Секція 1

# РОЗРОБЛЕННЯ МЕТОДУ ЗАХИСТУ ВІД ФІЗИЧНОЇ ПІДМІНИ ПРИСТРОЇВ ОХОРОННОЇ СИГНАЛІЗАЦІЇ У ОБ'ЄКТАХ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

Григор'єв А. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

**Актуальність**. Сучасні технології значно змінюють наше повсякденне життя, роблять процеси більш ефективними та спрощують їх [1]. Однак, зі зростанням застосування пристроїв охоронної сигналізації в різних галузях, з'являються нові виклики стосовно їх безпеки та захисту від можливих загроз. Тому проблема захисту від фізичної підміни таких охоронних пристроїв стає дуже актуальною, особливо в контексті збільшення застосування технології інтернету речей, де ці пристрої використовуються для збору та передачі даних у реальному часі [2]. Сучасні системи охоронних сигналізацій не завжди забезпечують ефективний захист від фізичної підміни пристроїв, що може стати причиною можливих вторгнень і крадіжок інформації. Недолік в захисті може бути використаний зловмисниками для незаконного доступу до системи та викрадення даних з метою їх подальшого використання з особистою користю [3].

**Метою** роботи є розроблення та впровадження ефективних методів захисту, які забезпечують надійність та безпеку використання пристроїв охоронних сигналізації в умовах збільшеного ризику фізичної підміни [4].

**Основні положення.** Дослідження та розроблення методів захисту включають в себе використання криптографічних методів шифрування даних, що забезпечують конфіденційність та цілісність даних, що пережаються, ускладнюючи їх перехоплення та підміну зловмисниками. Важливим аспектом є проєктування фізичних захисних корпусів для охоронних пристроїв, що ускладнюють доступ до внутрішніх компонентів за допомогою ударостійких матеріалів, датчиків розкриття та механізмів самознищення при спробі несанкціонованого доступу. Інтеграція систем виявлення вторгнень (IDS) дозволяє слідкувати за активністю та виявляти аномальні дії, які можуть свідчити про спробу фізичної підміни або несанкціонованого доступу, автоматично сповіщаючи адміністраторів про підозрілі події та запускаючи контрзаходи [5].

**Висновки**. Захист від фізичної підміни охоронних пристроїв є критично важливим завданням у сучасному технологічному середовищі. Його вирішення вимагає комплексного підходу та спільних зусиль фахівців у галузі технологій та безпеки для забезпечення надійності та безпечне використання цих пристроїв. Це включає впровадження передових криптографічних методів, фізичних захисних механізмів, систем виявлення вторгнень, регулярне оновлення стандартів безпеки, багатофакторну аутентифікацію, постійний моніторинг та аудит. Тільки завдяки комплексному підходу та використанню новітніх технологій можна ефективно знизити ризики, пов'язані з фізичною підміною охоронних пристроїв, та забезпечити їх безперебійну та безпечну роботу в умовах сучасних загроз.

## Список літератури

1. Іванов П. О., Петрова Л. М. Аналіз ефективності сучасних охоронних датчиків у системах безпеки. У кн.: Технології безпеки: матеріали конференції «Сучасні виклики безпеки», 15-16 жовтня 2020 р., м. Київ, м. Львів, м. Одеса, м. Дрезден : [у 2 т.]. Т. 2 / Київський нац. ун-т [та ін.]. – Київ: Видавництво Науковий світ, 2020. – 112 с.

2. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури / ДержНДІ Спецзв'язку УДК 004.056, 2015. – 58-60 с.

3. Системи контролю і управління доступом від А до Я. *Deps*. URL: https://deps.ua/ua/knowegable-base/reference-information/7824.html (дата звернення: 23.10.2024).

4. Професійна безпека системи. *Ajax*. URL: https://ajax.systems/ua/ (дата звернення: 23.10.2024).

5. Мазур Ю. О., Зелінська О. В. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. Прикладні аспекти сучасних міждисциплінарних досліджень: матеріали І Всеукраїнської науковопрактичної конференції (м. Вінниця, 26 листопада 2021 р.). Вінниця: ДонНУ імені Василя Стуса, 2021. С. 102–103. URL: https://jpasmd.donnu.edu.ua/issue/view/403 (дата звернення: 23.10.2024).

## Відомості про авторів

Григор'єв Андрій Олексійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.o.hryhoriev@student.csn.khai.edu

Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, o.morozova@csn.khai.edu