УДК 004.056

В. О. Дейбук

Проблеми побудови захищених систем відеоспостереження у медичних закладах

Вінницький національний технічний університет

Анотація.

Розглянуто основні тенденції і проблеми побудови захищених систем відеоспостереження для медичних закладів. Визначено, що більшість сучасних систем відеоспостереження в медичних закладах є незахищеними від різних кібератак та інформаційних втручань та зовнішнього зловмисника.. Відзначено актуальність кіберзахисту схем відеоспостереження на базі відеореєстраторів у сучасному світі та галузі охорони здоров'я. Визначено проблематику їх кібербезпеки.

Ключові слова: система відеоспостереження(СВС), система відеонагляду (СВН), Інтернет речей (IoT), кіберзагроза, кібератака, кіберзахист, канали передачі даних, мережа відеоспостереження, шифрування, інформаційний та кіберзахист, вразливості.

Abstract.

The main trends and problems of building protected video surveillance systems for medical institutions are considered. It is determined that the majority of the existing video surveillance systems in medical institutions are unprotected from various cyberattacks and information interference and external attackers. The relevance of cyber protection of surveillance schemes based on video recorders in the modern world and the healthcare industry is noted. The issues of their cybersecurity are determined.

Keywords:

Keywords: video surveillance system (VSS), video surveillance system (VSS), Internet of Things (IoT), cyber threat, cyber attack, cyber defense, data transmission channels, video surveillance network, encryption, information and cyber defense, vulnerabilities.

Вступ

Останнім часом поряд із розвитком інформаційних технологій значно розвиваються технології відеоспостереження (СВС, СВН) [1, 2]. Сучасні технології інформаційних систем на базі IP-відеокамер та на базі IP-контролерів управління набули широкого розвитку у різних галузях і в т.ч. і у медичній галузі, і використовуються у закладах охорони здоров'я, приватних медичних закладах та інших установах, поряд із системами Інтернету речей (IoT) (наприклад, таких як «Розумний будинок»). Однак, як зазначено у роботах [1, 2] дуже гостро стоїть проблема кіберзахисту відеокамер у цих системах, яка не вирішена, так як наявні фактори кіберзагроз для СВН:

- складності і "не захищеності" архітектури мережі СВН/СВС та апаратної будови пристроїв;
- складності та відсутності гнучкості захисту відеокамер і зв'язків у СВН ;
- складності контролю взаємозв'язків інформаційних потоків і пристроїв СВН: як внутрішніх інформаційних систем і пристроїв, так і зовнішніх;
- складністю і важкістю контролю внутрішніх інформаційних комунікацій і кінцевих точок ;
- наявність радіо інтерфейсів і вразливостей в обладнанні СВН;
- наявністю не захищених логічних портів на камерах СВН та відеореєстраторів;
- наявність відкритих і доступних портів та інших ресурсів в СВН, які доступні із зовнішньої сторони (наприклад, мережі Інтернет);
- наявність відкритої інформації про СВН та додаткові компоненти мережі у вільному доступі (наприклад, IP-адреси).

Вирішення проблеми кібератак та зовнішніх інформаційних втручань по стороннім і внутрішнім каналам в СВН [1-2] вимагає нових підходів і залишається актуальним у СВН для медичних закладів і системах із відкритими зовнішніми інтерфейсами, зв'язками і незахищених каналах зв'язку.

Метою роботи є покращення рівня кіберзахисту СВН(СВС) для сфери охорони здоров'я. Розробка ефективних підходів і рекомендацій кіберзахисту для СВН для сфери охорони здоров'я, основаних на нових принципах дозволить враховувати й компенсувати сумарні і поодинокі інформаційні впливи і кібератаки на СВН, та забезпечити повну нейтралізацію найбільш критичних кіберзагроз в системах відеонагляду, в складі як спеціалізованих і загальних систем відеоспостереження.

Проблема кібербезпеки систем відеоспостереження

Оцінка кібератак і шкідливих впливів на медичні СВС(СВН) по основним та вторинним каналам [1-3], показує, що основні кібер-втручання та інформаційні впливи здійснюються саме по інформаційним каналам та зовнішнім інтерфейсам камер СВН (близько 60-75% серед всіх інцидентів) – прямий злам камер відеоспостереження, 5-10%- злам серверів відеоспостереження і відеореєстратора, ще 5-10%- злам мереж і каналів систем відеоспостереження, в т.ч. ЛОМ(локальних обчислювальних мереж). Інша частина незначний відсосток загроз – 3-5% - не прямі і складні атаки по вторинним каналам. Незначне число інцидентів (близько 1-2%) відбувається по незалежним технічним причинам чи помилкам користувачів чи персоналу.

Для захисту СВН на якісному рівні в сучасному середовищі СВН із підключенням до Інтернету , враховуючи широкий набір кіберзагроз і фронт кібератак, дуже складно забезпечити ефективний і дієвий кіберзахист для СВН. Тим більше без сучасних актуальних оновлень ПЗ та апаратних оновлень продуктів та пристров СВН (наприклад, відеокамер) без перевипуску (нового виготовлення) нової архітектури апаратури чи ПЗ із закритими вразливостями CWE апаратного і програмного рівня. Основна проблема кібербезпеки СВН полягає у складності архітектури СВН, неможливістю усунення окремих основних вразливостей, наявних слабких місць і наявних доступних місць для підключення до мереж СВН.

З погляду і точки зору зловмисника (хакера), сама система чи мережа представляється набором вразливих місць і доступних сокетів(IP+порт), MAC-адрес та інших ресурсів для підключення. Таке представлення не дозволяє точно і ефективно, а головне – повно охопити і розглянути безпеку СВН, адже виникають і існують "сліпі зони" безпеки і апаратні і програмні вразливості, які неможливо виправити швидко. Є основні характерні вразливості CWE для СВН, які пов'язані із кібератаками на пам'ять, порти, адреси, адмін-панель і окремі функції камер СВН , які реалізуються дистанційно. Окремий крас атак – на відео сервер СВН та сам механізм і алгоритм роботи і представлення ресурсів СВН порядку виконання машинних команд управління та реалізації принципів підвищення привілеїв доступу і виконання несанкціонованих інструкцій в системах СВН, та зокрема на відеосервері СВН .

Більшість класичних практик і засобів кібербезпеки для систем відеоспостереження не завжди дозволяють закрити класичні інформаційні загрози в системах СВН, особливо для критичних систем СВН, якими є системи у медичній сфері. Також проблема полягає у багатофункціональності сучасних пристроїв СВН у закладах охорони здоров'я. Різноманіття та відкриті функції окремих IT -пристроїв в складі СВН лікарень із не зовсім безпечними ОС роблять можливими різні кібератаки на них. Окремі технології захисту неможливо застосувати безпосередньо на рівні архітектури СВН в т.ч. окремих до окремих пристроїв і схем СВН на базі IP-камер, в силу відсутності гнучкості і безпеки ПЗ та гнучкості ОС.

Одним із основних завдань кіберзахисту СВН– є актуальні і точні оцінки впливу кіберзагроз у мережі відеоспостереження, а також оцінки наслідків від їх впровадження .

Також слід враховувати специфіку побудови мереж ЛОМ та інтерфейсів СВН ля можливості моніторингу та керування відеокамерами.

Висновки

Розглянуто основні тенденції і проблеми побудови захищених систем відеоспостереження для медичних закладів. Визначено , що більшість сучасних систем відеоспостереження в медичних закладах є незахищеними від різних кібератак та інформаційних втручань та зовнішнього зловмисника та не завжди відповідають стандартам безпеки.

В роботі наведено проблеми кібербезпеки СВН для сучасних закладів охорони здоров'я, напрацьовані на базі досліджень і аналізу реальних кіберзагроз. Наведені загальні кібератаки і їх причини в СВН.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Топчій Н.В. Аналіз захищеності IP-камер відеоспостереження : [Електронний ресурс] / Н.В. Топчій, О.С. Білевська // Інформатика, обчислювальна техніка та автоматизація - №2 - 2023. - С.157-161. - Режим доступу URL : https://www.tech.vernadskyjournals.in.ua/journals/2021/3_2021/27.pdf (Дата звернення : 28.04.2025р.).

2. Відеоспостереження у публічних місцях: основи захисту персональних даних (посібник для органів місцевого самоврядування):[Електронний речурс] / В.К. Батчаєв, У.С. Шадська. — К.. Компринт, 2021. —98 с.- Режим доступу URL : http://labs.journ.univ.kiev.ua/hrj/wp-content/uploads/2021/07/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D1%81%D0%BF%D0%BE%D1%81%D1%82%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F-%D0%B2-%D0%BF%D1%83%D0%B1%D0%BB%D1%96%D1%87%D0%BD%D0%B8%D1%85-%D0%BC%D1%96%D1%81%D1%86%D1%8F%D1%85_%D0%9F%D0%9E%D0%A1%D0%86%D0%91%D0%9D%D0%98%D0%9A.pdf (Дата звернення : 28.04.2025р.).

Дейбук В'ячеслав Олександрович — студент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, Україна.

Ніковий керівник :

Маліновський Вадим Ігоревич — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, Україна.

Deibuk Viacheslav Oleksandrovich – student of the Department of Information Protection, Faculty of Information Technology and Computer Engineering, Vinnitsa National Technical University, Vinnitsa, Ukraine.

Vadym Ihorevych Malinovskyi — PhD in Technical Sciences, Associate Professor of the Department of Information Security, Vinnitsa National Technical University, Vinnitsa, Ukraine.