The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.19

Обґрунтування змісту етапів і заходів та розроблення пропозицій щодо раціонального вибору системи захисту інформації під час створення інформаційно-комунікаційних систем

Олександр Леоненко
начальник науково-дослідного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: leonenkols@ukr.net
ORCID: 0009-0009-1994-438X

Володимир Ремез
доктор філософії
доцент кафедри управління військами
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: remezv93145@gmail.com
ORCID: 0000-0002-2561-1081

Алевтина Гетьман
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
Київ, Україна
e-mail: getman2017@gmail.com
ORCID: 0000-0002-6397-7412

Юрій Мельничук
старший викладач кафедри оперативного мистецтва
інституту державного військового управління
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: um777@ukr.net
ORCID: 0000-0003-2043-1353

Олексій Смілянський
помічник заступника Головнокомандувача Збройних Сил України
Апарат Головнокомандувача Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: lesha.smeliansky@gmail.com
ORCID: 0009-0006-8573-2068

Юлія Пятова
науковий співробітник – інженер випробувач науково-дослідної лабораторії
Державний науково-дослідний інститут
випробувань та сертифікації озброєння та військової техніки
Черкаси, Україна
e-mail: pyatova463@gmail.com
ORCID: 0009-0001-2713-8435

Анотація. З початком повномасштабної агресії російської федерації проти України значно зросло значення інформаційної безпеки в умовах гібридної війни. Інформаційний простір, який охоплює як військову, так і цивільну складову, трансформувався в критично важливу складову сучасного театру воєнних дій. Агресор активно використовує інструменти інформаційного впливу та кібероперацій, спрямованих на особовий склад, системи управління Збройних Сил України, а також на інформаційні платформи загального призначення. Оскільки функціонування ЗСУ все більше залежить від інформаційно-комунікаційних систем (ІКС), захист цих систем від зовнішніх і внутрішніх загроз набуває першочергового значення. Цифровізація процесів управління, з одного боку, підвищує ефективність та швидкість обміну інформацією, з іншого — створює нові вектори уразливості кіберпростору. У зв'язку з цим, формування ефективних систем захисту інформації є обов'язковою умовою під час проєктування та впровадження ІКС.

Метою цієї статті є обґрунтування структури етапів і заходів побудови систем захисту інформації, а також формування підходів до вибору раціональної моделі захисту залежно від функціональних і технічних характеристик ІКС, включаючи особливості інтеграції в загальну архітектуру системи.

У процесі дослідження використано метод системного аналізу, що дозволив структурувати етапи створення систем захисту, а також метод порівняльного аналізу, за допомогою якого здійснено оцінку ефективності різних підходів до побудови захисних механізмів в ІКС.

У статті запропоновано узагальнений підхід до вибору між комплексною системою захисту інформації (КСЗІ) та системою управління інформаційною безпекою (СУІБ) на основі законодавчих вимог і функціональних характеристик ІКС. Також систематизовано процедури створення захисних систем і наведено умови їх ефективної реалізації.

Матеріали статті можуть бути використані при розробці, проєктуванні та впровадженні ІКС у Збройних Силах України та інших структурах сектору безпеки й оборони. Запропонований підхід сприятиме підвищенню рівня захищеності інформаційної інфраструктури в умовах сучасної війни та цифрових трансформацій.

Ключові слова: інформаційно-комунікаційна система, система захисту інформації, комплексна система захисту інформації, система управління інформаційною безпекою, середовище функціонування інформаційно-комунікаційних систем.

Вступ (Introduction)

Сучасні телекомунікаційні та інформаційні технології дозволяють створювати складні за архітектурою та функціональним наповненням інформаційно-комунікаційні системи (ІКС), які стають невід'ємними та актуально необхідними елементами системи управління, що підвищують ефективність керівництва життєдіяльністю, розвитком, підготовкою і застосуванням Збройних Сил України. Проведення заходів з організації створення, розвитку, інтеграції та підтримки ІКС відбувається відповідно до визначеного життєвого циклу ІКС. Обов'язковою умовою під час створення такої системи є захист інформації, який є сукупністю заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. Будуючи систему захисту в ІКС, насамперед необхідно враховувати, яка інформація за порядком доступу буде циркулювати в цій системі – відкрита чи з обмеженим доступом, щоб оцінити ризики безпеки.

Інформаційна безпека в інформаційно-комунікаційних системах (ІКС) є важливою та невід'ємною складовою їх розробки та подальшої експлуатації. Забезпечення захисту має здійснюватися на кожному етапі життєвого циклу ІКС. Вітчизняна нормативно-правова база дозволяє паралельне проектування як самих ІКС, так і засобів захисту інформації в них. Проте на практиці нерідко спостерігається роздільне виконання цих робіт, що супроводжується відсутністю координації організаційно-технічних рішень. У результаті виникає необхідність

їх перегляду через труднощі із впровадженням вимог інформаційної безпеки. Під час створення ІКС необхідно враховувати низку чинників, що впливають на вибір відповідних організаційно-технічних підходів, зокрема: тип і рівень конфіденційності інформації, що обробляється, архітектурні особливості системи, методи керування доступом, місця зберігання даних та інші параметри.

Ще одним аспектом, який варто взяти до уваги, є те, що інформаційний обмін України з країнами Європейського Союзу (ЄС), включаючи вектор руху до повноправного членства в ЄС, передбачає необхідність синхронізації регулювання захисту інформації в України з європейським законодавством.

Потреба у глибокому розумінні загроз безпеки ґрунтується на реалістичному оцінюванні ризиків безпеки, що залежить від вразливості інформаційних систем і організаційної побудови в цілому та ґрунтується на їх реалізації, при порушенні конфіденційності та цілісності відбувається виникнення події імовірності негативних наслідків, а також порушення доступності та інших властивостей безпеки. З урахуванням стратегії управління ризиками мають бути сформульовані вимоги безпеки. При цьому пропонується звернути особливу увагу на практичну експлуатацією та ефективність впровадження заходів, пов'язаних із проєктуванням, що, у свою чергу, має передбачати особливості, витрати та порядок розроблення, придбання, розгортання.

Вибір заходів захисту інформації має ґрунтуватися на результатах аналізу ризиків, що супроводжують функціонування інформаційно-комунікаційних систем (ІКС). Визначення відповідного комплексу засобів безпеки починається з обрання профілю безпеки, який має відповідати специфічним потребам установи чи організації. Для того щоб забезпечити адаптивність до динамічних умов роботи ІКС і змін у зовнішньому середовищі, процес вибору заходів захисту повинен залишатися гнучким.

Методологічна основа (Methodological Framework)

Згідно із Законом України "Про захист інформації в інформаційно-комунікаційних системах", державні інформаційні ресурси або інформація з обмеженим доступом, захист якої передбачено законодавством, повинні оброблятися лише в ІКС із впровадженою та підтвердженою комплексною системою захисту інформації (КСЗІ). У випадку, коли система не оперує державною таємницею, службовою інформацією або даними з державних чи єдиних реєстрів, допускається функціонування без КСЗІ, за умови підтвердження відповідності системи управління інформаційною безпекою (СУІБ) чинним національним стандартам. Таким чином, для захисту відкритої або конфіденційної інформації можливе застосування одного з двох підходів: КСЗІ або СУІБ.

Для обґрунтування вибору оптимального варіанта системи захисту інформації у дослідженні подано їх порівняльну характеристику. Комплексна система захисту охоплює впровадження різноманітних технічних і організаційних рішень, спрямованих на запобігання витоку інформації через фізичні й технічні канали (зокрема акустоелектричні, електромагнітні, залишкові наведення тощо). Вона також забезпечує протидію спробам несанкціонованого доступу за допомогою використання чужих облікових даних, втручанню в програмне середовище, впровадженню шкідливого програмного забезпечення або технічних пристроїв. Крім того, до її функцій належить захист від навмисного знищення або викривлення інформації, у тому числі через генерацію штучних впливів або сигналів, здатних порушити роботу системи.

Концепція розробки комплексної системи захисту інформації (КСЗІ) передбачає створення відкритої архітектури безпеки, яка дозволяє незалежно проєктувати, впроваджувати, тестувати та експлуатувати кожен елемент системи окремо. Такий підхід сприяє уніфікації процесів, зниженню витрат на розробку та дає змогу здійснювати окрему оцінку кожного компонента КСЗІ під час будь-яких видів випробувань.

Побудова КСЗІ включає низку послідовних етапів, першим із яких є визначення

загальних вимог до системи в межах конкретної ІКС.

На цьому початковому етапі виконуються такі дії:

1.1 Обґрунтування потреби у впровадженні КСЗІ.

Під час аналізу приймається рішення щодо доцільності створення системи захисту на основі таких чинників:

- аналіз нормативно-правових актів (законів, указів, постанов, внутрішньовідомчих документів), які встановлюють обмеження на доступ до певної категорії інформації або вимагають обов'язкового її захисту;
- визначення необхідності гарантування цілісності, доступності або конфіденційності інформації, що підлягає обробці в автоматизованому режимі, згідно з чинними вимогами законодавства;
- у випадку впровадження КСЗІ на етапі експлуатації ІКС — проведення оцінювання можливих переваг такого рішення, серед яких можуть бути економічні, морально-психологічні, політичні, військові або соціальні вигоди.

1.2 Проведення багаторівневого аналізу середовищ функціонування ІКС.

Підготування основних засад та концептуальних даних у ході обстеження для формування вимог до КСЗІ з формуванням детального висвітлення кожного середовища функціонування ІКС з виділенням особливої уваги в ньому на об'єктах, що у будь-якій формі можуть передбачати вплив на безпеку інформації, визначення організації та порядку обміну інформацією між елементами та різних середовищах, проведення статистичного збору результатів обстеження, їх документування та архівування, що у подальшому має використовуватись при організації та проведенні наступних етапів робіт.

Обстеженню підлягають: обчислювальні системи ІКС, інформаційне середовище, технології оброблення інформації, фізичне середовище, середовище користувачів.

Формування Плану захисту інформації в ІКС відбувається за результатами обстеження середовищ функціонування ІКС, виявлення ризиків та визначення потенційних загроз для інформації, у складі якого затверджується перелік об'єктів захисту, окремими документами розробляються: модель загроз і модель порушника.

1.3 Постановка завдання на розробку КСЗІ.

На цьому етапі визначаються ключові завдання захисту інформації в ІКС, формулюється мета створення КСЗІ, обирається підхід до реалізації захисту та встановлюються основні напрями забезпечення інформаційної безпеки.
Також проводиться аналіз ризиків, у межах якого уточнюються моделі загроз і потенційних зловмисників, оцінюються можливі наслідки реалізації загроз і визначаються ймовірні втрати. На основі цього формується перелік критичних загроз. Окреслюється структура та складові КСЗІ, формулюються вимоги до технічних і організаційних заходів, засобів та методів захисту. Визначаються допустимі обмеження на їх застосування, середовище функціонування ІКС, допустимі витрати, умови створення, введення в експлуатацію та функціонування системи або її компонентів. Також встановлюються загальні принципи розподілу організаційних, інженерних, технічних, криптографічних та інших захисних заходів між підсистемами ІКС.

2-й етап — формування політики інформаційної безпеки в ІКС.
Цей етап включає:

2.1 Аналіз об'єкта впровадження.

Розробник вивчає характеристики об'єкта, де буде впроваджена КСЗІ, деталізує моделі загроз і порушників, перевіряє можливості ефективного управління ризиками.

2.2 Вибір концептуальної моделі КСЗІ. Аналізуються можливі варіанти побудови КСЗІ, оцінюються їх переваги та недоліки, після чого приймається рішення щодо найоптимальнішого варіанту.

2.3 Розробка політики безпеки. На цьому етапі визначаються основні підходи до захисту інформації, формуються загальні вимоги та правила використання безпечних

технологій, а також перелік конкретних захисних заходів, ролі користувачів і вимоги до документального оформлення політики безпеки.

3-й етап — підготовка технічного завдання на створення КСЗІ. Технічне завдання є базовим документом, який регламентує вимоги до захисту інформації в ІКС, порядок реалізації КСЗІ, проведення випробувань і введення її в експлуатацію в складі системи.

4-й етап — проєктування КСЗІ.

Проєкт КСЗІ формується згідно з технічним завданням і включає технічні рішення, що забезпечують сумісність компонентів і реалізацію вимог до безпеки.

Проєктування проходить у кілька стадій:

- **Ескізний проєкт.** На цьому етапі формуються попередні проєктні рішення, створюється проєктна документація, виконується погодження й затвердження.
- **Технічний проєкт.** Здійснюється деталізація проєктних рішень, зокрема: організаційно-технічна структура, опис середовища функціонування, програма випробувань, підготовка експлуатаційної документації.
- **Робочий проєкт.** Остаточна розробка та затвердження усієї документації, включно з робочими матеріалами та інструкціями для окремих підсистем КСЗІ (якщо потрібно).

5-й етап — запуск КСЗІ та оцінювання рівня інформаційної безпеки в ІКС. На цьому завершальному етапі здійснюється впровадження системи в реальне середовище, а також перевіряється ефективність реалізованих заходів із захисту даних.

На цьому етапі виконуються такі дії:

- **Розробка регламентуючої документації.** Створюються внутрішні нормативні документи, що визначають порядок забезпечення захисту інформації в ІКС. Паралельно формуються організаційні структури, готується сама КСЗІ до вводу в експлуатацію.
- **Підготовка персоналу.** Особи, відповідальні за адміністрування системи та всі категорії користувачів, проходять навчання з урахуванням участі технічного персоналу, що забезпечує обслуговування засобів захисту.
- **Комплектування КСЗІ.** Закуповуються технічні засоби захисту інформації, обладнання, необхідні матеріали та інші компоненти, відповідно до вимог комплектування системи.
- **Будівельно-монтажні роботи.** Здійснюються інженерні роботи, передбачені технічним завданням, з урахуванням архітектури системи.
- **Пусконалагоджувальні заходи.** Проводиться монтаж обладнання, випробування системи захисту інформації на відповідність вимогам ТЗІ, налаштування функціонування механізмів захисту від несанкціонованого доступу, тестування в автономному режимі та в умовах взаємодії з іншими компонентами. Атестація ТЗІ проводиться шляхом оцінки повноти робіт у захищених приміщеннях, за результатами оформлюється відповідний акт.
- **Попереднє тестування.** Виконується перевірка працездатності системи за встановленими критеріями, результати оформлюються протоколами, які передаються контролюючим структурам.
- **Дослідна експлуатація.** У процесі тимчасової експлуатації тестуються практичні аспекти: обробка інформації, взаємодія носіїв, розмежування прав доступу, дії користувачів, перевірка ефективності обраних засобів захисту. У разі потреби вносяться коригування до програмного забезпечення або документації.
- **Державна експертиза.** Окремою стадією є оцінка відповідності КСЗІ технічному завданню та нормативним документам. За необхідності допускається окрема експертиза кожного модуля КСЗІ. Нові модулі можуть додаватися без повторної повної перевірки, за умови оцінки їх сумісності з чинною системою.

6-й етап — супровід КСЗІ. На цьому етапі забезпечується постійна підтримка функціонування КСЗІ, зокрема обслуговування захисних засобів згідно з експлуатаційною

документацією, планами захисту та регламентами гарантійного й післягарантійного обслуговування.

Система управління інформаційною безпекою (СУІБ) є складовою загальної системи менеджменту, що реалізується на основі оцінки ризиків. Вона забезпечує побудову, впровадження, моніторинг і вдосконалення заходів інформаційного захисту. СУІБ гарантує збереження конфіденційності (захист від несанкціонованого доступу та поширення), цілісності (захист від несанкціонованих змін або знищення) та доступності (захист від блокування) інформації шляхом управління ризиками. Її основою є постійний моніторинг стану безпеки системи, аналіз змін в інформаційному середовищі, а також регулярна переоцінка ефективності обраних засобів захисту. Важливою перевагою СУІБ є її здатність до інтеграції національних і міжнародних стандартів інформаційної безпеки.

Процес створення СУІБ складається з таких етапів:

1-ий етап – проведення аналізу виникнення ризиків на різних рівнях (організаційному та системному). Реалізація методики управління ризиками безпекової сфери на організаційному рівні передбачає заходи підготовки що включає:

надання посадовим особам визначених ролей у сфері управління ризиками безпеки;

проведення робіт щодо створення Концепції інформаційної безпеки;

формулювання мети, обрання визначених цілей, формування часткових завдань, затвердження переліку функцій та складових процесів, які розглядаються до підтримування ІКС;

окреслення меж та визначення сторін та їх повноваження, які зацікавлені у функціонуванні ІКС;

роз’яснення категорії загроз та передбачувані потенційні збитки у разі реалізації впливу загроз на фізичних осіб та інформаційні системи;

здійснення постійного оцінювання ризиків на всіх рівнях інформаційного обміну;

ранжування переліку та його адаптація, узгодження та розстановку пріоритетів вимог безпеки;

побудову ІКС.

2-ий етап –визначення важливості рівнів та категорій безпеки. Визначення категорій всіх активів ІКС за результатами проведеного аналізу та ранжування відбувається на ґрунті оцінювання рівня критичності активів установи (організації) та ІКС в цілому. Визначення важливості рівнів та категорій безпеки здійснюється з урахуванням оцінювання рівня збитків та негативного впливу, що може відбутися при порушенні політики безпеки визначеної активів ІКС. Рівні критичності (низький, середній, високий) визначаються показниками оцінювання впливу за кожною політикою та властивістю ІКС. До цього етапу входять наступні заходи: детальний та повний опис суб’єктів та об’єктів системи, формування політик та категорій безпеки, затвердження порядку аналізу та ухвалення рішень щодо визначення політик та категорій безпеки в системі та інформації. Формування політик та категорій безпеки відбувається відповідно до положень [1].

3-ій етап – послідовність та порядок побудови вибору заходів захисту. Формування Програми безпеки інформації та обирання набору заходів захисту відбувається за результатами оцінювання збитків та ризиків безпеки та політик та категорій безпеки. З метою розширення повноважень та функціональних можливостей під час визначення заходів захисту враховуються вимоги міжнародних та міжвідомчих стандартів.

4-й етап — реалізація заходів інформаційної безпеки. Цей етап виконується відповідно до затвердженої Концепції безпеки інформації з використанням сучасних методів проєктування систем захисту. Він охоплює такі дії:

- налаштування початкового (базового) профілю безпеки;
- конкретизація та затвердження цільового профілю безпеки;
- інсталяція і конфігурація технічних засобів захисту інформації;
- проведення навчання персоналу, що користується системою.

5-й етап — оцінювання рівня захищеності. На цьому етапі перевіряється відповідність впроваджених заходів вимогам інформаційної безпеки. Він включає:

- підготовку до оцінювання впроваджених заходів;
- безпосереднє оцінювання ефективності засобів захисту в ІКС;
- оформлення та фіксацію результатів оцінювання у відповідній документації.

6-й етап — сертифікація та авторизація засобів технічного захисту в ІКС. Затвердження конфігурації та підтвердження функціональності системи управління інформаційною безпекою (СУІБ) оформлюється шляхом отримання сертифіката, що засвідчує законне право на експлуатацію системи. Інформація про авторизовану систему заноситься до відповідного державного реєстру. Всі рішення вважаються чинними після затвердження їх уповноваженим органом у сфері авторизації відповідно до положень нормативних документів з технічного захисту інформації (НД ТЗІ).

7-й етап — безперервний моніторинг.

Постійне спостереження за станом інформаційної безпеки є важливим для своєчасного виявлення змін як у самій ІКС, так і в організаційному середовищі. З цією метою формується стратегія постійного моніторингу, яка включає:

- відслідковування змін у безпековому середовищі;
- оновлення адаптованого профілю безпеки;
- підготовку звітів про поточний стан захищеності.

Результатом моніторингу є:

- актуалізований адаптований профіль безпеки;
- оновлені політики та плани захисту інформації;
- оновлений план дій у сфері безпеки;
- звіт про фактичний стан інформаційної безпеки в ІКС.

Результати та дискусія (Results and discussions)

Проведений аналіз свідчить про те, що створення КСЗІ відбувається за таким алгоритмом:

визначення й оцінювання загроз для інформації, формування вимог до захисту інформації на підставі аналізу середовищ функціонування ІКС;

вибір варіанта системи захисту інформації, в якому оптимально підібрані засоби і заходи з максимальної протидії всім суттєвим загрозам. Розроблення технічного завдання на створення КСЗІ;

виконання організаційних, інженерних та технічних заходів, спрямованих на створення та введення в дію КСЗІ;

супроводження КСЗІ.

Таким чином, набір способів, методів та механізмів КСЗІ реалізує гарантований захист інформації від: витоку технічними каналами; несанкціонованих дій та несанкціонованого доступу до інформації; спеціального впливу на інформацію. Такий алгоритм є чітким та лінійним, передбачає закриття всіх теоретично можливих шляхів витоку інформації, впливу на неї та ІКС в цілому, відповідає вимогам щодо захисту відкритої інформації та інформації з обмеженим доступом, але позбавлений гнучкості в реалізації захисту інформації, тому у разі виникнення будь-яких змін у середовищах функціонування ІКС або технології оброблення інформації потребує повторного проведення державної експертизи відповідності КСЗІ.

Створення СУІБ відбувається за схожим алгоритмом:

аналіз ризиків на організаційному та системному рівнях, формування вимог до захисту інформації;

вибір оптимального варіанта заходів захисту інформації (базового профілю безпеки);

виконання організаційних, інженерних та технічних заходів, спрямованих на створення та введення в дію (авторизацію) СУІБ;

постійний моніторинг системи (відстеження змін, формування адаптованого профілю

безпеки).

Отже, набір способів, методів та механізмів СУІБ спрямований на реалізацію заходів захисту в ІКС із забезпечення конфіденційності, цілісності та доступності інформації, відповідає вимогам щодо захисту відкритої (конфіденційної) інформації. Такий алгоритм є циклічним, що надає змогу визначення поточного стану ефективності заходів захисту, оперативного формування адаптивного профілю безпеки та необхідних змін в інформаційній системі й робочих середовищах, а також стану безпеки в цілому, при цьому повторна авторизація безпеки інформаційної системи не потрібна.

Висновок (Conclusion)

За результатами аналізу можна дійти висновку, що КСЗІ є надійним механізмом захисту інформації в ІКС, незалежно від ступеня обмеження доступу інформації, що в ній циркулює, за умови, що функціонування цієї ІКС не передбачає вихід за межі України. З огляду на той факт, що Україна має на меті стати повноправним членом ЄС, об'єми інформаційного обміну з країнами ЄС будуть надалі зростати, що зумовлює більшу інтеграцію в європейські інформаційні системи. Отже, все більш актуальним стає питання щодо необхідності синхронізації регулювання захисту інформації в України з європейським законодавством. Алгоритм побудови СУІБ формується відповідно до вимог міжнародних стандартів, що надає можливість власнику ІКС, за потреби, отримати відповідний міжнародний сертифікат. Тому вибір СУІБ під час створення ІКС, де циркулює відкрита інформація, які навіть потенційно можуть інтегруватись в міжнародні інформаційні системи, є актуальним та необхідним. Матеріали цієї статті можуть бути корисними власникам інформаційно-комунікаційних систем у виборі системи захисту інформації під час їх побудови.

Використані джерела

1. *НД ТЗІ 3.7-003-2023 Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі*.
2. *НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.*
3. Закон України *"Про захист інформації в інформаційно-комунікаційних системах"* № 1089-IX (2020, 16 груд.).
4. Процюк, Ю. О., Паламарчук, Н. А., Паламарчук, С. А., & Штонда, Р. М. (2019). Пропозиції з вибору організаційно-технічних рішень для автоматизованих систем з врахуванням вимог до їх захисту. *Зб. наук. пр. ВІТІ, 3,* 77–83.
5. Тарасенко, Ю. С., Клим, В. Ю., Гарагатая, С. В., & Солянников, В. Г. (2021, 13–15 груд.). Аспекти безпеки та захищеності критичної інфраструктури. У Зб. матер. міжн. наук.-практ. інтернет- конференції, *Інноваційні технології, моделі управління кібербезпекою – ІТМК – 2021*. Ч. 2. Дніпро.
6. Скіцько, Олексій, & Ширшов, Роман. (2023). Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об'єктів критичної інфраструктури. *International Science Journal of Engineering & Agriculture, 2,* (6), 12–22. https://doi.org/10.46299/j.isjea.20230206.02.

References

1. *ND TZI 3.7-003-2023 Procedure for carrying out work on creating a comprehensive information protection system in the information and communication system.*
2. *ND TZI 3.6-004-21 Procedure for implementing an information security system in state bodies, enterprises, organizations whose information and communication systems process information, the protection requirement for which is established by law and does not constitute a state secret.*

3. Law of Ukraine “On Information Protection in Information and Communication Systems” No. 1089-IX (2020, Dec. 16).
4. Protsyuk, Yu. O., Palamarchuk, N. A., Palamarchuk, S. A., & Shtonda, R. M. (2019). Proposals for the selection of organizational and technical solutions for automated systems taking into account the requirements for their protection, *Coll. of Scientific Proceedings of VITI, 3*, 77–83.
5. Tarasenko, Yu. S., Klym, V. Yu., Garagataya, S. V., & Solyannikov, V. G. (2021, December 13–15). Aspects of security and security of critical infrastructure. In Collection of materials of the international scientific-practical internet conference, *Innovative technologies, models of cybersecurity management – ITMK* – 2021. Part 2. Dnipro.
6. Skitsko, Oleksiy, & Shirshov, Roman. (2023). Information Security Management System as a Tool for Improving the Security and Efficiency of Critical Infrastructure Facilities. *International Science Journal of Engineering & Agriculture, 2*, (6), 12–22. https://doi.org/10.46299/j.isjea.20230206.02.

Substantiation of the content of stages and measures and development of proposals for a rational choice of information protection system when creating information and communication systems

Oleksandr Leonenko
head of the research department
The Central research institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: leonenkols@ukr.net
ORCID: 0009-0009-1994-438X

Volodymyr Remez
Doctor of Philosophy
Associate Professor of the Military Command and Control Chair
National Defence University of Ukraine
03049, Povitrianykh Syl avenue, 28, Kyiv, Ukraine
e-mail: remezv93145@gmail.com
ORCID: 0000-0002-2561-1081

Alevtyna Hetman
Senior Researcher
Military Institute of Telecommunications and Informatization named after Heroes of Kruty
Kyiv, Ukraine
e-mail: getman2017@gmail.com
ORCID: 0000-0002-6397-7412

Yurii Melnychuk
Senior Lecturer of the Operational Art Department
at the Institute of State Military Management
National Defence University of Ukraine
03049, Povitrianykh Syl avenue, 28, Kyiv, Ukraine
e-mail: um777@ukr.net
ORCID: 0000-0003-2043-1353

Oleksii Smilianskyi
Assistant to the Deputy Commander-in-Chief of the Armed Forces of Ukraine
Office of the Commander-in-Chief of the Armed Forces of Ukraine
03168, Povitrianykh syl avenue, 6, Kyiv, Ukraine
e-mail: lesha.smeliansky@gmail.com
ORCID: 0009-0006-8573-2068

Yuliia Piatova
Researcher – Test Engineer of the Scientific Research Laboratory
State Scientific Research Institute
of Armament and Military Equipment Testing and Certification
Cherkasy, Ukraine
e-mail: pyatova463@gmail.com
ORCID: 0009-0001-2713-8435

Annotation. With the onset of the full-scale aggression by the Russian Federation against Ukraine, the importance of information security has significantly increased in the context of hybrid warfare. The information space, encompassing both military and civilian sectors, has transformed into a critically important domain of modern warfare. The aggressor actively employs tools of informational influence and cyber operations targeting personnel, the command and control systems of the Armed Forces of Ukraine, and general-use information platforms. As the functioning of the Ukrainian Armed Forces increasingly relies on information and communication systems (ICS), protecting these systems from both external and internal threats has become a top priority. On the one hand, the digitalization of command processes improves efficiency and speed of information exchange; on the other hand, it introduces new vulnerabilities into cyberspace. Consequently, establishing effective information protection systems is a necessary condition in the design and deployment of ICS.

The purpose of this article is to substantiate the structure of stages and measures in building information protection systems, as well as to develop approaches for selecting a rational protection model based on the functional and technical characteristics of ICS, including integration features within the overall system architecture.

This study employs the method of systems analysis to structure the stages of protection system development, along with comparative analysis to evaluate the effectiveness of different approaches to designing protective mechanisms within ICS.

The article proposes a generalized approach for choosing between a Comprehensive Information Protection System (CIPS) and an Information Security Management System (ISMS), based on legal requirements and the operational specifics of ICS. Additionally, the paper systematizes the procedures for developing protection systems and outlines the conditions necessary for their effective implementation.

The article's findings can be applied during the development, design, and implementation of ICS in the Armed Forces of Ukraine and other entities within the national security and defense sector. The proposed approach will help enhance the resilience of the information infrastructure under conditions of modern warfare and digital transformation.

Keywords: information and communication system, information protection system, comprehensive information protection system, information security management system, information and communication systems operating environment.