УДК 004.056

**А.М. Котенко**

# ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗА РАХУНОК ВИКОРИСТАННЯ ТЕХНІЧНИХ СИСТЕМ ОХОРОНИ

Досліджені: властивості інформації які впливають на її захищеність, причини порушення конфіденційності інформації на об’єктах інформаційної діяльності, загальне призначення технічної системи охорони, склад технічної системи охорони. Визначено функціональну можливість використання технічних систем охорони на об’єктах інформаційної діяльності. На підставі цього зроблено висновок про можливість використання технічних систем охорони для забезпечення конфіденційності інформації.

*Ключові слова:* технічна система охорони, сповіщувач, об’єкт інформаційної діяльності, конфіденційність інформації, критерії безпеки інформації, матеріально-речовий канал витоку інформації..

**Вступ.**

Сучасному світу характерна така тенденція як постійне підвищення ролі інформації. З підвищенням значущості та цінності інформації відповідно зростає важливість її захисту. Захищеність інформації характеризується певними ії властивостями, а саме конфіденційність, цілісність та доступність [1]. За визначенням конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення, цілісність – властивість інформації бути захищеною від несанкціонованої модифікації або знищення, доступність – властивість інформації бути захищеною від несанкціонованого блокування. Зважаючи на це забезпечення захищеності інформації є актуальною задачею. В межах даної статті розглядається забезпечення конфіденційності інформації.

**Основна частина.**

Загроза інформації - сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення конфіденційності, доступності та (або) цілісності інформації.

Якщо говорити про загрози інформаційно-технічного характеру, можна виділити такі елементи як крадіжка інформації, шкідливе програмне забезпечення, хакерські атаки, СПАМ, недбалість співробітників, апаратні і програмні збої, фінансове шахрайство, крадіжка обладнання.

Згідно зі статистикою щодо цих загроз, можна навести такі дані (за результатами досліджень, проведених в Росії компанією InfoWath) [2]:

- крадіжа інформації – 64%;
- шкідливе програмне забезпечення – 60%;
- хакерские атаки – 48%;
- спам – 45%;
- халатность сотрудников – 43%;
- недбалість співробітників - 43%;
- апаратні та програмні збої - 21%;
- крадіжка обладнання - 6%;
- фінансове шахрайство - 5%.

Як видно, з наведених даних, найбільш поширені крадіжка інформації та шкідливе програмне забезпечення. В даний час широкий розвиток отримали такі загрози інформаційної безпеки, як розкрадання баз даних, зростання інсайдерських загроз, застосування інформаційного впливу на різні інформаційні системи, зріс збиток що наноситься зловмисником.

Серед внутрішніх загроз безпеки інформації виділяють порушення конфіденційності інформації, спотворення, втрата інформації, збої в роботі обладнання

та інформаційних систем, крадіжка обладнання. І знову ж таки, спираючись на статистику, найбільше поширення мають порушення конфіденційності і спотворення. Так чи інакше, витік інформації відбувається по каналам витоку. Більшу частину в даному аспекті являє, так званий «людський фактор». Тобто співробітники організації, що не дивно, тому що хто, як не вони мають досить повноважень і можливостей для заволодіння інформацією.

Але зовсім не обов'язково викрадати інформацію з метою, наприклад, подальшого продажу. Якщо співробітнику захочеться зіпсувати репутацію компанії, або нанести будь-якої шкоди в силу якихось обставин (зниження за посадою, скорочення, розбіжності з керівництвом і т.д.), в повніше досить спотворити інформацію представляє цінність для організації, в наслідок чого, дана інформація може втратити свою актуальність і цінність, або ж виявиться просто недостовірної, що не справжньої, що може обернутися, наприклад, обдуреними клієнтами, партнерами. На щастя, таких співробітників не так багато.

Найбільш небезпечним є ненавмисні дії персоналу. Прикладом може бути, вже буденна річ для сучасної людини - «флешка», або USB накопичувач на основі Flash-memory. Нерідко, співробітники організації використовують «флешки» в роботі. Або з найкращих спонукань, людина, може взяти деяку інформацію додому, для того щоб попрацювати над нею (наприклад, підготовка будь-якої звітності чи інших документів). В даному випадку великий відсоток витоку інформації через втрату самого носія - «флешки», в силу її габаритних характеристик.

Обробка інформації з обмеженим доступом здійснюється в спеціалізованих приміщеннях – об’єктах інформаційної діяльності. Отже загрозою витоку інформації, що зберігається на матеріальних носіях, з об’єкту інформаційної діяльності є крадіжка цього матеріального носія. В наслідок цього інформація, що зберігається на цьому матеріальному носію, несанкціоновано стає відомою особам які не мають до неї доступу. Тобто має випадок порушення конфіденційності інформації.

З багатьох джерел [3], [4] та інших відомо, що технічні системи охорони, (ТСО) встановлені на об'єктах охорони, повинні в комплексі з силами фізичної охорони і системою інженерних споруджень задовольняти сучасним (виходячи з криміногенної обстановки) вимогам по охороні об'єктів від устремлінь потенційного порушника. Проте жодне з джерел не розглядає використання технічних систем охорони як інструменту інформаційної безпеки для забезпечення конфіденційності інформації з обмеженим доступом. Метою даної статті є обґрунтування можливості використання технічних систем охорони для забезпечення конфіденційності інформації.

В загальному випадку ТСО складаються з наступних елементів [4]:

сповіщувачі (засоби виявлення) – чутливі елементи ТСО які реагують на тривожні події (проникнення, або спроба проникнення об’єкт), і характеристики яких визначають основні характеристики всієї ТСО:

прилад приймально-контрольний охоронний (ППКО) – пристрій, який отримує сигнал тривоги від сповіщувачів та здійснює управління по заданому алгоритму виконавчими пристроями (у найпростішому випадку вмикання та вимикання сповіщувачів, фіксація сигналів тривоги, у більш складних розгалужених системах сигналізації контроль та управління здійснюється за допомогою комп’ютерів);

виконавчі пристрої – агрегати, які забезпечують виконання заданого алгоритму дій системи у відповідь на те чи інше тривожне повідомлення (сигнал оповіщення (звуковий, світловий), включення механизмів блокування об’єктів, автодозвон по заданим номерам телефонів і т. і.);

шлейф охоронний – електрична мережа, яка з’єднує електричні ланцюги сповіщувачів, допоміжні елементи (діоди, резістори і т.і.), коробки та ППКО та призначена для передачі сповіщень про проникнення, або спроби проникнення, а у деяких випадках і для подачі електроживлення на сповіщувачі.

Очевидно, при своєму русі людина-порушник залишає безліч різноманітних слідів свого руху і/або перебування, які можуть бути зафіксовані (а при необхідності зміряні) різними приладами. Насправді, людина володіє цілком певними (кажучи в термінах математики, розташованими в цілком певних областях існування) параметрами, як то: геометричними розмірами, масою, температурою тіла, запахом, електричними, біомеханічними і біодинамічними характеристиками, швидкостями руху, частотою кроку і ін.

При своєму русі він порушує звукові і ультразвукові коливання в атмосфері і навколишніх предметах, а також сейсмічні коливання в ґрунті і будівельних конструкцій. В процесі виконання тих або інших дій чоловік надає безпосередню силову дію на предмети, що цікавлять його, а також динамічну дію на поля електромагнітної і акустичної енергії, викликаючи порушення їх структури в просторі.

Рух людини супроводжується генерацією наднизькочастотних електричних полів, що виникають внаслідок перенесення індукованого в результаті тертя взуття об поверхню підлоги і взаємного тертя елементів тіла і одягу електростатичного заряду.

Крім того відомо, що в процесі фізичної діяльності чоловік випромінює електромагнітні сигнали в дуже широкому спектрі частот, а органи дихання і кровообігу генерують акустичні коливання. Потові залози людини виділяють в навколишню атмосферу продукти, у складі яких налічуються десятки хімічних речовин, деякі з яких є характерними тільки для людини.

В процесі проникнення в приміщення порушник відкриває двері, вікна, кватирки; іноді вимушений вирізувати і/або вибивати стекла, або пробляти отвори і проломи в стелях, підлозі або стінах. Усередині приміщення він пересуває предмети, обстановку, намагається розкрити металеві шафи або сейфи, фотографувати документи або вироби. Для виконання цих дій він може мати з собою фотоапаратуру, різний інструмент, а також зброю або вибухові речовини. Вказані чинники володіють самостійними інформативними характеристиками, що виявляють присутність (або сліди перебування) людини в приміщенні, що охороняється, одночасно збільшуючи об'єм інформації про нього.

Так, зброя, що є у порушника, або інструмент володіють певними фізичними параметрами і їх наявність може привести до зміни напруженості магнітного поля, частоти опромінюючого сигналу НВЧ. Застосування механічного інструменту для відкриття дверей і металевих шаф, створення проломів і отворів в стінах і підлогах приміщень супроводиться збудженням характерних коливань (вібрацій) в твердих тілах і акустичних хвиль в повітряному середовищі приміщення.

При використанні газового пальника має місце теплове випромінювання полум'я, змінюється температура об'єкту на який діє порушник, з'являється специфічний запах горючої суміші, який, як і у разі застосування вибухових речовин, приводить до зміни хімічного складу повітря.

Таким чином, поява порушника в приміщенні, що охороняється, а в даному випадку об’єкті інформаційної діяльності, може бути виявлена по великому числу фізикохімічних явищ. Це виявлення здійснюється за допомогою технічних засобів (сповіщувачів ТСО), в основу побудови яких покладені самі різні принципи реєстрації змін стану середовища. Для досягнення поставленої в статті мети розглянемо їх докладніше.

Найбільш поширені на практиці оптико-електронні засоби виявлення [5]. Оптико-електронні, більш відомі як інфрачервоні сповіщувачі руху, є пристроями, які найчастіше використовуються для виявлення руху людини-порушника в контрольованій зоні. Ефективність виявлення проникнення в зону, що охороняється, визначається тим, що інфрачервоні сповіщувачі дозволяють контролювати весь об’єм, або периметр приміщення. Тим самим вирішується задача реєстрації вторгнення практично при будь-якому шляху проникнення: через вікна, двері, проломи підлоги,

стелі, стіни, периметр об'єкту. Блокування першого рубежу охорони дозволяє в більшості випадків отримати ранній сигнал тривоги і мати більше часу на відповідну реакцію. Контроль об’єму, або периметру обєкту – це не єдина задача, яку розв'язують інфрачервоні сповіщувачі. Можна також ефективно контролювати вузьку смугу (наприклад, коридор) чи формувати вертикальну зону виявлення уздовж стін з вікнами чи дверима.

Для інфрачервоного сповіщувача як і для будь-якого іншого пристрою виявлення, необхідна деяка ознака (зміна яких-небудь фізичних характеристик чи параметрів об'єкта), що дозволяє прийняти рішення про рух порушника на об'єкті. У даному випадку такою ознакою є зміна інфрачервоного випромінювання в контрольованій зоні.

Інфрачервоні сповіщувачі бувають пасивні та активні. Активні формують інфрачервоний луч уздовж периметра об’єкту і видають сигнал тривоги при перетинанні порушником цього луча. Пасивний інфрачервоний сповіщувач реєструє зміну інфрачервоного випромінювання з появою на об'єкті порушника, тобто реєструє інфрачервоне випромінення людського тіла.

Акустичний сповіщувач розбиття скла призначений для реєстрації акустичних коливань, що виникають при руйнуванні скла об’єкту інформаційної діяльності. За допомогою одного сповіщувача можливо контролювати декілька вікон об’єкту. Відомо [ ], що при руйнуванні скла виникають акустичні коливання різних частот. У перший момент при ударі по склу воно деформується. Ця деформація, тобто вигін скла, викликає появу акустичних коливань низьких частот. Коли величина деформації досягає визначеного розміру, відбувається механічне руйнування скла. Воно супроводжується акустичними коливаннями високих частот. У такий спосіб для виявлення факту розбиття скла потрібно реєструвати звукові коливання визначеного спектрального складу і звукові коливання, які з’являються один за одним в деякому часовому інтервалі. Дану задачу і вирішують акустичні сповіщувачі розбиття скла.

Магнітоконтактний сповіщувач призначенням якого є фіксація моменту відкривання дверей, вікон або аналогічних конструктивних елементів об’єкту інформаційної діяльності порушником інформаційної безпеки. Магнітоконтактний сповіщувач містить у собі два основних елементи. Перший елемент – це геркон (рис.1), що складається з герметичної колби 1, у якій знаходяться пластини 2 з контактами, які мають малий опір. До пластин під’єднані провідники 3, що забезпечують підключення сповіщувача. Під впливом магнітного поля від розташованого поруч магніту 4 відбувається замикання чи розмикання контактів. У більшості випадків під впливом магнітного поля контакти нормально замкнуті. При знятті магнітного поля під дією пружних сил відбувається розмикання.

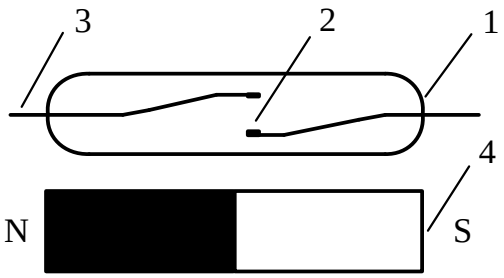


Рисунок 1. Основні елементи магнітоконтактного сповіщувача

Контакти, які підключаються в шлейф, розташовуються на нерухомій, а магніт – на рухомій частині конструкції, яка блокується.

Сповіщувачі ємнісні призначені для охорони сейфів, металевих шаф. Видають сигнал тривоги при приближенні людини-порушника до об’єкту, що охороняється. Фізичний

принцип дії засновано на виміру електричної ємності між об'єктом, що охороняється та підлогою. При наближенні людини до об'єкту ємність змінюється і видається сигнал тривожного сповіщення.

Вібраційні сповіщувачі призначені для виявлення руйнування будівельних споруд (стіни, підлога, металеві сейфи, шафи) порушником. В основі принципу дії лежить п'єзоелектричний ефект (зміна електричного сигнала при вібрації пєзоелементу). Електричний сигнал, що виникає при вібрації п'єзоелементу оброблюється схемою за спеціальним алгоритмом для селекції завад.

**Висновок.**

Таким чином усі вище перераховані засоби виявлення ТСО дозволяють виявити людину-порушника на об'єкті інформаційної діяльності та прийняти заходи щодо його нейтралізації. У свою чергу це означає, що конфіденційність інформації, яка знаходиться на цьому об'єкті інформаційної діяльності буде забезпечена.

**Список використаних джерел:**

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

2. [Електронний ресурс] // Режим доступу: (www.dehack.ru)

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

4. 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.

5. Синилов Вячеслав Григорьевич. Системы охранной, пожарной и охранно-пожарной сигнализации: Учебник – М.: Издательство: «Академия» 2006 г. – 512 с.

Надійшла: 20.01.2018 Рецензент: к.т.н. Курченко О.А.