УДК 004.94:378.147.6
DOI https://doi.org/10.26661/2786-6254-2024-2-10

АНАЛІЗ ПІДХОДІВ ДО СТВОРЕННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЛЯ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ ТА НАУКОВИХ УСТАНОВ

Шило Г. М.
здобувач освіти другого (магістерського) рівня
кафедри інфокомунікаційної інженерії імені В. В. Поповського
Харківський національний університет радіоелектроніки
просп. Науки, 14, Харків, Україна;
доктор технічних наук, професор,
завідувач кафедри комп'ютерних наук
Запорізький національний університет
вул. Університетська, 66, Запоріжжя, Україна
orcid.org/0000-0002-5020-6707
shilo.gn@gmail.com

Добринін І. С.
кандидат технічних наук, доцент,
доцент кафедри інфокомунікаційної інженерії імені В. В. Поповського
Харківський національний університет радіоелектроніки
просп. Науки, 14, Харків, Україна
orcid.org/0000-0001-8910-2609
ihor.dobrynin@nure.ua

Матвіїшина Н. В.
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних наук
Запорізький національний університет
вул. Університетська, 66, Запоріжжя, Україна
orcid.org/0000-0001-7938-4622
mnv2902@gmail.com

Ключові слова: *інформаційна безпека, метод аналізу ієрархій, методи прийняття рішень, багатокритеріальна оптимізація, кіберстійкість.*

У статті розглянуто особливості впровадження систем управління інформаційною безпекою (СУІБ) у закладах вищої освіти та наукових установах. Показано актуальність захисту інформаційних активів, зокрема персональних даних здобувачів і співробітників, конфіденційних досліджень і технологій подвійного призначення в умовах зростання кіберзагроз. Проведено аналіз поточного стану інформаційної безпеки в українських навчальних закладах, що виявляє основні проблеми, як-от обмежене фінансування, нестача кваліфікованих фахівців та відсутність стандартизованих підходів. Досліджено досвід упровадження систем управління інформаційною безпекою в університетах різних країн.

У статті розглядаються різні методики побудови СУІБ, що містить лінійку міжнародних стандартів ISO/IEC 27000, методологію IT-Grundschutz та вимоги Національного банку України. Здійснено порівняння цих підходів із погляду ефективності, гнучкості та відповідності нормативним вимогам. Для вибору оптимальної методики використано метод аналізу ієрархій (AHP), що дає змогу оцінити й порівняти альтернативи на основі

багатьох критеріїв: сфера застосування; орієнтація; гнучкість; технічна деталізація; сертифікація; юридична відповідність; витрати на впровадження.
З огляду на специфіку діяльності навчальних закладів і відповідність міжнародним стандартам, зроблено висновок, що найбільш ефективним підходом до створення СУІБ є використання лінійки міжнародних стандартів ISO/IEC 27000. Основними перевагами розробки СУІБ на базі стандарту ISO/IEC 27001:2022 для університетів є універсальність та можливість проведення сертифікації, яка зміцнює довіру партнерів і державних структур, а також розширює можливості міжнародного співробітництва. Запропоновано основні поступові кроки впровадження СУІБ за ISO/IEC 27001:2022, починаючи від діагностичного аудиту й розробки політик до сертифікації та постійного вдосконалення. Підкреслено важливість системного підходу до інформаційної безпеки у вищих навчальних закладах і наукових установах, що дасть змогу забезпечити стабільну роботу та міжнародну співпрацю.

ANALYSIS OF APPROACHES TO CREATING INFORMATION SECURITY MANAGEMENT SYSTEMS FOR HIGHER EDUCATION INSTITUTIONS AND RESEARCH ESTABLISHMENTS

Shilo G. M.
Master's Degree Student at the V. V. Popovskyy Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics
Nauky Ave., 14, Kharkiv, Ukraine;
Doctor of Technical Sciences, Professor,
Head of the Department of Computer Science
Zaporizhzhia National University,
Universytetska str., 66, Zaporizhzhia, Ukraine
orcid.org/0000-0002-5020-6707
shilo.gn@gmail.com

Dobrynin I. S.
Ph.D. in Technical Sciences, Associate Professor,
Associate Professor at the V. V. Popovskyy Department of Infocommunication Engineering
Kharkiv National University of Radio Electronic
Nauky Ave., 14, Kharkiv, Ukraine
orcid.org/0000-0001-8910-2609
ihor.dobrynin@nure.ua

Matviyishyna N. V.
Ph.D. in Technical Sciences, Associate Professor,
Associate Professor at the Department of Computer Science
Zaporizhzhia National University
Universytetska str., 66, Zaporizhzhia, Ukraine
orcid.org/0000-0001-7938-4622
mnv2902@gmail.com

Key words: *Information Security, Analytic Hierarchy Process, Decision-Making Methods, Multi-Criteria Optimization, Cyber Resilience.*

The article examines the peculiarities of implementing Information Security Management Systems (ISMS) in higher education institutions and research establishments. It highlights the relevance of protecting information assets, particularly students' and staff's personal data, confidential research, and dual-use technologies, amid growing cyber threats. The current state of information

security in Ukrainian educational institutions is analyzed, identifying key issues such as limited funding, a lack of qualified professionals, and the absence of standardized approaches. The experience of implementing ISMS in universities across different countries is also explored.
The article reviews various ISMS construction methodologies, including international standards ISO/IEC 27000, the IT-Grundschutz methodology, and the requirements of the National Bank of Ukraine. These approaches are compared in terms of efficiency, flexibility, and compliance with regulatory requirements. The Analytic Hierarchy Process (AHP) is utilized to select the optimal methodology, allowing the evaluation and comparison of alternatives based on multiple criteria: scope of application, orientation, flexibility, technical detailing, certification, legal compliance, and implementation costs.
The conclusion is drawn that, given the specifics of educational institutions and the need for international standards compliance, the most effective approach to ISMS creation is the use of ISO/IEC 27000 international standards. The main advantages of developing an ISMS based on the ISO/IEC 27001:2022 standard for universities include its universality and the possibility of certification, which strengthens trust among partners and government bodies and expands opportunities for international cooperation. The article proposes key incremental steps for implementing ISMS under ISO/IEC 27001:2022, starting from initial auditing and policy development to certification and continuous improvement. The importance of a systematic approach to information security in higher education institutions and research establishments is emphasized, ensuring stable operation and international collaboration.

Вступ. У сучасному світі питання забезпечення інформаційної безпеки набуває особливого значення. Це стосується не лише комерційних організацій, а й закладів вищої освіти та наукових установ, які зберігають великий обсяг даних, що містять результати наукових досліджень, інноваційні розробки, технології подвійного призначення, внутрішню конфіденційну інформацію, персональні дані співробітників та здобувачів. В умовах зростаючої кількості кіберзагроз виникає потреба у створенні ефективних систем управління інформаційною безпекою (СУІБ), які забезпечать можливість захисту інформаційних ресурсів та усунення ризиків, що є критичними для діяльності закладів і установ. Однак відсутність стандартизованих підходів для навчальних закладів і наукових установ України, труднощі з виділенням достатніх фінансових ресурсів, проблеми з пошуком фахівців з інформаційної безпеки ускладнюють процес впровадження та підтримки СУІБ.

Актуальність проведення цього дослідження зумовлена потребою в забезпеченні конфіденційності, цілісності та доступності інформаційних ресурсів і розробці уніфікованого підходу для створення СУІБ закладів вищої освіти та наукових установ. Крім того, належний рівень інформаційної безпеки є ключовим фактором для підтримки довіри партнерів і розвитку міжнародної співпраці. Упровадження ефективних СУІБ сприятиме не лише підвищенню рівня кіберстійкості цих установ, а й створенню умов для їхнього сталого розвитку.

Об’єктом цього дослідження є процеси створення та впровадження систем управління інформаційною безпекою в закладах вищої освіти й наукових установах України. Метою дослідження є вибір оптимальної методики побудови СУІБ, яка забезпечить високий рівень захисту інформації, відповідність міжнародним стандартам і сприятиме розвитку міжнародної співпраці.

Основними завданнями дослідження є:

– визначення критеріїв для порівняння різних методик створення СУІБ;

– аналіз наявних підходів до побудови СУІБ за допомогою методів багатокритеріальної оптимізації;

– визначення основних кроків впровадження вибраної методики для підвищення кіберстійкості організацій.

Гіпотезою дослідження є припущення, що застосування методу аналізу ієрархій для вибору методики побудови СУІБ дасть змогу знайти оптимальне рішення, яке враховуватиме специфіку діяльності навчально-наукових закладів, забезпечить їхню інформаційну безпеку, відповідність нормативно-правовим актам і міжнародним стандартам.

Отже, проведення цього дослідження є важливим кроком у підвищенні рівня інформаційної безпеки закладів вищої освіти й наукових установ України та сприятиме їхній успішній інтеграції у світову наукову спільноту.

Огляд літератури. Під час створення моделі інформаційної безпеки в університетах України основний акцент робиться на захисті персональних даних здобувачів і співробітників, збереженні конфіденційності дослідницької інформації, на дотриманні законодавства України щодо захисту інформації, а також інтеграції з національними системами: системою електронного документообігу й електронними кабінетами здобувачів. Університети стикаються з такими проблемами, як відсутність стандартизованих підходів щодо створення СУІБ, обмежене фінансування, нестача кваліфікованих кадрів, складність інтеграції сучасних засобів захисту із застарілими інформаційними системами. Враховуючи такі умови, в університетах вирішують окремі задачі щодо інформаційної безпеки: створю-

ють відділи, наприклад служби захисту інформації, до основних завдань яких входить організація та координація робіт, пов'язаних із захистом інформації в автоматизованих системах. В окремих університетах також розробляють політики інформаційної безпеки, проте аналіз показав, що проблема потребує комплексного вирішення у всіх закладах вищої освіти та наукових установах України.

Досвід закордонних університетів демонструє використання міжнародних стандартів ISO/IEC 27001, NIST, GDPR (для країн ЄС) та інших, що забезпечують високий рівень відповідності міжнародним вимогам. Значна увага приділяється захисту наукових досліджень, захисту інтелектуальної власності, а також управлінню ризиками. Аналіз впровадження СУІБ у вищих навчальних закладах наведено в публікаціях [1]–[5]. А саме автори наголошують на важливості проведення аналізу ризиків, розробки політик безпеки та наводять детальний план впровадження СУІБ на основі стандарту ISO/IEC 27001:2013 [1]. Також дослідження підтверджують, що впровадження СУІБ дає змогу значно зменшити ризики втрати даних і підвищити рівень довіри з боку партнерів і здобувачів [2]. У публікаціях підкреслюється значення стандартів ISO/IEC 27001 та NIST Cybersecurity Framework у забезпеченні кібербезпеки у вищих навчальних закладах [3]. Особливу увагу також приділено аналізу ключових загроз і вразливостей, з якими стикаються університети, та пропонуються стратегії їхньої мінімізації [4]. Для планування подальших кроків у вдосконаленні систем безпеки пропонується модель для оцінки зрілості інформаційної безпеки [5]. Отже, впровадження СУІБ є ключовим фактором у забезпеченні інформаційної безпеки вищих навчальних закладів і наукових установ. Вибір відповідної методики та її адаптація до конкретних умов є критично важливими для досягнення високого рівня захисту інформаційних ресурсів.

Заклади вищої освіти та наукові установи потребують ефективної системи управління інформаційною безпекою для забезпечення захисту даних, підтримки стабільності роботи й відповідності нормативним вимогам. Найчастіше для створення таких системи застосовують стандарти ISO/IEC 27001:2022, методологію IT-Grundschutz та вимоги Національного банку України. Аналіз переваг і недоліків цих підходів надає можливість вибрати ефективний спосіб створення СУІБ. Вибір оптимальної методики потребує врахування критеріїв, пов'язаних із вартістю впровадження, можливістю міжнародної сертифікації, урахування ризик-орієнтованого підходу тощо.

До вивчення проблеми прийняття рішень в умовах наявності багатьох критеріїв долучалися відомі вітчизняні та зарубіжні вчені як у сфері економіки, так і у сфері математичного моделювання. Це насамперед Т. Сааті [6], А. В. Лотов, В. В. Вітлінський, М. О. Перестюк, С. І. Наконечний та багато інших. Значна кількість наукових праць присвячена можливостям використання методу аналізу ієрархій у різних галузях економіки та соціології, зокрема, це роботи В. І. Дубровіна, І. С. Скітера, Е. Ю. Сахна, С. В. Мамалиги, М. А. Синенко [7].

Методи. Для вирішення задачі багатокритеріальної оптимізації та вибору оптимальної методики створення СУІБ організацій може бути використано метод аналізу ієрархій [8] (Analytic Hierarchy Process, AHP) – це потужний інструмент, розроблений Томасом Сааті, який використовується для вирішення складних задач прийняття рішень, де присутні множинні, часто суперечливі критерії [6]. Цей метод дає змогу структурувати складну проблему, розбиваючи її на ієрархію більш простих елементів, і порівнювати ці елементи попарно.

Основні принципи AHP:

– ієрархічна структура (проблема розбивається на ієрархію рівнів: мета, критерії, альтернативи; кожен наступний рівень деталізує попередній);

– попарні порівняння (елементи кожного рівня порівнюються попарно за важливістю або бажаністю; для цього можна використовувати шкалу Сааті, яка дає змогу виразити відносну важливість одного елемента щодо іншого);

– синтез суджень (отримані за результатами попарних порівнянь судження синтезуються для визначення вагових коефіцієнтів кожного елемента);

– консистентність суджень (метод AHP дає можливість перевірити, наскільки судження експерта є узгодженими; якщо судження несуперечливі, то отримані результати будуть більш надійними).

Етапи застосування AHP:

– формулювання проблеми (чітке формулювання мети й визначення альтернативних рішень);

– побудова ієрархії (розбиття проблеми на ієрархію рівнів);

– попарні порівняння (порівняння елементів кожного рівня за шкалою Сааті);

– перевірка консистентності (оцінка узгодженості суджень експерта);

– синтез суджень (обчислення вагових коефіцієнтів для кожного елемента);

– прийняття рішення (вибір альтернативи з найбільшим загальним ваговим коефіцієнтом).

Результати

Визначення критеріїв для порівняння різних методик створення СУІБ

Для визначення критеріїв та вибору ефективного способу створення СУІБ було проведено аналіз переваг і недоліків стандартів ISO/IEC 27001:2022 [9], методології IT-Grundschutz [10] та вимог Національного банку України [11].

Стандарт ISO/IEC 27001:2022 пропонує міжнародно визнану структуру для управління ризиками інформаційної безпеки. Він забезпечує адаптацію до будь-якого типу організацій, включно з навчальними закладами та науковими центрами. Використання стандарту надає можливість:

– врахувати контекст організації та середовища, а саме технологічну інфраструктуру, законодавство України та міжнародне партнерство;

– провести оцінювання ризиків, а саме ідентифікацію вразливостей для інформаційної інфраструктури;

– розробити заходи контролю, що спрямовані на забезпечення конфіденційності, цілісності й доступності інформаційних активів, а саме впровадити заходи безпеки з каталогу стандарту;

– проводити моніторинг, що забезпечить постійний контроль за ефективністю СУІБ і її вдосконалення.

Основними перевагами розробки СУІБ на базі стандарту ISO/IEC 27001:2022 для університетів є універсальність і можливість інтеграції з іншими міжнародними стандартами та можливість проведення сертифікації, яка зміцнює довіру партнерів і державних структур, а також розширює можливості міжнародного співробітництва.

До обмежень можна віднести високі витрати на впровадження та відсутність технічних специфікацій, які потрібно розробляти окремо.

На відміну від стандарту ISO/IEC 27001:2022 методологія компанії IT-Grundschutz орієнтована на використання шаблонних підходів до забезпечення інформаційної безпеки, а саме пропонує стандартизовані заходи, які можна адаптувати для навчальних закладів і наукових установ. Застосування методології дає можливість:

– вибрати захисні механізми з готових рішень для інфраструктури організації;

– проводити моделювання загроз і використовувати шаблони для оцінювання ризиків. Наприклад, сценарії атак на хмарні сервіси, IoT-обладнання;

– застосовувати практичні інструкції щодо впровадження захисту для апаратного забезпечення, програмного коду, мережевих інтерфейсів.

Основними перевагами використання методологія IT-Grundschutz є чіткі рекомендації щодо технічної реалізації, скорочення часу на впровадження стандартних рішень. Однак цей підхід менш гнучкий порівняно з ISO/IEC 27001 і потребує додаткових ресурсів для адаптації до українського законодавства.

Вимоги Національного банку України (НБУ) стосуються фінансових установ, але їх можна застосувати для державних і критичних об'єктів інфраструктури, зокрема наукових установ. Розробка СУІБ відповідно до вимог НБУ дає змогу:

– провести класифікації критичних активів;

– забезпечити контроль доступу, а саме впровадження жорстких механізмів автентифікації та моніторингу доступу до даних;

– розробити політику реагування на кіберінциденти, регулярне тестування планів реагування;

– забезпечити юридичну відповідність, а саме забезпечення узгодженості з GDPR та ЗУ «Про захист інформації в інформаційно-комунікаційних системах».

До переваг використання вимог НБУ для закладів вищої освіти та наукових установ можна віднести жорсткий регламент, який забезпечує високий рівень захисту; орієнтацію на ризик-орієнтоване управління; врахування локальних нормативних вимог. Однак у цьому підході виникають складнощі інтеграції з міжнародними стандартами без адаптації та необхідність модифікації для навчальних закладів, тому що основний фокус вимог на банківський сфері. Для порівняння підходів було визначено критерії: сфера застосування, орієнтація, гнучкість, технічна деталізація, сертифікація, юридична відповідність та витрати на впровадження (табл. 1).

Таблиця 1

Порівняльна таблиця підходів до створення СУІБ для навчально-наукових центрів закладів вищої освіти

Критерій	ISO/IEC 27001:2022	IT-Grundschutz	Вимоги НБУ
Сфера застосування	Універсальна	Шаблонні рішення для державних і великих організацій	Банківський сектор і критична інфраструктура
Орієнтація	Ризик-орієнтований підхід	Технічні шаблони та заходи	Регуляторний контроль
Гнучкість	Висока	Середня	Низька
Технічна деталізація	Загальний підхід	Детальні технічні рекомендації	Деталізовані вимоги
Сертифікація	Міжнародна сертифікація можлива	Сертифікація Grundschutz-Profil	Внутрішній аудит, контроль НБУ
Юридична відповідність	Локальні та міжнародні закони	Переважно локальний контекст Німеччини	Відповідність українському законодавству
Витрати на впровадження	Високі	Середні	Високі (через потребу в адаптації до навчально-наукового центру

Аналіз наявних підходів до побудови СУІБ за допомогою методу аналізу ієрархій

Формулювання проблеми – вибрати оптимальну методику побудови СУІБ для університетів і наукових установ за методом аналізу ієрархій. Визначено альтернативи: ISO/IEC 27001:2022, IT-Grundschutz, Вимоги НБУ. Визначено критерії: сфера застосування (1), орієнтація (2), гнучкість (3), технічна деталізація (4), сертифікація (5), юридична відповідність (6) і витрати на впровадження (7).

Побудова ієрархії. На рис. 1 представлено ієрархічну модель побудови СУІБ для закладів вищої освіти та наукових установ, на якій зазначено мету, перелік критеріїв та альтернатив.

Попарні порівняння за шкалою Сааті. Визначається відносна важливість кожної пари критеріїв. Для цього використовується шкала Сааті [6]:

– 1 – критерії однаково важливі;

– 3 – один критерій дещо важливіший за інший;

– 5 – значно важливіший;

– 7 – суттєво важливіший;

– 9 – абсолютно важливіший;

– проміжні значення (2, 4, 6, 8) використовуються для уточнень.

Для критеріїв, визначених у формулюванні проблеми, за результатами експертних оцінювань отримано матрицю парних порівнянь (табл. 2).

Матриця вказує, що основними пріоритетами у виборі методики побудови СУІБ є такі:

− наскільки методика охоплює потрібну сферу застосування;

− наскільки методика відповідає орієнтації на певний вид управління;

− якими є витрати на впровадження.

Таблиця 2

Матриця парних порівнянь для критеріїв другого рівня ієрархії

Критерії	1	2	3	4	5	6	7
1	1	3	5	7	5	3	2
2	1/3	1	3	5	3	2	1
3	1/5	1/3	1	3	2	1	1/2
4	1/7	1/5	1/3	1	2	1	1/3
5	1/5	1/3	1/2	1/2	1	3	2
6	1/3	1/2	1	1	1/3	1	2
7	1/2	1	2	3	1/2	1/2	1

Визначення вектора пріоритетів – нормалізованого набору значень, де кожний елемент вектора є часткою важливості певного критерію.

Для розрахунку вектора пріоритетів виконано такі кроки:

– обчислено суму стовпців матриці парних порівнянь для критеріїв другого рівня ієрархії (табл. 2):

S = [2,7095; 6,3666; 12,8333; 20,5000; 13,8333; 11,5000; 8,8300];

– визначено нормалізовану матрицю, кожний елемент якої поділено на суму відповідного стовпця (табл. 3).

Таблиця 3

Нормалізована матриця

0,3691	0,4712	0,3896	0,3415	0,3614	0,2609	0,2265
0,1230	0,1571	0,2338	0,2439	0,2169	0,1739	0,1133
0,0738	0,0524	0,0779	0,1463	0,1446	0,0870	0,0566
0,0527	0,0314	0,0260	0,0488	0,1446	0,0870	0,0374
0,0738	0,0524	0,0390	0,0244	0,0723	0,2609	0,2265
0,1230	0,0785	0,0779	0,0488	0,0241	0,0870	0,2265
0,1845	0,1571	0,1558	0,1463	0,0361	0,0435	0,1133

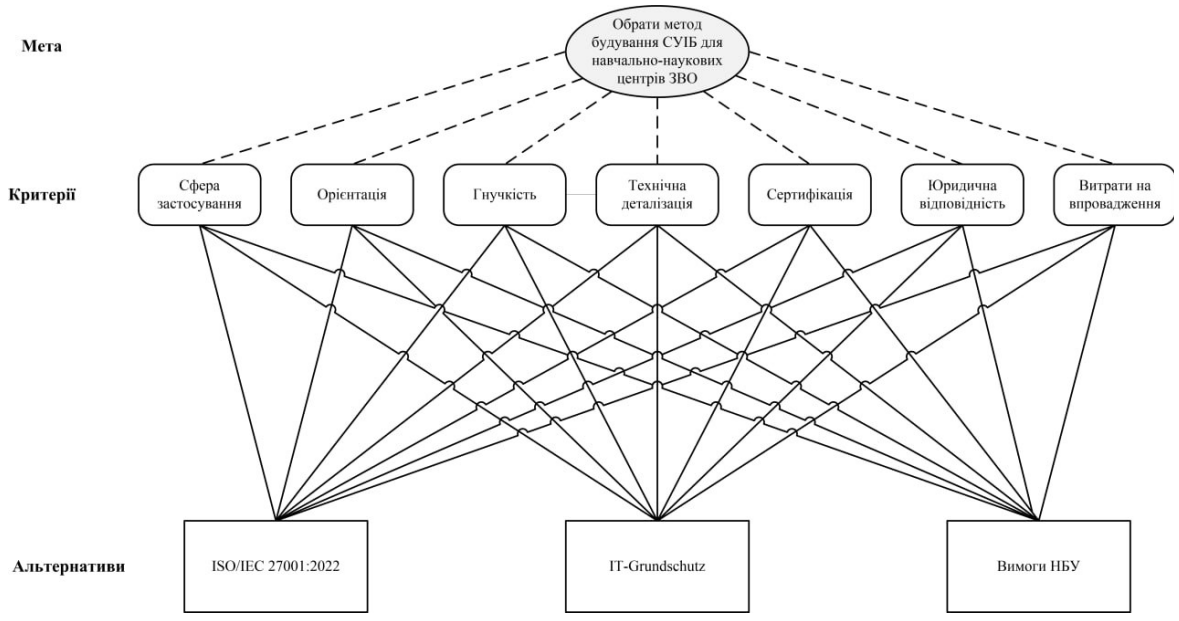

Рис. 1. Ієрархічна модель вибору методу побудови СУІБ

Вектор пріоритетів для критеріїв наведеної задачі дорівнює середньому значенню рядків нормалізованої матриці W = [0,3457; 0,1802; 0.0912; 0,0612; 0,1070; 0,0951; 0,1195] (табл. 4).

Таблиця 4

Критерії та їхні вагові коефіцієнти

Критерій	Вага
Сфера застосування	0,3457 (34,47 %)
Орієнтація	0,1802 (18,2 %)
Гнучкість	0,0912 (9,12 %)
Технічна деталізація	0,0612 (6,12 %)
Сертифікація	0,1070 (10,70 %)
Юридична відповідність	0,0951 (9,51 %)
Витрати на впровадження	0,1195 (11,95 %)

Оцінка альтернатив. Альтернативи, які розглядаються для оцінювання:

− ISO/IEC 27001:2022 – міжнародний стандарт із загальними вимогами до СУІБ;

− IT-Grundschutz – німецька методика з фокусуванням на деталізацію та готові шаблони;

− вимоги НБУ – нормативна база для українських фінансових установ.

Для кожного критерію оцінюється кожна альтернатива (табл. 5):

– 1 – низький рівень відповідності критерію;

– 3 – середній рівень;

– 5 – високий рівень.

Таблиця 5

Оцінки альтернатив

Критерій	ISO/IEC 27001:2022	IT-Grundschutz	Вимоги НБУ
Сфера застосування	5	4	3
Орієнтація	4	3	5
Гнучкість	4	5	2
Технічна деталізація	3	5	2
Сертифікація	5	4	2
Юридична відповідність	4	3	5
Витрати на впровадження	3	4	5

Розрахунок. Рейтинг альтернативи обчислюється за формулою:

$$\text{Рейтинг альтернативи} = \sum_{i=1}^{n} (\text{вага критерію}_i \cdot \text{оцінка}_i)$$

Результати обчислень наведено в табл. 6.

Таблиця 6

Рейтинг альтернатив

Альтернатива	Рейтинг
ISO/IEC 27001:2022	4,2716
IT-Grundschutz	3,8767
Вимоги НБУ	3,5299

Отже, ISO/IEC 27001:2022 має найвищий рейтинг, який дорівнює 4,27, оскільки добре відповідає таким важливим критеріям, як *сфера застосування*, *сертифікація* і *юридична відповідність*. IT-Grundschutz має рейтинг 3,88, цей підхід отримав сильні оцінки за *гнучкість* і *технічну деталізацію*, але поступається за *орієнтацією* та *сферою застосування*. Вимоги НБУ отримали рейтинг 3,53 та показали найкращий результат за *юридичною відповідністю* та *витратами*, але мають низькі оцінки за *гнучкість* і *технічну деталізацію*.

Висновки. Запровадження систем управління інформаційною безпекою (СУІБ) в університетах і наукових установах є критично важливим для захисту інформаційних активів в умовах зростання кіберзагроз. Підхід, базований на стандарті ISO/IEC 27001:2022, забезпечує комплексний процес створення СУІБ. Для ефективного впровадження в університетах і наукових установах України потрібно стандартизувати основні етапи для цього типу організацій. Пропонується здійснювати впровадження СУІБ в університетах і наукових установах у п’ять основних етапів:

– підготовчий етап, що дасть можливість проведення діагностичного аудиту для оцінки поточного стану інформаційної безпеки; ідентифікації критичних активів і загроз; розробки та впровадження політик інформаційної безпеки; формування команди з інформаційної безпеки;

– впровадження основних заходів, що забезпечить налаштування технічних засобів захисту, як-от системи контролю доступу, антивірусне програмне забезпечення; проведення навчання персоналу з основ інформаційної безпеки; розробку плану реагування на інциденти;

– посилення й оптимізація, що містить процедури проведення детального аналізу ризиків та управління; встановлення систем моніторингу та контролю мережевого трафіку; оновлення політик відповідно до нових законодавчих вимог і технологічних змін;

– проведення аудиту для оцінки відповідності вимогам ISO/IEC 27001:2022; підготовка до зовнішніх аудитів (другою та третьою стороною); отримання сертифікату відповідності;

– підтримка та вдосконалення, що забезпечує регулярний внутрішній та зовнішній аудит для підтримання відповідності стандарту; постійне вдосконалення політик і процедур; підвищення обізнаності персоналу про нові загрози та методи захисту.

Опис кожного етапу дає чітке розуміння проблеми, яка має бути вирішена. Етапи розроблено так, щоб перехід від початкового етапу до кожного наступного не потребував надмірних фінансових витрат і надмірного часу.

Отже, такий підхід сприятиме запровадженню поступового введення нових процедур і забезпеченню високого рівня кіберстійкості, що дасть змогу університетам та науковим установам не лише ефективно захищати свої інформаційні ресурси, а й зміцнити довіру партнерів і державних структур, а також розширити можливості міжнародної співпраці.

ЛІТЕРАТУРА

1. Marhad S.S., Abd Goni S.Z., Abdullah Sani M.K.J. Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal*. 2024. Vol. 9, SI18. P. 197–203. DOI: https://doi.org/10.21834/e-bpj.v9isi18.5483 (date of access: 30.11.2024).
2. Hernandez Collante L., Pranolo A., Prasetya Wibawa A. Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis. Case study: Higher education institution. *Transactions on Energy Systems and Engineering Applications*. 2024. Vol. 5, no. 2. P. 1–20. DOI: https://doi.org/10.32397/tesea.vol5.n2.635 (date of access: 30.11.2024).
3. Amine A.M., Chakir E.M., Issam T., Khamlichi Y.I. A Review of Cybersecurity Management Standards Applied in Higher Education Institutions. *International Journal of Safety and Security Engineering*. 2023. Vol. 13, no. 6. P. 1109–1116. DOI: https://doi.org/10.18280/ijsse.130614 (date of access: 30.11.2024).
4. Ulven J.B., Wangen G. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*. 2021. Vol. 13, no. 2. P. 39. DOI: https://doi.org/10.3390/fi13020039 (date of access: 30.11.2024).
5. Makupi D. A Design of Information Security Maturity Model for Universities Based on ISO 27001. The International Journal of Business & Management. 2019. Vol. 7, no. 6. P. 134–139. DOI: https://doi.org/10.24940/theijbm/2019/v7/i6/bm1906-038 (date of access: 30.11.2024).
6. Saaty T. L. Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process. Pittsburgh : RWS Publications, 2013. 477 p.
7. Синенко М. Метод Сааті при прийнятті управлінських рішень на прикладі підприємства малого бізнесу. *Інтелект XXI*. 2018. № 1. С. 235–238.
8. Фукс М. Моделювання багатокритеріальної задачі оптимізації вибору методики побудови СУІБ методами Томаса Сааті. *Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій* : матеріали 28-го Міжнар. молодіж. форуму, м. Харків, 16–18 квіт. 2024 р. Харків, 2024. С. 92–93.
9. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL: https://www.iso.org/standard/27001 (date of access: 30.11.2024).
10. IT-Grundschutz. A systematic basis for information security. Federal Office for Information Security. URL: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (дата звернення: 30.11.2024).
11. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : постанова Нац. банку України від 28.09.2017 № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (дата звернення: 30.11.2024).

REFERENCES

1. Marhad, S.S., Abd Goni, S.Z., Abdullah Sani, M.K.J. (2024). Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal.* Vol. 9, SI18. P. 197–203. DOI: https://doi.org/10.21834/e-bpj.v9isi18.5483 (date of access: 30.11.2024).
2. Hernandez Collante, L., Pranolo, A., Prasetya Wibawa, A. (2024). Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis. Case study: Higher education institution. *Transactions on Energy Systems and Engineering Applications*. Vol. 5, no. 2. P. 1–20. DOI: https://doi.org/10.32397/tesea.vol5.n2.635 (date of access: 30.11.2024).
3. Amine, A.M., Chakir, E.M., Issam, T., Khamlichi, Y.I. (2023). A Review of Cybersecurity Management Standards Applied in Higher Education Institutions. *International Journal of Safety and Security Engineering*. Vol. 13, no. 6. P. 1109–1116. DOI: https://doi.org/10.18280/ijsse.130614 (date of access: 30.11.2024).
4. Ulven, J.B., Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*. Vol. 13, no. 2. P. 39. DOI: https://doi.org/10.3390/fi13020039 (date of access: 30.11.2024).
5. Makupi, D. (2019). A Design of Information Security Maturity Model for Universities Based on ISO 27001. *The International Journal of Business & Management.* Vol. 7, no. 6. P. 134–139. DOI: https://doi.org/10.24940/theijbm/2019/v7/i6/bm1906-038 (date of access: 30.11.2024).

6. Saaty, T.L. (2013). Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process. Pittsburgh: RWS Publications, 477 p.
7. Synenko, M. (2018). Metod Saati pry pryiniatti upravlinskykh rishen na prykladi pidpryiemstva maloho biznesu. *Intelekt XXI*. No. 1. P. 235–238.
8. Fuks, M. (2024). Modeliuvannia bahatokryterialnoi zadachi optymizatsii vyboru metodyky pobudovy SUIB metodamy Tomasa Saati. *Perspektyvy rozvytku infokomunikatsii ta informatsiino-vymiriuvalnykh tekhnolohii*: materialy 28-ho Mizhnar. molodizh. forumu, m. Kharkiv, 16–18 kvit. 2024 r. Kharkiv, p. 92–93.
9. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL: https://www.iso.org/standard/27001 (date of access: 30.11.2024).
10. IT-Grundschutz. A systematic basis for information security. Federal Office for Information Security. URL: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (date of access: 30.11.2024).
11. Pro zatverdzhennia Polozhennia pro orhanizatsiiu zakhodiv iz zabezpechennia informatsiinoi bezpeky v bankivskii systemi Ukrainy: postanova Nats. banku Ukrainy vid 28.09.2017 № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (date of access: 30.11.2024).