МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

АКТУАЛЬНІ ПРОБЛЕМИ ОСВІТИ ТА НАУКИ

Збірник матеріалів

XXVII підсумкової науково-практичної конференції викладачів

20 лютого 2025 року

Київ 2025

УДК 061.3(063)

АКТУАЛЬНІ ПРОБЛЕМИ НАУКИ ТА ОСВІТИ: Збірник матеріалів XXVII підсумкової науково-практичної конференції викладачів МДУ / За заг. ред. М.В. Трофименка. Київ: МДУ, 2025. 385 с.

Рекомендовано до друку та поширення через мережу Інтернет вченою радою Маріупольського державного університету (протокол № 7 від 26.02.2025)

Збірник містить матеріали XXVII підсумкової науково-практичної конференції викладачів МДУ, яка відбулася 20 лютого 2025 року в Маріупольському державному університеті.

У матеріалах висвітлені актуальні проблеми розвитку міжнародних відносин та зовнішньої політики, філософії та соціології, історії, економіки та менеджменту, права, екології, кібербезпеки, документознавства, культурології, журналістики, філології, літературознавства, методики викладання, педагогіки та психології.

Видання адресоване науковцям, викладачам, аспірантам та здобувачам вищої освіти, а також усім, хто цікавиться сучасними проблемами науки та освіти.

Редакція не несе відповідальності за авторський стиль тез, опублікованих у збірнику.

СЕКЦІЯ
«СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА АНАЛІЗ ДАНИХ»

Дрейс Юрій,
кандидат технічних наук, доцент,
доцент кафедри системного аналізу та інформаційних технологій,
Маріупольський державний університет

АКТУАЛЬНІСТЬ РОЗРОБКИ МЕТОДОЛОГІЇ ОЦІНЮВАННЯ НАСЛІДКІВ ВИТОКУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У період перебування України у військовому стані, досить гостро постає питання у забезпеченні безпеки критичної інфраструктури держави від можливих загроз, інцидентів, кібератак, несанкціонованого втручання та кризових ситуацій, тобто у підтримці такого стану захищеності, за якого забезпечуються її функціональність, безперервність роботи, відновлюваність, цілісність і стійкість до надання об’єктами цієї критичної інфраструктури основних послуг та життєво важливих функцій, порушення яких призведе до негативних наслідків для національної безпеки України.

Головною вимогою до об’єкта критичної інформаційної інфраструктури є ефективне забезпечення стійкого і безперервного функціонування об’єкта критичної інфраструктури для надання ним основних послуг та життєво важливих функцій, реалізовуючи при цьому захист критичної інформаційної інфраструктури. Ефективність захисту критичної інформаційної інфраструктури визначається її здатністю до своєчасного виявлення, запобігання і нейтралізації загроз безпеці об’єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації. Тобто виконувати функції захищеності від подій або ряду несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) та/або таких, що мають ознаки несанкціонованого втручання в функціонування об’єкта критичної інфраструктури, які становлять загрозу його безпеці, системі управління технологічними процесами об’єкта критичної інфраструктури, створюють ймовірність порушення штатного режиму функціонування такого об’єкта (у тому числі зриву та/або блокування роботи, функціонування та/або несанкціонованого управління його ресурсами, витоку інформації), ставлять під загрозу його захищеність. Недостатнє забезпечення захисту

критичної інформаційної інфраструктури від реалізації загрози витоку інформації з обмеженим доступом, необхідної у процесі надання об'єктом критичної інфраструктури основних послуг та життєво важливих функцій, може призвести до порушення його стійкого і безперервного функціонування, що матиме негативні наслідки для безпеки критичної інфраструктури держави та національної безпеки України.

Однак існує певне протиріччя між ефективністю забезпечення стійкого і безперервного функціонування об'єкта критичної інфраструктури у процесі надання основних послуг і життєво важливих функцій та ефективністю реалізованих методів, засобів та заходів, які не забезпечують достатнього рівня захисту об'єктів критичної інформаційної інфраструктури. Це протиріччя може бути вирішеними шляхом розробки методології з новими та удосконаленими моделями, методами, засобами та системами оцінювання можливих наслідків реалізації загрози витоку інформації з обмеженим доступом на об'єкті критичної інфраструктури для своєчасної їх мінімізації та ліквідації, дозволить забезпечити підтримку такого стану захищеності критичної інформаційної інфраструктури, за якого забезпечується безперервність функціонування і стійкість надання основних послуг та життєво важливих функцій, що є однією з найактуальніших науково-технічних задач сьогодення.

Тому, з метою підвищення рівня захищеності критичної інформаційної інфраструктури та оцінювання можливих наслідків від загрози витоку інформації з обмеженим доступом (персональних даних, службової та таємної інформації), які можуть завдати шкоди особі, суспільству, державі, розроблені відповідні моделі, методи та засоби [1-7].

Література

1. Корченко О., Дрейс Ю., Лозова І. Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах. *Захист інформації*. 2016. Т. 18, № 1: С. 39-47. https://doi.org/10.18372/2410-7840.18.10111

2. Дрейс Ю. Модель параметрів оцінювання наслідків витоку службової інформації об'єкта критичної інфраструктури. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2024. 2 (26): С.200-211. https://doi.org/10.28925/2663-4023.2024.26.691

3. Дрейс Ю. Метод оцінювання наслідків втрати об'єкта критичної інфраструктури за узагальненими критеріями. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2024. 1 (25): С.487-504. https://doi.org/10.28925/2663-4023.2024.25.487504

4. Dreis Yu., et al. Restricted Information Identification Model. *Cybersecurity Providing in Information and Telecommunication Systems 2022. CEUR.* 2022. Vol. 3288: 89-95.

5. Dreis Yu., et al. Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection. *Cybersecurity Providing in Information and Telecommunication Systems 2024*, *CEUR*. 2024. Vol. 3654: 277-289.

6. Dreis Yu., et al. Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection. *Cyber Security and Data Protection 2024, CEUR*. 2024. Vol. 3800: 1-11. *(Scopus)*

7. О. Корченко, Ю. Дрейс, І. Лозова, Є. Педченко, Теоретико-множинна GDPR-модель параметрів персональних даних. *Захист інформації*. 2020. 22 (2): С.120-141.

Єнікєєв Олександр,
доктор технічних наук, доцент, професор кафедри системного аналізу та інформаційних технологій
Маріупольський державний університет

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОПРАЦЮВАННЯ ДАНИХ НЕПРЯМИХ ВИМІРЮВАНЬ НА ОСНОВІ ВЗАЄМНІЙ КОРЕЛЯЦІЙНІЙ ФУНКЦІЇ

Програмно-апаратні засоби задавання штатного налаштування подач палива у циліндри двигунів використовують форсунки із п’єзоелектричним керуванням. За умов неповної інформації побудова алгоритмічного забезпечення базується на виборі методу моніторингу фазових пророщень відносно штатного налаштування подач палива із використанням зворотного зв’язку за станом сигналу ЧМ-сигналу швидкості обертання колінчастого валу. Для визначення розподілу запізнень пропонується ідея використати методи кореляційного аналізу для опрацювання сигналу вимірювальної інформації. Розробляння методології нового методу моніторингу штатних фазових запізнень подач палива забезпечать менші невизначеність та швидкодією опрацювання даних непрямих вимірювань, що й визначає актуальність даної науково-прикладної задачі.

Розроблено концептуальні засади побудови програмно-апаратних засобів зі зворотнім зв’язком за станом сигналу вимірювальної інформації. Використано механічну систему із трьома ступенями волі за умов врахування тертя при моделюванні крутної схеми силового агрегату. Рухи мас моделі описано нормалізованою системою лінійних диференціальних рівнянь. Для її розв’язання застосовано перетворення Лапласу за нульових початкових умов. Встановлено інформаційні зв’язки між крутними моментами циліндрів та сигналом