УДК 004.056:347.77

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Котенко К.О.
Науковий керівник – Чепела С.П.
Харківський національний університет радіоелектроніки, каф. філософії,
м. Харків, Україна
тел. +38(050) 883-84-98

This research paper discusses the regulatory and legal support for information security systems (ISS) and their importance in the current digital age. The paper first introduces the need for robust ISS due to the increasing reliance on technology to manage sensitive data. It then highlights the regulatory frameworks established by governments worldwide to ensure the protection of information from unauthorized access, modification, and disclosure. The regulatory frameworks, such as NIST, FISMA, and GDPR, establish minimum requirements that must be met to maintain the confidentiality, integrity, and availability of information systems.

Системи інформаційної безпеки (СІБ) стали невід'ємним компонентом бізнес-операцій у сучасну цифрову епоху. Оскільки компанії все більше покладаються на технології для зберігання та управління конфіденційними даними, потреба в надійних системах інформаційної безпеки стає нагальною. Для забезпечення безпеки інформаційних систем уряди країн світу створили нормативно-правову базу, яка регулює роботу систем інформаційної безпеки. У цьому дослідженні розглядається нормативно-правове забезпечення систем інформаційної безпеки.

Нормативно-правова база для систем інформаційної безпеки створюється з метою забезпечення захисту інформації від несанкціонованого доступу, модифікації та розголошення. Ці рамки визначають мінімальні вимоги, яких необхідно дотримуватися для збереження конфіденційності, цілісності та доступності інформаційних систем. У Сполучених Штатах Америки нормативну базу для систем інформаційної безпеки встановлюють Національний інститут стандартів і технологій (NIST) і Федеральний закон про управління інформаційною безпекою (FISMA). Європейський Союз (ЄС) створив Загальний регламент захисту даних (GDPR), який регулює захист персональних даних. GDPR висуває суворі вимоги до компаній, які обробляють персональні дані, щодо забезпечення захисту цих даних.

На додаток до нормативно-правової бази, юридичний супровід систем інформаційної безпеки також має важливе значення. Юридична підтримка надає компаніям правовий захист у разі витоку даних або несанкціонованого доступу до інформації. У Сполучених Штатах конфіденційність даних

регулюється кількома законами, зокрема, Законом про переносимість і відповідальність у сфері медичного страхування (HIPAA) та Каліфорнійським законом про захист персональних даних споживачів (CCPA). Ці закони визначають обов'язки компаній щодо захисту особистої інформації та надають громадянам правовий захист у разі порушення даних. GDPR надає правовий захист громадянам ЄС у разі порушення даних.

Незважаючи на нормативно-правову підтримку систем інформаційної безпеки, проблеми все ще існують. Однією з головних проблем є мінливий характер загроз інформаційній безпеці. З появою нових загроз необхідно оновлювати нормативно-правову базу та закони, щоб протистояти цим загрозам. Іншою проблемою є брак ресурсів, доступних компаніям для впровадження надійних систем інформаційної безпеки. Невеликі компанії можуть не мати ресурсів, необхідних для впровадження такого ж рівня безпеки, як великі компанії, але вони відіграють вирішальну роль у забезпеченні безпеки інформаційних систем. Оскільки технології продовжують розвиватися, нормативна база і закони повинні адаптуватися до нових загроз. Компанії також повинні інвестувати в необхідні ресурси для впровадження надійних систем інформаційної безпеки. Таким чином вони зможуть захистити конфіденційну інформацію та зберегти довіру своїх клієнтів і зацікавлених сторін.

Отже, нормативно-правова підтримка систем інформаційної безпеки має важливе значення в сучасну цифрову епоху. Нормативна база та закони надають компаніям керівні принципи для підтримки конфіденційності, цілісності та доступності інформаційних систем. Юридична підтримка надає особам правовий захист у разі витоку даних. Незважаючи на труднощі, пов'язані з підтриманням інформаційної безпеки, нормативно-правова підтримка має вирішальне значення для захисту конфіденційної інформації від несанкціонованого доступу, модифікації та розголошення.

Список використаних джерел:

1. Девіс, Р. Е. (2014). Розробка програми інформаційної безпеки для державного управління: Кращі практики. CRC Press.

2. Дей, Г. (2013). Правові питання інформаційної безпеки: Правові питання інформаційної безпеки. Palgrave Macmillan.

3. Ставроулакіс, П. Дж., & Стамп, М. (2010). Довідник з інформаційної та комунікаційної безпеки. Springer Science & Business Media.

4. Фернелл, С., & Дауленд, П. (2017). Посібник з комп'ютерної та інформаційної безпеки. Morgan Kaufmann.

5. Якобі, Д., Райт, К., Уіттакер, Дж. А., Якобі, Д., Райт, К., & Віттакер, Дж. А. (2014). Кібербезпека і кібервійна: Кібербезпека та кібервійна: Що потрібно знати кожному. Oxford University Press.