УДК 342.1
DOI https://doi.org/10.24144/2788-6018.2023.04.43

ВИКЛИКИ ТА МОЖЛИВОСТІ СУЧАСНОСТІ: КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Ляпін К.Е.,
аспірант кафедри державно-правових дисциплін юридичного факультету ХНУ імені В.Н. Каразіна;
ORCID ID: https://orcid.org/0009-0000-1984-4711
staff_lsi@ukr.net

Ляпін К.Е. Виклики та можливості сучасності: комплексна система захисту інформації.

У сучасному цифровому світі, інформація виступає ключовим ресурсом, а її захист є надзвичайно важливою задачею у наш час. Кібербезпека стає все більш значущою для організацій, держав та людей. Кіберзагрози еволюціонують, традиційні методи захисту можуть бути недостатніми для забезпечення високого рівня безпеки, тому необхідно розвивати ефективні підходи до захисту інформації. Відповідь на виклики зосереджена у комплексній системі захисту, вона стає важливою стратегією для забезпечення стійкості і надійності інформаційних ресурсів та мереж.

Стаття висвітлює деякі виклики та можливості, з якими стикається сучасна інформаційна безпека, а також розглядає роль комплексної системи захисту в протидії кіберзагрозам. Серед викликів можна виділити швидкий темп розвитку технологій, що вимагає постійного оновлення захисних стратегій. Крім того, зростаюча кількість кібератак та їх складність заставляють організації переглядати свої підходи до кібербезпеки. Іншим викликом є забезпечення безпеки в глобальних мережах, де інформація пересувається через різні території з різними правилами та законодавством.

З іншого боку, комплексні системи захисту інформації відкривають нові можливості для ефективної боротьби з кіберзагрозами. Вони поєднують різноманітні методи та технології захисту. Такий підхід дозволяє знизити ризик успішних кібератак. Окрім того, комплексні системи захисту інформації можуть використовувати штучний інтелект та аналіз даних для автоматичного виявлення аномалій та небезпек у реальному часі. Це дозволяє швидко реагувати на нові загрози та атаки, забезпечуючи високий рівень безпеки.

Важливість впровадження комплексних систем захисту, які враховують різноманітність кіберзагроз та забезпечують надійний та стійкий захист інформаційних ресурсів у майбутньому буде набувати значущості кожного дня. Такий підхід допоможе забезпечити захищеність мереж, знизити ризик успішних кібератак та забезпечити безпеку та конфіденційність інформації у сучасному цифровому світі.

Загалом, комплексні системи захисту інформації стають невід'ємною частиною сучасної інформаційної безпеки. Вони допомагають організаціям забезпечити надійний захист своїх цінних даних та інформаційних ресурсів, що має вирішальне значення для їх діяльності та успіху. Однак, для досягнення максимальної ефективності, важливо постійно оновлювати та покращувати такі системи, враховуючи нові технологічні відкриття та зростаючі загрози кібербезпеки.

Ключові слова: Захист інформації, комплексна система, кібербезпека, протидія кіберзагрогам, інформаційне середовище, кіберзагроза, інформаційні ресурси.

Liapin K.E. Challenges and opportunities of modernity: a comprehensive system of information protection.

In today's digital world, information is a key resource, and its protection is an extremely important task in our time. Cyber security is becoming more and more important for organizations, governments and people. Cyber threats are evolving, traditional protection methods may not be sufficient to ensure a high level of security, so it is necessary to develop effective approaches to information protection. The response to challenges is concentrated in a complex protection system, it becomes an important strategy for ensuring the stability and reliability of information resources and networks.

The article highlights some of the challenges and opportunities facing modern information security, and also considers the role of a comprehensive defense system in countering cyber threats. Among the challenges, we can highlight the rapid pace of technology development, which requires constant updating of protective strategies. In addition, the increasing number of cyber attacks and their complexity are forcing organizations to rethink their approaches to cyber security. Another challenge is ensuring security in global networks, where information moves through different territories with different rules and laws.

On the other hand, complex information protection systems open up new opportunities for effective fight against cyber threats. They combine various protection methods and technologies. This approach reduces the risk of successful cyber attacks. In addition, complex information protection systems can use artificial intelligence and data analysis to automatically detect anomalies and threats in real time. This allows you to quickly react to new threats and attacks, ensuring a high level of security.

The importance of implementing comprehensive protection systems that take into account the variety of cyber threats and ensure reliable and sustainable protection of information resources in the future will become more important every day. This approach will help ensure the security of networks, reduce the risk of successful cyber attacks and ensure the security and confidentiality of information in today's digital world.

In general, complex information protection systems are becoming an integral part of modern information security. They help organizations ensure reliable protection of their valuable data and information resources, which is critical to their operations and success. However, in order to achieve maximum effectiveness, it is important to constantly update and improve such systems, taking into account new technological discoveries and growing cyber security threats.

Key words: Information protection, complex system, cyber security, countering cyber threats, information environment, cyber threat, information resources.

Постановка проблеми. У сучасному цифровому віці, де інформаційні технології переплітаються з усіма аспектами життя, захист інформації стає надзвичайно актуальною та критичною задачею. З ростом кількості зв'язаних пристроїв, масштабуванням хмарних сервісів та зростанням кількості кіберзагроз, традиційні методи захисту стають недостатніми для забезпечення стійкої інформаційної безпеки.

Постановка проблеми полягає в тому, щоб знайти оптимальний баланс між комплексністю та ефективністю захисту, розробити адаптивні підходи до боротьби з постійно змінними загрозами, і впровадити інтегровані системи захисту, які забезпечать високий рівень безпеки в умовах сучасного цифрового світу.

Стан опрацювання проблематики комплексної системи захисту інформації є актуальним і надзвичайно важливим у сучасному світі. З моменту виникнення перших загроз в кіберпросторі пройшла значна кількість часу.

Дослідженням цього питання займалися багато науковців, серед вагомих праць в Україні, варто згадати Яремчук Ю.Є., Павловський П.В., Катаєв В.С., Сінюгін В.В., Полотай О.І., Рожко Д.І. та багато інших.

Метою статті є висвітлення проблем з якими стикається інформаційна безпека у сучасному світі, аналіз значення комплексної системи захисту інформації та її нормативно-правової бази.

Виклад основного матеріалу. Основним шляхом пошуку захисту інформації в складних інформаційних системах є вдосконалення системного підходу до самої проблеми захисту. Під системністю розуміється, що захист інформації передбачає не лише створення відповідних захисних механізмів, але також включає регулярний процес, який застосовується на всіх етапах життєвого циклу інформаційної системи та використовує всі наявні засоби захисту. Це означає, що захист інформації повинен бути розглянутий як невід'ємна частина всієї інформаційної системи, а не просто як окремий компонент.

У сучасних умовах глобалізації та зростаючої конкуренції, захист інформації стає надзвичайно важливим аспектом як для організацій, так і для державних підприємств та корпорацій України. Створення надійних систем захисту і збереження інформаційних ресурсів на рівні всієї організації і її окремих підрозділів стає все більш актуальним, а успішність таких заходів безпосередньо впливає на конкурентоспроможність організації в цілому.

На сьогоднішній день, існують два основних підходи до визначення оптимальної стратегії побудови систем захисту інформації організацій. Перший підхід базується на перевірці відповідності рівня захищеності інформації в організації вимогам законодавчих актів або стандартів в галузі інформаційної безпеки. Однак цей підхід має свої недоліки, зокрема, коли рівень захисту інформації не визначений чітко, ускладняється вибір оптимального варіанту системи захисту.

Другий підхід використовує методи та моделі оптимізації складних систем для визначення найкращого варіанту побудови систем захисту інформації. Цей підхід дозволяє більш ефективно враховувати особливості конкретної організації та знаходити оптимальні рішення з урахуванням різноманітних факторів.

Стрімкий розвиток інформаційних технологій привів до проблем захисту інформації або забезпечення безпеки інформації. Комплексні системи захисту інформації (КСЗІ) допомагають у вирішенні цих проблем. Дослідження та огляд методів і засобів, об'єднаних єдиним цільовим призначенням, які забезпечують необхідну ефективність захисту інформації в автоматизованих системах (АС) є актуальними в цей час. Інформаційна безпека – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [3, с. 460].

Українське законодавство по своєму захищає інформацію, відповідно до ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» «Умови обробки інформа-

ції в системі Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.» [4].

Також законодавець визначає низку нормативно-правових документів у сфері комплексної системи захисту інформації:

- Закон України «Про інформацію»;
- Закон України «Про доступ до публічної інформації»;
- Закон України «Про захист персональних даних»;
- Закон України «Про електронні документи та електронний документообіг»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;
- «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» (затверджені ПКМУ від 29.03.2006 №373).

КСЗІ – це система технічних і нетехнічних заходів, що дозволяють запобігти або ускладнити можливість доступу до інформації, оброблюваної автоматизованим способом в інформаційно телекомунікаційних системах (ІТС) [2, с. 7].

До процесу створення КСЗІ залучаються такі сторони:

– організація, для якої здійснюється побудова КСЗІ (Замовник);

– організація, що здійснює заходи з побудови КСЗІ (Виконавець);

– Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) (орган контролю);

– організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);

– організація, у разі необхідності, залучена Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник) [1, с. 27].

Основною проблемою реалізації систем захисту є:

– з одного боку, забезпечення надійного захисту ідентифікації, що знаходиться в системі: унеможливлення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації та обслуговуючого персоналу;

– з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи. Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних, організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів із ЗІ [1, с. 16].

Ефективність функціонування комплексних систем захисту інформації (КСЗІ) залежить від багатьох взаємопов'язаних елементів, які взаємодіють між собою. Зазвичай, оцінка ефективності КСЗІ здійснюється шляхом аналізу різноманітних критеріїв. Відсутність єдиного підходу до розв'язання таких завдань призводить до застосування різних, незалежних один від одного, методів оцінки рівня захисту інформації.

Процес визначення ефективності систем захисту розпочинається з вибору та обґрунтування показників або критеріїв, які використовуються для оцінки ефективності КСЗІ. Після цього переходять до розробки або вибору методик розрахунку цих показників, що дозволяють оцінити рівень захисту системи.

Істотна частина проблем забезпечення захисту такої інформації може бути вирішена відомими правовими та організаційними заходами, однак, враховуючи розвиток інформаційних технологій, наявна тенденція зростання необхідності застосування технічних заходів і засобів її захисту. Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів [2, с. 7].

Комплексний (системний) підхід до побудови будь-якої системи містить в собі: перш за все, вивчення об'єкта впроваджуваної системи; оцінювання загроз безпеки об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінювання економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх і зовнішніх чинників; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця [1, с. 15].

Основні завдання, які повинна вирішувати комплексна система захисту інформації включають:

- Управління доступом користувачів до ресурсів інформаційної системи, забезпечення захисту від несанкціонованого доступу та втручання з

боку сторонніх осіб, а також з обмеженням повноважень персоналу організації та користувачів.

- Захист даних, які передаються по каналах зв'язку, щоб забезпечити конфіденційність і цілісність інформації.
- Реєстрація, збір, зберігання, обробка і видача інформації про всі події, пов'язані з безпекою системи, для забезпечення контролю та аналізу потенційних загроз.
- Контроль діяльності користувачів системи з боку адміністрації, а також оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу.
- Забезпечення цілісності критичних ресурсів системи та перевірка середовища виконання прикладних програм з метою попередження можливих загроз безпеці.
- Створення замкнутого середовища для перевіреного програмного забезпечення з метою захисту від шкідливих програм, вірусів та засобів обходу системи захисту.
- Управління засобами комплексної системи захисту, що включає їх конфігурацію, моніторинг та аналіз ефективності.

Основні принципи організації КСЗІ:

- системність;
- комплексність;
- безперервність захисту;
- розумна достатність;
- гнучкість управління і застосування;
- відкритість алгоритмів і механізмів захисту;
- простота застосування захисних заходів і засобів [1, с. 31].

Висновки. Забезпечення безпеки і захисту інформації стає надзвичайно важливим у сучасних умовах глобалізації та зростаючої конкуренції для організацій і державних підприємств України. Підхід до захисту інформації повинен бути системним і охоплювати всі аспекти процесу, від початкового проектування та розробки системи до експлуатації, підтримки та оновлення.

Стрімкий розвиток інформаційних технологій призводить до проблем захисту інформації, але комплексні системи захисту інформації (КСЗІ) допомагають у їх вирішенні. Ефективність КСЗІ залежить від взаємодії багатьох елементів, і оцінка їх ефективності вимагає вибору відповідних показників та методик розрахунку.

Законодавство України також регулює питання захисту інформації, вимагаючи застосування комплексної системи захисту з підтвердженою відповідністю для інформації з обмеженим доступом.

Загалом, ефективність систем захисту інформації визначається ретельним аналізом, плануванням та впровадженням комплексу організаційних, технологічних і технічних заходів, які забезпечують надійний захист інформації в умовах зростаючих загроз та вимог сучасного світу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Комплексні системи захисту інформації: навч. посіб. / Ю.Є. Яремчук та ін. 63-тє вид. Вінниця: ВНТУ, 2018. 119 с.
2. Матеріали VI Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології": тези доповідей, 20-21 квітня 2023 р. Кропивницький: ЦНТУ, 2023. 96 с.
3. Остапов С.Е. Технологія захисту інформації: навчальний посібник. Х.: Вид. ХНЕУ, 2013. 476 с.
4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР: станом на 1 лип. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 25.07.2023).