УДК 004.056

АРХІТЕКТУРА ІНТЕГРОВАНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ТА 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 examines the architecture of an integrated video surveillance and information security management system. A multi-level model combining IP cameras, edge processing, video analytics, and a SIEM platform is analyzed. It is shown that such an architecture reduces network load and shortens incident response time by correlating video data with digital security events. Particular attention is paid to personal data protection requirements. The results demonstrate that the proposed approach improves the efficiency of monitoring and enhances the resilience of organizations to hybrid threats.

У сучасних умовах захист інформаційної інфраструктури не може обмежуватися лише засобами кібербезпеки, оскільки фізичний доступ до критичних приміщень і обладнання безпосередньо впливає на стан інформаційної безпеки організації. Відповідно до ISO/IEC 27001:2022, система управління інформаційною безпекою має враховувати організаційні, технічні й фізичні заходи захисту [1]. Тому інтеграція відеоспостереження із системами управління інформаційною безпекою є важливим напрямом побудови комплексних систем захисту.

Метою роботи є аналіз архітектури інтегрованої системи відеоспостереження та управління інформаційною безпекою та оцінювання її ефективності. Сучасні засоби відеоаналітики на базі моделей YOLO дозволяють виявляти об’єкти в реальному часі, що дає змогу використовувати відеоспостереження для автоматичного виявлення підозрілих подій [2]. Інтеграція відеоданих із мережевими журналами, системами контролю доступу та серверними логами формує єдине середовище моніторингу інцидентів [3].

Архітектура інтегрованої системи є багаторівневою: IP-камери здійснюють захоплення відеопотоку, edge-пристрої виконують первинну обробку та формують метадані інцидентів, після чого інформація надходить до VMS або серверів аналітики, а далі – до SIEM-платформи для кореляції подій. Такий підхід дозволяє передавати до центрального вузла лише релевантні фрагменти та службові дані, що зменшує мережеве навантаження і прискорює реагування [3].

На рисунку 1 для представлення зображена архітектура інтегрованої системи відеоспостереження.

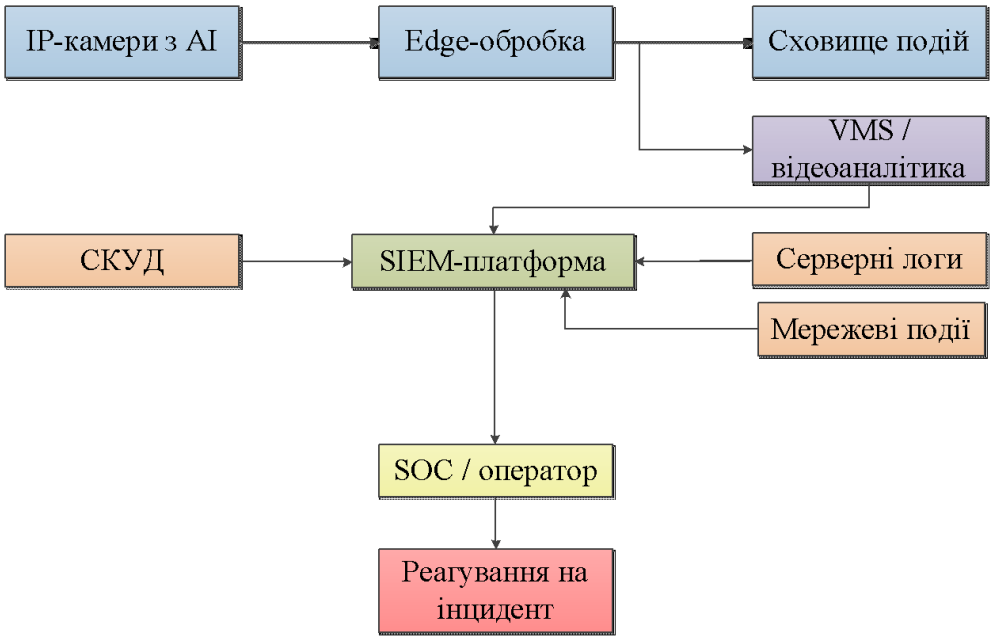

Рисунок 1 – Архітектура інтегрованої системи відеоспостереження та управління інформаційною безпекою

Камери та edge-пристрої виконують первинне виявлення подій, після чого метадані й потрібні фрагменти відео передаються до системи відеоаналітики. SIEM-платформа поєднує ці дані з подіями контролю доступу, серверними журналами та мережевими подіями, у результаті чого оператор отримує скорельований інцидент. Це підвищує достовірність спрацювань і скорочує час реагування [3].

Ефективність запропонованої архітектури доцільно оцінювати за двома показниками: зменшенням мережевого навантаження та скороченням часу реагування. Обсяг переданих даних визначимо за формулою:

$$V = B \cdot T,$$

де V – обсяг даних; B – швидкість потоку; T – час [2], [3].

Якщо система містить 8 IP-камер, кожна з яких формує потік 4 Мбіт/с, то без edge-обробки за одну годину до центрального вузла передається близько 14,1 ГБ даних. Якщо після edge-обробки до центральної системи надходить лише 25% початкового потоку, цей обсяг зменшується до приблизно 3,5 ГБ. Тоді коефіцієнт зменшення мережевого навантаження становить:

$$K_v = \frac{14{,}1}{3{,}5} \approx 4.$$

Отже, використання edge-обробки дозволяє приблизно у 4 рази зменшити обсяг даних, що передаються до центральної системи [2], [3].

Час реагування на інцидент доцільно оцінювати як суму часу виявлення, аналізу та передавання сповіщення:

$$T_r = T_d + T_a + T_n,$$

де T_d – час виявлення; T_a – час аналізу; T_n – час передавання сповіщення [3].

Для традиційної системи сумарний час реагування становить 180 с, тоді як для інтегрованої системи з edge-детекцією та SIEM-кореляцією – 60 с. Тоді коефіцієнт прискорення реагування дорівнює:

$$K_t = \frac{180}{60} = 3.$$

Таким чином, інтегрована архітектура дозволяє приблизно у 3 рази скоротити час реагування на інцидент завдяки автоматизації виявлення та обробки подій [2], [3].

Оскільки система обробляє відеозаписи й журнали доступу, вона має відповідати вимогам Закону України «Про захист персональних даних» [4].

Отже, інтегрована система поєднує фізичний і цифровий контури захисту, зменшуючи мережеве навантаження приблизно у 4 рази та час реагування у 3 рази.

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 05.03.2026).

2. Home - Ultralytics YOLO Docs. Ultralytics : вебсайт. URL: https://docs.ultralytics.com/ (дата звернення 05.03.2026).

3. What is Microsoft Sentinel SIEM? Microsoft Learn : вебсайт. URL: https://learn.microsoft.com/en-us/azure/sentinel/overview (дата звернення 07.03.2026).

4. Закон України :Про захист персональних даних від 01.06.2010 № 2297-VI. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 08.03.2026)