УДК 004.056.5

ВИМОГИ ДО КОНСТРУКЦІЇ СУЧАСНИХ ТЕХНІЧНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Когутенко М. Є., здобувач вищої освіти групи МКБп-201
Науковий керівник: **Петренко Т.А**, к.т.н., доцент
Національний університет «Чернігівська політехніка»

За останні кілька десятиліть із збільшенням попиту на безпеку, відеоспостереження стало актуальним напрямком для досліджень. Такі сфери, як запобігання, виявлення та втручання, які призвели до розвитку реальних та послідовних систем відеоспостереження, здатні до інтелектуальних компетенцій з обробки відео. Загалом, вдосконалене відеоспостереження можна охарактеризувати як інтелектуальну техніку обробки відеоматеріалу, яке розроблено для надання допомоги персоналу служби безпеки, шляхом надійних оповіщень у режимі реального часу та підтримки ефективного відеоаналізу для судових розслідувань.

Водночас, для того, щоб розробити надійну сучасну технічну систему відеоспеостреження, потрібно чітко розуміти основні вимоги, які висуваються до конструкції зазначених систем та систематизувати їх.

Саме тому, в даному дослідження ми систематизуємо ці вимоги на такі як: 1) камери та їх типи; 2) системи управління відео; 3) типи систем управління відео; 4) типи сховищ; 5) види відеоаналітики; 6) відображення відеоспостереження.

1. Камери та їх типи

Типи камер, що використовуються за різних умов, є важливими факторами відеоспостереження. Зазвичай, для побудови інтелектуальної системи відеоспостереження розглядають такі типи камер:

PTZ-камери: одні з найбільш часто використовуваних камер для цілей безпеки; де P означає панорамування, T – нахил, Z – масштабування. Ці камери мають можливість обертатися на 360 градусів, щоб охоплювати широку область і збільшувати деталі.

Box-камери: зовнішні камери, де можна налаштувати об’єктив з надвисокою роздільною здатністю. Виготовлені з процесором датчика зображення, який здатний знімати відео з кольоровою роздільною здатністю. Лінзи цих камер можуть бути змінними або фіксованими.

Купольні камери: поєднання об'єктива, камери та стельового кріплення, упакованого у форму купола. Добре підходять для середовища, яке має тенденцію забруднюватися, наприклад, кухні, комори тощо.

IP-камери: камери які, зазвичай, передають цифровий сигнал за допомогою Інтернет-протоколу по мережі. Особливостями є висока роздільна здатність та масштабованість.

Бездротові IP-камери: тип камер абсолютно бездротовий, установка проста і знижує швидкість прокладки мережевих кабелів. Мають функції нахилу та обертання, що допомагає забезпечувати максимальну чіткість огляду навіть в умовах недостатнього освітлення.

Денні та нічні камери: використовується як для внутрішнього, так і для зовнішнього середовища з низьким або слабким освітленням. Мають відмінні лінзи, що дозволяють інфрачервоному випромінюванню проходити та діставатися до пристрою, що з'єднаний із зарядом, або додатковим чіпом всередині камери. Як результат, кінцевий користувач може бачити зображення в повній темряві на відстані інфрачервоного випромінювання, що створюється світлодіодами [1].

Теплові камери: створюють чіткі зображення в режимі реального часу з високою роздільною здатністю, що робить їх важливим інструментом для промислового застосування. Можуть виявити аномалії, які, як правило, невидимі неозброєним людським оком. Швидко та точно сканують та візуалізують розподіл температури певних поверхонь, що зменшує витрати та економить час.

2. Системи управління відео

Система управління відео – це запис і управління доступом до відео, яке фіксується камерою, а потім передається в модуль системи відеоспостереження [2]. Існує два типи з'єднань, через які передається захоплене відео: відео може передаватися через IP-адресу комп'ютерної мережі або як аналогові відео; залежно від того, чи використовується IP-камера або аналогова відеокамера, зняте відео може передаватися по кабелю або по повітрю.

3. Типи систем управління відео

У цифровому відеореєстраторі (DVR) відеозаписи записуються з камери спостереження на жорсткий диск. Вони більш гнучкі в порівнянні з аналоговими стрічковими системами (VHS) і дозволяють полегшити передачу відео через комп'ютерну мережу.

Гібридні цифрові відеореєстратори (HDVR) підтримують IP-камери, можуть виконувати всі функції цифрового відеореєстратора, і додають підтримку IP та мегапіксельних камер.

Мережеві відеореєстратори (NVR) підтримують лише IP-камери, можуть записувати відео з номерів цифрових камер відеоспостереження, які передаються по мережі.

4. Типи сховищ

Існує три основних типи сховищ:

Жорсткі диски, вбудовані в цифровий відеомагнітофон, мережевий відеореєстратор або сервер, представляють собою внутрішню пам'ять. Найдоступніші в ціновій категорії, але можуть бути менш надійними.

Приєднані сховища – жорсткі диски, розташовані за межами цифрового відеомагнітофона, мережевого відеореєстратора або сервера. Це дорожче порівняно з внутрішньою пам'яттю, але вони мають більшу масштабованість, гнучкість та надмірність.

Кластери ємності – ємності на базі IP, що можуть адаптувати потоки відео з великої кількості камер. Дають професійні і універсальні можливості та адаптовану здатність роботи.

5. Види відеоаналітики

Оптимізація сховища: здійснюється на основі виявлення поміченого руху у спостережуваній сцені та вирішується, як саме зберігати в залежності від виявленого руху з більшою/меншою частотою кадрів або більшою/меншою роздільною здатністю, щоб заощадити місце для зберігання. Це допомагає зменшити споживання пам'яті на 60–80% порівняно з безперервним записом.

Визначення загрозливих подій: корисне для ідентифікації будь-якого пропуску в інцидентах безпеки, настороженості та їх припиненні; наприклад, розпізнавання номерного знаку, порушення периметра, виявлення покинутих об'єктів та підрахунок людей, тощо [1].

6. Відображення відеоспостереження

Відео, зняті системою відеоспостереження, врешті переглядаються людьми і зазвичай використовуються для розслідувань. Відео можна переглядати 3-ма різними способами:

Місцевий: він переглядається безпосередньо з цифрового відеомагнітофона.

Віддалений: він переглядається на стандартних віддалених ПК для перегляду прямих і записаних відео через попередньо встановлене ПЗ.

Мобільний телефон: такий перегляд дозволяє миттєво під рукою перевірити зняте відео.

В цілому, конструкція сучасних технічних систем відеоспостереження, що заснована на інтернет-протоколі (IP), враховує в собі універсальність, адаптованість і цифрову безпеку. Дотримування вищерозглянутих шести пунктів вимог, дасть можливість побудувати надійну систему відеоспостереження, яка дозволить підвищити загальний рівень кіберзахисту на підприємстві чи в організації.

Список використаних джерел

1. Advance Intelligent Video Surveillance System (AIVSS): A Future Aspect [Електронний ресурс]. – Режим доступу до ресурсу: https://www.intechopen.com/books/intelligent-video-surveillance/advance-intelligent-video-surveillance-system-aivss-a-future-aspect

2. Kraus K. Security management process for video surveillance system. Proceedings in Advanced Intelligent Video Surveillance, Proceedings of IFIP Wireless Days, 6th IFIP Network Control Conference; November 2008

УДК 004.056.5

АНАЛІЗ МЕХАНІЗМІВ ЗАХИСТУ СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Койдан Ю. Г., здобувач вищої освіти гр. МКБп-201
Науковий керівник: **Петренко Т. А**, к.т.н., доцент
Національний університет «Чернігівська політехніка»

Вимоги що встановлюються НД ТЗІ 1.1-002-99 - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу жорстко регламентують схему (або модель) адміністрування механізмів захисту. Це повинна бути централізована схема, єдиним елементом якої виступає виділений суб'єкт, зокрема адміністратор. При цьому кінцевий користувач виключений у принципі зі схеми адміністрування механізмів захисту.

При реалізації концепції побудови системи захисту, регламентованої розглянутими вимогами, користувач не наділяється елементом довіри, оскільки він може вважатися потенційним зловмисником, що і відбувається на практиці.

Розглянемо концепцію, реалізовану в сучасних універсальних ОС. Тут "власником" файлового об'єкта, тобто особою, яка одержує право на завдання атрибутів доступу до файлового об'єкта, є особа, котра створює файловий об'єкт. Оскільки файлові об'єкти створюють кінцеві користувачі, вони й призначають атрибути доступу до створюваних ними файлових об'єктів. Інакше кажучи, в ОС реалізується розподілена схема призначення атрибутів доступу, де елементами схеми адміністрування є власне кінцеві користувачі [2].

У цій схемі користувач повинен наділятися практично такою ж довірою, як і адміністратор безпеки, при цьому нести поряд із ним відповідальність за забезпечення комп'ютерної безпеки.

Зазначимо, що централізована й розподілена схеми адміністрування - це дві діаметрально протилежні точки зору на захист, що вимагають різних підходів до побудови моделей і механізмів захисту. При цьому скільки-небудь гарантований захист інформації можна реалізувати тільки при прийнятті концепції повністю централізованої схеми адміністрування, що підтверджується відомими загрозами ОС.

Можливості моделей, методів і засобів захисту розглядатимемо стосовно реалізації саме концепції централізованого адміністрування, одним із елементів якої є розгляд користувача як потенційного зловмисника, здатного здійснити НСД до інформації, що захищається.

Захист ОС сімейства Unix і Windows у загальному випадку базується на трьох основних механізмах:

- ідентифікація й аутентифікація користувача при вході у систему;
- розмежування прав доступу до файлової системи, в основі якого лежить реалізація дискреційної моделі доступу;
- аудит, тобто реєстрація подій.

Передусім в ОС сімейства Unix, внаслідок реалізованої в ній концепції адміністрування (нецентралізована), неможливо забезпечити замкнутість (або цілісність) програмного середовища. Це пов'язано з неможливістю установки атрибута "виконання" на каталог. Тому при розмежуванні адміністратором доступу користувачів до каталогів користувач як "власник" створюваного ним файла може занести у свій каталог виконуваний файл і установити на файл атрибут "виконання", після чого запустити записану ним програму. Ця проблема безпосередньо пов'язана з реалізованою в ОС концепцією захисту інформації.[4]