УДК 004.056

МЕТОДИ ІНТЕГРАЦІЇ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ З СИСТЕМАМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Буграк Б.В.
e-mail: bohdan.buhrak@nure.ua
Науковий керівник – доц. Добринін І.С.
Харківський національний університет радіоелектроніки каф. ІКІ
м. Харків, Україна

The paper analyzes methods of integrating video surveillance systems with information security management systems. The study considers modern approaches to combining physical and information security using software interfaces, centralized monitoring platforms and intelligent video analytics. A simplified model of integrated security architecture is proposed. The effectiveness of system integration is evaluated using an analytical indicator based on incident detection probability, automation level and response time. The results show that integrated security systems significantly improve the efficiency of incident detection and response.

У сучасних умовах забезпечення інформаційної безпеки є одним із ключових завдань будь-якої організації. Зростання кількості кіберзагроз, розвиток мережевих технологій і збільшення обсягів критичних даних потребують комплексного підходу до захисту інформаційних ресурсів. Традиційні засоби захисту, зокрема міжмережеві екрани, системи виявлення вторгнень та антивірусне програмне забезпечення, забезпечують контроль цифрового середовища, однак не дають змоги повною мірою враховувати фізичні аспекти безпеки. Відповідно до ISO/IEC 27001:2022, система управління інформаційною безпекою повинна охоплювати організаційні, технічні та фізичні заходи захисту [1]. Саме тому інтеграція систем відеоспостереження із системами управління інформаційною безпекою є важливим напрямом побудови сучасних комплексних систем захисту.

Сучасні системи відеоспостереження здатні не лише здійснювати запис відео, а й автоматично аналізувати відеопотоки, виявляти аномальні події та передавати інформацію про них до інших підсистем безпеки [2]. Інтегрована система безпеки поєднує камери відеоспостереження, систему управління відео, модулі відеоаналізу, системи контролю доступу, сервери обробки даних і платформу моніторингу інцидентів. Їх взаємодія часто реалізується через стандартизовані інтерфейси, зокрема ONVIF, що забезпечує сумісність пристроїв різних виробників [3]. Основними методами інтеграції є API-інтеграція, централізовані платформи моніторингу, системи аналізу та кореляції подій, а також інтелектуальний відеоаналіз. Використання цих підходів дозволяє об’єднати фізичні та цифрові події в єдиному середовищі моніторингу, підвищити оперативність виявлення загроз і зменшити навантаження на персонал служби безпеки [2], [4].

Узагальнену схему інтеграції систем безпеки наведено на рисунку 1.

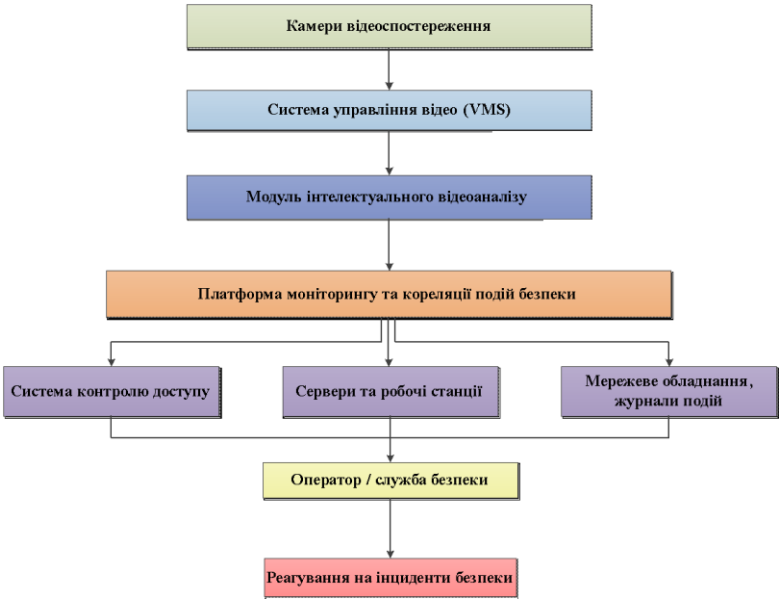

Рисунок 1 – Схема інтеграції систем безпеки

На схемі показано інтеграцію фізичних та інформаційних компонентів безпеки. Камери відеоспостереження передають відеодані до системи управління відео, після чого інформація може оброблятися модулем інтелектуального відеоаналізу. Платформа моніторингу та кореляції подій отримує дані не лише від відеосистеми, а й від систем контролю доступу, серверів і мережевого обладнання. У результаті оператор або служба безпеки отримують узагальнену інформацію про інцидент і можуть оперативно реагувати на загрози [3], [4].

Для порівняльного оцінювання в роботі використано умовний узагальнений показник, сформований на основі підходів до побудови метрик інформаційної безпеки, викладених у NIST SP 800-55:

$$E = \frac{P_d \cdot A}{T_d},$$

де E – ефективність системи; P_d – ймовірність виявлення інциденту; A – коефіцієнт автоматизації; T_d – середній час виявлення інциденту [5].

Значення P_d , A і T_d прийнято як умовні модельні характеристики для двох типів систем: традиційної та інтегрованої. Для традиційної системи обрано нижчу ймовірність виявлення інциденту та більший час виявлення, оскільки значна частина аналізу виконується вручну. Для інтегрованої системи прийнято вищі значення ймовірності виявлення та автоматизації й менший час виявлення, що пояснюється використанням відеоаналізу, кореляції подій і централізованого моніторингу [2], [4].

Для традиційної системи без інтеграції відеоспостереження приймемо такі модельні значення: P_d = 0,6, A = 0,5, T_d = 10 хв. Тоді:

$$E_1 = \frac{0{,}6 \cdot 0{,}5}{10} = 0{,}03.$$

Для інтегрованої системи безпеки з використання відеоаналізу та платформи кореляції подій приймемо такі модельні значення: P_d = 0,9 A = 0,8, T_d = 4 хв. Тоді:

$$E_2 = \frac{0{,}9 \cdot 0{,}8}{4} = 0{,}18.$$

Порівняємо отримані значення:

$$K = \frac{E_2}{E_1} = \frac{0{,}18}{0{,}03} = 6.$$

Отже, інтеграція систем відеоспостереження з системами управління інформаційною безпекою може підвищити ефективність моніторингу приблизно у 6 разів. Це підтверджує доцільність поєднання фізичних та цифрових засобів захисту в межах єдиної системи безпеки.

Список використаних джерел:

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO : вебсайт. URL: https://www.iso.org/standard/27001 (дата звернення 03.03.2026).
2. Duong H.–T., Le V.–T., Hoang V.–T. Deep Learning–Based Anomaly Detection in Video Surveillance: A Survey. Sensors. 2023. Vol. 23, No. 11. Art. 5024. URL: https://doi.org/10.3390/s23115024 (дата звернення 03.03.2026).
3. Profiles, Add–ons and Specifications. ONVIF : вебсайт. URL: https://www.onvif.org/profiles-add-ons-specifications/ (дата звернення 04.03.2026).
4. Kent K., Souppaya M. Guide to Computer Security Log Management. Gaithersburg : National Institute of Standards and Technology, 2006. 72 p. URL: https://doi.org/10.6028/NIST.SP.800-92 (дата звернення 05.03.2026).
5. Schroeder K., Trinh H., Pillitteri V. Measurement Guide for Information Security. Volume 1: Identifying and Selecting Measures. Gaithersburg : National Institute of Standards and Technology, 2024. URL: https://doi.org/10.6028/NIST.SP.800-55v1 (дата звернення 05.03.2026).