УДК 004.056 **А.М. Котенко**

ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ ЗА РАХУНОК ВИКОРИСТАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Досліджені: існуючі технічні канали витоку інформації з об´єктів інформаційної діяльності, джерела інформації матеріально-речового каналу, причини витоку інформації матеріально-речовим каналом, приймачі інформації матеріально-речового каналу, склад систем відеоконтролю. Визначено функціональну можливість застосування систем відеоспостереження у якості охоронних систем. На підставі цього зроблено висновок про можливість використання систем відеоспостереження для запобігання витоку інформації матеріально-речовим каналом.

Ключові слова: відеоспостереження, канал витоку інформації, інформація з обмеженим доступом, семантична інформація, відео контроль, детектор руху, об'єкт інформаційної діяльності.

Вступ

Сучасні системи відеоспостереження представляють собою програмно-апаратний комплекс призначений для запису відеоінформації та передачі її до місця перегляду чи зберігання. Для цього використовують відеозапис на спеціалізовані пристрої, які можуть робити як у безперервному режимі, так і в режимі покадрового запису із заданим інтервалом часу між кадрами, з обов'язковим записом поточного часу й дати.

Основна частина

З багатьох джерел [1], [2], [3] та інших відомо, що напрямами використанням систем відеоспостереження є охорона та забезпечення безпеки різноманітних об'єктів, використання в інтелектуальних системах розпізнавання образів. Проте жодне з джерел не розглядає використання системи відеоспостереження як інструмент інформаційної безпеки для захисту інформації з обмеженим доступом (ІзОД). Метою даної статті є обґрунтування доцільності використання систем відеоспостереження для захисту ІзОД від витоку одним з технічних каналів витоку інформації, а саме матеріально-речовим каналом.

З теорії захисту інформації відомо, що існують наступні технічні канали витоку інформації: електричний, радіоканал, оптичний, акустичний, матеріально-речовий [1].

Розглянемо що являє собою матеріально-речовий канал витоку інформації. Особливість цього цього каналу викликана специфікою джерел і носіїв інформації у порівнянні з іншими каналами. Джерелами і носіями інформації в ньому є суб'єкти (люди) і матеріальні об'єкти (макро і мікрочастинки), які мають чіткі просторові межі локалізації, за винятком випромінювань радіоактивних речовин. Витік інформації в цих каналах супроводжується фізичним переміщенням людей та матеріальних тіл з інформацією за межами контрольованої зони. Для більш чіткого опису розглянутого каналу доцільно уточнити склад джерел і носіїв інформації.

Основними джерелами інформації матеріально-речового каналу витоку інформації є наступні:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, що ведуться в організації;
- відходи діловодства та видавничої діяльності в організації, в тому числі використана копіювальний папір, забраковані листи при оформленні документів і їх розмноженні;
- жорсткі диски ПЕОМ, оптичні диски, флеш-носії, що містять інформацію з обмеженим доступом ;
- бракована продукція і її елементи;

Перенесення інформації в цьому каналі за межі контрольованої зони можливо наступними суб'єктами і об'єктами:

- співробітниками організації;
- сторонніми особами (злочинцями);

- повітряними масами атмосфери;

- рідким середовищем.

Ці суб'єкти та об'єкти можуть переносити всі види інформації: семантичну, ознакову а також демаскуючі речовини.

Семантична інформація міститься в документах, схемах, кресленнях; інформація про ознакові та сигнальні демаскуючі ознаки у бракованих вузлах і деталях, в характеристиках радіоактивних випромінювань тощо; демаскуючі речовини - в газоподібних, рідких і твердих відходах виробництва. Структурна схема матеріально-речового каналу витоку інформації наведена на рис. 1.

Рис.1. Структура матеріально-речового каналу витоку інформації

Приймачі інформації цього каналу досить різноманітні. Це експерти зарубіжної розвідки або конкурента, прилади для фізичного та хімічного аналізу, засоби обчислювальної техніки, приймачі радіоактивних випромінювань і ін.

Втрати носіїв з цінною інформацією можливі при відсутності в організації чіткої системи обліку її носіїв або при навмисній крадіжці. Наприклад, зіпсований співробітником аркуш звіту, що містить інформацію з обмеженим доступом, може бути викинутий їм в кошик для паперу, з якого він буде прибиральницею перенесений в бак для сміття на території організації, а далі при перевантаженні бака або транспортуванні сміття на звалище лист може бути винесений вітром і піднято перехожим. Звичайно, ймовірність забезпечення випадкового контакту з цим листом зловмисника невелика, але якщо останній активно займається добуванням інформації, то область простору, в якому можливий контакт, значно звужується і ймовірність витоку підвищується.

Для підприємств хімічної, парфумерної, фармацевтичної та інших сфер розробки і виробництва продукції, технологічні процеси яких супроводжуються використанням або отриманням різних газоподібних або рідких речовин, можливе утворення каналів витоку інформації через викиди в атмосферу газоподібних або слив в водойми рідких демаскуючих речовин.

Подібні канали утворюються при появі можливості добування демаскуючих речовин в результаті взяття зловмисниками проб повітря, води, землі, снігу, пилу на листках чагарників і дерев, на траві і квітах в околицях організації.

Залежно від напряму і швидкості вітру демаскуючі речовини в газоподібному вигляді або у вигляді суспендованих твердих частинок можуть поширюватися на відстані в одиниці і десятки км, достатні для безпечного взяття проб зловмисниками. Аналогічне становище спостерігається і для рідких відходів.

Звичайно, концентрація демаскуючих речовин при віддаленні від джерела убуває, але при витоку їх протягом деякого часу концентрація може перевищувати допустимі значення за рахунок накопичення демаскуючих речовин в землі, рослинності, підводного флорі і фауні.

Виток інформації про радіоактивні речовини можливий в результаті виносу радіоактивних речовин співробітниками організації або реєстрації зловмисником їх випромінювань за допомогою відповідних приладів. Різноманіття розглянутих каналів витоку інформації надає зловмисникові великий вибір шляхів, способів і засобів добування інформації.

Таким чином, розглянувши що собою являє матеріально-речовий канал витоку інформації можна зробити висновок, що причинами витоку інформації з нього є наступні:

- крадіжка носіїв інформації;

- внутрішні канали витоку (через персонал);
- виробничі та технологічні відходи (папір з принтерів, виробничі відходи підприємств).
- погано прихована видова інформація про хід виробничого процесу на підприємстві;
- рекламна інформація, інформація з вистав про роботу підприємства.

Для матеріальних носіїв інформації з обмеженим доступом, які зберігаються на об’єктах інформаційної діяльності, причиною витоку буде крадіжка їх.

Для запобігання витоку інформації з обмеженим доступом матеріально-речовим каналом використовуються фізична, або технічна, у вигляді технічних систем охорони, складові [2].

Проте відомо, що сучасні системи відеоспостереження можуть виконувати функцію технічних систем охорони.

Взагалі система відеоспостереження представляє собою програмно-апаратний комплекс, призначений для запису відеоінформації та передачу її до місця перегляду або зберігання. Системи відеоспостереження умовно діляться на системи відеоконтролю та системи відеоохорони [4].

Системи відеоконтролю.

Найважливішою функцією телевізійних систем є можливість здійснення реєстрації та документування протягом тривалого часу подій які відбуваються на об'єктах, що охороняються. Для цього використовують відеозапис на спеціалізовані самописці, які можуть працювати як в безперервному режимі, так і в режимі покадрового запису з заданим інтервалом часу між кадрами, з обов'язковим записом поточного часу і дати. При відтворенні такого запису можливий багаторазовий контроль всієї обстановки в спостережувальних зонах, детальне вивчення тривожної ситуації в спостережувальних зонах з визначенням часу подій.Таким чином системи відеоконтролю - це системи відеоспостереження з відеозаписом які надають величезну допомогу службі безпеки в об'єктивній оцінці обстановки на об'єкті, ідентифікації об'єктів контролю, а також дозволяють оцінити якість роботи операторів.

Системи відеоохорони.

Як вже зазначалося вище, на об'єктах, що охороняються можуть бути створені зони відеоохорони, або більш строго - зони відеоохоронної сигналізації, в яких сигнал тривоги формується телевізійною системою при зміні зображення, яке надходить із телекамери відповідної зони. Для цієї мети в телевізійній системі використовуються одно і багатоканальні детектори руху. Призначення охоронного телебачення полягає в підвищенні рівня безпеки об'єкта, тобто в мінімізації можливих наслідків небажаних впливів на людей, на матеріальні цінності і на інформаційні ресурси. У загальному вигляді систему охоронного телебачення можна розглядати як замкнуту систему управління (рис. 2), яка складається з наступних елементів.

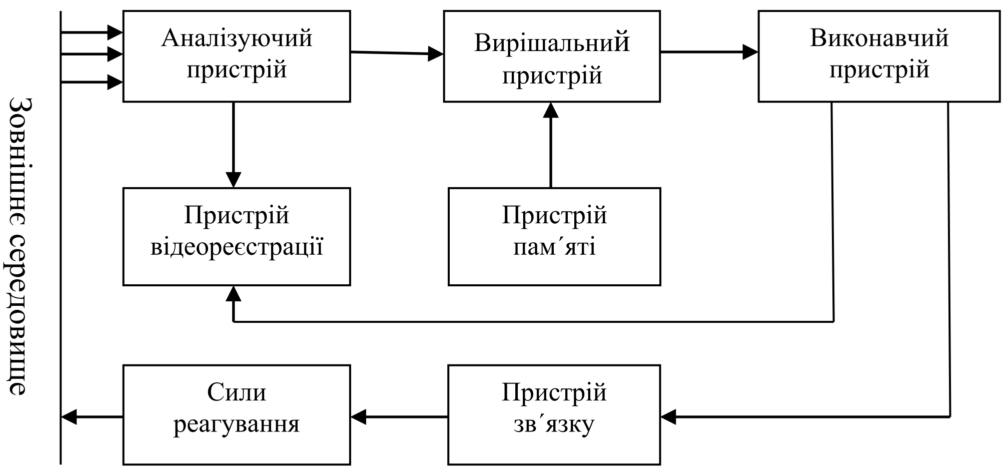

Рис.2. Система охоронного телебачення

Аналізуючий пристрій сприймає вплив із зовнішнього середовища і перетворює його до виду, прийнятного для прийняття рішення, тобто по суті є системою отримання сигналів телевізійних зображень. Якщо в якості вирішального пристрою виступає людина, то на виході аналізую чого пристрою (на екрані відеомонітора) повинно бути присутнім зображення контрольованої зони; в цьому випадку реалізується функція відеоспостереження. Якщо вирішальним пристроєм є електронний пристрій, зокрема, комп'ютер, то на виході аналізуючого пристрою повинен бути відповідний відеосигнал.

Пристрій пам'яті зберігає апріорну інформацію про можливу небезпеку. У пристрою пам'яті електронного приладу або комп'ютера можуть зберігатися порогові значення напруги або коду, відповідні тривожної ситуації, інформація про дозволені тимчасових «вікнах» і ін.

Вирішальний пристрій (на входи якого приходять сигнали з двох попередніх пристроїв) виробляє сигнал тривоги при виконанні встановлених умов - в цьому випадку реалізується функція відеоконтролю. В якості вирішального пристрою, як правило, використовується людина, проте останнім часом йому на допомогу все більше приходять технічні засоби. Вирішальний пристрій виробляє сигнал для виконавчого пристрою; з метою отримання більшої інформації воно може автоматично змінювати режим роботи аналізуючого пристрою на заздалегідь встановлений.

Виконавчий пристрій може автоматично впливати на зовнішнє середовище - по тривозі включати сирену, виконавчі механізми, і т.п., крім того, воно може включати пристрій відеореєстрації, а також керувати роботою пристрою зв'язку.

Пристрій зв'язку служить для передачі тривожної інформації силам реагування. Передача інформації може здійснюватися за допомогою локальних комп'ютерних мереж, Інтернету, електронної пошти, телефонних мереж, SMS-повідомлень тощо.

Сили реагування безпосередньо впливають на негативні явища зовнішнього середовища з метою мінімізації втрат зони, що охороняється. Функціонування сил реагування неодмінно має враховуватися в роботі

Перевага охоронного телебачення в порівнянні з іншими охоронними системами полягає в його високій інформативності (90% всієї інформації про навколишній світ людина отримує завдяки органам зору). Перевірити достовірність функціонування систем безпеки, переконатися в реальності тривоги, виробленої сигналізацією (охоронної, пожежної, периметрової та. ін.) можна не тільки відвідуванням людиною місця події, а й дистанційно - за допомогою охоронного телебачення. Ще важливіше запобігти подіям, виявивши небезпечний рух на підступах до зони, що охороняється, розшифрувавши можливу загрозу з екрану відеомонітора, що особливо актуально для віддалених об'єктів. І з цим охоронне телебачення також успішно справляється.

Як відзначалося системи відеоохоронні прізначені для реагування та видачу сигналу тривоги при ознака руху людини-порушника в полі її спостереження. Це можливо за рахунок використання детекторів руху в системі.

Функцією детектору руху є пошук реального руху у зоні спостереження об´єкту та активізацію тривоги у разі його виявлення. Детектор руху використовується для моніторингу ділянок, де не дозволено або не передбачається переміщення людей. Якщо рух виявляється, то найбільш імовірно, що він був викликаний чиїмось вторгненням. Природно, що для ефективної роботи системи охоронного телебачення детектори руху повинні викликати мінімум помилкових тривог внаслідок зміни освітленості, вібрації відеокамери, випадкових відображень світла в зоні спостереження і т.п. Детектори руху класифікуються наступним чином:

- аналогові або цифрові;
- одноканальні або багатоканальні (з паралельною обробкою кожного відеосигналу);
- з апаратною або програмною реалізацією.

Аналогові детектори руху мають досить прості функції, що визначають їх економічну ефективність. Такий прилад зазвичай має один наскрізний відеопрохід; прилад дозволяє довільним чином встановлювати на екрані відеомонітора розташування, наприклад, чотирьох маркерів (у вигляді напівпрозорих прямокутників), в яких контролюється зміна зображення, причому чутливість спрацьовування детектора руху може регулюватися. Наприклад, один з маркерів може бути встановлений по екрану в те місце, де розташовується двері - при виявленні зміни в сигналі (викликаного, відкриванням дверей) звучить зумер, і спрацьовують контакти реле. Для підвищення секретності роботи пристрою відображення маркерів на екрані відеомонітора може бути відключено. Подібні детектори зручно використовувати в місцях з постійним освітленням (здебільшого в приміщеннях).

Цифрові детектори руху дозволяють здійснювати виявлення тривоги з досить високим ступенем достовірності за рахунок диференціальної, а не інтегральної (як в аналогових приладах) оцінки параметрів відеосигналів.

Відображення тривожної ситуації супроводжується кольоровим забарвленням областей, в яких виявлено рух.

Програмування цифрових детекторів руху здійснюється вибором в меню приладу спеціальної крапкової сітки (наприклад 16x16), що накладається на зображення, з подальшим указанням активних зон, чутливості та ін. Подібний метод дозволяє досить гнучко програмувати охоронні зони (наприклад, можна розмістити активні зони вздовж зображення забору, організовуючи таким чином охорону периметра).

У зв'язку з розвитком комп'ютерних систем охоронного телебачення з'явилися детектори руху з програмною реалізацією; можливості таких детекторів руху набагато ширше в порівнянні з описаними вище приладами з апаратною реалізацією. В першу чергу це відноситься до кількості контрольованих зон (яких може бути більше 1500). Крім того, детектори руху дозволяють вирішити проблеми, які приніс з собою прогрес в області цифрових систем охоронного телебачення, а саме:

- протиріччя між бажанням записувати зображення з максимальною швидкістю при максимальній роздільній здатності і обмеженістю дискового простору комп'ютера;
- необхідність оперативного пошуку необхідного фрагмента відеозапису в великих архівах.

Не менш перспективним є активне використання детекторів руху в периметрових охоронних системах.

Висновок

Таким чином можна зробити висновок, що використання функції детектор руху в системах відеоспостереження дозволяє використовувати їх для виконання функцій притаманних технічним системам охорони. З цього слідує висновок, що системи відеоспостереження слід використовувати на об’єктах інформаційної діяльності для запобігання витоку ІзОД.

Література

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. – К.: , 2010. –465 с.

2. Торокін А.О., Інженерно-технічний захист інформації: навч. Посібник для студентів які навчаються по спеціальностям у галузі інформаційної безпеки. – М.: Геліос АРВ, 2005. – 906 с.

3. Хорев А.А. Способы и средства зашиты информации. - М.: МО РФ, 2000. - 316 с.

4. Гедзберг Ю. М. Охоронне телебачення. - М.: Горячая линия-Телеком, 2005. -312 с.

Надійшла 17.02.2017 р. Рецензент: д.т.н., проф. Хорошко В.О.