Implementation of an Information Security Management System in Modern Enterprises [Electronic resource]. – Accessed mode: https://ctrl-disrupt.nl/-insights-news/the-role-and-implementation-of-an-information-security-management-system-in-modern-enterprises.

12. Information security management – definition & overview [Electronic resource]. – Accessed mode: https://www.sumologic.com/glossary/information-security-management.

13. What is Information Security Management? [Electronic resource]. – Accessed mode: https://www.checkpoint.com/cyber-hub/network-security/what-is-security-management/what-is-information-security-management.

References

1. Atamas, O.P., & Maister, T.M. (2023). Udoskonalennia systemy upravlinnia informatsiinoiu skladovoiu finansovo-ekonomichnoi bezpeky pidpryiemstva [Improving the management system of the information component of the financial and economic security of the enterprise]. *Problemy suchasnykh transformatsii. Seriia: ekonomika ta upravlinnia – Problems of modern transformations. Series: Economics and management,* (8). https://doi.org/10.54929/2786-5738-2023-8-04-02.

2. Bosak, A.O., Verzhykovskyi, V.P., & Kalinin, I.Ye. (2023). Zasady formuvannia informatsiinoi bezpeky pidpryiemstva [Principles of formation of information security of the enterprise]. *Mizhnarodnyi naukovyi zhurnal «Internauka». Seriia: «Ekonomichni nauky» – International scientific journal "Internauka". Series: "Economic Sciences"*, (11). https://doi.org/10.25313/2520-2294-2023-11-9157.

3. Vereskun, M.V. (2014). Metodychne zabezpechennia systemy informatsiinoi bezpeky promyslovykh pidpryiemstv [Methodological support of the information security system of industrial enterprises]. *Ekonomika i orhanizatsiia upravlinni – Economics and organization of management*, 1-2, 54-60.

4. Volot, O. (2019). Informatsiina ta kibernetychna bezpeka suchasnoho pidpryiemstva: zabezpechennia ta modeliuvannia [Information and cybersecurity of a modern enterprise: provision and modeling]. *Tsentralnoukrainskyi naukovyi visnyk. Ekonomichni nauky – Central Ukrainian Scientific Bulletin. Economic sciences,* 3(36), 238–247. https://doi.org/10.32515/2663-1636.2018.3(36).238-247.

5. Deineha, O. (2019). Informatsiina bezpeka pidpryiemstv v umovakh hlobalizatsii [Information security of enterprises in the context of globalization]. *Ekonomika ta suspilstvo – Economy and Society*, *20*, 70–79.

6. Kontseptsiia informatsiinoi bezpeky Ukrainy [The concept of information security of Ukraine]. (n.d.). http://mip.gov.ua/files/banners/Final%20Proekt%20kontseptsii%20(Tekst)%20-%2030.09.15.pdf.

7. Kostiuchenko, V.V., & Shykovets, K.O. (2017). Ocoblyvocti ophanizatsii infopmatsiinoi bezpeky cuchacnoi infopmatsiinoi cyctemy ta yii ekonomichna dotsilnict [Features of the organization of information security of the modern information system and its economic feasibility]. *Ekonomika i suspilstvo – Economy and Society*, *10*, 89-93.

8. Markina, I.A., & Diachkov, D.V. (2016). Osnovy formuvannia systemy menedzhmentu informatsiinoi bezpeky pidpryiemstva [Fundamentals of formation of the enterprise information security management system], *Problemy i perspektyvy rozvytku pidpryiemnytstva – Problems and prospects of entrepreneurship development*, *3*(1), 80–88.

9. Onyshchenko, S.V., & Kivshyk O.P. (2022). Upravlinnia informatsiinoiu bezpekoiu stratehichno vazhlyvykh pidpryiemstv v umovakh vyklykiv y zahroz [Management of information security of strategically important enterprises in the face of challenges and threats]. *Ekonomika i rehion – Ekonomika i region*, *3*(86), 80-85. https://doi.org/10.26906/EiR.2022.3(86).2817.

10. Panchenko, V. (2020). Upravlinnia informatsiinoiu bezpekoiu derzhavy ta pidpryiemstv: pravovi ta orhanizatsiini aspekty [Management of information security of the state and enterprises: legal and organizational aspects]. *Aktualni problemy pravoznavstva – Actual problems of jurisprudence*, *1*(21), 103-109.

11. Brandenburg, G. (2023). The Role and Implementation of an Information Security Management System in Modern Enterprises. https://ctrl-disrupt.nl/-insights-news/the-role-and-implementation-of-an-information-security-management-system-in-modern-enterprises.

12. Information security management – definition & overview. (n.d.). https://www.sumologic.com/glossary/information-security-management.

13. What is Information Security Management? (n.d.). https://www.checkpoint.com/cyber-hub/network-security/what-is-security-management/what-is-information-security-management.

Отримано 03.12.2023

UDC 332.12

Oleksandr Khrapkin
PhD Student
Zaporizhzhia National University (Zaporizhzhia, Ukraine)
E-mail: atomaders98@gmail.com. **ORCID:** https://orcid.org/0000-0002-2281-9581

STRATEGIC MANAGEMENT OF ENTERPRISE INFORMATION SECURITY: MODERN APPROACHES AND CHALLENGES

The article deals with the peculiarities of ensuring strategic management of information security of modern enterprises. Nowadays, information security systems are designed to ensure the full functioning of an enterprise's information infrastructure using various types of information services, automation of financial and production activities, as well as its business processes.

The basic provisions of information security are formalized and enshrined in the Information Security Strategy of Ukraine. Other regulatory documents and standards of enterprises must comply with the laws and regulatory framework of Ukraine, international law, industry standards and EU and NATO directives.

The article considers the need to form an information security management system, which is caused by the existence of internal and external threats, their destructive consequences for the activities and image of an enterprise. The tasks of information security are analyzed: data confidentiality, integrity, availability, ensuring the reliability of information, ensuring the legal significance of information, ensuring the untraceability of user actions. Information security management involves identifying potential risks to an enterprise, assessing the potential impact, developing and implementing strategies to eliminate problems designed to minimize risks with the available resources.

The main stages of developing an information security policy are identified: complete registration of all information resources that require protection; formation of a list of possible threats to each resource from the list; assessment of the probability of occurrence of each threat; application of actions for the effective protection of each resource. The basic principles of an information security management system for an enterprise are outlined: ease of use, full control, open architecture, access limits, least privileges, sufficient stability, and minimization of duplication. It is also about storing and processing significant amounts of information of varying degrees of confidentiality, so the issue of protecting important enterprise information data from various internal and external threats is relevant.

Keywords: *enterprise; enterprise information security; information security management; strategic management; information resources; data confidentiality; protection.*

References: 13.

Храпкін О. Стратегічне управління інформаційною безпекою підприємства: сучасні підходи та виклики. *Проблеми і перспективи економіки та управління.* 2023. № 4(36). С. 86-94.