УДК 621.396:004.056]:621.397.43

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

Куцин Г.Г.
e-mail: hryhorii.kutsyn@nure.ua
Науковий керівник – ст. викладач Олейнікова О.І.
Харківський національний університет радіоелектроніки, каф. ІРТЗІ
м. Харків, Україна

The paper examines the issue of information protection in modern video surveillance systems. Key methods for ensuring the confidentiality, integrity and availability of video information are described, including encryption, user authentication, the use of checksums and backup. Organizational and technical measures to improve the security of video surveillance systems are also considered. The importance of compliance with regulatory requirements for the protection of personal data is emphasized.

Захист інформації в системах відеоспостереження є важливою складовою загальної системи інформаційної безпеки державних установ, підприємств та приватних організацій. Відеоспостереження використовується для контролю доступу, забезпечення безпеки людей і майна, фіксації правопорушень та аналізу подій. В умовах цифровізації суспільства та поширення IP-технологій відеоспостереження перетворюється не лише на інструмент фізичної безпеки, а й на об’єкт кіберзахисту. Відеодані можуть містити персональну інформацію, службові відомості або комерційну таємницю, тому їх захист регулюється законодавством України та нормативними документами у сфері технічного й криптографічного захисту інформації.

Сучасна система відеоспостереження складається з відеокамер, мережевої інфраструктури, серверів зберігання та програмного забезпечення для керування відеопотоком, відеореєстраторів. Усі ці компоненти можуть бути вразливими до кіберзагроз. Найбільш поширеними загрозами є злам облікових записів, перехоплення відеопотоку через незахищені мережі, впровадження шкідливого програмного забезпечення, фізичне пошкодження обладнання, а також внутрішні загрози з боку персоналу. Особливо вразливими є IP-камери, підключені до мережі Інтернет без належного захисту. Вони можуть стати об’єктами несанкціонованого доступу, перехоплення трафіку або використання в бот-мережах [1]. В системах відеоспостереження виникають ризики, пов’язані з порушенням конфіденційності, цілісності, доступності відеоданих.

Одним із ключових напрямів захисту є забезпечення конфіденційності відеоданих. Для цього застосовується шифрування під час передачі інформації мережею, використання захищених криптографічних протоколів зв’язку, а також шифрування архівів на серверах зберігання. Важливу роль відіграє автентифікація користувачів: використання складних паролів, ба-

гатофакторної автентифікації, обмеження прав доступу відповідно до службових обов'язків, регулярне оновлення програмного забезпечення та ведення журналів обліку дій користувачів.

Не менш важливою є збереження цілісності інформації. Відеозаписи повинні бути захищені від несанкціонованого редагування або видалення. Цілісність відеоданих забезпечується шляхом ведення журналів подій, застосування контрольних сум і цифрових підписів, що унеможливлює непомітне редагування або видалення записів [2]. Резервне копіювання даних є необхідною умовою збереження інформації у випадку технічних збоїв або кібератак. Рекомендується зберігати резервні копії окремо від основної системи, у захищеному середовищі.

Доступність систем відеоспостереження також має критичне значення. Захист від атак типу відмови в обслуговуванні, використання мережевих екранів, сегментація мережі та постійний моніторинг стану обладнання, впровадження резервного електроживлення та дублювання ключових елементів системи дозволяють мінімізувати ризик переривання роботи системи [2].

Окрему увагу слід приділяти нормативно-правовим аспектам захисту інформації. Відеозаписи, на яких можна ідентифікувати особу, є персональними даними, а отже їх обробка повинна здійснюватися на законних підставах. Організації повинні дотримуватися вимог законодавства щодо захисту персональних даних, інформувати осіб про ведення відеоспостереження та визначати терміни зберігання записів.

Таким чином, захист інформації в системах відеоспостереження є комплексним завданням, що поєднує технічні, організаційні та правові заходи. Лише системний підхід до інформаційної безпеки дозволяє забезпечити належний рівень інформаційної безпеки та мінімізувати ризики витоку або втрати відеоданих [3].

Список використаних джерел:

1. ENISA. Baseline Security Recommendations for IoT. - European Union Agency for Cybersecurity, 2017. URL: https://www.enisa.europa.eu /publications/baseline-security-recommendations-for-iot/ (дата звернення 12.03.2026).

2. Stallings W. Network Security Essentials: Applications and Standards. - Pearson Education, 2017. URL: https://www.emgywomenscollege. ac.in/templateEditor/kcfinder/upload/files/Network-security-essentials.pdf/ (дата звернення 12.03.2026).

3. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910 (дата звернення 12.03.2026).