УДК 33+004.056.5
JEL G32, M21, L1
DOI 10.32782/2786-765X/2024-6-9

Котляров В.О.
докторант,
Національний авіаційний університет
ORCID: https://orcid.org/0000-0002-2291-3199

СТРАТЕГІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ УКРАЇНИ

У статті досліджено питання щодо стратегічного управління інформаційною безпекою України. Наголошено на тому, що інформаційна безпека є ключовим напрямом розвитку інформаційного суспільства. Одночасно процеси цифровізації призвели до зростання нових інформаційних загроз та значних кібератак від росії, що виявили критичні проблеми в інформаційній безпеці. Водночас процеси цифровізації призвели до зростання нових інформаційних загроз та значних кібератак з боку росії, що виявили критичні проблеми інформаційної безпеки. Усі ці загрози зумовлюють необхідність формування системи безпеково орієнтованого інформаційного середовища як для суб'єктів господарювання, так і для зміцнення національної безпеки в цілому. Вивчення стратегічного управління інформаційною безпекою є надзвичайно важливим і своєчасним. Як висновок, у статті висвітлено те, що в епоху цифровізації, яка породила нові ризики та загрози для національних економік і виявила критичні проблеми у сфері інформації, забезпечення інформаційної безпеки стає необхідною передумовою стабільного функціонування не лише стратегічно важливих підприємств, а й стратегічних галузей у цілому. Побудова надійної системи захисту інформації має базуватися на своєчасній ідентифікації загроз інформаційній безпеці.

Ключові слова: безпека, ймовірність, операційні ризики, захист інформації, об'єкт, активи, загроза інформаційній безпеці.

Постановка проблеми. У XXI столітті відкрита й широкомасштабна війна, яку розпочала рф проти України, створила нові реалії й безпекові виклики у світі. Глобальний масштаб загроз та небезпек вимагає негайних структурних змін національної економіки під час воєнного конфлікту. Одночасно процеси цифровізації призвели до зростання нових інформаційних загроз та значних кібератак від росії, які виявили критичні проблеми в інформаційній безпеці.

Усі ці загрози обумовлюють необхідність формування системи безпекоорієнтованого інформаційного середовища як для суб'єктів господарювання, так і для зміцнення національної безпеки в цілому. Надзвичайно важливим і вчасним є дослідження стратегічного управління інформаційною безпекою.

Аналіз останніх досліджень та публікацій. Питанню щодо стратегічного управління інформаційною безпекою України були присвячені праці таких вчених як Бєлай С.В., Войціховський А.В., Гуржій Т.В., Данілова О.С., Корнієнко Д.М., Носок О.С., Ткач В М., Шемчук В.В., Фаль О.М. та інших.

Мета статті: проаналізувати та всебічно дослідити стратегічне управління інформаційною безпекою України.

Виклад основного матеріалу дослідження. Інформаційна безпека включає в себе сукупність засобів, методів та процесів, що забезпечують захист інформаційних активів і збереження ефективності та корисності технічної інфраструктури інформаційних систем. Основна мета полягає в збереженні цілісності, повноти та точності інформації, а також у зменшенні ризику несанкціонованих змін в системах обробки інформації.

Наразі українське законодавство визначає основні загрози для національної безпеки, зокрема в інформаційній сфері [4, с. 286]. Серед цих загроз варто відзначити:

- обмеження свободи слова та доступу до інформації;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення конфіденційної інформації, що становить державну та іншу, передбачену законом, таємницю;
- намагання маніпулювати суспільною свідомістю шляхом поширення недостовірної або упередженої інформації.

Зовнішні чинники також впливають на пріоритети політики національної безпеки, зокрема в інформаційній сфері. До них відносяться:

- посилення загроз національній безпеці через прагнення країн до домінування у світовому інформаційному просторі;
- витіснення України з інформаційних ринків;
- формування негативного іміджу України шляхом поширення неправдивої інформації;
- діяльність міжнародних терористичних організацій та іноземних структур з метою дезінформації.

Внутрішні чинники також впливають на національну безпеку з погляду формування стратегічних напрямів інформаційної безпеки. Серед них варто відзначити:

• відставання України у галузі інформаційних технологій, що створює ризик для безпеки держави;

• недостатній рівень захищеності державних інформаційних ресурсів, що може призвести до втрати важливої інформації та порушення нормального функціонування систем управління.

Інформаційна безпека є ключовим напрямом розвитку інформаційного суспільства. Вона передбачає не лише розвиток технологій обміну інформацією, але й усвідомлення всіма учасниками інформаційних відносин, включаючи власників, користувачів, розробників технологій та державу, необхідності захисту інформаційних ресурсів та забезпечення інформаційної безпеки держави.

Актуальність проблеми захисту інформаційних ресурсів пояснюється зростанням доступу до мереж загального користування, вразливістю окремих мереж, попитом злочинних елементів на руйнування інформації, а також вразливістю ефірних теле- та радіоканалів.

Надійний захист інформаційних об'єктів вимагає подальшого розвитку системи криптографічного та технічного захисту інформації, а також удосконалення нормативно-правового підґрунтя в цій сфері.

В Україні захист інформації розглядається як система правових, організаційних, технічних та інших заходів, спрямованих на забезпечення збереження фізичної та логічної цілісності, доступності і правомірного використання інформації відповідно до встановленого регламенту. Дослідження наявної нормативно-правової бази України з питань кіберзахисту державних інформаційних ресурсів свідчить про уніфікацію значної кількості діючих керівних нормативно-правових документів та стандартів з урахуванням міжнародного права, галузевих стандартів та директив ЄС та НАТО, що закріплені у законах та нормативно-правовій базі України [2, с. 45].

Загальні положення інформаційної безпеки визначені у Стратегії інформаційної безпеки, згідно з якою інформаційна безпека України є складовою національної безпеки і забезпечує захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших важливих інтересів [1].

Однак, система аналітичної інформації для управління рішеннями відрізняється складністю, а тенденція до ускладнення взаємозв'язків в інформаційному потоці призводить до систематичного зростання обсягів інформації, її надмірності при недостатності для прийняття оптимальних рішень. Більшість заходів щодо оцінки захищеності систем також вимагають значних зусиль.

Багато програм захисту створено власними силами підприємств і установ, але навіть сучасні методи і засоби не можуть повністю гарантувати надійну обробку зростаючих масивів інформації. Також важливо відзначити, що існуючі методи несанкціонованого доступу та атаки спрямовані на порушення цілісності інформації побудовані на основі двійкового позиційного коду, що може створювати недоліки у функціонуванні сучасних інформаційних технологій.

Досвід показує, що ефективне вирішення завдань з захисту інформації, яка перебуває в інформаційних та телекомунікаційних системах, а також надійний захист інформаційно-телекомунікаційних систем державних органів від злочинних посягань (в тому числі із-за меж України), можливий лише через створення комплексних систем захисту інформації. Ці системи поєднують в собі правові, організаційні, інженерні, технічні та програмні заходи забезпечення безпеки [3].

Таким чином, розробка та вдосконалення правового підґрунтя у цій сфері, зокрема нормативної бази, є одним із ключових чинників у процесі забезпечення безпеки інформації в Україні.

Процеси формування та вдосконалення нормативно-правової бази системи захисту інформації включають в себе як внесення змін до існуючих, так і розробку нових нормативно-правових актів [5, с. 22]. Ці акти повинні враховувати вимоги щодо гармонізації українського законодавства з міжнародним правом і законодавством Європейського Союзу.

Вони мають створити можливість для України стати рівноправним учасником міжнародного інформаційного обміну, зберігаючи при цьому інформаційний суверенітет країни.

Для забезпечення розвитку та конкурентоспроможності підприємства необхідно впровадити систему управління інформаційною безпекою (СУІБ). Ця система включає розробку, впровадження, моніторинг, аналіз та постійне вдосконалення заходів інформаційної безпеки [6, с. 30].

Процеси СУІБ ґрунтуються на моделі PDCA (Plan-Do-Check-Act):

• планування включає розроблення переліку активів, оцінку ризиків та вибір заходів;

• дія означає впровадження відповідних заходів;

• перевірка оцінює ефективність СУІБ, часто здійснюється внутрішніми аудиторами;

• дії спрямовані на поліпшення і включають превентивні та коригуючі заходи.

Система управління інформаційною безпекою дозволяє чітко визначити відповідальних за процеси та підсистеми, потреби у фінансових та людських ресурсах для їх функціонування.

Основні функції СУІБ включають виявлення та аналіз ризиків, планування процесів мінімізації ризиків, контроль цих процесів і внесення коригувань для мінімізації інформаційних ризиків.

Керування інформаційною безпекою базується на принципах комплексного підходу, узгодженості з бізнес-задачами, високої керованості, адекватності інформації, ефективності, безперервності управління та процесного підходу [7, с. 20].

В Україні існує структурно повна система забезпечення інформаційної безпеки, яка базується на нормативно-правових актах різного рівня, включаючи Конституцію, закони, укази Президента, постанови Кабінету Міністрів та інші нормативні документи. Однак потрібне удосконалення розподілу функцій між суб'єктами системи та схеми їх взаємодії.

Висновки. Отже, в епоху цифровізації, що породила нові ризики та загрози для національних економік і виявила критичні проблеми у сфері інформації, забезпечення інформаційної безпеки стає необхідною передумовою стабільного функціонування не лише стратегічно важливих підприємств, а й стратегічних галузей в цілому. Побудова надійної системи захисту інформації має базуватися на своєчасній ідентифікації загроз інформаційній безпеці.

Серед пріоритетних завдань державної інформаційної політики виокремлюються такі: створення, розвиток і вдосконалення системи кібербезпеки; захист незалежності ЗМІ і прав громадян на свободу слова; забезпечення суверенітету та інформаційної безпеки органів держави та суб'єктів господарювання; запобігання злочинам у сфері інформаційних технологій.

Бібліографічний список

1. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
2. Носок С. О., Фаль О. М., Ткач В. М. Управління інформаційною безпекою: конспект лекцій : навч. посіб. для студ. спец. 125 «Кібербезпека». КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.
3. Данілов О. Кіберзахист державних інформаційних ресурсів – важлива складова у процесі цифрової трансформації країни. 2020. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html
4. Шемчук В. В. Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління.* 2020. № 1(7). С. 285–296.
5. Бєлай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ : Національна академія Служби безпеки України, 2018. 408 с.
6. Войціховський А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права.* 2018. № 53. С. 26–37.
7. Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право.* 2018. № 4. С. 16–26.

References

1. Information security strategy: Decree of the President of Ukraine dated December 28, 2021 No. 685/2021. Available at: https://zakon.rada.gov.ua/laws/show/685/ 2021#Text
2. Nosok S. O., Fal O. M., Tkach V. M. (2021) Information security management: lecture notes: a textbook for students of speciality 125 'Cybersecurity'. Igor Sikorsky Kyiv Polytechnic Institute. Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 258 p.
3. Danilov O. (2020) Cyber protection of state information resources is an important component in the process of digital transformation of the country. Available at: https://www.rnbo.gov.ua/ua/Diialnist/4606.html
4. Shemchuk V. V. (2020) Threats to information security: problems of definition and overcoming. *Expert: paradigms of legal sciences and public administration,* no. 1(7), pp. 285–296.
5. Belai S. V., Kornienko D. M. (2018) Today's information security is an integral part of military security. Actual problems of state information security management. Kyiv: National Academy of the Security Service of Ukraine, 408 p.
6. Voytsikhovsky A. V. (2018) Cyber security as an important component of the national security protection system of European countries. *Journal of East European Law,* no. 53. pp. 26–37.
7. Gurzhii T. (2018) Information law: challenges of hybrid warfare. *Foreign trade: economy, finance, law,* no. 4, pp. 16–26.

Стаття надійшла до редакції 03.06.2024

Valerii Kotliarov
Doctoral Student,
National Aviation University
ORCID: https://orcid.org/0000-0002-2291-3199

STRATEGIC MANAGEMENT OF INFORMATION SECURITY OF UKRAINE

Objective. The article examines the issue of strategic information security management of Ukraine. It is emphasized that information security is a key direction of information society development. **Results.** It involves not only the development of information exchange technologies, but also the awareness of all participants in information relations, including owners, users, technology developers and the state, of the need to protect information resources and ensure state information security. At the same time, digitalization processes led to the growth of new information threats and significant cyberattacks from russia, which revealed critical problems in information security. The general provisions of information security are defined in the Information Security Strategy, according to which information security of Ukraine is a component of national security and ensures the protection of state sovereignty, territorial integrity, democratic constitutional order and other important interests. At the same time, digitalization processes led to the growth of new information threats and significant cyberattacks from russia, which revealed critical problems in information security. All these threats necessitate the formation of a system of security-oriented information environment both for business entities and for strengthening national security as a whole. The study of strategic management of information security is extremely important and timely. As a conclusion, it is said that in the era of digitalization, which has created new risks and threats for national economies and revealed critical problems in the field of information, ensuring information security becomes a necessary prerequisite for the stable functioning of not only strategically important enterprises, but also strategic industries as a whole. Building a reliable information protection system should be based on timely identification of threats to information security. Among the priority tasks of the state information policy, the following are highlighted: creation, development and improvement of the cyber security system; protection of media independence and citizens' rights to freedom of speech; ensuring sovereignty and information security of state bodies and business entities; prevention of crimes in the field of information technologies.Among the priority tasks of the state information policy, the following are highlighted: creation, development and improvement of the cyber security system; protection of media independence and citizens' rights to freedom of speech; ensuring sovereignty and information security of state bodies and business entities; prevention of crimes in the field of information technologies.

Keywords: security, probability, operational risks, information protection, object, assets, threat to information security.