УДК 004.056

**М. М. Маркевич**
**Л. О. Майданевич**

# ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ: ОСОБЛИВОСТІ ОЦІНЮВАННЯ СТАНУ КІБЕРЗАХИСТУ

Вінницький національний технічний університет

**Анотація**

*У доповіді розглянуто підходи оцінювання стану кіберзахисту державних інформаційних ресурсів. Проаналізовано нормативно-правовий, ризик-орієнтований, практичний та моніторинговий підходи. Встановлено, що жоден метод окремо не забезпечує надійний кіберзахист. Нормативно-правовий підхід створює юридичний фундамент, ризик-орієнтований оптимізує ресурси, практичний виявляє вразливість, моніторинговий інтегрує всі методи. Оптимально визнано комплексне застосування підходів в єдиній системі управління кіберзахистом на базі SIEM-системи. Запропоновано інтегративну модель захисту державних інформаційних ресурсів.*

**Ключові слова**: державні інформаційні ресурси, кібербезпека, кіберзахист, підходи оцінювання стану захищеності державних інформаційних ресурсів.

***Abstract***

*The report considers approaches to assessing the state of cyber protection of state information resources. The regulatory, risk-oriented, practical and monitoring approaches are analyzed. It is established that no method separately provides reliable cyber protection. The regulatory approach creates a legal foundation, the risk-oriented optimizes resources, the practical one identifies vulnerabilities, and the monitoring one integrates all methods. The comprehensive application of approaches in a single cyber protection management system based on the SIEM system is recognized as optimal. An integrative model for protecting state information resources is proposed.*

**Keywords**: state information resources, cybersecurity, cyber protection, approaches to assessing the security status of state information resources.

## Вступ

У сучасних умовах повномасштабної кібервійни питання про захист державних інформаційних ресурсів набуває більш вагомого значення, оскільки кількість хакерських атак постійно зростає. Тому потрібно вміти їм ефективно протистояти, для цього слід знати підходи до оцінювання стану захищеності інформаційних структур та вміти їх застосовувати.

## Результати дослідження

Забезпечення результативного плану захисту державних інформаційних ресурсів вимагає системного перегляду наявних методичних рекомендацій. Аналіз нормативно-правової бази України та практичний підхід дозволяє виділити основні підходи щодо оцінювання стану захищеності інформаційних активів держави.

Почнемо з нормативно-правового підходу, який базується на створенні Комплексної системи захисту інформації (КСЗІ). До складу КСЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів [1]. Процес оцінювання здійснюється через процедуру державної експертизи на відповідність вимогам нормативних документів системи технічного захисту інформації (НД ТЗІ). Перевагою даного методу є створення нормативного підґрунтя та юридична верифікація безпеки і водночас недоліком ускладнене своєчасне реагування на нові загрози після проходження атестації через незмінність документа.

Наступним не менш важливим підходом до оцінювання стану захищеності державних інформаційних ресурсів є ризик-орієнтований підхід, який базується на застосуванні міжнародних

стандартів, зокрема ISO/IEC 27001:2022 та відповідних методичних рекомендаціях. Він містить вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою [2]. Даний метод спеціалізується на ідентифікації критичних активів, аналізі ймовірних векторів атак та прогнозуванні потенційних збитків. Пріоритетом ризик-орієнтованого підходу є можливість раціонального розподілення ресурсів та зосередження на захисті найбільш вразливих складових інформаційної безпеки системи. Проте суттєвим недоліком цього підходу є високий ступінь суб'єктивності при оцінюванні ризиків та складність прогнозування рідкісних, але критичних подій. Також слід враховувати те, що ефективна реалізація ризик-менеджменту потребує експертів високої кваліфікації та значних витрат часу.

Теоретичні підходи до оцінювання стану захищеності інформаційних ресурсів потребують практичного підтвердження, що здійснюється за допомогою технічного підходу. Він передбачає застосування постійного інструментального сканування вразливостей та проведення тестів на проникнення. Важливим етапом у нормативному регулюванні цього процесу стало прийняття Постанови КМУ № 1799 від 31.12.2025 року, яка визначає порядок здійснення державного контролю за станом захищеності інформації в інформаційно-комунікаційних системах за допомогою спеціальних технічних засобів та інструментальних методів [3]. Перевагою цього підходу є можливість виявлення суттєвих недоліків у системі до моменту використання цих вразливостей кіберзловмисниками. Недоліком – фіксування стану системи лише у час перевірки.

Найкращим підходом є моніторинговий метод до оцінювання стану захищеності інформаційних ресурсів, оскільки він поєднує у собі усі три вищезгадані підходи. Він базується на використанні систем класу SIEM (Security Information and Event Management), що дозволяють здійснювати автоматизоване оцінювання захищеності на основі аналізу мережевого трафіку та журналів подій [4]. Головною перевагою моніторингового підходу є виявлення інцидентів на ранніх стадіях. Проте впровадження такої моделі має значні недоліки: надзвичайно висока вартість апаратних і програмних засобів, а також гострий дефіцит кваліфікованих кадрів, здатних аналізувати величезні масиви даних.

**Висновки**

Отже, в умовах сучасної кібервійни жоден із розглянутих підходів не є самодостатнім для гарантування оцінювання стану кіберзахисту державних інформаційних ресурсів. Нормативно-правовий підхід через створення КСЗІ забезпечує юридичний фундамент захисту, тоді як ризик-орієнтований дозволяє ефективно розподіляти ресурси на важливі складові системи безпеки. Практичний підхід надає об'єктивну оцінку вразливостей системи за допомогою спеціальних технічних засобів. Найбільш сучасним є моніторинговий підхід, що інтегрує у собі три попередні підходи. Оптимальним варіантом для забезпечення стану захищеності державних інформаційних ресурсів є поєднання всіх методів у єдину систему управління кіберзахистом при використанні систем класу SIEM.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Державна служба спеціального зв'язку та захисту інформації України. Поради (рекомендації) щодо створення КСЗІ в ІКС, які використовуються для надання послуг доступу до мережі Інтернет. URL: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet (дата звернення: 18.02.2026)
2. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf (дата звернення: 18.02.2026)
3. Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури. Кабінет Міністрів України: постанова від 31 грудня 2025 р. № 1799. Київ, 2025. URL: https://zakon.rada.gov.ua/laws/show/1799-2025-%D0%BF#Text (дата звернення: 18.02.2026)
4. Моніторинг процесів функціонування інформаційно-комунікаційних систем (ІКС). Луцьк : ЛНТУ. URL: https://e-tk.lntu.edu.ua/pluginfile.php/25373/mod_resource/content/1/%D0%A2%D0%95%D0%9C%D0%90%2014.pdf (дата звернення: 19.02.2026)

***Маркевич Мар'яна Михайлівна*** – студентка групи 1БКС-23б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: 7mariaanaa@gmail.com

***Майданевич Леонід Олександрович*** – канд. філос. наук, доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com

***Markevych Mariana*** – student of group 1BKS-23b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: 7mariaanaa@gmail.com

***Maidanevych Leonid*** – PhD in Philosophical Sciences, Associated Professor, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: lmaidanevych@gmail.com