об'єктивності оцінювання. Практичне значення полягає у можливості застосування запропонованої моделі для проведення аудиту інформаційної безпеки державних інформаційних систем; підтримки прийняття управлінських рішень; визначення пріоритетних напрямів підвищення рівня захищеності; моніторингу змін стану інформаційної безпеки у динаміці.

Результати дослідження свідчать, що використання інтегрального показника дозволяє отримати узагальнену оцінку стану інформаційної безпеки та своєчасно виявляти критичні вразливості. Запропонована модель є гнучкою та може бути адаптована до специфіки конкретних державних інформаційних систем.

У роботі запропоновано модель оцінювання рівня інформаційної безпеки державних інформаційних ресурсів на основі інтегрального показника та ризикоорієнтованого підходу. Використання системи індикаторів та вагових коефіцієнтів дозволяє здійснювати кількісну оцінку стану захищеності інформаційних систем. Запропонований підхід забезпечує підвищення об'єктивності оцінювання та може бути використаний у практиці управління інформаційною безпекою державного сектору.

1. Ящук В., Балацька В. Підвищення кіберстійкості критичної інформаційної інфраструктури держави через вдосконалення процесів реагування на кіберінциденти // Цивільний захист в умовах війни : збірник тез доповідей II Міжнародної науково-практичної конференції, м. Львів, 15 квітня 2026 року. Львів : ЛДУБЖД, 2026. С. 92–95.
2. Венгерський П.С., Вишневська Н.С., Хохлачова Ю.Є., Хорошко В.О., Чобаль О.І. Кількісна оцінка кіберзахищеності інформації. Захист інформації. 2023. Т. 25, №2. С. 53–61.

Проблеми інтервального моніторингу цілісності інформаційного стану корпоративних кіберфізичних систем

УДК 004.056:681.5

Павло Матусяк[1], Ярослав Тарасенко[2]

[1]Державний університет інформаційно-комунікаційних технологій, Pavelmatusyak@gmail.com,
[2]Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, yaroslav.tarasenko93@gmail.com

В умовах цифровізації виробничих і сервісних процесів корпоративні кіберфізичні системи виступають у ролі середовища з особливими ознаками порушення безпеки. Вторгнення у такому середовищі супроводжується поступовим спотворенням сукупності контрольованих параметрів на відміну від миттєвих відмов, спричинених порушенням цілісності інформаційного стану. Під цілісністю інформаційного стану мається на увазі збереження узгодженості, допустимості та відсутності спотворення поточних оцінок параметрів у часі. Для корпоративних кіберфізичних систем таке формулювання набуває особливого значення через можливість накопичення

спотворень на рівні сенсорів, шлюзів, сервісів обробки та під час формування керуючих рішень. У таких умовах інтервальний моніторинг передбачає здійснення контролю в межах допустимого інтервалу змін, який залежить від режиму функціонування, шумів, затримок та невизначеностей моделі. Підтвердження цьому висвітлено в роботі [1], де розглядаються інтервальні спостерігачі, стійкі до атак у ролі засобу оцінювання стану. Такий стан розглядається за умов прихованих атак, які спричиняють маскування порушення цілісності в допустимих межах фіксованого порогу.

Аналіз роботи [2], де представлено удосконалений метод інтервального оцінювання дозволив виявити та сформувати три основні взаємопов'язані проблеми інтервального моніторингу: складність відокремлення початкової фази вторгнень від штатних коливань системи, швидка втрата інформативності фіксованих меж контролю у змінних умовах функціонування, збільшення кількості хибних спрацювань за умов підвищення чутливості моніторингу.

Отже, перспективним напрямком вирішення зазначених проблем є поєднання інтервального моніторингу з інтелектуальним уточненням меж штатного функціонування системи. Важливим є інтелектуальне коригування інтервалів за поточним профілем функціонування системи. Доцільно формалізувати правила коригування, вибір ознак порушення цілісності та узгодження моніторингу з допустимим рівнем хибних спрацювань тривог.

1. Degue K.H., Ny J.L., Efimov D. Stealthy attacks and attack-resilient interval observers. *Automatica*. 2022. Vol. 146. URL: https://doi.org/10.1016/j.automatica.2022.110558 (дата звернення: 04.05.2026).
2. Fan J., Huang J., Zhao. X. Improved interval estimation method for cyber-physical systems under stealthy deception attacks. *IEEE Transactions on Signal and Information Processing Over Networks*. 2022. Vol. 8. P. 1-11.

Алгоритм аудіостеганографії без внесення змін у файл-контейнер

УДК 004.056.5

Костянтин Фріга[1], Юрій Дорофєєв[2], Ірина Назарова[3]

Національний університет «Одеська політехніка»,
[1]10252733@stud.op.edu.ua, [2]dym@op.edu.ua, [3]nazarova.i.v@op.edu.ua

Переважна більшість методів аудіостеганографії передбачає вбудовування корисного повідомлення безпосередньо в аудіоконтейнер, причому одним з основних показників якості методу є степень непомітності внесених змін з точки зору слухової системи людини [1], [2].

В [3], [4] розглянуто спосіб прихованого передавання інформації за допомогою монохромних, кольорових графічних файлів та аудіофайлів без зміни контейнера на основі методу Zero Distortion Technique (метод нульового спотворення - МНС). На відміну від традиційних методів аудіостеганографії, де повідомлення безпосередньо вбудовується в сигнал і може змінювати його структуру, у МНС контейнер використовується як готова бітова послідовність.