КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.767
УДК 004.056

Лаптєв Олександр Анатолійович
д.т.н., с.н.с., доцент кафедри кібербезпеки та захисту інформації
КНУ імені тараса Шевченка, Київ, Україна
ORCID ID: 0000-0002-4194-402X
olaptiev@knu.ua

Савченко Віталій Анатолійович
д.т.н., професор, професор кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-3014-131X
savitan@ukr.net

Кобозева Алла Анатолійовна
д.т.н., професор, професор кафедри технічної кібернетики та
інформаційних технологій імені професора Р.В. Меркта
Одеський національний морський університет, Одеса, Україна
ORCID ID: 0000-0001-7888-0499
alla_kobozeva@ukr.net

Салій Анатолій Григорович
к.в.н., професор, начальник інституту авіації та протиповітряної оборони
Національний університет оборони України, Київ, Україна
ORCID ID: 0000-0002-3491-9301
a.salii@ed.nuou.org.ua

Куртсеітов Тимур Ленурович
д.т.н., професор, начальник кафедри електромагнітної боротьби
Інститут інформаційно-комунікаційних технологій та кібероборони
Національний університет оборони України, Київ, Україна
ORCID ID: 0000-0001-6478-6469
kurttimur@ukr.net

МЕТОДИ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В МЕРЕЖАХ ЗВ'ЯЗКУ

Анотація. У статті розглядаються методологічні підходи до визначення та оцінки показників захищеності інформації в сучасних системах захисту. Автори акцентують увагу на складності процесу вибору показників для оцінки рівня безпеки, який потребує врахування широкого спектра факторів. До них належать характеристики захищених компонентів, дестабілізуючі впливи зовнішнього середовища, механізми захисту та часовий аспект, що відіграє ключову роль у прогнозуванні ефективності захисних заходів. Пропонується узагальнений підхід до побудови інтегрального показника, який дозволяє комплексно оцінювати стан захищеності інформації. Цей підхід базується на формуванні системи векторів, які включають вихідні характеристики, комплексні показники захищеності, параметри захищеності та вагові коефіцієнти. Такий метод забезпечує можливість врахування різних аспектів безпеки та їх взаємозв'язків. Для практичного застосування моделей оцінки безпеки виділено три основні методологічні підходи: емпіричний, теоретичний та комбінований теоретико-емпіричний. Наводяться практичні рекомендації щодо ефективного застосування моделей оцінки. Зокрема, наголошується на необхідності залучення фахівців високої кваліфікації, які здатні адекватно інтерпретувати отримані дані. Важливо враховувати поведінку показників при зміні вхідних даних, що дозволяє прогнозувати реакцію системи на нові загрози. Для вибору оптимального варіанту системи захисту запропоновано використовувати модифікований мінімаксний критерій. Цей підхід дозволяє враховувати сукупність приватних критеріїв якості та забезпечує найкраще значення серед найгірших нормованих показників. Такий метод забезпечує баланс між різними аспектами безпеки, допомагаючи знайти оптимальне рішення при проектуванні та оцінці систем захисту інформації. Запропоновані методологічні підходи та практичні рекомендації мають велике значення для

підвищення ефективності систем захисту інформації. Вони дозволяють не лише оцінювати поточний стан безпеки, але й прогнозувати можливі ризики, що є важливим для забезпечення довгострокової стійкості інформаційних систем.

Ключові слова: захист інформації; кібербезпека; показник захищеності системи; вагові коефіцієнти; моделі; вразливості; мережи.

ВСТУП

Інформація є одним із ключових ресурсів, її захист стає пріоритетним завданням для організацій та установ різного рівня. Зростання кіберзагроз, несанкціонованих дій та технічних збоїв вимагає розробки ефективних методів та моделей оцінки вразливості інформації в мережах зв'язку. Проблема полягає не лише у виявленні потенційних загроз, а й у визначенні оптимальних способів забезпечення безпеки інформації, які враховують технічні, економічні та часові аспекти її обробки та зберігання. Особливу актуальність ця тема набуває на тлі зростання складності автоматизованих систем обробки даних (АСОД) та розширення їх функціональності. Уразливість інформації може проявлятися через порушення її цілісності, конфіденційності або доступності, що призводить до значних економічних та репутаційних втрат. Тому важливо розробити науково обґрунтовані підходи до оцінки ризиків та формування інтегральних показників захищеності інформації.

У цій статті розглядаються методологічні підходи до визначення та оцінки показників захищеності інформації в системах захисту інформації (СЗІ). Вибір показників для оцінки безпеки є складним дослідницьким завданням, яке потребує врахування великої кількості факторів, таких як характеристики захищених компонентів, дестабілізуючі фактори, механізми захисту та часовий аспект. Пропонується узагальнений підхід до побудови інтегрального показника безпеки інформації, який включає формування векторів вихідних характеристик, комплексних показників захищеності, параметрів захищеності та вагових коефіцієнтів. Для практичного застосування моделей оцінки безпеки розглядаються три основні методологічні підходи: емпіричний, теоретичний та теоретико-емпіричний.

Особливу увагу приділено часовому аспекту оцінки захищеності, який дозволяє структурувати аналіз на різних часових інтервалах. Також наводяться рекомендації щодо ефективного використання моделей, серед яких наголошується на необхідності залучення кваліфікованих фахівців, оцінки поведінки показників при зміні вхідних даних та постійного вдосконалення вихідних даних. Для вибору оптимального варіанту СЗІ запропоновано використовувати модифікований мінімаксний критерій, який дозволяє враховувати сукупність приватних критеріїв якості та забезпечує найкраще значення серед найгірших нормованих показників.

Уразливість інформації є подією, що виникає як результат такого збігу обставин, коли в силу якихось причин використовувані в автоматизованих системах обробки даних засоби захисту не в змозі надати достатньої протидії прояву факторів, що дестабілізують, і небажаного їх впливу на інформацію, що захищається. Модель уразливості інформації у мережах зв'язку у загальному вигляді демонструє взаємозв'язок між факторами загроз та їх наслідками, що дозволяє детально проаналізувати процеси порушення цілісності, конфіденційності та доступності інформації. Ця модель деталізується щодо конкретних видів уразливості інформації, таких як порушення фізичної чи логічної цілісності, несанкціонованої модифікації, несанкціонованого отримання, несанкціонованого розмноження. При деталізації загальної моделі основна увага акцентується на тому, що переважна більшість порушень фізичної цілісності інформації має місце у процесі її

обробки на різних ділянках технологічних маршрутів. У цьому контексті цілісність інформації залежить не лише від процесів, які відбуваються в об'єкті, а й від цілісності інформації, що надходить на його вхід. Основну небезпеку становлять випадкові дестабілізуючі фактори (відмови, збої та помилки компонентів автоматизованих систем обробки даних), які потенційно можуть проявитися у будь-який час, і щодо цього можна говорити про регулярний потік цих факторів. Зі стихійних лих найбільшу небезпеку становлять пожежі, небезпека яких більшою чи меншою мірою також є постійною. Небезпека побічних явищ практично може бути зведена нанівець шляхом належного вибору місця для приміщень автоматизованої системи обробки даних та їх обладнання. Щодо зловмисних дій, то вони пов'язані головним чином з несанкціонованим доступом до ресурсів автоматизованої системи обробки даних. При цьому найбільшою небезпекою є занесення вірусів. Таким чином, аналіз проблеми захищеності інформації та вразливостей, які можуть виникати в мережах зв'язку, є важливим кроком у забезпеченні інформаційної безпеки. У роботі представлено системний підхід до оцінки та прогнозування загроз, що дозволяє розробити ефективні стратегії захисту інформації.

Постановка проблеми. Проблема полягає у тому, що незважаючи на існуючі дослідження та розробки в галузі захисту інформації, залишається невирішеною задача створення комплексного системного підходу для оцінки вразливостей та визначення інтегральних показників захищеності інформації в мережах зв'язку. Таким чимон проблема формулюється як протиріччя між: Існуючими окремими дослідженнями та методами захисту інформації та відсутністю єдиного системного підходу для комплексної оцінки вразливостей і ефективності систем захисту інформації. Розв'язання цієї проблеми визначається як актуальне наукове завдання, що потребує подальших досліджень та розробок.

Аналіз останніх досліджень і публікацій. Вивченню питань оцінки захищеності інформації в телекомунікаційних мережах присвячено значну кількість наукових праць. Дослідники активно шукають нові підходи до вирішення цієї проблеми, пропонуючи різні методології та моделі.

У джерелі [1] запропоновано покращений підхід до оцінки захищеності мережевого сегмента спеціалізованих комунікаційних систем. Цей метод базується на алгоритмах розподільчої ідентифікації та принципах динамічного програмування. Особливістю підходу є послідовна оцінка ризиків на кожному етапі процесу захисту з подальшим вибором оптимальних засобів захисту.

Автори роботи [2] досліджують теоретичні аспекти моделювання кібератак, використовуючи методи теорії диференціальних ігор та перетворень. Вони розробили спектральні моделі атак та запропонували векторну оптимізацію захисних механізмів, хоча не розглянули основні методологічні підходи.

У працях [3], [4] представлена модель системи виявлення вторгнень, яка фокусується на оптимізації розподілу ресурсів для захисту інформації, однак не враховує якісні показники. Роботи [5] – [7] аналізують сучасний стан розробок у сфері інформаційної безпеки, детально описуючи структуру стандарту ISO 15408, але не надають конкретних показників оцінки захищеності.

У джерелах [8] – [10] запропоновано методику оцінки порушень захищеності інформаційних ресурсів, яка враховує вразливості інформаційно-телекомунікаційних систем та множину потенційних загроз. Проте вона не містить аналізу показників оцінки вразливостей.

Роботи [11], [12] присвячені захисту інформації в автоматизованих системах. Автори розробили модель системи захисту з повним перекриттям загроз, яка враховує взаємозв'язки між загрозами, архітектурою системи захисту та об'єктами захисту.

Представлена модель дозволяє провести кількісну оцінку ефективності захисних механізмів і забезпечити мінімізацію пропуску загроз.

Кожне з досліджень має свої особливості та обмеження, що свідчить про складність проблеми оцінки захищеності інформації та необхідність подальших досліджень у цій галузі.Разом з тим, незважаючи на значну кількість публікацій щодо вирішення питань із виявлення дезінформації, на сьогоднішній день залишається невирішеною проблема. Яка полягає у відсутності системного підходу до оцінки вразливості інформації та визначення показників захищеності інформації в мережах зв'язку тому необхідність розробки методологічних підходів та моделей для комплексної оцінки вразливості інформації, визначення інтегральних показників захищеності та оптимізації систем захисту інформації з урахуванням технічних, економічних та часових аспектів є актуальним науковим завданням. Розв'язання цього наукового завдання дозволить покращити ефективність захисту інформації в мережах зв'язку та забезпечити її безпечне використання.

Метою даної статті є розгляд методологічних підходів до визначення та оцінки показників захищеності інформації в системах захисту інформації (СЗІ). У рамках цієї мети пропонується узагальнений підхід до побудови інтегрального показника безпеки інформації, який враховує вектори вихідних характеристик, комплексні показники захищеності, параметри захищеності та вагові коефіцієнти. Стаття спрямована на аналіз трьох основних методологічних підходів до оцінки вразливості інформації (емпіричного, теоретичного та теоретико-емпіричного), а також на розробку рекомендацій щодо ефективного використання моделей для оптимізації систем захисту інформації. Особлива увага приділяється часовому аспекту оцінки захищеності та вибору оптимального варіанту СЗІ за допомогою модифікованого мінімаксного критерію. Таким чином, стаття має практичну спрямованість і покликана допомогти у розробці ефективних стратегій захисту інформації в мережах зв'язку, враховуючи технічні, економічні та часові аспекти.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Уразливість інформації є подія, що виникає як результат такого збігу обставин, коли в силу якихось причин використовувані в автоматизованих системах обробки даних засоби захисту не в змозі надати достатньої протидії прояву факторів, що дестабілізують, і небажаного їх впливу на інформацію, що захищається. Модель уразливості інформації у мережах зв'язку у загальному вигляді показано на рис. 1.

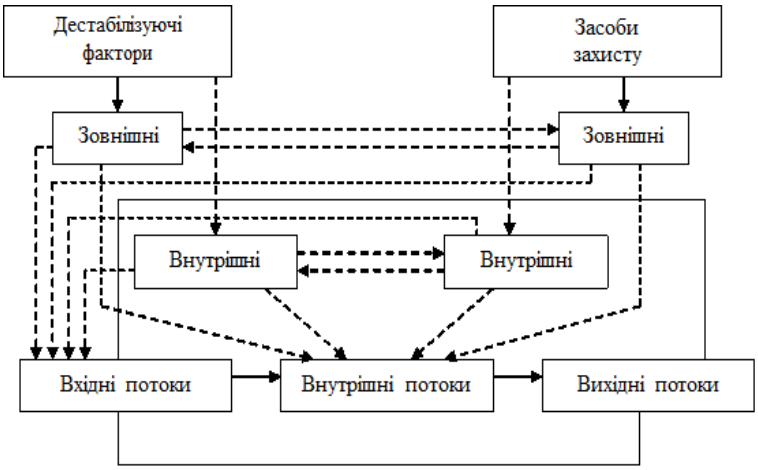

Рис. 1. Загальна модель впливу на інформацію

Ця модель деталізується щодо конкретних видів уразливості інформації: порушення фізичної чи логічної цілісності, несанкціонованої модифікації, несанкціонованого отримання, несанкціонованого розмноження.

При деталізації загальної моделі основна увага акцентується на тому, що переважна більшість порушень фізичної цілісності інформації має місце у процесі її обробки на різних ділянках технологічних маршрутів. У цьому цілісність інформації залежить тільки від процесів, які відбуваються об'єкті, а й від цілісності інформації, що надходить з його вхід. Основну небезпеку становлять випадкові дестабілізуючі фактори (відмови, збої та помилки компонентів автоматизованих систем обробки даних), які потенційно можуть проявитися у будь-який час, і щодо цього можна говорити про регулярний потік цих факторів. Зі стихійних лих найбільшу небезпеку становлять пожежі, небезпека яких більшою чи меншою мірою також є постійною. Небезпека побічних явищ практично може бути зведена нанівець шляхом належного вибору місця для приміщень автоматизованої системи обробки даних та їх обладнання. Щодо зловмисних дій, то вони пов'язані головним чином з несанкціонованим доступом до ресурсів автоматизованої системи обробки даних. При цьому найбільшою небезпекою є занесення вірусів.

Відповідно до викладеного, загальна модель процесу порушення фізичної цілісності інформації на об'єкті автоматизованої системи обробки даних представлена на рис. 2.

Рис. 2. Загальна модель процесу порушення фізичної цілісності інформації

З точки зору несанкціонованого отримання інформації принципово важливою є та обставина, що в сучасних автоматизованих системах обробки даних воно можливе не лише шляхом безпосереднього доступу до баз даних, а й багатьма шляхами, які не потребують такого доступу. При цьому основну небезпеку становлять зловмисні дії людей. Вплив випадкових факторів безпосередньо не веде до несанкціонованого одержання інформації, воно лише сприяє появі каналів несанкціонованого одержання інформації, якими може скористатися зловмисник.

Розглянемо трансформацію загальної моделі вразливості з погляду несанкціонованого розмноження інформації. Принциповими особливостями цього процесу є:

- будь-яке несанкціоноване розмноження є зловмисною дією;
- несанкціоноване розмноження може здійснюватися в організаціях-розробниках компонентів автоматизованої системи обробки даних, безпосередньо в автоматизованій системі обробки даних та сторонніх організаціях, причому останні можуть отримувати носій, з якого робиться спроба зняти копію як законним, так і незаконним шляхом.

У процесі розвитку теорії та практики захисту інформації сформувався методологічний підхід до оцінки вразливості інформації: емпіричний, теоретичний і теоретико-емпіричний.

Емпіричний підхід до оцінки уразливості інформації в мережах зв'язку

Сутність емпіричного підходу полягає в тому, що на основі тривалого збору та обробки даних про реальні прояви загроз інформації та про розміри того збитку, який при цьому мав місце, суто емпіричним шляхом встановлюються залежності між потенційно можливим збитком та коефіцієнтами, що характеризують частоту прояву відповідної загрози. і значення розміру шкоди, що мав при її прояві.

Найбільш характерним прикладом моделей розглянутого різновиду є моделі, розроблені фахівцям американської фірми IBM. Розглянемо підходи, що розвиваються на цих моделях.

Вихідним посилом розробки моделей є майже очевидне припущення: з одного боку, у разі порушення захищеності інформації завдається певні збитки, з іншого — забезпечення захисту інформації пов'язані з витрачанням коштів. Повна очікувана вартість захисту може бути виражена сумою витрат на захист та втрат від її порушення. Цілком очевидно, що оптимальним рішенням було б виділення на захист інформації засобів, що мінімізують загальну вартість робіт із захисту інформації.

Для того, щоб скористатися цим підходом до вирішення проблеми, необхідно знати (або вміти визначати), по-перше, очікувані втрати при порушенні захищеності інформації, а по-друге, залежність між рівнем захищеності та засобами, що витрачаються на захист інформації.

Вирішення першого питання, тобто оцінки очікуваних втрат при порушенні захищеності інформації, принципово може бути отримано лише тоді, коли йдеться про захист промислової, комерційної та подібної до них таємниці, хоча і тут зустрічаються дуже серйозні труднощі. Щодо оцінки рівня втрат при порушенні статусу захищеності інформації, що містить державну, військову та їм подібну таємницю, то тут досі суворих підходів до їх отримання не знайдено. Ця обставина істотно звужує можливу область використання моделей, заснованих на підходах, що розглядаються.

Для визначення рівня витрат, що забезпечують необхідний рівень захищеності інформації, необхідно принаймні знати, по-перше, повний перелік загроз інформації, по-друге, потенційну небезпеку для інформації для кожної загрози і, по-третє, розміри витрат, необхідних для нейтралізації. кожній із загроз.

Оптимальне вирішення щодо доцільного обсягу витрат на захист інформації полягає у встановленні цього рівня таким чином, щоб він відповідав очікуваним втратам у разі порушення безпеки. Таким чином, ключовим завданням є визначення можливого рівня втрат. Фахівці компанії IBM запропонували емпіричну модель, яка дозволяє оцінити очікувані втрати від конкретної *i*-ої інформаційної загрози.

$$R_i = 10^{(S_i + V_i - 4)} \quad (1)$$

де S_i — коефіцієнт, що характеризує можливу частоту виникнення відповідної *i*-ої загрози; V_i — коефіцієнт, що характеризує значення можливої шкоди при її виникненні.

Сумарна вартість втрат визначається формулою

$$R = \sum_{V_i} R_i \quad (2)$$

Отже, якщо б вдалося зібрати достатню кількість реальних даних про загрози та їх наслідки, запропоновану модель можна було б застосовувати для вирішення широкого

спектру завдань із захисту інформації. Крім того, ця модель не лише допомагає знаходити оптимальні рішення, а й оцінювати їх точність. Однак у контексті України така статистика майже відсутня. Натомість у США, наприклад, збір та аналіз подібних даних активно проводяться рядом установ, таких як Стенфордський дослідницький інститут. Це дозволило отримати достатньо надійні дані щодо різних типів загроз, які можуть слугувати основою для орієнтовних розрахунків і в інших країнах.

Розробка алгоритму оптимізації захищених мереж зв'язку

Велика кількість технічних і економічних параметрів, які впливають на ефективність системи технічного захисту інформації (ТСЗІ), потребує вибору узагальненого техніко-економічного критерію *К* для оптимізації. Відомі методи поєднання технічних і економічних характеристик ТСЗІ (наприклад, парних критеріїв) не завжди є обґрунтованими. Найпоширенішим підходом є представлення узагальненого критерію як функції нормованих приватних показників, зважених за допомогою «вагових» коефіцієнтів, або побудова ієрархії приватних критеріїв. Однак суб'єктивний характер у виборі «ваг» і визначення пріоритетів серед критеріїв значно обмежує застосовність таких методів. Використання обмежень також не завжди можливе через невизначеність у величинах, які накладаються.

Створення будь-якої ТСЗІ має бути економічно виправданим: ефект від її застосування *Е* повинен перевищувати витрати на її розробку та впровадження *С*. При цьому ТСЗІ слід розглядати як складову комплексної системи захисту, яка взаємодіє з іншими елементами для досягнення загальної мети — забезпечення необхідного рівня захищеності інформації протягом усього періоду її використання. Справді, кожен захисний захід має на меті не лише безпосереднє захист інформації, а й створення умов для ефективного використання інформації у майбутньому для вирішення поставлених завдань. Тому:

$$K=Э-C, \tag{3}$$

витрати на впровадження системи С визначаються безліччю економічних $\{X_g\}$,

$g=\overline{1,Q}$ параметрів (заборони проектування. виготовлення C_i, експлуатацію $Cэ = EcCэгод$ ТСЗІ і каналів зв'язку системи $Cкс= CoZкс$):

$$C = C(X_g) = C_u + T_c C_{згод} + C_{КС} \tag{4}$$

Ефективність використання ТСЗІ Е є різницею між величиною ефекту Е*, що визначається при заданих технічних вимогах до захисту об'єкта $Xd \le Xd^*$, та втратами ефективності від неідеальності технічних характеристик ТСЗІ

$$Э = Э^* - \sum_{f}^{F} \Delta Э_f \tag{5}$$

Очевидно, що $f \ne d, Д \le F$ і задача оптимізації ТСЗІ з врахуванням (4) і (5) буде мати вигляд

$$\max K = \max \left\{ Э(X^* d) - \sum_{\substack{j=1 \\ f=2}}^{F,Q} \left[C(X_g) + \Delta(X_f) \right] \right\}. \tag{6}$$
$$d=1,\ldots,Д \le F$$
$$f \ne d$$
$$X_d \le X_d^*$$

ISSN 2663 - 4023

Узагальнений техніко-економічний критерій (6) є критерієм повних витрат $K^1 = \left(C + \sum_{\Delta} Э\right)$ [2] з обмеженнями на технічні характеристики X_d^*. Параметри X_d^* визначають величину Е* при проведеному передпроектному дослідженні з урахуванням доцільності проектування ТСЗІ взагалі та є обмеженнями при виборі набору технічних засобів ТСЗІ

$$H_\varphi^n = \left\{\{h_i\}\alpha_\varphi^n\right\}; \quad \alpha_\varphi^n = 1,..., \beta_\varphi^n .$$

Безліч технічних засобів H_φ^n відповідає певним параметрам $n = \overline{1, N}$ при заданому законі функціонування системи $\{3\}\varphi, \varphi = \overline{1, \phi}$. Для визначення оптимальної ТСЗІ найбільш ефективний шлях перебору набору технічних засобів з розрахунком для кожного з них *max K* або min K^1 відповідно до виразів (4) – (6) згідно з алгоритмом (рис. 3).

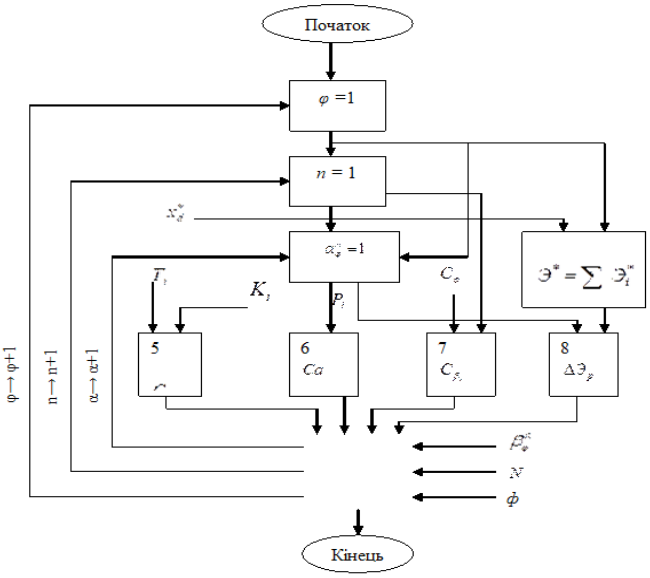

Рис. 3. Алгоритм оптимізації ТСЗІ за узагальненим критерієм ефективності

Алгоритм синтезу оптимальної ТСЗІ є послідовним перебором варіантів за координатами $\alpha_\varphi^n \to n \to \varphi$, причому підцикли оптимізації допускають автономне рішення, що спрощує процес проектування ТСЗІ.

При технічному вдосконаленні ТСЗІ необхідний попередній аналіз залежності $Э\left(X_d^*\right)$, яка може бути отримана в результаті об'єкта захисту. Найбільший вплив на величину Е* надає точність та надійність функціонування ТСЗІ, що характеризується хибними спрацьовуваннями або перепустками атак на об'єкт. Втрати ефективності визначаються переважно ненадійністю технічних засобів ТСЗІ.

Якщо $Э^* = Э_o \gamma^{-\gamma}$, $C = C_o \delta^{-g}$, $\Delta Э_p = Э^* P$, де γ, g — показники ступеня, що визначаються експериментальним шляхом (цілі, дробові, позитивні), то відповідно до (6) можна знайти оптимальне — доцільне — значення похибки δ_{opt}, виправдане економічно. Так, при γ=1,g=2:

$$\delta_{opt} = \frac{^2 C_o}{Э_{o(1-p)}}.$$

Передбачуваний підхід до вибору критерію ефективності дозволяє обґрунтовано проектувати ТСЗІ та визначати ефективність технічного вдосконалення та модернізації технічних засобів, елементів та вузлів системи.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Визначення показників захищеності інформації є складним дослідницьким завданням, що потребує системного підходу та врахування великої кількості факторів. Для оцінки захищеності інформації пропонується використовувати інтегральний показник безпеки Q, який будується на основінаступних показників: вектора вихідних характеристик системи, комплексних показників захищеності, параметрів захищеності, вагових коефіцієнтів окремих показників та синтезуючої функції. Пропонується використовувати модифікований мінімаксний критерій для вибору оптимального варіанту системи захисту інформації серед доступних альтернатив.

Для практичного застосування моделей оцінки безпеки інформації важливо мати кваліфікованих фахівців, оцінювати поведінку показників при зміні вхідних даних, залучати експертів для оцінки адекватності моделей, постійно вдосконалювати вихідні дані. Для ефективного застосування моделей необхідно мати достатній обсяг достовірних вихідних даних, що часто є проблемою на практиці.

Подальші дослідження мають бути спрямовані на удосконалення методів збору та аналізу статистичних даних, а також на розробку нових моделей прогнозування загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Brailovskyi, M. M., Khoroshko, V. O., & Khoroshko, O. V. (1999). Optimization of parameter choice of information protection system. *Proceedings of the National Aviation University, 2(1).* https://doi.org/10.18372/2306-1472.2.9319
2. Laptiev, O. A., Sobchuk, V. V., & Savchenko, V. A. (2019). A method of increasing the noise immunity of the system for detection, recognition and localisation of digital signals in information systems. *Collection of scientific papers of the Military Institute of Taras Shevchenko National University of Kyiv, 66,* 124–132.
3. Laptiev, O., Pohasii, S., Milevskyi, S., Sobchuk, A., & Barabash, A. (2021). Detection illegal of means of obtaining of information by the method of determining the deviation of characteristics of radio signal from the specified parameters. *Znanstvena misel journal. Slovenia, 1(61),* 23–29.
4. Kyrychok, R., Laptiev, O., Lisnevsky, R., Kozlovsky, V. & Klobukov, V. (2022). Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. *Eastern-European Journal of Enterprise Technologies, 1(9(115),* 93–101. https://doi.org/10.15587/1729-4061.2022.253530.
5. Berkman, L. N., Barabash, O. V., Tkachenko, O. M., Musiienko, A. P., Laptiev, O. A., & Svynchuk, O. V. (2022). Intelligent control system for information and communication networks. *Navigation and communication control systems, 3(69),* 54–59. https://doi.org/10.26906/SUNZ.2022.3
6. Kudinov, V. O., & Khoroshko, V. O. (2005). Methodology of system design of the corporate network of the internal affairs agencies of Ukraine. *Protection of information, 2,* 4–13.
7. Kudinov, V. O., Plus, D. V., Khoroshko, V. O., & Chyrkov, D. V. (2005). Methodology for synthesising the optimal topology of a corporate network structure. *Information security, 1,* 12–21.
8. *Information Security Management Systems — Requirements . International Organization for Standardization* (ISO/IEC 27001:2022) (2022).
9. Hryshchuk, R. V. (2008). Quantitative assessment of the level of security of electronic computing equipment objects taking into account their functioning in the conditions of information conflict. *Bulletin of the Higher Technical School of the State Technical University of Ukraine Technical sciences: computer science, computer engineering, 3(46),* 113–120.
10. Buriachok, V. L. (2011). Algorithm for assessing the degree of security of special information and telecommunication systems. *Protection of information, 3(52),* 19–27.

11. Laptiev, O., & Zozulia, S. (2023). The method of exclusion of known signals when scanning a specified radio range. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique"*, *2(22)*, 31–38. https://doi.org/10.28925/2663-4023.2023.22.3138
12. Laptiev, S. (2022). The advanced method of protection of personal data from attacks using social engineering algorithms. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique"*, *4(16)*, 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Oleksandr Laptiev
Doctor of Technical Science, Senior Researcher
Associate Professor the Department of Cyber Security and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0002-4194-402X
olaptiev@knu.ua

Vitalii Savchenko
Doctor of Technical Sciences, Professor,
Professor Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-3014-131X
savitan@ukr.net

Alla Kobozieva
Doctor of Technical Sciences, Professor, Professor Department of
Technical Cybernetics and Information Technology n.a. Prof. R.V. Merkt
Odesa National Maritime University, Odesa, Ukraine
ORCID ID: 0000-0001-7888-0499
alla_kobozeva@ukr.net

Anatolii Salii
Candidate of Military Sciences, Professor
Chief of the Aviation and Air Defence Institute
National Defence University of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-3491-9301
a.salii@ed.nuou.org.ua

Tymur Kurtseitov
Doctor of Technical Sciences, Professor
Head of the Department of Electromagnetic Warfare
Institute of Information and Communication Technologies and Cyber Defense
National Defense University of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-6478-6469
kurttimur@ukr.net

METHODS FOR ASSESSING INFORMATION SECURITY IN COMMUNICATION NETWORKS

Abstract. The article considers methodological approaches to determining and assessing information security indicators in modern security systems. The authors focus on the complexity of the process of selecting indicators to assess the level of security, which requires taking into account a wide range of factors. These include the characteristics of protected components, destabilizing environmental influences, protection mechanisms, and the time aspect, which plays a key role in predicting the effectiveness of protective measures. A generalized approach to constructing an integral indicator is proposed, which allows for a comprehensive assessment of the state of information security. This approach is based on the formation of a system of vectors that include initial characteristics, complex security indicators, security parameters, and weighting factors. This method provides the ability to take into account various aspects of security and their relationships. For the practical application of security assessment models, three main methodological approaches are distinguished: empirical, theoretical, and combined theoretical-empirical. Practical recommendations are given for the effective application of assessment models. In particular, the need to involve highly qualified specialists who are able to adequately interpret the data obtained is emphasized. It is important to consider the behavior of indicators when changing input data, which allows predicting the system's response to new threats. To select the optimal variant of the protection system, it is proposed to use a modified minimax criterion. This approach allows taking into account the set of private quality criteria and provides the best value among the worst normalized indicators. This method provides a balance between various aspects of security, helping to find the optimal

solution when designing and evaluating information protection systems. The proposed methodological approaches and practical recommendations are of great importance for increasing the effectiveness of information protection systems. They allow not only to assess the current state of security, but also to predict possible risks, which is important for ensuring the long-term stability of information systems.

Keywords: information protection; cybersecurity; system security indicator; weighting coefficients; models; vulnerabilities; networks.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Brailovskyi, M. M., Khoroshko, V. O., & Khoroshko, O. V. (1999). Optimization of parameter choice of information protection system. *Proceedings of the National Aviation University, 2(1).* https://doi.org/10.18372/2306-1472.2.9319
2. Laptiev, O. A., Sobchuk, V. V., & Savchenko, V. A. (2019). A method of increasing the noise immunity of the system for detection, recognition and localisation of digital signals in information systems. *Collection of scientific papers of the Military Institute of Taras Shevchenko National University of Kyiv, 66,* 124–132.
3. Laptiev, O., Pohasii, S., Milevskyi, S., Sobchuk, A., & Barabash, A. (2021). Detection illegal of means of obtaining of information by the method of determining the deviation of characteristics of radio signal from the specified parameters. *Znanstvena misel journal. Slovenia, 1(61),* 23–29.
4. Kyrychok, R., Laptiev, O., Lisnevsky, R., Kozlovsky, V. & Klobukov, V. (2022). Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. *Eastern-European Journal of Enterprise Technologies, 1(9(115),* 93–101. https://doi.org/10.15587/1729-4061.2022.253530.
5. Berkman, L. N., Barabash, O. V., Tkachenko, O. M., Musiienko, A. P., Laptiev, O. A., & Svynchuk, O. V. (2022). Intelligent control system for information and communication networks. *Navigation and communication control systems, 3(69),* 54–59. https://doi.org/10.26906/SUNZ.2022.3
6. Kudinov, V. O., & Khoroshko, V. O. (2005). Methodology of system design of the corporate network of the internal affairs agencies of Ukraine. *Protection of information, 2,* 4–13.
7. Kudinov, V. O., Plus, D. V., Khoroshko, V. O., & Chyrkov, D. V. (2005). Methodology for synthesising the optimal topology of a corporate network structure. *Information security, 1,* 12–21.
8. *Information Security Management Systems — Requirements . International Organization for Standardization* (ISO/IEC 27001:2022) (2022).
9. Hryshchuk, R. V. (2008). Quantitative assessment of the level of security of electronic computing equipment objects taking into account their functioning in the conditions of information conflict. *Bulletin of the Higher Technical School of the State Technical University of Ukraine Technical sciences: computer science, computer engineering, 3(46),* 113–120.
10. Buriachok, V. L. (2011). Algorithm for assessing the degree of security of special information and telecommunication systems. *Protection of information, 3(52),* 19–27.
11. Laptiev, O., & Zozulia, S. (2023). The method of exclusion of known signals when scanning a specified radio range. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 2(22),* 31–38. https://doi.org/10.28925/2663-4023.2023.22.3138
12. Laptiev, S. (2022). The advanced method of protection of personal data from attacks using social engineering algorithms. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 4(16),* 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562