Секція 1

# ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Набока С. А.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

**Актуальність.** Дослідження засобів забезпечення кібербезпеки інтелектуальних систем відеоспостереження є надзвичайно важливою у сучасному світі. Зростання використання відеоспостереження у різних сферах, таких як громадська безпека, бізнес, транспортна інфраструктура та інші, призводить до збільшення кількості цифрових відеоданих, які потребують захисту від кібератак [1]. Оскільки інтелектуальні системи відеоспостереження використовуються для розпізнавання облич, виявлення аномальної поведінки, відстеження об'єктів та інших функцій, вони стають привабливим мішенями для кіберзлочинців. Шахраї можуть намагатися зламати систему відеоспостереження для отримання незаконного доступу до відеоданих або зміни їх з метою вводу в оману, впливу на прийняття рішень або завдання шкоди [2].

Дослідження засобів забезпечення кібербезпеки інтелектуальних систем відеоспостереження спрямовані на виявлення потенційних вразливостей систем, розробку захисних механізмів, протоколів шифрування, аутентифікації та інших методів, що дозволяють забезпечити конфіденційність, цілісність і доступність відеоданих. Актуальність цих досліджень підвищується з поширенням нових технологій, таких як розподілені системи відеоспостереження, використання хмарних обчислень та штучного інтелекту [3].

**Метою** роботи є аналіз засобів забезпечення інтелектуальних систем відеоспостереження та відеоданих від кіберзагроз.

**Основні положення** дослідження засобів забезпечення кібербезпеки інтелектуальних систем відеоспостереження можуть включати наступні аспекти:

1. Аналіз загроз та вразливостей: Визначення потенційних загроз та вразливостей, яким піддаються інтелектуальні системи відеоспостереження. Це включає виявлення вразливих місць у системі, можливих шляхів атаки та потенційних кіберзагроз [4].
2. Розробка захисних механізмів: Розробка та впровадження захисних механізмів для запобігання кібератак та забезпечення безпеки інтелектуальних систем відеоспостереження. Це може включати розробку протоколів шифрування, систем аутентифікації, контролю доступу, систем виявлення вторгнень тощо.

3. Тестування та оцінка ефективності: Проведення тестування та оцінка ефективності розроблених захисних механізмів. Це включає проведення випробувань системи на наявність вразливостей, симуляцію кібератак та оцінку відповідності системи стандартам кібербезпеки.
4. Управління ризиками: Визначення та управління ризиками, пов'язаними з кібербезпекою інтелектуальних систем відеоспостереження. Це включає ідентифікацію потенційних загроз, оцінку ризиків, розробку стратегій запобігання і реагування на інциденти, а також розробку планів відновлення після кібератаки.
5. Свідомість та навчання: Залучення операторів систем відеоспостереження та користувачів до свідомого використання безпеки. Це включає проведення навчання, розробку освітніх матеріалів та розповсюдження кращих практик забезпечення кібербезпеки [5].
6. Розробка стандартів і рекомендацій: Внесення внеску у розробку стандартів і рекомендацій щодо кібербезпеки інтелектуальних систем відеоспостереження. Це допомагає створити загальноприйняті норми та вимоги до безпеки таких систем.

Ці основні положення спрямовані на створення надійних та безпечних інтелектуальних систем відеоспостереження, які забезпечують захист від кіберзагроз та збереження конфіденційності, цілісності та доступності відеоданих.

**Висновки.** Результатами досліджень засобів забезпечення кібербезпеки інтелектуальних систем відеоспостереження є методологія розробки ефективних механізмів захисту цих засобів від кіберзагроз, забезпечення конфіденційності та цілісності відеоданих, а також підвищення ефективності та надійності відеоспостереження.

**Список літератури**

1. Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security. Cengage Learning.
2. Kizza, J. M. (2019). Guide to Computer Network Security. Springer.
3. Dargahi, V., & Mittal, S. (2019). Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications. IGI Global.
4. Khalid, M. S., & Khan, M. K. (2018). Internet of Things Security: Fundamentals, Techniques, and Applications. CRC Press.
5. Chen, C., Leung, V. C. M., Shu, L., & Zhang, Y. (Eds.). (2016). Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Springer.

**Відомості про авторів**

Набока Сергій Андрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», s.a.naboka@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, доцент, v.pevnev@csn.khai.edu