DOI 10.15276/imms.v15.no1.137
УДК 004.04

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No.1, pp. 137-149

МЕТОДОЛОГІЯ ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ БАГАТОРІВНЕВОЇ МОДЕЛІ КІБЕРЗАХИСТУ ЗГІДНО З ВИМОГАМИ ЗАКОНОДАВСТВА УКРАЇНИ

В.В. Яцків, С.В. Івасьєв, А.Я. Давлетова, Л.М. Тимошенко

Західноукраїнський національний університет
11, Львівська вул., м. Тернопіль, 46020, Україна
Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Emails: jazkiv@ukr.net, stepan.ivasiev@gmail.com, a7davletova@gmail.com, l.m.timoshenko@op.edu.ua

Робота присвячена практичним аспектам впровадження системи управління інформаційною безпекою (СУІБ) у державних установах відповідно до вимог Закону України №4336-IX. В межах дослідження проведено комплексний аналіз законодавчих вимог до організації та функціонування СУІБ, зокрема щодо побудови, впровадження, моніторингу і постійного удосконалення заходів кібербезпеки. Визначено п'ятирівневу структуру системи кіберзахисту, яка включає політичний, організаційний, технічний, оперативний та контрольний рівні, кожен із яких виконує свої функції у забезпеченні цілісності, конфіденційності та доступності інформації. Розроблено алгоритм організації та поетапного впровадження СУІБ на основі міжнародного стандарту ISO/IEC 27001, який адаптовано до особливостей українського законодавчого поля та практичних вимог державного сектору. З метою підвищення ефективності реалізації системи створено таблицю відповідності між положеннями Закону України №4336-IX та вимогами ISO/IEC 27001, що дозволяє перетворити нормативні вимоги у конкретні елементи СУІБ. В роботі представлено детальний план-графік впровадження СУІБ із чітким визначенням етапів, відповідальних виконавців, контрольних точок та очікуваних результатів, що забезпечує прозорість і керованість процесу. Окрему увагу приділено практичним рекомендаціям щодо технічних і організаційних заходів, спрямованих на підвищення рівня кіберзахисту інформаційних ресурсів. Запропоновані рішення сприяють не лише виконанню вимог чинного законодавства, але й формуванню системного підходу до управління кіберризиками, що є критично важливим в умовах сучасних викликів інформаційної безпеки. Результати дослідження можуть бути використані для оптимізації процесів забезпечення інформаційної безпеки, підвищення кіберстійкості та захисту критичної інформаційної інфраструктури.

Ключові слова: кіберзахист, інформаційна безпека, система управління інформаційною безпекою, ISO/IEC 27001, Закон України №4336-IX, критична інформаційна інфраструктура, державні інформаційні ресурси.

Вступ. В умовах загострення кіберзагроз та активізації інформаційної війни питання захисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури набули особливої актуальності. Прийняття Закону України №4336-IX "Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури" [1] стало важливим кроком у формуванні комплексної системи національної кібербезпеки.

Закон визначає основні рівні системи кіберзахисту, які повинні функціонувати як єдиний взаємопов'язаний механізм. Особливого значення набувають вимоги щодо резервного копіювання, шифрування даних, заборони розміщення інформаційних систем на території держави-агресора, а також створення національної системи реагування на кіберінциденти.

Практична реалізація положень цього закону потребує розробки конкретних

методичних підходів та алгоритмів впровадження системи управління інформаційною безпекою (СУІБ) на основі міжнародних стандартів, зокрема ISO/IEC 27001 [2], адаптованих до українських реалій та законодавчих вимог.

Аналіз досліджень і публікацій. Питання впровадження СУІБ в державному секторі на основі міжнародних стандартів, зокрема ISO/IEC 27001 [2], активно досліджуються у вітчизняній та зарубіжній науковій літературі. Особливої актуальності ці дослідження набувають в умовах розбудови кіберзахисту державних установ в Україні відповідно до Закону №4336-IX [2].

Комплексне дослідження правових та організаційних ІБ державних органів України представлено у роботі [3], де проаналізовано подібності та відмінності українського та європейського законодавства у сфері інформаційної безпеки. Проаналізовано вплив процесів інформатизації на ефективність державного управління та виявлено нові загрози, що виникають у результаті активного використання інформаційної сфери. Розглянуто необхідність удосконалення доктринальних підходів до національної безпеки в інформаційній сфері, особливо в частині правового регулювання та уніфікації українського законодавства з європейськими стандартами.

В роботі [4] досліджено управління ІБ в контексті євроінтеграційних процесів. Проаналізовано стадії розвитку українського законодавства в інформаційній сфері. Виявлено, що підвищення ефективності адміністративно-правового забезпечення ІБ можливе через комплекс правових заходів, до яких належать чітке законодавче відображення балансу публічних і приватних інтересів в інформаційній сфері; послідовне застосування механізмів захисту прав людини для врегулювання інформаційних конфліктів; підвищення правової свідомості та компетентності державних службовців, представників усіх гілок влади та населення.

В роботі [5] досліджено практичні аспекти реалізації СУІБ на основі міжнародного стандарту ISO/IEC 27001 в організаціях різних типів. Виявлено, що рівень прийняття стандарту значно відрізняється між між IT-галуззю та іншими сферами діяльності. В результаті моделювання структурних рівнянь проаналізовано фактори низької прийнятності стандарту поза IT-сферою. Розроблено рекомендації для законодавців, органів стандартизації та сертифікації з метою стимулювання ширшого впровадження стандарту, де підкреслено важливість адаптації ISO/IEC 27001 до особливостей конкретної галузі.

Дослідження [6] акцентує увагу на методах оцінки ефективності реалізованих заходів ІБ в державному управлінні, зокрема на важливості внутрішнього аудиту та ризик-менеджменту. Авторами проаналізовано основні поняття та умови впровадження СУІБ на базі нормативних джерел. Визначено ряд ключових проблем, таких як відсутність організації СУІБ, застаріла документація, недостатній аналіз ризиків та обмежене застосування заходів захисту. Запропоновано впровадження регламентів ЄС, зокрема GDPR та директиви NIS, що сприяє підвищенню рівня захисту інформації та зменшенню порушень.

В роботі [7] досліджено сучасні виклики, що виникають у контексті гібридної війни, зокрема на прикладі конфлікту в Україні. Особливу увагу приділено ролі сучасних інформаційних та комунікаційних технологій, які використовуються для кібератак, дезінформації та оперативної координації військових дій. Проведено аналіз впливу цих технологій на міжнародну безпеку, зокрема підвищення ризиків для сусідніх країн, зокрема Польщі, у зв’язку з її геополітичним розташуванням. Авторами визначено специфіку захисту державних інформаційних систем в умовах гібридної агресії, яка включає як технічні, так і інформаційно-психологічні компоненти.

В роботі [8] досліджено роль політичної дипломатії в протидії інформаційним загрозам. Підкреслено роль цих заходів у забезпеченні інформаційної безпеки України та захисті демократичних цінностей.

В роботі [9] проаналізовано сучасні підходи та технології у сфері кібербезпеки,

зокрема застосування шифрування, криптографії та хмарних технологій у публічному секторі для ефективного захисту інформації. Дослідження зосереджене на стратегіях підвищення рівня безпеки та захисту критичної інфраструктури державних установ. Висвітлено необхідність адаптації до швидкозмінного цифрового середовища шляхом впровадження сучасних технологічних рішень і посилення міжнародної співпраці. Визначено важливість інтеграції міжнародних стандартів і практик для створення глобального цифрового простору.

В роботі [10] досліджено ефективність протидії України російській кіберагресії з початку повномасштабного вторгнення у лютому 2022 року. Визначено кроки для розвитку кіберзахисту і координації міжнародної допомоги, а також оцінено можливості їх застосування у майбутніх кризових ситуаціях. Результати дослідження містять рекомендації щодо пріоритетів у формуванні політики та практики у сфері кібербезпеки, зокрема у контексті посилення співпраці між державним і приватним секторами.

В роботі [11] запропоновано методологію оцінювання ризиків гібридних загроз, що поєднує логіко-лінгвістичний підхід із теорією нечітких множин. Цей підхід дозволяє враховувати багатовимірність та невизначеність сучасних кіберзагроз, що є особливо актуальним для державних установ, які стикаються з комплексними атаками, що поєднують технічні та інформаційно-психологічні елементи. Методологія включає дев'ять етапів, починаючи з ідентифікації загроз та експертної оцінки, і завершуючи визначенням рівня ризику та його інтерпретацією. Використання нечіткої логіки дозволяє інтегрувати експертні судження та моделювання ризиків, що сприяє більш точному розподілу ресурсів та підвищенню ефективності управління ризиками.

В роботі [12] досліджено методи порівняльної оцінки ризиків кіберзагроз, використовуючи середні значення та теорію нечітких множин. Такий підхід дозволяє враховувати як кількісні, так і якісні аспекти загроз, що є критично важливим для державних установ при формуванні стратегій кіберзахисту. Запропонована методика сприяє більш обґрунтованому прийняттю рішень щодо пріоритезації заходів безпеки та оптимізації ресурсів, що відповідає вимогам Закону України №4336-IX щодо впровадження ефективних СУІБ.

У дослідженні [13] представлено комплексний огляд організаційної та координаційної структури кіберзахисту держави, зокрема проаналізовано функціональні ролі ключових інституцій - Національного координаційного центру кібербезпеки (НКЦК) при РНБО України та Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ). Особливу увагу приділено процесу розробки й впровадження нової законодавчої бази у сфері кібербезпеки, включаючи нормативне регулювання розподілу повноважень, реагування на кіберінциденти, управління критичною інформаційною інфраструктурою та побудову стратегії кіберстійкості.

Проведений аналіз джерел показав, що сучасна наукова література відображає багатовимірність проблематики впровадження СУІБ у державних установах, охоплюючи як нормативно-правові аспекти, так і технічні, організаційні, а також питання міжнародної співпраці. Більшість досліджень підтверджують доцільність використання моделі ISO/IEC 27001 як основи для реалізації вимог Закону України №4336-IX, підкреслюючи необхідність інтегрованого підходу до кіберзахисту.

Мета роботи полягає у розробці практичних рекомендацій та методичних засад для впровадження СУІБ державних установ та об'єктів критичної інформаційної інфраструктури (КІІ) відповідно до законодавства у сфері інформаційної безпеки (ІБ).

Аналіз структури системи кіберзахисту. Закон України №4336-IX від 27 березня 2025 року, який набрав чинності 20 квітня 2025 року, [1] спрямований на посилення моніторингу та управління інформаційної безпеки (ІБ) в державному секторі та на об'єктах критичної інформаційної інфраструктури (КІІ). Згідно з текстом Закону визначено державну політику та основні складові системи кіберзахисту. Передбачено

створення та функціонування національної системи реагування на кіберінциденти, кібератаки та кіберзагрози, яка включає CERT-UA, а також галузеві та регіональні команди реагування, що формуються органами державної влади та місцевого самоврядування [14]. Визначено роль Державної служби спеціального зв'язку та захисту інформації України у забезпеченні формування та реалізації державної політики з кіберзахисту, здійсненні. стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту та протидії технічним розвідкам, а також забезпеченні створення та функціонування національної системи реагування.

Закон передбачає створення резервних копій державних інформаційних ресурсів та їх зберігання відповідно до встановлених вимог. Визначено порядок авторизації з безпеки систем, об'єктів КІІ, що включає оцінку відповідності вимогам законодавства та стандартам у сфері захисту інформації. Встановлено вимоги до технічного захисту інформації, включаючи використання засобів технічного та криптографічного захисту інформації, які мають позитивний експертний висновок або документ про відповідність стандарту ІБ. Визначено обов’язки операторів критичної інфраструктури щодо дотримання вимог у сфері кіберзахисту, повідомлення про кіберінциденти, кібератаки, кіберзагрози та виконання інших зобов'язань щодо захисту інформації та кіберзахисту відповідно до законодавства. Закон передбачає проведення експертних досліджень засобів криптографічного захисту інформації та криптографічних алгоритмів з метою перевірки їх на відповідність вимогам нормативно-правових актів, оцінки ступеня захищеності інформації або науково-технічного рівня..

На основі аналізу положень Закону України № 4336-IX, можна визначити п’ять основних рівнів організації системи кіберзахисту, які є взаємопов’язаними і взаємозалежними. На рисунку 1 наведено схему рівнів кіберзахисту, побудовану на основі законодавчих вимог. Така структуризація ґрунтується на аналізі функцій суб’єктів забезпечення кіберзахисту, вимог до технічного та криптографічного захисту інформації, а також процедур реагування на кіберінциденти, передбачених законодавством.

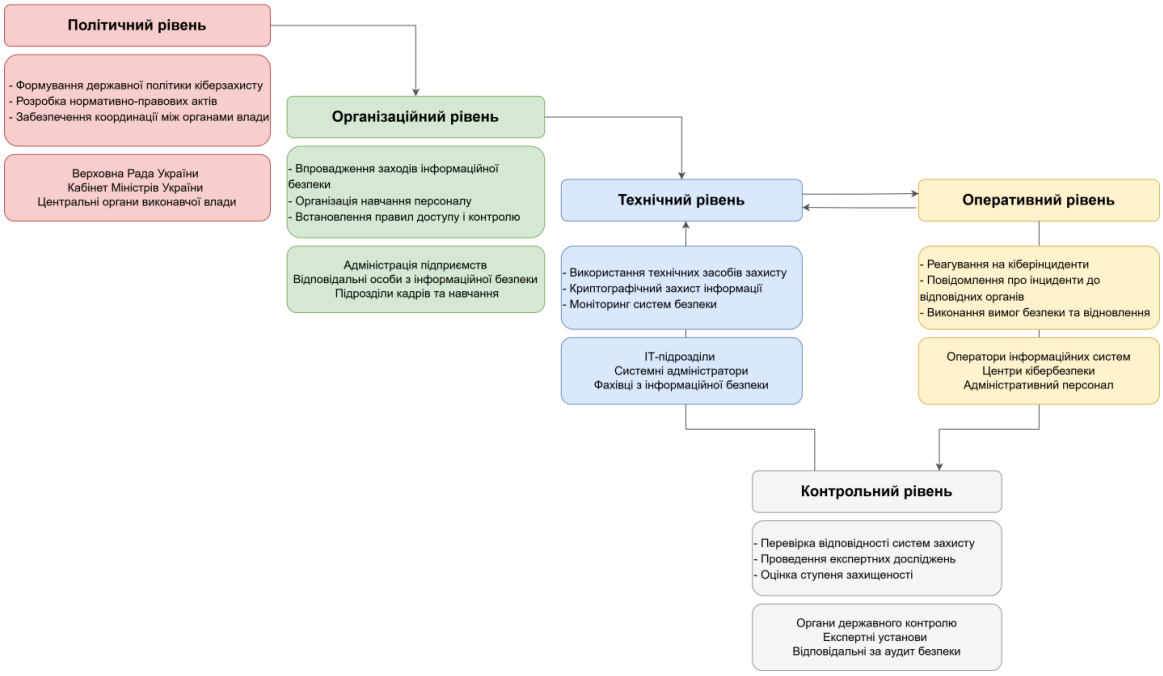

Рис. 1. Схема рівнів організації системи кіберзахисту

Кожен із наведених рівнів має власну сферу відповідальності, проте вони тісно взаємодіють між собою для забезпечення цілісної, ефективної системи захисту

державних інформаційних ресурсів і об’єктів КІІ.

Політичний рівень формує нормативну та стратегічну основу, на яку спираються інші рівні. Визначає загальну політику в галузі кіберзахисту, спрямовує діяльність організаційного, технічного, оперативного та контрольного рівнів.

Організаційний рівень реалізує політичні рішення через координацію заходів на технічному та оперативному рівнях. Відповідає за розробку та впровадження організаційних процедур, а також за підготовку систем до перевірок і аудитів, що здійснюються на контрольному рівні.

Технічний рівень забезпечує впровадження визначених політичними стандартами та організаційними планами конкретних технічних рішень та засобів захисту. Підтримує оперативний рівень, надаючи необхідні технічні інструменти реагування та є об’єктом оцінки на контрольному рівні.

Оперативний рівень використовує технічні інструменти для реагування на інциденти згідно з організаційними процедурами. Забезпечує безперервність функціонування системи та надає зворотний зв'язок для контрольного та політичного рівня.

Контрольний рівень здійснює аудит усіх попередніх рівнів та формує аналітичні висновки для зворотного зв'язку. Основним завданням є перевірка дотримання політик і стандартів, аудит організаційних процедур, оцінка технічних рішень та аналіз ефективності реагування на інциденти. Результати аналізу формують основу для коригування стратегії на політичному рівні.

Проаналізована структура системи кіберзахисту в контексті національного законодавства визначає загальнодержавні принципи та вимоги, які повинні бути імплементовані на рівні окремих суб'єктів господарювання (організацій) та операторів (об'єктів) критичної інфраструктури.

Алгоритм організації та впровадження СУІБ. Алгоритм організації СУІБ згідно із Законом №4336-IX включає наступні етапи:

1. Ініціація проекту та аналіз вимог:

- призначення відповідальної особи (CISO) або створення підрозділу ІБ;
- аналізу нормативно-правових вимог: Закон №4336-IX, Закон «Про інформацію», Закон «Про захист інформації в інформаційно-телекомунікаційних системах», НД ТЗІ та ін.;
- визначення об’єктів захисту, зокрема інформаційних систем, ресурсів, сервісів, сховищ, резервних копій, тощо.

2. Формування політик:

- розробка політик ІБ, резервного копіювання, реагування на інциденти, криптографічного захисту, зберігання копій;
- визначення порядку класифікації інформації.

3. Оцінка ризиків:

- визначення об'єкти критичної інфраструктури;
- проведення оцінку ризиків щодо конфіденційності, цілісності, доступності;
- категоризація систем (з високим, середнім, низьким ризиком).

4. Впровадження заходів:

- налаштування автоматичного резервного копіювання, шифрування за держстандартами (ДСТУ, AES тощо);
- зберігання копій у безпечних локаціях (в т.ч. за кордоном при потребі);
- впровадження систем управління подіями та інцидентами інформаційної безпеки SIEM (наприклад, Splunk, Wazuh);
- забезпечення контролю доступу, зокрема заборона доступу до ІТ-систем з територій РФ або окупованих регіонів.
- інтеграція з CERT-UA або створення власного SOC.

5. Реагування на інциденти та аудит:

- впровадження процедури виявлення та реагування на інциденти;
- проведення регулярних внутрішніх аудитів та тестування систем (наприклад, пентестинг);
- забезпечити навчання персоналу з питань ІБ;
- повідомлення про кіберінциденти до компетентних органів.

6. Актуалізація системи:

- проходження сертифікації КСЗІ (за потреби):
- підготовка звітів до компетентних органів ДССЗЗІ / НКЦК / профільного міністерства;
- регулярне оновлення політик або після критичних змін.

Для реалізаціїи вимог Закону України №4336-IX у вигляді СУІБ для державного органу або об'єкта КІІ, доцільно орієнтуватися на міжнародний стандарт ISO/IEC 27001, адаптований до українського законодавства. В таблиці 1 наведено відповідності положень Закону України №4336-IX та вимог ISO/IEC 27001, що демонструють, які заходи СУІБ відповідають нормам закону і як їх можна реалізувати.

Таблиця 1.

Відповідності Закону №4336-іх та ISO/IEC 27001

Положення Закону №4336-IX	Вимога ISO/IEC 27001	Механізм реалізації у СУІБ
Захист інформації в ІТС (CIA)	A.5.1, A.13.1	Політика ІБ, оцінка ризиків, контроль доступу, шифрування, аудит
Заборона розміщення даних на території ворога	A.11.1.1, A.13.2.1	Географічне обмеження хостингів, угоди з ЦОД, перевірка розміщення резервних копій
Резервне копіювання та зберігання копій	A.12.3.1, A.12.3.2	Розклад резервного копіювання, тестування відновлення, шифрування копій
Шифрування резервних копій	A.10.1.1, A.10.1.2	Використання криптографічних модулів, контроль ключів
Моніторинг та реагування на кіберінциденти	A.16.1.1 - A.16.1.7	SIEM-система, журнали подій, план реагування на інциденти, тестування готовності
Обмін інформацією про кіберінциденти	A.13.2.1, A.6.1.3	Взаємодія з CERT-UA, міжвідомчі протоколи, стандартизована звітність
Визначення об'єктів критичної інформаційної інфраструктури КІІ	A.6.1.2, A.8.1.1	Інвентаризація активів, класифікація, оцінка впливу, ризик-аналіз
Навчання персоналу	A.7.2.2	Регулярні навчання, внутрішні тренінги, курси з кіберзахисту
Контроль доступу до ІТС	A.9.1 - A.9.4	Аутентифікація, розмежування прав доступу, реєстрація дій користувачів
Координація з державними органами	A.6.1.4, A.6.2.1	Регламент взаємодії, звітність, технічне узгодження з регуляторами
Аудит та перевірка відповідності вимогам безпеки	A.18.2.1 - A.18.2.3	Внутрішній аудит, аналіз інцидентів, перевірка заходів контролю

Наведена таблиця дозволяє трансформувати законодавчі вимоги у конкретні елементи СУІБ на основі міжнародного стандарту. Для практичної реалізації цих вимог необхідно розробити алгоритм організації та впровадження СУІБ на рівні окремих об'єктів.

Представлена на рисунку 2 схема процесу впровадження СУІБ ілюструє взаємозв'язки між ключовими компонентами та етапами процесу. Така структура відображає класичний цикл PDCA, що відповідає принципам міжнародних стандартів

та забезпечує системний підхід до управління ІБ через постійне планування, впровадження, контроль та вдосконалення заходів захисту.

Схема відображає повний життєвий цикл СУІБ, що складається з основних рівнів управління:

Рівень управління розпочинається з керівництва, яке ініціює процес та затверджує політику ІБ - основоположний документ, що визначає стратегічні напрями забезпечення інформаційної безпеки організації.

Операційний рівень включає розробку процедур та стандартів, які деталізують політику ІБ та переходять у відділ ІБ - структурний підрозділ, відповідальний за впровадження заходів безпеки. Цей рівень також охоплює навчання персоналу, що забезпечує розуміння та дотримання вимог ІБ усіма співробітниками.

Технічний рівень представлений засобами захисту (технічні та програмні рішення), інфраструктурою (апаратно-програмний комплекс) та моніторингом і журналюванням (системи виявлення та реєстрації подій безпеки).

Рівень управління інцидентами та контролю включає моніторинг інцидентів (постійне відстеження подій безпеки), реагування на інциденти (процедури усунення загроз) та відновлення (заходи з повернення до нормального функціонування).

Рівень аудиту та оцінки завершує цикл аудитом ІБ (перевірка ефективності СУІБ), оцінкою ефективності (аналіз досягнення цілей безпеки) та звітуванням (документування результатів та рекомендацій).

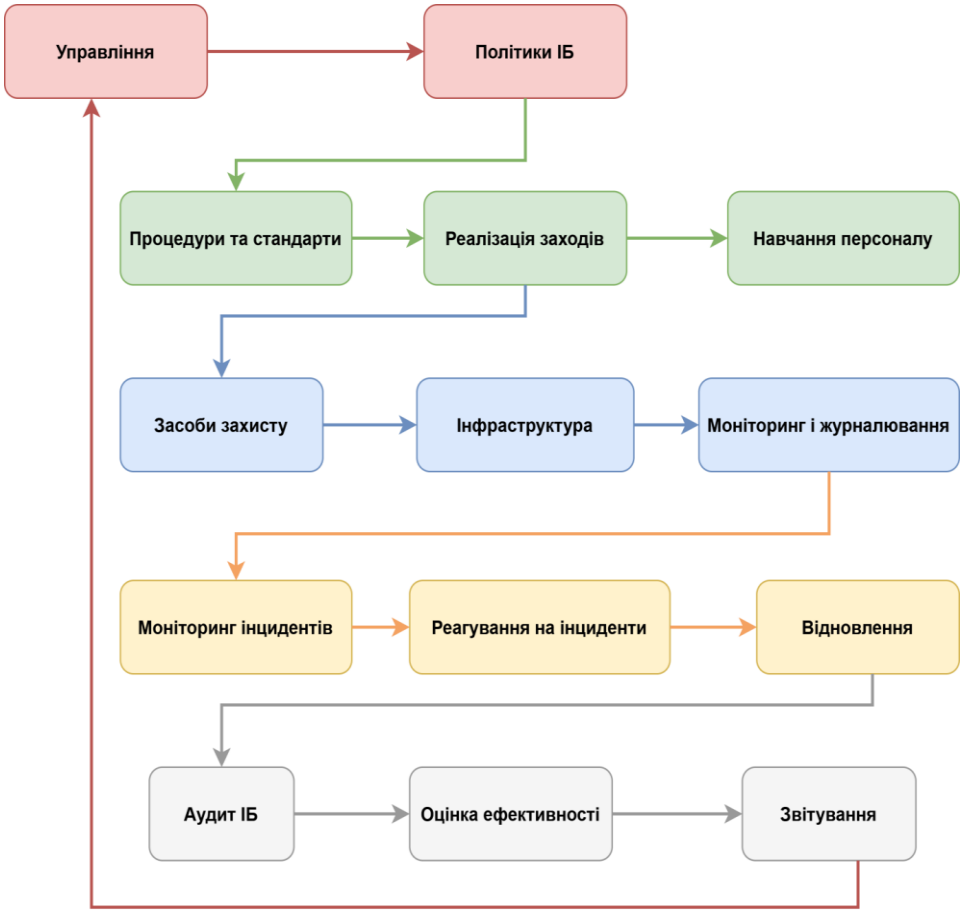

Рис. 2. Схема процесу впровадження СУІБ

Ключовою особливістю схеми є зворотний зв'язок, що з'єднує етап звітування з керівництвом, забезпечуючи безперервне вдосконалення СУІБ на основі отриманих результатів аудиту та оцінки ефективності.

Кожен із визначених п’яти рівнів організації національної системи кіберзахисту

корелює з етапами створення та впровадження СУІБ окремого об'єкта. Вимоги політичного рівня формалізуються через аналіз нормативно-правових актів та розробку внутрішніх політик ІБ. Організаційний рівень реалізується шляхом створення відповідних структур та процедур в організації. Технічний рівень - у впровадженні конкретних засобів захисту та моніторингу. Функції оперативного рівня забезпечуються за допомогою систем реагування на інциденти та звітування. Контрольний рівень реалізується шляхом внутрішнього аудиту та оцінки ефективності.

Трансформація державних вимог у процеси управління ІБ демонструє перехід від теоретичних положень законодавства до практичних заходів їх впровадження.

Розробка план-графіка впровадження СУІБ. Для забезпечення ефективного впровадження СУІБ та досягнення поставлених цілей ІБ необхідно здійснити детальне планування всіх етапів процесу з чітким визначенням часових рамок, відповідальних осіб та контрольних точок. План-графік впровадження СУІБ є ключовим інструментом управління проектом, який дозволяє трансформувати теоретичний алгоритм у практичний інструмент та послідовність конкретних дій.

Розробка та використання план-графіка забезпечує системний підхід до впровадження СУІБ через визначення тривалості кожного етапу, оптимальний розподіл ресурсів та координацію роботи між різними підрозділами. Це дозволяє уникнути хаотичного виконання завдань, мінімізувати ризики пропуску критично важливих заходів та забезпечити своєчасне досягнення проміжних результатів. Крім того, він служить основою для контролю та моніторингу процесу впровадження, надаючи можливість відстежувати прогрес виконання робіт, своєчасно виявляти відхилення від запланованих термінів та приймати корегувальні рішення. Документування планових та фактичних показників виконання також є важливим елементом звітності перед регуляторними органами та демонстрації відповідності нормативним вимогам у сфері кіберзахисту.

На основі даних таблиці 1 реалізовано план-графік впровадження СУІБ згідно із Законом України №4336-IX та ISO/IEC 27001 (таблиця 2).

Таблиця 2.

План-графік впровадження СУІБ

Етап	**Тривалість**	**Основні дії**	**Відповідальні**	**Результат**
Ініціація проєкту та аналіз вимог	4 тижні (1 місяць)	Призначення відповідальних, аналіз нормативної бази, визначення об'єктів захисту	Органи управління, відділ ІБ, юридичний відділ	Проєктний план
Формування політик ІБ	6 тижнів (1,5 місяці)	Створення політик резервного копіювання, управління доступом, реагування на інциденти	CISO, відділ ІБ, юридичний відділ	Пакет затверджених політик ІБ; Регламенти та процедури; Розподіл ролей та відповідальності
Оцінка ризиків та критичності	4 тижні (1 місяць)	Ідентифікація активів, виявлення загроз та вразливостей, оцінка ризиків	Відділ ІБ, IT- відділ, CISO, бізнес-підрозділи, зовнішні експерти	Реєстр активів; Звіт про оцінку ризиків; План управління ризиками
Впровадження технічних заходів	8 тижнів (2 місяці)	Налаштування систем шифрування, резервного копіювання, моніторингу та	Відділ ІБ, IT-відділ, системні адміністратори	Функціональні технічні засоби; Документація конфігурацій

Етап	Тривалість	Основні дії	Відповідальні	Результат
		SIEM		
Навчання персоналу	4 тижні (1 місяць)	Проведення тренінгів, роз'яснення політик, тестування знань персоналу	CISO, HR-департамент, тренери	Протоколи навчання; Сертифіковані користувачі
Реагування на інциденти	6 тижнів (1,5 місяці)	Створення CERT, налаштування систем сповіщення, тестування процедур реагування та відновлення	CERT-команда, відділ ІБ, ІТ- відділ	Функціонуюча система реагування; Процедури виявлення інцидентів
Аудит та оцінка ефективності	4 тижні (1 місяць)	Проведення внутрішнього аудиту, тестування на проникнення, оцінка відповідності стандартам	Зовнішні аудитори, відділ ІБ	Акт внутрішнього аудиту; Рекомендації з удосконалення
Сертифікація та звітність	2 тижні (0,5 місяця)	Оформлення звітів, узгодження, сертифікаційний аудит, планування подальшого розвитку СУІБ	CISO, відділ ІБ, керівництво, сертифікаційний орган	Сертифікат відповідності; Звіти регуляторам; Функціонуюча СУІБ

Представлений в таблиці 2 приклад план-графіка може бути адаптований відповідно до специфіки конкретного об'єкта, масштабу інформаційної системи та наявних ресурсів.

На рисунку 3 наведено графічне представлення плану впровадження СУІБ, що має поетапну структуру. Діаграма відображає послідовність, чіткі часові рамки та залежності між окремими етапами, що допомагає ідентифікувати завдання, затримка яких може вплинути на загальні терміни впровадження, та сконцентрувати увагу на найбільш важливих аспектах реалізації СУІБ. Такий підхід дозволяє ефективно планувати ресурси та оптимізувати загальну тривалість реалізації проекту.

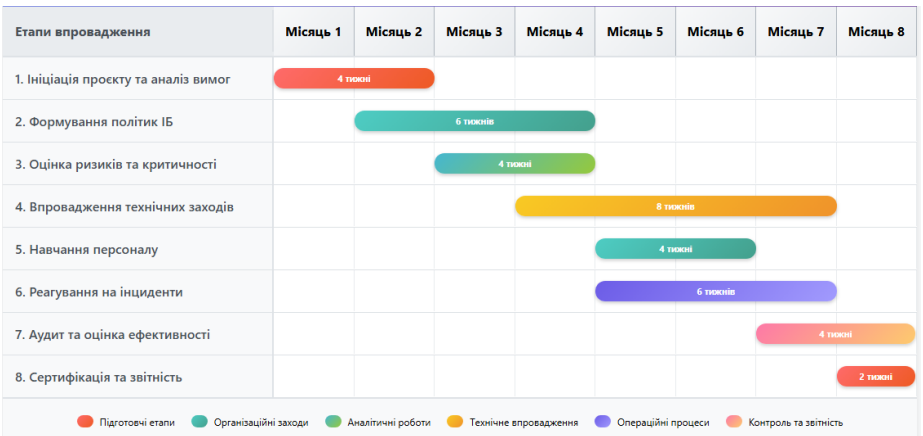

Рис. 3. Графічне представлення етапів впровадження СУІБ

Особливістю представленої діаграми є демонстрація того, що деякі етапи

можуть розпочинатися до повного завершення попередніх, зокрема технічне впровадження може частково перекриватися з розробкою процедур, а навчання персоналу може проводитися паралельно з налаштуванням технічних засобів. Такий підхід дозволяє скоротити загальний час впровадження та забезпечити більш ефективне використання ресурсів.

Практичні рекомендації щодо реалізації системи управління інформаційною безпекою. Результати дослідження дозволяють визначити пріоритетні напрями практичного впровадження СУІБ, що охоплюють як технічні, так і організаційні аспекти забезпечення кіберзахисту відповідно до вимог законодавства.

Проведення формальної категоризації інформаційних систем за рівнем критичності та розробка детальних карт ІТ-систем і ресурсів, а також узгодження з НКЦК забезпечують чітке визначення пріоритетів захисту та ефективний розподіл ресурсів. Впровадження процедур реагування на кіберінциденти, які охоплюють розробку процесів реагування на різні типи інцидентів, а також підключення до CERT-UA та встановленням цільових показників RTO - часу відновлення, RPO - допустимого рівня втрати даних, забезпечує оперативне відновлення функціонування інформаційних систем у разі інцидентів.

Використання сучасних технічних засобів кіберзахисту, серед яких SIEM-системи, рішень для захисту кінцевих точок та систем управління вразливостями - забезпечує проактивний захист і безперервний моніторинг загроз. Налагодження взаємодії з державними органами, що включає своєчасне надсилання звітів про кіберінциденти, виконання вимог нормативних актів, а також координацію з НКЦК, ДССЗЗІ та СБУ, підвищує рівень кібербезпеки на національному рівні.

Реалізація зазначених напрямів у рамках СУІБ дозволить організаціям відповідати вимогам національного законодавства, ефективно управляти кіберризиками та забезпечувати надійний захист критично важливої інформаційної інфраструктури.

Висновки. В роботі проаналізовано встановлену Законом України №4336-IX комплексну систему вимог до кіберзахисту державних інформаційних ресурсів. Виявлено ключові взаємозв'язки між її елементами визначено пять рівнів організації системи кіберзахисту та управління ІБ, що дозволяє забезпечити цілісне функціонування СУІБ.

Практична реалізація законодавчих вимог можлива шляхом адаптації положень міжнародних стандартів до українського правового поля. Побудована таблиця відповідності між положеннями Закону №4336-IX та вимогами стандарту ISO/IEC 27001 забезпечує інтеграцію міжнародних практик з національним регуляторним середовищем.

Запропоновано алгоритм розробки та впровадження СУІБ, який враховує законодавчі вимоги та створює методичну основу для її реалізації в державних установах.

Розроблено план-графік реалізації СУІБ із визначенням відповідальних осіб і контрольних точок дає змогу організовано управляти процесом реалізації вимог Закону України №4336-IX.

Сформульовано практичні кроки технічного й організаційного характеру, які спрямовані на підвищення ефективності функціонування СУІБ і забезпечення її відповідності вимогам державної політики у сфері кіберзахисту.

Список літератури

1. Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» ЗУ № 4336-IX, від 27.03.2025 URL: https://zakon.rada.gov.ua/laws/main/4336-20?utm_source=chatgpt.com#Text
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements URL:

https://www.iso.org/standard/27001
3. Klietsova N., Ahmadov V., Bieliakov K., Klochko A., Kravtsova T. Legal Issues of Information Security of Public Authorities in Ukraine and the European Union: Experience and Realities. *AD Alta: Journal of Interdisciplinary Research*. 2021. 11(2), 12-17. URL: https://www.magnanimitas.cz/ADALTA/110221/PDF/110221.pdf
4. Fedorenko V., Lytvyn N., Luchenko D. Legal Aspects of Information Security Management in the Conditions of Ukraine's European Integration. *Journal of Security and Sustainability Issues*. 2020. 10(2), 477-489. DOI: https://doi.org/10.9770/jssi.2020.10.2(9).
5. Mirtsch M., Blind K., Koch C., Dudek G. Information Security Management in ICT and Non-ICT Sector Companies: A Preventive Innovation Perspective. *Computers & Security.* 2021. 109. 102383. DOI: https://doi.org/10.1016/j.cose.2021.102383.
6. Szczepaniuk E.K., Szczepaniuk H., Rokicki T., Klepacki B. Information Security Assessment in Public Administration. *Computers & Security*. 2019. 90. 101709. DOI: https://doi.org/10.1016/j.cose.2019.101709.
7. Wróblewski W., Wiśniewski M. Cybersecurity in the context of Hybrid Warfare in Ukraine: Analysis of its impact on the public sector and society in Poland. *Central European Journal of Security Studies.* 2024. 1. 48-60. DOI: https://doi.org/10.15804/CEJSS.2023105.
8. Taranenko A. Ensuring information security: Countering Russian disinformation in Ukrainian speeches at the United Nations, *Social Sciences & Humanities Open*. 2024. Volume 10, 100987. DOI: https://doi.org/10.1016/j.ssaho.2024.100987.
9. Chumak O., Holovkin S, Piroh O., Pushkar T, Diegtiar O. Information protection and cyber security in the public and financial sectors. *Edelweiss Applied Science and Technology*. 2024. 8(5), 1164–1174. DOI: https://doi.org/10.55214/25768484.v8i5.1819
10. Axon L., Saunders J., Esteve-Gonzalez P., Carver J., Dutton W., Goldsmith M., Creese S. Private-public initiatives for cybersecurity: the case of Ukraine. *Journal of Cyber Policy.* 2025. 9. 1-24. DOI: https://doi.org/10.1080/23738871.2025.2451256.
11. Zybin S., Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S. Method for the Risk Assessing of Hybrid Threats in Cyber Security Based on Fuzzy Set Theory. URL: http://dx.doi.org/10.2139/ssrn.5143937
12. Korystin O.E., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O.O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory *International Journal of Computer Network and Information Security(IJCNIS)*. 2024. Vol.16, No.1, pp.24-34. DOI: https://doi.org/10.5815/ijcnis.2024.01.02
13. Davydiuk A., Potii O. New Report on National Cybersecurity Governance: Ukraine URL: https://ccdcoe.org/news/2024/new-report-on-national-cybersecurity-governance-ukraine/?utm_source=chatgpt.com
14. 14.Президент України підписав закон про кіберзахист державних інформаційних ресурсів. URL: https://duikt.edu.ua/ua/news-1-569-14204-prezident-ukraini-pidpisav-zakon-pro-kiberzahist-derzhavnih-informaciynih-resursiv_kafedra-cistem-tehnichnogo-zahistu-informacii

METHODOLOGY FOR IMPLEMENTING AN INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON A MULTILEVEL CYBERSECURITY MODEL IN ACCORDANCE WITH THE REQUIREMENTS OF UKRAINIAN LEGISLATION

V.V. Yatskiv, S.V. Ivasiev, A.Ya. Davletova, L.M. Tymoshenko

West Ukrainian National University
11, Lvivska Str. Ternopil, 46009, Ukraine
National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: jazkiv@ukr.net, stepan.ivasiev@gmail.com, a7davletova@gmail.com, l.m.timoshenko@op.edu.ua

The paper is devoted to the practical aspects of implementing an Information Security Management System (ISMS) in public institutions in accordance with the requirements of the Law of Ukraine No. 4336-IX. The study presents a comprehensive analysis of legislative requirements related to the organization and functioning of ISMS, particularly regarding the development, implementation, monitoring, and continuous improvement of cybersecurity measures. A five-level structure of the cybersecurity system has been defined, encompassing political, organizational, technical, operational, and control levels, each of which performs specific functions to ensure the integrity, confidentiality, and availability of information. An algorithm for organizing and gradually implementing the ISMS based on the ISO/IEC 27001 international standard has been developed, adapted to the specifics of Ukrainian legislation and the practical needs of the public sector. To enhance the effectiveness of the system's implementation, a mapping table was created between the provisions of the Law of Ukraine No. 4336-IX and the requirements of ISO/IEC 27001, enabling the transformation of regulatory provisions into specific ISMS elements. The study presents a detailed implementation roadmap with clearly defined stages, responsible actors, control points, and expected results, which ensures transparency and manageability of the process. Special attention is given to practical recommendations regarding technical and organizational measures aimed at strengthening the cybersecurity of information assets. The proposed solutions not only support compliance with current legislation but also contribute to the development of a systematic approach to cyber risk management, which is critically important in the face of modern information security challenges. The research results can be used to optimize information security processes, enhance cyber resilience, and protect critical information infrastructure.

Keywords: cybersecurity, information security, information security management system, ISO/IEC 27001, Law of Ukraine No. 4336-IX, critical information infrastructure, state information resources.