МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 004.725.5

До захисту допущено
Завідуючий кафедрою СІКЗ
кандидат технічних наук,
_____Г.В. Шуклін
«____» _____2022 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ОБ’ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗАСТОСУВАННЯМ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ**

Студент групи СЗДМ 61 Калініченко Олександр Генадійович _____

Науковий керівник: к.т.н**.** доцент Котенко Андрій Миколайович _____

Нормоконтроль: Гребенніков Асаді Болдхоягович _____

Київ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Шуклін Г.В.
. «_____»_____ 2022 р.

ЗАВДАННЯ

на атестаційну роботу магістра

Студенту Калініченку Олександру Генадійовичу

1. Тема роботи: «Підвищення ефективності захисту об’єкту інформаційної діяльності застосуванням інтегрованої системи безпеки», затверджена наказом по університету від « » 2021 р. №
2. Термін здачі студентом оформленої роботи « » січня 2022 р.
3. Об’єкт дослідження: Процес захисту інформації на об’єкті інформаційної діяльності
4. Предмет дослідження: Інтегрована система безпеки
5. Мета роботи: Підвищити ефективність захисту інформації на об’єкті інформаційної діяльності.
6. Перелік питань, які мають бути розроблені:
1. Проаналізувати існуючі загрози інформації на об’єктах інформаційної діяльності.
2. Проаналізувати існуючі системи безпеки об’єктів інформаційної діяльності.
3. Підвищити ефективність захисту об’єкту інформаційної діяльності застосуванням інтегрованої системи безпеки.
7. Перелік публікацій

8. Перелік ілюстративного матеріалу
1. Презентація виконана на 14 слайдах для подання за допомогою оверхедів (світлопроекторів) та комп’ютерних засобів.

Дата видачі завдання «____» _____ р.

Науковий керівник: Котенко Андрій Миколайович _____
Завдання прийняв до виконання: Калініченко Олександр Генадійович _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 10.09.21р.	
2	Обґрунтування актуальності теми роботи	до 07.10.21р.	
3	Написання першого розділу роботи	до 18.10.21р.	
4	Написання другого розділу роботи	до 20.11.21р.	
5	Написання третього розділу роботи	до 26.11.18р.	
6	Написання четвертого та п’ятого розділу	до 28.11.21р.	
7	Написання висновків по роботі	до 30.11.21р.	
8	Підготовка демонстраційних матеріалів	до 23.12.21р.	
9	Підготовка доповіді	до 10.01.22р.	
10	Захист у ДЕК	01.22р.	

Студент групи СЗДМ-61 Калініченко Олександр Генадійович _____
(підпис)

Науковий керівник: к.т.н., доцент Котенко Андрій Миколайович _____
(підпис)

Нормоконтроль: Гребенніков Асаді Болдхоягович _____
(підпис)

РЕФЕРАТ

Дипломна робота містить: 71 сторінку, 10 рисунків, 3 таблиці, 17 джерел.

Об'єкт дослідження – процес захисту об'єкту інформаційної діяльності.

Предмет дослідження – інтегрована система безпеки.

Мета роботи – підвищити ефективність захисту об'єкту інформаційної діяльності.

Методи дослідження – теорія кіл, системний аналіз, чисельні методи.

Робота присвячена розробці рекомендацій по підвищенню ефективності захисту інформації на об'єкті інформаційної діяльності за рахунок застосування інтегрованої системи безпеки.

Проаналізовано загрози інформації на ОІД. Зроблено огляд існуючих систем безпеки ОІД.

На підставі проведених досліджень розроблені рекомендації по підвищенню ефективності захисту інформації на ОІД.

Галузь використання – інформаційна безпека.

Ключові слова: інтегровані системи безпеки, об'єкт інформаційної діяльності, захист інформації, система відеоспостереження, технічна система охорони, система контролю та управління доступом.

ANNOTATION

Thesis contains: 71 pages, 10 figures, 3 tables, 17 sources.

The object of research is the process of protection of the object of information activity.

The subject of research is an integrated security system.

The purpose of the work is to increase the effectiveness of protection of the object of information activities.

Research methods - circuit theory, systems analysis, numerical methods.

The work is devoted to the development of recommendations for improving the effectiveness of information protection at the object of information activities through the use of an integrated security system.

The threats of information on OID are analyzed. An overview of existing OID security systems is made.

On the basis of the conducted researches recommendations on increase of efficiency of protection of the information on OID are developed.

Field of use - information security.

Keywords: integrated security systems, object of information activity, information protection, video surveillance system, technical security system, access control and management system.

ЗМІСТ

ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

ІСБ – інтегрована система безпеки

ІБ – інформаційна безпека

ІзОД – інформація з обмеженим доступом

ІЛЗ – інформаційна лінія зв'язку

НВЧ – надвисокі частоти

НСД – несанкціонований доступ

ОІД – об’єкт інформаційної діяльності

ПЗ – програмне забезпечення

ПВІО – пристрої введення ідентифікаційних ознак

ПК – пристрої керування

СВС – система відеоспостереження

СКУД – система контролю управління доступом

ТСО – технічна система охорони

ВСТУП

З найдавніших часів питання забезпечення безпеки життя людини у повсякденній діяльності було і залишається відкритим, фактори ризику різного роду впливів щороку поповнюються новими загрозами.

Виникнення загроз спонукало світ до створення «індустрії безпеки» - це малі або великі колективи різного роду фахівців, які в свою чергу розробляють засоби нападу і засоби захисту включаючи такі напрямки, як законодавство і способи ухилення від його виконання, засоби економічної розвідки, промислового шпигунства, електронної розвідки і захисту інформації, фізичного впливу на людину, будівлю і споруду, пожежної та охоронної сигналізації, відеоспостереження, систем контролю управління доступом та ін. Такі системи забезпечення безпеки можуть надавати послуги захисту як за допомогою однієї автономної системи (пожежна, охоронна сигналізація, відеоспостереження, система контролю управління доступом) так і створювати абсолютно новий етап в побудові системи безпеки – інтеграцію.

Інтегрована система безпеки – є спільне використання ресурсів підсистем (пожежної та охоронної сигналізації, відеоспостереження, систем контролю управління доступом та іншого), в результаті чого система як ціле набуває нових якісних властивостей, на відміну від автономної роботи підсистем.

Не дивлячись на те, що ринок пропонує широкий асортимент моносистем безпеки, які працюють окремо від інших складових, жодна з них не здатна на достатньому рівні забезпечити інформаційну безпеку ОІД. Тому більш ефективними є інтегровані системи безпеки, які складаються не тільки з підсистем, а й з власних каналів зв'язку, баз даних, алгоритмів роботи та програмного забезпечення.

Основні напрями визначаються наступними вимогами:

1. Зниження ролі людини в процесі забезпечення безпеки за рахунок підвищення інтелектуальності систем;

2. Зниження рівня помилкових спрацьовувань за рахунок більш тісного використання підсистем;

3. Вимога відкритості. Розробники ІСБ повинні забезпечити замовнику за допомогою відкритих протоколів можливості підключення систем і устаткування інших виробників і гнучкого настроювання ІСБ під свої потреби.

Оскільки сучасність вимагає більш удосконалених та ефективних засобів захисту інформації на ОІД, можна вважати, що тема магістерської роботи, яка присвячена питанням підвищення рівня захисту на ОІД за рахунок використання ІСБ, як високоефективного методу є актуальною науковою задачею.

Мета роботи – Підвищити ефективність захисту об’єкту інформаційної діяльності.

Об′єкт дослідження - процес захисту інформації на ОІД.

Предмет дослідження – інтегровані системи безпеки.

Для досягнення поставленої мети у роботі вирішені такі основні завдання**:**

- проаналізовано існуючі загрози інформації на об’єктах інформаційної діяльності;
- зроблено огляд існуючих систем безпеки об’єктів інформаційної діяльності;
- підвищено ефективність захисту об’єкту інформаційної діяльності застосуванням інтегрованої системи безпеки.

Наукова новизна результатів

Вперше розроблена методика оцінки ефективності інтегрованої системи безпеки з урахуванням за критерієм ефективність-вартість.

Галузь застосування: інформаційна безпека

РОЗДІЛ 1
ІНФОРМАЦІЙНА БЕЗПЕКА ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1. Види інформації за режимом доступу

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

За своїм змістом інформація поділяється на такі види [1]:

–інформація про фізичну особу;

–інформація довідково-енциклопедичного характеру;

–інформація про стан довкілля (екологічна інформація);

–інформація про товар (роботу, послугу);

–науково-технічна інформація;

–податкова інформація;

–правова інформація;

–статистична інформація;

–соціологічна інформація;

– інші види інформації.

Втім для практичного використання більш важливою є класифікація інформації за порядком доступу до неї. У відповідності до цього інформація поділяється на: відкриту та з обмеженим доступом [2] (Рис. 1.1).

Відкрита - будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Основними ознаками відкритої інформації є те, що доступ до неї надається будь-яким зацікавленим особам, а будь-яке обмеження права на одержання відкритої інформації забороняється.

Способи забезпечення доступу до відкритої інформації:

– систематична публікація її в офіційних друкованих виданнях (бюлетенях, збірниках);

– поширення її засобами масової комунікації;

– безпосереднє надання її зацікавленим громадянам, державним органам та юридичним особам.

Рис.1.1. Види інформації за режимом доступу

ІзОД - інформація, що становить державну або іншу передбачену законом таємницю, а також конфіденційна інформація, що є власністю держави або вимога щодо захисту якої встановлена законом [2].

Таємна інформація - вид інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані, у порядку встановленому Законом, державною таємницею і підлягають охороні державою. Інформація, що становить державну таємницю, в свою чергу, поділяється на категорії відповідно до Закону України “Про державну таємницю” [2].

Конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та

організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ - надано статус конфіденційної [2].

У відповідності до Закону "Про захист інформації в інформаційно-телекомунікаційних системах" захисту в системі підлягає:

- відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі - конфіденційна інформація);

- інформація, що становить державну або іншу передбачену законом таємницю (таємна інформація).

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Усі дії, що пов’язані з обробкою інформації з обмеженим доступом виконуються на об’єктах інформаційної діяльності. Відповідно до визначення об'єкт інформаційної діяльності — будівлі, приміщення, транспортні засоби чи

інші інженерно-технічні споруди функціональне призначення яких передбачає обіг інформації з обмеженим доступом [2]. Інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Обробка ІзОД на об’єктах інформаційної діяльності дозволяє забезпечити безпеку інформації, яка заключається в збереженні наступних критеріїв інформаційної безпеки [3]**:**

- цілісність - властивість інформації бути захищеною від несанкціонованого знищення, модифікації.
- конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення.
- доступність - властивість інформації бути захищеною від несанкціонованого блокування.

З метою задоволення інформаційних потреб, органи державної влади, місцевого й регіонального самоврядування створюють інформаційні служби, системи, мережі, бази й банки даних. Порядок їх формування, структура, права і обов'язки визначаються Кабінетом Міністрів України або іншими органами державної влади, а також органами місцевого й регіонального самоврядування.

Основними видами інформаційної діяльності є одержання, використання, поширення й зберігання інформації [4].

Одержання інформації – це придбання й накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою.

Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб і держави. Поширення інформації - це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації.

Зберігання інформації – це забезпечення належного стану інформації її матеріальних носіїв.

Одержання, використання, поширення і зберігання документованої або публічно оголошуваної інформації здійснюється у порядку, передбаченому цим Законом та іншими законодавчими актами в галузі інформації. Крім того, можна виділити діяльність, пов’язану з інформаційним забезпеченням –одержання, оцінки, зберігання та переробки даних, створена з метою вироблення управлінських рішень. Це стосується різних видів діяльності, наприклад виробничої і збутової, сервісного обслуговування, включаючи підвищення технологічності виробництва, якості вироблюваної продукції, зниження її собівартості, рекламу, інформацію про асортимент продукції, ціни, форми організації сервісу тощо.

Будь який вид інформаційної діяльності (включно інформаційний бізнес) не може здійснюватись в умовах ізоляції. Його учасники (контрагенти), тобто продавець чи покупець, роботодавець чи найманий робітник функціонують у певному середовищі, яке визначає їх позиції і називається середовищем підприємницької діяльності (підприємництва) [5].

1.2. Загрози інформації на об’єктах інформаційної діяльності

Захист інформації є одним із найважливіших у загальному комплексі заходів технічного захисту інформації (ТЗІ). Несанкціоноване ознайомлення із інформацією з метою її подальшого використання є можливим шляхом перехоплення її зловмисниками [3].

Для нелегального знімання інформації використовуються різні технічні засоби. Інформація з об'єкта надходить зловмисникові по різним фізичним каналам.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення повідомлення, технічні канали витоку можна розділити на [6]:

- радіоканал;
- електричний;

- акустичний;
- оптичний;
- матеріально-речовий.

Аналіз фізичної природи численних випромінювачів показує, що:

- джерелами небезпечного сигналу є елементи, вузли і провідники технічних засобів забезпечення виробничої та трудової діяльності, а також радіо- і електронна апаратура;
- кожне джерело небезпечного сигналу за певних умов може утворити технічний канал витоку інформації;
- кожна електронна система, що містить в собі сукупність елементів, вузлів і провідників, володіє безліччю технічних каналів витоку інформації.

Радіоканали витоку інформації утворюються за рахунок [6], [7]:

- мікрофонного ефекту;
- магнітного поля;
- паразитної генерації;
- по ланцюгах живлення;
- по ланцюгам заземлення;
- за рахунок взаємного впливу;
- електромагнітного випромінювання;
- ВЧ нав'язування;
- із волоконно-оптичних систем зв'язку.

Структура радіоканалу витоку інформації в загальному випадку включає (рис. 1.2) джерело сигналу або передавач, середу поширення електричного струму або електромагнітної хвилі і приймач сигналу[6].

Рис. 1.2. Склад радіоканалу витоку інформації

У радіоканалах витоку інформації джерела сигналів можуть бути чотирьох видів:

- передавачі функціональних каналів зв'язку;
- джерела небезпечних сигналів;
- об'єкти, що відображають енергію радіочастоти;
- об'єкти, що випромінюють власні (теплові) радіохвилі.

Середовищем поширення радіоелектронного каналу витоку інформації є атмосфера, безповітряний простір і направляючі - електричні дроти різних типів і хвильоводи. Носій у вигляді електричного струму поширюється по дротах, а електромагнітне поле - в атмосфері, в безповітряному просторі або по направляючим - хвилєводам. У приймачі проводиться виділення (селекція) носія з цікавою одержувачу інформацією по частоті, посилення виділеного слабкого сигналу і зняття з нього інформації - демодуляція.

При перехопленні сигналів функціональних каналів зв'язку передавачі цих каналів є одночасно джерелами радіоканалів витоку інформації. У загальному випадку напрям поширення електромагнітної хвилі від передавача до санкціонованого одержувача і зловмисникові відрізняються. У функціональних каналах зв'язку максимум випромінювання енергії електромагнітної хвилі орієнтують в напрямку розташування приймача санкціонованого одержувача. Тому потужність джерела сигналів радіоканалу витоку інформації, як правило, істотно менше потужності випромінювання в функціональному каналі зв'язку.

Причини виникнення електричних каналів витоку інформації [6]:

- гальванічні зв'язки з'єднувальних ліній ТЗПІ (технічний засіб перетворення інформації) з лініями ДТЗС (допоміжні технічні засоби системи) і сторонніми провідниками;
- наведення побічних електричних випромінювань ТЗПІ на з'єднувальні ліній ДТЗС і сторонні провідники;
- наведення побічних електричних випромінювань ТЗПІ на ланцюзі електроживлення і заземлення ТЗПІ;

- «просочування» інформаційних сигналів у колі електроживлення і заземлення ТЗПІ.

Одним з видів технічних каналів витоку інформації, що виникають при роботі засобів і систем інформатизації (електронно-обчислювальна, телевізійна й інша техніка), є канали, що з'являються за рахунок побічних електромагнітних випромінювань і наведень. До найбільш поширених каналах витоку інформації внаслідок наведень відносяться канали, які утворюються в мережі електроживлення технічних засобів і систем.

Крім заземлюючих провідників, які слугують для безпосереднього з'єднання ТЗПІ з контуром заземлення, гальванічний зв'язок з землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносяться нульовий провід мережі електроживлення, екрани (металеві оболонки) з'єднувальних кабелів, металеві труби систем опалення та водопостачання, металева арматура залізобетонних конструкцій і т.д. Всі ці провідники разом з заземлювальним пристроєм утворюють розгалужену систему заземлення, на яку можуть наводитися інформаційні сигнали. Крім того, у грунті навколо заземлювального пристрою виникає електромагнітне поле, яке також є джерелом інформації.

Перехоплення інформаційних сигналів в лініях електроживлення і колах заземлення ТЗПІ можливий при гальванічному підключенні до них засоби розвідки ПЕВІН (побічні електромагнітні випромінювання і наведення).

При правильному проектуванні система заземлення виконує всі перераховані функції, сприяє поліпшенню умов електромагнітної сумісності радіоелектронних засобів. У той же час помилки, допущені при проектуванні заземлений, можуть створювати умови для витоку секретної інформації за межі контрольованої зони.

Одна з основних причин утворення каналів витоку інформації лініями заземлення пов'язана з тим, що перераховані типи заземлення рідко вдається виконати відокремленими. Поєднання декількох функцій однієї системою провідників і провідних поверхонь призводить до того, що по ним відбуваються

різні струми, в тому числі і небезпечні. У загальному випадку небезпечними потоками є зворотні струми для різних сигналів основних технічних засобів і систем (ОТЗС), а також струми, обумовлені наведеннями небезпечних сигналів на лінію заземлення. Причому найбільшу небезпеку представляють зворотні струми, так як вони можуть мати досить велику величину.

Витік інформації по ланцюгах заземлення може виникнути [6]:

- при наявності рознесених точок заземлення інформативних ланцюгів в разі утворення в різних точках системи заземлення різниці потенціалів і виникнення в результаті цього струмів в ланцюгах заземлення;
- при великому значенні опору заземлення;
- внаслідок недосконалості екранів, що приводить до асиметрії ліній відносно екрана і виникнення в ланцюзі між корпусом екрана та землею інформативних струмів.

Акустичні канали витоку інформації утворюються за рахунок [6], [7]:

- поширення акустичних коливань у вільному повітряному просторі;
- впливу звукових коливань на елементи і конструкції будівель;
- впливу звукових коливань на технічні засоби.

Механічні коливання стін, перекриттів, трубопроводів, що виникають в одному місці від впливу на них джерел звуку, передаються по будівельним конструкціям на значні відстані, майже не затухаючи, і випромінюються в повітря як чутний звук. Небезпека такого акустичного каналу витоку інформації за елементами будівлі полягає в великий і неконтрольованої дальності поширення звукових хвиль, перетворених в пружні поздовжні хвилі в стінах і перекриттях, що дозволяє прослуховувати розмови на значних відстанях.

Ще один канал витоку акустичної інформації утворюють системи повітряної вентиляції приміщень, різні витяжні системи та системи подачі чистого повітря. Можливість виникнення таких каналів визначаються конструктивними особливостями повітропроводів і акустичними характеристиками їх елементів: засувок, переходів, розподільників і ін.

Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їх перехоплення, акустичні канали витоку інформації також можна розділити на повітряні, вібраційні, електроакустичні, оптико-електронні та параметричні [7].

У повітряних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря, а для їх перехоплення використовуються мініатюрні високочутливі мікрофони і спеціальні спрямовані мікрофони.

Мікрофони об'єднуються або з'єднуються з портативними звукозаписуючими пристроями (диктофонами) або спеціальними мініатюрними передавачами [7].

Перехоплена інформація може передаватися по радіоканалу, оптичного каналу (в інфрачервоному діапазоні довжин хвиль), по мережі змінного струму, з'єднувальним лініях ДТЗС, стороннім провідникам (трубах водопостачання і каналізації, металоконструкцій і т.п.). Причому для передачі інформації по трубах і металоконструкцій можуть застосовуватися не тільки електромагнітні, а й механічні коливання.

У вібраційних (структурних) каналах витоку інформації середовищем поширення акустичних сигналів є конструкції будівель, споруд (стіни, стелі, підлоги), труби водопостачання, опалення, каналізації та інші тверді тіла. Для перехоплення акустичних коливань в цьому випадку використовуються контактні мікрофони (стетоскопи).

Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів в електричні. Перехоплення акустичних коливань здійснюється через ДТЗС, що володіють "мікрофонним ефектом" (перетворення акустичних мовних коливань повітряного середовища в електричні сигнали), а також шляхом "високочастотного нав'язування".

Оптико-електронний (лазерний) канал витоку інформації утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких відображаючих поверхонь (скла, вікон, картин, дзеркал і т.д.). Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється за амплітудою і фазою

(згідно із законом вібрації поверхні) і приймається приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація.

Візуально-оптичне спостереження є найбільш відомим, досить простим, широко поширеним і добре оснащеним найсучаснішими технічними засобами розвідки. Цей вид дій володіє:

- достовірністю і точністю видобутої інформації;
- високою оперативністю отримання інформації;
- доступністю реалізації;
- документальністю отриманих відомостей (фото, кіно, TV).

Ці особливості визначають небезпеку даного виду каналів витоку інформації.

Оптичні методи є одними з найстаріших методів отримання інформації.

До них відносяться:

- візуальні методи спостереження;
- фотозйомка;
- відеозйомка.

Ці методи дозволяють отримувати інформацію як в звичайних умовах, так і при мінімальній освітленості, в інфрачервоному спектрі і за допомогою термографії, а також в повній темряві. В даний час для збору інформації по візуально-оптичним каналам широко застосовують волоконні світловоди і ПЗЗ-мікросхеми. Сучасні системи фотозйомки і відеозйомки дозволяють здійснювати дистанційне керування. Розроблено системи, здатні проводити зйомку практично в абсолютній темряві, що дозволяють фотографувати через найменші отвори.

У практиці розвідки широко використовується отримання інформації з відходів виробничої та трудової діяльності [8]. Залежно від профілю роботи підприємства це можуть бути зіпсовані накладні, фрагменти складаються документів, чернетки листів, браковані заготовки деталей, панелей, кожухів та інших пристроїв для розроблюваних підприємством нових моделей різної техніки. Особливе місце серед такого роду джерел займають залишки бойової техніки і озброєння на випробувальних полігонах.

За своїм фізичним станом відходи виробництва можуть являти собою тверді маси, рідини і газоподібні речовини; по фізичній природі вони діляться на хімічні, біологічні, радіаційні, а по середовищу поширення на що містяться в землі, у воді і в повітрі.

Особливість матеріально-речового каналу, в порівнянні з іншими каналами, обумовлена специфікою джерел і носіїв видобувається по ньому інформації. Джерелами і носіями інформації в даному випадку є суб'єкти (люди) і матеріальні об'єкти (макро- і мікрочастинки), які мають чіткі просторові межі локалізації (за винятком випромінювань радіоактивних речовин). Витік інформації по матеріально-речовим каналах супроводжується фізичним переміщенням людей і матеріальних тіл з інформацією за межі об'єкта, що захищається.

Основними джерелами інформації матеріально-речового каналу витоку інформації є [7], [8]:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, які ведуться в організації;
- вийшли з ладу магнітні та інші носії інформації ПЕОМ, на яких під час експлуатації містилася інформація з обмеженим доступом;
- секретні бібліотеки;
- інші місця зберігання матеріальних носіїв ІзОД.

Перенесення інформації в матеріально-речовому каналі може здійснюватися такими суб'єктами та середовищами:

- співробітниками організації;
- повітряними атмосферними масами;
- рідкими середовищами.

Втрата носіїв цінної інформації можлива за відсутності в організації чіткої системи їх обліку. Наприклад, друкарка, зіпсувавши аркуш звіту, викидає його в кошик для сміття, з якої він переноситься прибиральницею в сміттєвий бак, що знаходиться на території організації. Потім при вантаженні або продовження транспортування сміття лист несеться вітром і потрапляє в руки випадкового

перехожого. Звичайно, ймовірність забезпечення випадкового ознайомлення зловмисника з вмістом цього листа невелика. Однак якщо зловмисник активно займається добуванням інформації, область простору, в якій можливий контакт, значно звужується, що призводить до підвищення ймовірності витоку інформації по матеріально-речовим каналам.

Витік інформації через матеріально-речові канали витоку інформації можливий через:

- розкрадання носіїв інформації;
- внутрішні канали витоку (через обслуговуючий персонал);
- виробничі та технологічні відходи (папір з принтерів, виробничі відходи підприємств);
- погано прихована видова інформація про хід виробничого процесу на підприємстві.

1.3. Причини виникнення загроз інформаційній безпеці

Глобальні фактори загроз інформаційній безпеці:

–недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації, розповсюдження інформації та нових інформаційних технологій;

–діяльність іноземних розвідувальних та спеціальних служб;

–діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави;

–злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:

–використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації;

–невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;

–відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій;

–недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;

–розвиток зарубіжних технічних засобів розвідки, та промислового шпигунства, що дозволяє одержати несанкціонований доступ до конфіденційної інформації, у тому числі такої що складає державну таємницю;

–зростання злочинності в інформаційній сфері;

–використання старих методів та засобів захисту національних інформаційних мереж, широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку;

–відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці

–перехоплення електронних випромінювань;

–застосування підслуховуючих пристроїв або закладок;

–дистанційне фотографування;

–розкрадання носіїв інформації та промислових відходів;

–копіювання носіїв інформації з подоланням заходів захисту;

–незаконне приєднання до апаратури та ліній зв'язку;

–упровадження та використання комп'ютерних вірусів і т. ін.[9].

Класифікація можливостей реалізації загроз, тобто атак, являє собою сукупність можливих варіантів дій джерела загроз певними методами реалізації з використанням уразливості, які приводять до реалізації цілей атаки.

Суб'єкти, дії яких можуть привести до порушення безпеки інформації можуть бути як зовнішні так і внутрішні (рис. 1.3).

Ґрунтуючись на результатах міжнародного й українського досвіду, дії суб'єктів можуть привести до ряду небажаних наслідків, серед яких стосовно до мережі, можна виділити наступні:

1. Крадіжка:

а) технічних засобів (вінчестерів, ноутбуків, системних блоків);

б) носіїв інформації (паперових, магнітних, оптичних й ін.);

в) інформації (читання й несанкціоноване копіювання);

г) засобів доступу (ключі, паролі, ключова документація й ін.).

2. Підміна (модифікація):

а) операційних систем;

б) систем керування базами даних;

в) прикладних програм;

г) інформації (даних), заперечення факту відправлення повідомлень;

д) паролів і правил доступу.

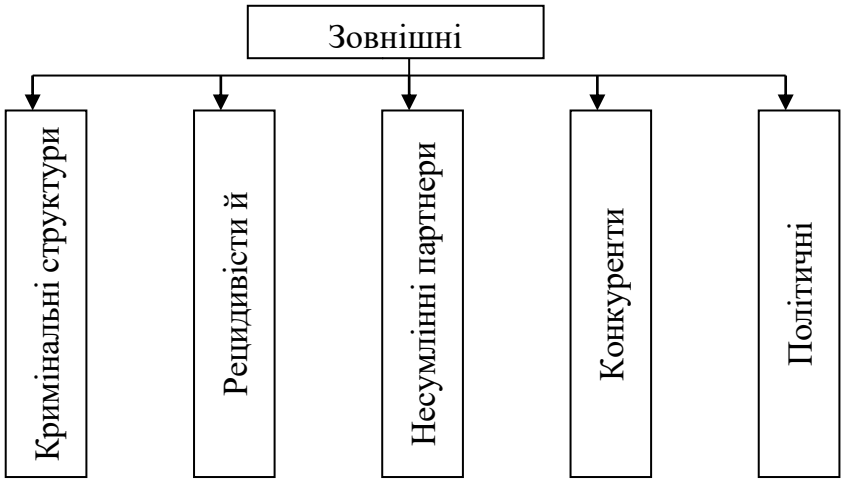

Рис. 1.3. Суб’єкти зовнішніх загроз.

3. Знищення (руйнування):

а) технічних засобів (вінчестерів, ноутбуків, системних блоків);

б) носіїв інформації (паперових, магнітних, оптичних й ін.);

в) програмного забезпечення ;

г) інформації (файлів, даних);

д) паролів і ключової інформації.

4. Порушення нормальної роботи (переривання):

а) швидкості обробки інформації;

б) пропускної здатності каналів зв'язку;

в) обсягів вільної оперативної пам'яті;

г) обсягів вільного дискового простору;

д) електроживлення технічних засобів;

5. Помилки:

а) при інсталяції програмного забезпечення, операційної системи;

б) при написанні прикладного програмного забезпечення;

в) при експлуатації програмного забезпечення;

г) при експлуатації технічних засобів.

6. Перехоплення інформації (несанкціоноване):

а) за рахунок передавання на комп’ютер від технічних засобів;

б) за рахунок наведень по лініях електроживлення;

в) за рахунок наведень по сторонніх провідниках;

г) по акустичному каналі від засобів виводу;

д) по акустичному каналі під час обговорення питань;

е) при підключенні до каналів передачі інформації;

ж) за рахунок порушення встановлених правил доступу (злом).

Можливо виділити три основні мотиви порушень: безвідповідальність, самоствердження, корисливий інтерес.

Усіх порушників можливо класифікувати в такий спосіб.

За рівнем знань про інформаційну систему:

- знає функціональні особливості інформаційної системи, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

- має високий рівень знань та досвід роботи з технічними засобами системи і їхнього обслуговування;

- має високий рівень знань у області програмування, проектування та експлуатації інформаційних систем;

- знає структуру, функції та механізм дії засобів захисту, їх сильні та слабкі сторони.

Усе викладене дозволяє звести у єдину таблицю всі загрози інформаційній безпеці та окремим її складовим, джерела загроз та порушників інформаційної безпеки.

Для побудови систем захисту необхідно не тільки мати чітке уявлення про можливі загрози та можливості їх реалізації, а й детально проаналізувати засоби і заходи захисту.

Висновок по розділу. Існують види інформації які відповідно до законодавства України підлягають захисту. Для класифікації шляхів витоку інформації існує поняття технічний канал витоку інформації. Виток інформації з обєкту інформаційної діяльності можливий через матеріально-речовий канал. Джерелом інформації у такому випадку є усі матеріальні носії інформації.

РОЗДІЛ 2

ІНТЕГРОВАНА СИСТЕМА БЕЗПЕКИ

2.1. Поняття про інтегровану систему безпеки

У теперішній час важко уявити виробництво, торговельний об'єкт, державну установу чи офіс необладнаною системою технічної безпеки. Система контролю та управління доступом (СКУД), охоронно-пожежна сигналізація (ОПС), відеоспостереження дуже часто використовуються на об'єктах різного типу та призначення.

Під час кваліфікованого підході до проектування та розумному вибору обладнання, кожен елемент підсистеми успішно виконує ті завдання, для яких він призначений.

Проте виникають ситуації, коли розрізнені системи не забезпечують потрібний рівень безпеки об'єкта.

Що робити, коли ми вибрали обладнання, запустили підсистеми, проте у нас невирішуються необхідні завдання:

- невідомо як приймати достовірні рішення у конкретній ситуації;
- збільшення швидкісті ухвалення рішень;
- збір всієї необхідної інформації для аналізу ситуації в одному місці;
- зниження впливу "людського фактора";
- забезпечення централізованого керування;
- підвищення відмовостійкості системи безпеки;
- забезпечення коректного спільного працювання обладнання різних брендів.

Усе це вирішує інтегрована система безпеки (рис. 2.1.).

Інтегрована система безпеки – поєднання систем безпеки різного призначення пов'язаних в єдине ціле. ІСБ – це більше ніж поєднання функціональних елементів, що входять до неї, це єдина система безпеки, що

забезпечує захист об'єкта на набагато вищому рівні [10]. Сучасні ІСБ це технічно складні комплекси з єдиною інформаційною платформою та централізованим керуванням.

При цьому до складу ІСБ входять, як правило, такі підсистеми [11]:

- охоронна сигналізація;
- пожежна сигналізація;
- система контролю та управління доступом;
- відеоспостереження та реєстрації;
- автоматичного оповіщення у випадку надзвичайної ситуації;
- захисту інформації;
- резервного освітлення та ін.

На даний час стандарти на інтегровані системи безпеки, знаходяться на етапі розробки.

Усі складові ІСБ зв'язані між собою апаратними та програмними засобами. ЗастІикористання двостороннього сприяє покращенню якісті зв'язку для передачі команд управління, обміну важливою інформацією. Окрім централізованого функціонування, кожна із складових ІСБ може функціонувати автономно, підтримуючи працездатність комплексу при виході з ладу окремих пристроїв.

Рис. 2.1. Приклад інтегрованої системи безпеки

По'єднання окремих підсистем, та управління ними за допомогою центрального процесора дозволяє:

- автоматизувати стандартні дії та реакцію на зовнішні події;

- зменшити до мінімуму вплив людського фактора на надійність;

- зробити можливою взаємодію апаратних засобів на рівнях із різним пріоритетом;

- спростити процес керування, забезпечивши розмежування доступу;

- зменшити витрати на апаратуру, що дублюється.

Застосування базових функціх ІСБ дозволить:

- обмежити доступ на об'єкт для співробітників, відвідувачів;

- поділити об'єкт на охоронні зони з реалізацією позонної постановки/зняття з охорони;

- забезпечити відеоконтроль, створити бази відеоархіву;

- управляти інженерними комунікаціями, приладами пожежогасіння, димовидалення;

- зберегти працездатність окремих підсистем ІСБ у випадку пошкодження однієї з них.

2.2. Функціональність інтегрованої системи безпеки

1. Прийняття вірного рішення у конкретній ситуації.

Щоб прийняти максимально обґрунтоване рішення, необхідна достовірна та вичерпна інформація щодо стану нашого об'єкта. ІСБ отримує дані від усіх своїх систем у єдиній точці. Керувальник ІСБ приймає рішення керуючись не лише повідомленням про подію, а й при цьому даними з інших систем.

Як приклад, при отриманні тривожного повідомлення про несанкціонований вторгнення оператор інтегрованої системи безпеки побачить на своєму екрані наступне:

- інформацію про спробу несанкціонованого вторгнення: час, місце;

- план приміщення об'єкта з показом відповідної області та сповіщувача, який подав тривожний сигнал;

- зображення з камер системи відео спостереження;

- інформацію про кількість людей на об’єкті;

- сигнали зі сповіщувачів руху і т.ін.

2. ІСБ підвищує операимвність прийняття рішень.

Безпека об'єкта – це взагалі реакція на можливі загрози. Виникає питання щодо збільшення швидкість відгуку на подію. Зокрема – методом автоматизації однотипних операцій. ІСБ може запрограмувати дії системи відповідно до певних подій, сигналів та їх комбінацій. Сукупність даних ій називається сценарієм.

Сценарій можна запуститти автоматично або вручну. Проте у будь-якому випадку контроль залишається оператору. Своїми діями оператор може не дозволити запуск сценарію або призупинити його виконання у будь-який час.

Приклад такого сценарію – реакція ІСБ на спрацювання сповішувача пожежної сигналізації. На автоматизоване робоче місце оператора приходить тривожне повідомлення, а також зображення з камер відеоспостереження, графічний план приміщення з показуванням відповідної області, інформація про кількість людей на об’єкті, тощо. У випадку підтвердження оператором повідомлення запускається наступний сценарій:

- на об’єкті включається оповіщення про пожежу;

- вмикаються системи пожежогасіння;

- повідомлення про пожежу надсилається до відповідних служб (до пожежної охорони, газову службу, швидку допомогу);

- на об’єкті вимикається централізоване електропостачання та вмикається аварійне освітлення, ліфти прямують до найближчого поверху, відкривають двері та блокуються в даному стані;

- здійснюється розблокування виконавчих пристроїв СКУД для безперешкодної евакуації людей.

Всі ці дії здійснюються у ІСБ автоматично: оперативно, узгоджено та у відповідній правильній логічній послідовності.

3. Концентрація усіх необхідних даних для аналізу подій – в одному ядрі інтегрованої системи безпеки.

Після усунення надзвичайної ситуації необхідно виявити її причини. Необхідно запитувати, зіставляти та аналізувати різну інформацію: зображення відеокамер, сигнали сповіщувачів, звіти СКУД, ін. Власник може взагалі не дізнатись про подію, у випадку невигідності виконавцю (черговому оператору).

Інтегрована система безпеки робить прозорість аналізу подій. У разі виникнення надзвичайної ситуації автоматично зберігаються показання датчиків, інформація з камер відео спостереження, ін. У єдиний для всіх систем журнал послідовно реєструються всі події та дії чергових операторів. Для відновлення перебігу подій достатньо проаналізувати звіт за потрібний інтервал часу.

4. ІСБ знижує вплив чиннику "людського фактора"

"Людський фактор" є слабкою ланкою у системах безпеки. Людина (адміністратор, черговий, користувач системи) може робити помилки та вчиняти умисні правопорушення, упускати з уваги важливі факти та приховувати інформацію. ІСБ дозволяє контролювати дії людини при цьому залишаючи за нею функції ухвалення рішення. Політика безпеки підприємства набуває статусу не рекомендаційного, а обов'язкового до виконання.

5. Централізоване управління об’єднаною системою безпеки.

Є проблема ефективного керування обладнанням різного призначення, що розташоване у різних приміщеннях об'єкта. Як же об’єднати розподілене функціональне обладнання в єдину систему безпеки.

Це можливо при використанні принципу централізованого управління. Збір даних від усіх модулів в єдиній точці дозволяє виробити оптимальну управлінську дію. ІСБ - надає змогу реагувати на подію, яка навіть сталася в іншому місці.

6. Підвищення стійкісті до відмови системи.

Відмовостійкість системи - здатність продовжувати виконувати свої функції при виході з ладу окремих елементів. В ІСБ це можливо завдяки наступним технологіям:

- перерозподіл навантаження. У випадку відключення окремих вузлів системи, або втрати зв’язку із ними, навантаження автоматично перерозподіляється між елементами на яких встановлено аналогічне обладнання. Інтегрована система продовжує функціонувати без зниження якості роботи.

- багаторівневе резервування ключових функцій. Логіка ІСБ та база даних зберігається на декількох ієрархічних рівнях: центральний сервер, контролери і. т. ін. При втраті зв'язку з верхніми рівнями обладнання переходить на автономний режим роботи, виконуючи функцію забезпечення безпеки «свого» сегмента;

- "гаряче" резервування ядра системи. У випадку виходу з ладу основного серверу ІСБ, керування переходить на резервний. ІСБ продовжує працювати без втрати функціоналу та зменшення рівня надійності. Після відновлення головного сервера резервний автоматично входить у режим очікування.

7. Коректна сумісна робота обладнання різних брендів.

Вона здійснюється в ІСБ методом дуже глибокої інтеграції на апаратному рівні. Наприклад якщо на об'єкті вже застосовуються різні технічні системи безпеки, їх можна об'єднати в ІСБ за допомогою спеціального програмного забезпечення: ПК LyriX або ПК APACS 3000 [13].

2.3. Інтеграційні платформи систем безпеки

Взагалі сучасні комплекси технічних засобів забезпечення безпеки різних та великих об'єктів реалізуються у вигляді інтегрованих систем.

Стандарти на ІСБ, у тому числі й терміни та визначення, перебувають у стадії розробки. Виходячи з цього, доречним видається навести визначення поняття "ІСБ". Необхідною умовою віднесення КЗБ до типу інтегрованих систем є:

- єдиний моніторинг, керування та протоколювання подій у системах, автоматична взаємодія між системами;

- автоматична робота між підсистемами.

Єдине конфігурування, будучи неоперативною функцією, бажано для ІСБ,

але не є обов'язковим, і тому не належить до необхідних та достатніх класифікаційних характеристик.

Доцільність побудови комплексу технічних засобів безпеки у вигляді ІСБ обумовлена низкою переваг. Для користувача є суттєвим наступне [12]:

- вбудований в ІСБ механізм автоматичних взаємодій, у тому числі й автоматичної підтримки дій оператора, дозволяєє підвищити оперативність та коректності прийняття рішень у критичних ситуаціях;

- цей же механізм наряду з об'єктивним протоколюванням подій забезпечує постійний контроль за діями персоналу охорони, що підвищує ефективність його роботи, а також забезпечує керівників інформацією, необхідною під час розслідування позаштатних ситуацій, розроблення заходів для підвищення кваліфікації персоналу та вдосконалення системи забезпечення безпеки об'єкта;

- існування єдиного інтерфейсу моніторингу та управління (Single Seat Interface), дозволяє оператору не перемикатися між вікнами окремих програм при роботі з ІСБ. Це полегшує освоєння та експлуатацію системи, знижує втомлюваність персоналу, дозволяє збільшити розміри контрольованого одним операто фрагмента ІСБ;

- єдинство програмного забезпечення виключає конфлікти програмних оболонок окремих підсистем, зроблених різними виробниками;

- єдині моніторинг, управління та протоколювання подій у підсистемах забезпепечують гнучкі можливості щодо створення робочих місць ІСБ з різними можливостями та повноваженнями, швидкого та маловитратного переконфігурування та розвитку ІСБ;

- єдина база подій забезпечує оператора максимально повною інформацією і максимально зручною формою при розслідувань позаштатних ситуацій.

Тенденція до інтеграції підсистем безпеки об'єктів є фундаментальним напрямком розвитку ринку. Однак підходи розробників та виробників до реалізації інтеграції різні.

Апаратна інтеграція передбачає об'єднання центральних процесорів підсистем безпеки (ПКП, ОЗ, контролерів СКУД і т.ін.) загальною

спеціалізованою інформаційною шиною за допомогою якої здійснюється моніторинг, конфігурація, управління та взаємодія систем між собою (рис. 2.2).

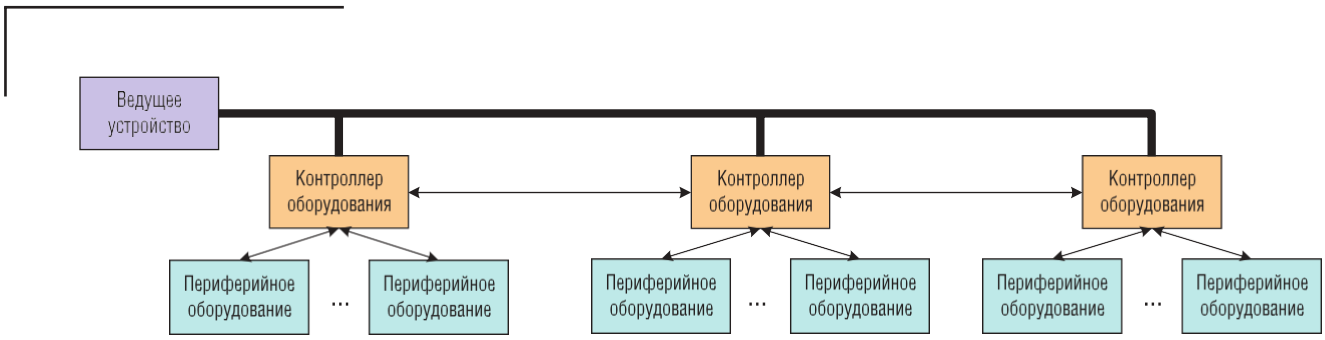

Рис. 2.2. Апаратна інтеграція

Варіантом такої інтеграції є релейна. Вона має високу надійність, застосовується, наприклад, для автоматичного розблокування аварійних виходів при пожежній тривозі.

Проте внаслідок малої інформативності більш складні алгоритми реалізуються із застосуванням специфічних шинних протоколів. При правильному виборі алгоритмів взаємодії та кодування, "шинна" апаратна інтеграція має високу надійність, так как обслуговується "жорсткими" обчислювачами з незмінюваною оперативно програмою. В основному виробники таких систем використовують власні унікальні закриті протоколи, що веде до обмеження можливостей апаратної інтеграції обладнання інших виробників. Також негативною стороною цього методу є подальша залежність користувача від спочатку обраного виробника [14].

В апаратно інтегрованих ІСБ використовуються і комп'ютери зі спеціалізованими програмами, але їх функція при цьому, як правило – один із пристроїв управління (реєстрації) з розширеними можливостями. Апаратна інтеграція реалізована наприклад у системах: "Кодос", "Оріон", Vista 250, "Рубіж 08" та ін.

Переваги: простота обладнання, мала вартість, існує можливість об'єднання підсистем різних розробників.

Недоліки: обмеженість видів повідомлень, якими обмінюються підсистеми; деякі проблеми з візуалізацією подій і стану системи в цілому; зі зростанням кількості реле і ліній зв'язку поступово втрачається перевага щодо низької вартості реалізації. Сумарна вартість такої релейної інтеграції може перевищувати вартість інтеграції іншого типу.

При реалізації програмної інтеграції, обладнання кожної (або кількох апаратно інтегрованих) підсистем безпеки контролюється власною програмою. Інтегруючим елементом при цьому є програмна надбудова (рис. 2.3), через яку здійснюється централізований моніторинг, протоколювання та управління обладнанням, а також міжсистемна (у даному випадку – міжпрограмна) взаємодія.

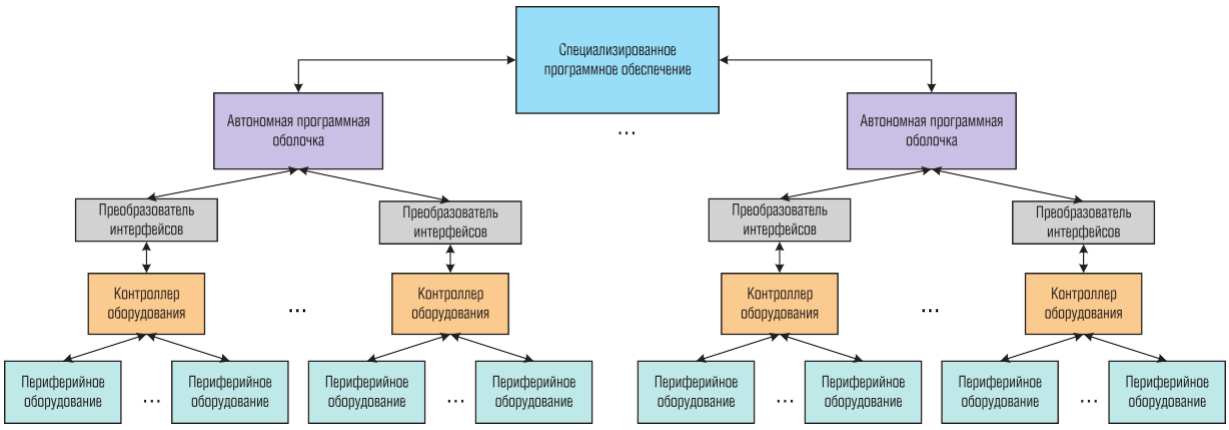

Рис. 2.3. Програмна інтеграція

Програмна інтеграція комплексу ІСБ характерна для комп'ютерних систем. Розуміючи можливість застосування обладнання, що використовується в ІСБ не тільки власної розробки, як одного з потужних інструментів просування продукції на ринок, більшість виробників застосовують заходи для створення можливостей інтеграції силами сторонніх розробників. Вони при цьому створюють єдину програму, що реалізує всі функції ІСБ і взаємодіє (прямо або через апаратні та програмні модулі перетворювачі) з обладнанням підсистем.

Переваги: використовуючи можливості сучасних іноваційних комп'ютерних технологій, можна створювати високоякісні програмні системи з багатьма

функціями. Існує можливість інтеграції з апаратними засобами інших виробників (для цього необхідне відповідний драйвер і відповідні інтерфейси обміну даними у самих використовуємих засобах). Побудова ІСБ за таким типом потребує меншої кількості ліній зв'язку між підсистемами у порівнянні з апаратною інтеграцією [14].

Недоліки: необхідність розробки драйверів для кожного використовуємого апаратного засобу. Не завжди при цьому розробник апаратного засобу предоставляє протоколи обміну даними. Навіть якщо вони відкриті і документовані, у них можуть бути реалізовані обмежені можливості, що не дозволить забезпечити поєднання. При цьому, фірма розробник програмної системи, поставляючи тільки свій програмний продукт, не може у повному обсязі гарантувати роботу всієї системи в цілому.

На відміну від попередньої, в такій ІСБ, яка називається **апаратно-програмною** (рис. 2.4), прийняття рішень і міжсистемна взаємодія відбувається

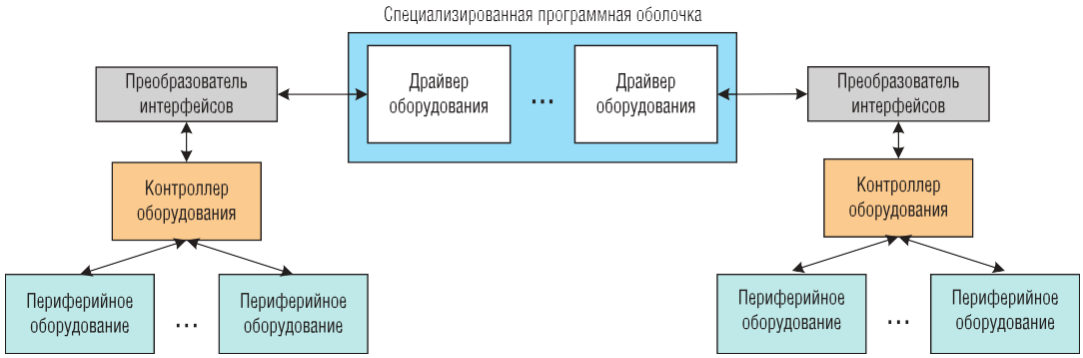

Рис. 2.4. Апаратно-програмна інтеграція

тільки в загальній для всіх підсистем програмі Протоколювання - тільки в єдиній базі подій, контроль і управління - тільки через загальний інтерфейс. Робота з обладнанням (програмна реалізація протоколу обміну) забезпечується прирладом, який називається драйвером.

Використання апаратно-програмної інтеграції надає можливість оптимізації програмного забезпечення з єдиних позицій. Це дозволяє створювати високопродуктивні, стійкі та надійні системи, спрощує оснащення їх засобами захисту інформації, сприяє зменшенню вартості інтегруючої надбудови, особливо для ІСБ з великою кількістю робочих місць співробітників. Також ІСБ, у порівнянні з апаратно інтегрованою системою, набуває необхідної гнучкості. Появляється можливість оптимізації вибору апаратури для вирішення різних завдань, обладнання існуючих комплексів новими приладами без повної заміни їх обладнання. Доволі суттєвим є збереження можливості автономної роботи підсистем при порушеннях у роботі керуючої надбудови [15].

Враховуючи привабливу для користувачів відкритість апаратно-програмних ІСБ, сильний розвиток комп'ютерних і комунікаційних технологій і все більшу зацікавленість розробників та виробників обладнання в його просуванні у складі ІСБ, необхідно визнати апаратно-програмну інтеграцію самою перспективною технологією створення ІСБ. Головною і необхідною умовою реалізації таких ІСБ є наявність у розробника алгоритму керування обладнанням. Чисельні виробники використовують низькорівневий протокол взаємодії підсистеми з управляючою комп'ютерною "надбудовою". У такому випадку від розробників ІСБ необхідно детальне володіння алгоритмами та особливостями роботи приладу.

Для полегшення робіт, виробники обладнання передають так званий Software Development Kit (SDK) розробника – програмний модуль, що здійснює двостороннє перетворення інформації між унікальним апаратним протоколом обладнання та формалізованим і описаним зовнішнім інтерфейсом модуля. Система команд управління доступна розробнику, спрощена, формалізована і коректно описана. Забезпечуючи повну реалізацію функціональності приладу, SDK як правило обмежує доступ до системних і службових операцій, таких наприклад як, перепрограмування внутрішнього процесору приладу. У розвитих зарубіжних країнах нанаявність SDK є головною умовою застосування обладнання, як засобу захисту інвестицій від шкоди, пов'язаної зі швидким моральним зносом обладнання.

Наприклад компанія ESMI надає повнофункціональний низькорівневий протокол, що забезпечує моніторинг, управління та конфігурування систем на основі ПКП серії ESA та MESA. Необхідно зазначити про наявність докладної документації, високу надійність роботи протоколу: існування механізмів гарантованої доставки повідомлень, виключення випадкового повтору команд, перевірки наявності комп'ютера на лінії зв'язку та ін. Контролер MESA дозволяє по'єднувати в єдину мережу кілька ПКП ESA, причому обмін даними між контролерами всередині мережі здійснюється за спеціальним закритим протоколу. Протокол дозволяє забезпечити реалізацію функції конфігурування системи з використанням створюваної інтегратором програми, але можна використовувати и безкоштовною програмою, що розповсюджується виробником.

Переваги: можна досягти оптимальних характеристик завдяки тому що вся розробка зосереджена, в одних руках. Оптимальні економічні показники.

Недолік: кожен розробник технічних засобів пропонує свою оригінальну систему, яка як правило, не сумісна з іншими засобами [9].

Цікавим є досвід інтеграції обладнання серії Vista, яке виробляється компанією Honeywell Security (колишня ADEMCO). Всі ПКП лінійки мають два інформаційних порти - "принтерний" та "клавіатурний". При цьому у жоден з портів, взятий окремо, не надходить повна інформація про роботу системи. У штатних модулях що обслуговують ці порти (4100SM і 4164E відповідно) відсутен механізм гарантованої доставки команди, а їх вартість дуже велика. Взагалі на ці порти надходять не дані про стан системи та його зміни, а лише "верхівка" реалізованого всередині ПКП протоколу, а саме: натискання управляючих клавіш і текстові повідомлення про події. При цьому, нормальна робота ПКП забезпечується тільки за певних часових параметрів керуючого впливу, що при використанні операційної системи Windows дуже важко.

При цьому виявилося доцільним розробка власного контролера, який підтримує роботу одночасно з обома портами. Контролер під керуванням відповідного драйвера відіграє роль усіх восьми можливих у системі пультів

керування та принтера, одночасно розвантажуючи комп'ютер від виконання завдання підтримки необхідного поточного обміну з системою. У результаті можливо розширити можливості систем на основі ПКП Vista, зокрема, підключити під єдиним управлінням до 16 ПКП на один порт комп'ютера, також реалізувати виконання макрокоманд, а саме, позонову постановку на охорону/зняття з охорони, фіксувати максимально повну інформацію про події, зокрема, прізвище співробітника, який працює з системою.

2.4. Переваги та недоліки ІСБ

Порівняно з простою сукупністю окремих систем та засобів захисту, застосування інтеграції забезпечує наступні переваги [16]:

1. Швидшу та точну реакцію на події, що відбуваються;

2. Істотне зменшення потоку інформації, що отримується оператором;

3. Полегшення роботи оператора за рахунок автоматизації процесів управління, контролю та прийняття рішень щодо забезпечення безпеки [6].

4. Суттєве зменшення ймовірності помилкових дій оператора (як наслідок двох попередніх пунктів);

5. Можливість аналізу та вироблення різноманітних керуючих впливів на основі єдиного інформаційного поля;

6. Простоту та можливість отримання максимуму різноманітної інформації;

7. Можливість створення та впровадження складних алгоритмів функціонування окремих елементів системи;

8. Зменшення витрат на обладнання через багатофункціональне використання окремих систем і більш повного їх завантаження;

До недоліків інтегрованих систем можна віднести підвищені вимоги до надійності підсистеми (за її наявності).

Висновок по розділу. Розглянуто принципи інтеграції систем безпеки. Існують три схеми інтеграції: програмна, апаратна та апаратно-програмна. Застосування інтеграції систем безпеки дозволяє покращити якісні показники забезпечення потрібного об’єкта.

РОЗДІЛ 3

СКЛАДОВІ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

3.1. Системи охоронної сигналізації

Технічний засіб охорони – це поняття, що позначає апаратуру (вид техніки), яка використовується у складі комплексів (систем) технічних засобів призначених для охорони об'єктів (територій, будівель, приміщень) від несанкціонованого проникнення [9].

Історично склалося декілька підходів до вирішення проблем класифікації ТЗО. Нами буде розглянутий підхід, який можна характеризувати як узагальнений, не провокуючий полеміки на предмет більшої або меншої коректності тих або інших підходів, бо їх відмінності виникають з відмінностей цілком певної мети класифікації. Деякі незручності для розуміння можуть створювати відмінності в термінології, коли близькі поняття позначаються різними словами, як то: засіб виявлення, датчик, сповіщувач. Іноді стосовно конкретних фізичних принципів дії застосовується слово “детектор,, як різновид сповіщувача. По суті до всіх цих термінів слід відноситися як до синонімів, що позначають близькі поняття - елементи апаратури технічних засобів охоронної сигналізації (ТЗОС), виконуючих функцію реагування на зовнішню дію. Наприклад, сейсмічний ЗВ реагує на коливання ґрунту, викликане рухом якого-небудь (людини, тварини) або чого-небудь (автомобіля, трактора і ін..). Кожний ЗВ будується на певному фізичному принципі, на основі якого діє його чутливий елемент (ЧЕ) (наприклад, електромагнітний, вібраційний, радіотехнічний, ємкісний, оптичний і ін.). Таким чином:

– засіб виявлення - це пристрій, призначений для автоматичного формування сигналу із заданими параметрами (сигналу тривоги, сигналу спрацьовування або сповіщення) унаслідок вторгнення або подолання об'єктом виявлення чутливої зони (говорять також – зони виявлення) даного пристрою.

–чутливий елемент - це первинний перетворювач, що реагує на дію на нього (пряме або непряме) об’єкта виявлення і сприймає зміну стану навколишнього середовища;

При виборі і впровадженні ТЗОС на об'єктах приділяється особлива увага досягненню високої захищеності апаратури від її подолання (обходу). Виробники ТЗОС пропонують різні способи реалізації цього завдання: контроль відкриття блоків, автоматична перевірка справності засобів виявлення і каналів передачі інформації, захист доступу до управління апаратурою за допомогою кодів (паролів), архівація всіх виникаючих подій, захист інформаційних потоків між складовими частинами ТЗОС методами маскування і шифрування і ін. Як правило, сучасні ТЗОС мають одночасно декілька ступенів захисту.

Таким чином, одним з головних завдань при проектуванні ТЗОС є створення засобів захисту від обходу їх зловмисником (порушником) і це є складним багатоплановим завданням.

Під комплексом ТЗОС розуміється сукупність функціонально зв'язаних засобів виявлення, системи збору і обробки інформації і допоміжних засобів і систем (системи тривожного сповіщення, системи охорони периметра і ін..), об'єднаних завданням по виявленню порушника.

Для захисту зовнішніх рубежів завжди використовують наступні засоби виявлення [13]:

– активні інфрачервоні засоби виявлення;
– сейсмічні засоби виявлення;
– ємнісні сповіщувачі;

Активні інфрачервоні засоби виявлення

Розробка вітчизняних активних ІЧЗВ ведеться з початку 60-х рр. У перших розробках як джерела випромінювання використовувалися лампи розжарювання. Модуляція випромінювання в цих виробах здійснювалася за допомогою механічних модуляторів. Такі ІЧЗВ мали низьку ефективність, великі габаритні розміри і значні струми споживання.

Оптична система джерела випромінювання (скорочено передавача - ПРД) створює вузькоспрямований промінь ІЧ-випромінювання. Як джерело ІЧ-випромінювання використовують напівпровідникові випромінюючі діоди з робочою довжиною хвилі 0,94 мкм, які розташовують у фокусі оптичної системи.

ІЧ-випромінювання фокусується оптичною системою ПРМ на чутливий майданчик фотоприймачів (фотодіодів). Отримувані з них імпульси фотоструму посилюються і поступають на пристрої обробки для формування сигналів тривоги.

Залежно від кількості променів і їх розташування (горизонтальне або вертикальне) ІЧЗВ можуть виконувати різні тактичні завдання. Горизонтальне розташування двох променів дозволяє за рахунок тимчасової обробки сигналів визначати напрям руху порушника. Вертикальне розташування променів в активних ІЧЗВ підвищує надійність блокування рубежів і периметрів в порівнянні з однопроменевими ЗВ (рис. 3.1).

Конвективні завади обумовлені дією потоків повітря, що переміщаються, наприклад протягів при відкритій кватирці, щілин у вікні, а також побутових опалювальних приладів – радіаторів і кондиціонерів. Потоки повітря викликають хаотичну флуктуаційну зміну температури фону, амплітуда і частотний діапазон якого залежать від швидкості потоку повітря і характеристик фонової поверхні.

Електричні завади виникають при включенні будь-яких джерел електро- і радіовипромінювання, вимірювальної і побутової апаратури, освітлення, електродвигунів, радіопередавальних пристроїв, а також при коливаннях струму в кабельній мережі і лініях електропередач. Значний рівень перешкод створюють також розряди блискавок.

Чутливість піроприймача дуже висока – при зміні температури на 1°С вихідний сигнал безпосередньо з кристала складає долі мікровольта, тому наведення від джерел завад в декілька вольт на метр можуть викликати завадовий імпульс, в тисячі разів більший за корисний сигнал. Проте велика частина електричних завад має малу тривалість або крутий фронт, що дозволяє відрізнити їх від корисного сигналу.

Власні шуми піроприймача визначають найвищу межу чутливості ІЧЗВ і мають вигляд білого шуму. У зв'язку з цим методи фільтрації тут не можуть бути використані. Інтенсивність завади збільшується при підвищенні температури кристала приблизно в два рази на кожні десять градусів. Сучасні піроприймачі мають рівень власних шумів, що відповідвють зміні температури на 0,05...0,15°С

Рис. 3.1. Активні інфрачервоні засоби виявлення

Сейсмічні засоби виявлення

Принцип роботи сейсмічних засобів виявлення технічної системи охорони базується на реєстрації коливань грунту який створює порушник.

Чутливими елементами таких систем є точкові елементи або трібокабель. Точкові чутливі елементи встановлюються в один або два ряди, утворюючи лінійну частину засобу сигналізації на рубежі, що охороняється. У зв'язку з тим, що на виході ЧЕ разом з корисним сигналом (КС) S(t) присутні перешкоди n(t) різного походження, завдання виявлення КС носить імовірнісний характер, тобто завжди є можливість прийняти перешкоду за корисний сигнал (помилкова тривога) з вірогідністю $P_{пт}$ або не виявити корисний сигнал, замаскований перешкодами з вірогідністю $P_{п}$ (пропуск сигналу). Зазвичай в тактико-технічних вимогах на засоби сигналізації задають середній час напрацювання на помилкове спрацьовування $T_{пт}$ >100...500 год. ($T_{пт}$ обернено пропорційно $P_{пт}$ ($P_{п}$ – ймовірність пропуску)) і вірогідність виявлення $P_{виявл}$ > 0,9.. .0,97 ($P_{виявл}$= 1– $P_{п}$). Імовірнісні характеристики ($T_{пт}$ і $P_{виявл}$) повинні зберігатися

при дії перешкод від автомобільного транспорту, промислових підприємств, літаків, коливань дерев і куща при вітрі і ін.

Надалі розглянемо СЗВ стосовно ділянок місцевості. Використання даного типу ЗВ усередині будівель і приміщень істотно утруднено з огляду на те, що споруди є складними резонуючими структурами з регулярними і нерегулярними вузлами жорсткості. До того ж в будівлях, як правило, зосереджені джерела різноманітних перешкод: електродвигуни ліфтів і холодильних установок, двері і так далі. Експериментальні вимірювання, проведені для виявлення з СЗВ в приміщеннях, показують, що $T_{ПТ}$ в цих умовах складає не більше 10-15 хв. При цьому не вдається забезпечити надійне виявлення об'єкту на всій площі приміщення, що охороняється.

Певні обмеження існують і при використанні СЗВ в умовах міста. Траси руху міського транспорту з інтенсивністю потоку більше один автомобіль в секунду допустимі на відстанях понад 100 м від ЗВ. По території об'єкту, що охороняється, на відстанях понад 20 м від зони виявлення можливий проїзд автомобілів з швидкістю до 40 км/год. (в середньому не більше один автомобіль за 5–10 год.). Враховуючи рідкість одиночних проїздів, допустима вірогідність помилкової тривоги не перевищує 0,05 ... 0,1. Проліт реактивного або гвинтового літака можливий на висоті більше 1 … 3 км. Зазвичай інтенсивності польотів одного літака в годину відповідає $P_{пт} < 0,002$.

СЗВ призначені для виявлення людини, що переміщається кроком і бігом із швидкістю 0,5.. .6 м/с. Найважче здійснима вимога по вірогідності виявлення людини, рухомої з мінімальною швидкістю, тому надалі завдання забезпечення надійного виявлення об'єкту-порушника ($P_{виявл} > 0,9$) розглядається стосовно швидкості подолання людиною ЗВ рівною 0,5 м/с.
При установці засобу сигналізації на рубежі, що охороняється, бажано мати візуально масковану лінійну частину, не порушувати екологію навколишнього середовища, наприклад, не проводити засолення ґрунту з метою запобігання її замерзанню. Безпосередньо у зоні виявлення допускається наявність трави, дрібного куща, а на відстані понад 5….10 м від зони виявлення –крупних дерев.

До теперішнього часу для охорони об'єктів, периметрів і рубежів розроблені комплекси охоронної сигналізації, що включають в свій склад станційну апаратуру управління і відображення інформації, а також певну номенклатуру засобів виявлення. Знов створювані СЗВ призначені для розширення функціональних можливостей цих комплексів, зокрема для охорони об'єктів, розташованих на територіях з сильно перетнутим рельєфом місцевості, а також для блокування таких ділянок, де необхідна максимальна замаскованість лінійної частини засобу виявлення.

Найпоширенішим типом точкового чутливого елементу є сейсмоприймач електродинамічного типу. Такі сейсмоприймачі широко використовуються в геології при сейсморозвідці і випускаються вітчизняною промисловістю для цієї мети (СВ-5, СВ-10, СГ-10, СВ-20). Конструкція їх вдає із себе герметичний корпус, усередині якого знаходиться магнітна система. У зазорі магнітної системи вільно переміщається котушка індуктивності, підвішена на гнучких підвісах. ЕРС самоіндукції, виникаюча при русі котушки, поступає на зовнішні виводи.

Відомі також інші типи точкових чутливих елементів: п'єзоелектричні, тензометричні і ін.

В якості протяжного чутливого елемента, як правило, використовується лінія, утворена ланцюжком послідовно сполучених електродинамічних сейсмоприймачі.

На виході такої лінії відбувається підсумовування сигналів від окремих СП. Типова кількість СП в лінії – 10 … 20 м, відстань між СП– 5 … 10 м.

У якості чутливих елементів також часто використовують протяжні елементи – трібоелектричний вібраційний кабель. Він перетворює механічні коливання інженерних загороджень (на якому закріплений) в електроімпульси. В результаті мікродеформацій у структурі кабельного сенсора, створюється внутрішня електризація, що викликає різницю потенціалів між провідниками, що отримала назву контактна електризація. Кабель, що працює на уфекті контактній електризації, вимагає використання їх на загородженнях, що мають видиму

гнучкість, у момент його подолання порушником. До таких загород відносяться сітка, решітка зварена з прутком, колючий дріт.

3.2. Пожежні системи

Пожежні сповіщувачі є основними елементами систем пожежної та охоронно-пожежної сигналізації. Пожежні сповіщувачі за способом приведення в дію поділяються класифікуються як:

• ручні;

• автоматичні.

У ручних пожежних сповіщувачах відсутня функція виявлення вогнища загоряння, їх дія зводиться до передачі тривожного сповіщення електричний ланцюг шлейфу сигналізації після виявлення загоряння людиною та активізації сповіщувача шляхом натискання відповідної пускової кнопки.

Автоматичні пожежні сповіщувачі працюють без участі людини. З їх допомогою здійснюється виявлення загоряння за однією або декількома аналізованими ознаками та формування повідомлення про пожежу при досягненні контрольованого фізичного параметра встановленого значення. Як контрольовані параметри можуть виступати підвищена температура повітря, виділення продуктів горіння, турбулентні потоки гарячих газів, електромагнітне випромінювання та ін. Відповідно до первинних ознак, що виявляються, пожежі сповіщувачі, як уже вказувалося раніше, поділяються на теплові, димові, полум'я, газові і комбіновані. Можливе використання інших ознак пожежі.

Все більшого поширення набувають пожежні сповіщувачі, створені з використанням елементної бази четвертого покоління: спеціалізованих контролерів та мікропроцесорів. Загальною особливістю таких сповіщувачів із розширеними тактико-технічними можливостями є використання для спільної роботи лише спеціальних приладів (контрольних панелей), що входять до складу системи охоронно-пожежної сигналізації відповідної фірми.

Застосування засобів обчислювальної техніки дозволяє створювати адресні та адресно-аналогові пожежні сповіщувачі, що передають на центральний процесор контрольної панелі інформацію про своє місцезнаходження, що забезпечує точне відтворення картини та аналіз процесу виникнення та розвитку пожежі. Вони здійснюють автоматично або на запит із центру контроль працездатності та передачу в цифровому вигляді даних про параметри свого функціонування. У таких сповіщувачах при необхідності можливе підстроювання чутливості при зміні умов довкілля.

Сповіщувачі аналогового типу передають інформацію про рівень контрольованого параметра. Розширення номенклатури сповіщувачів здійснюється за рахунок застосування нових технологій. Наприклад, сучасні закордонні лінійні теплові сповіщувачі (кабельного типу) вловлюють різницю між нормальною та підвищеною температурою, що дозволяє формувати сигнал тривоги ще до початку розвитку пожежі (появи диму чи вогню) при перегріві об'єкта, що контролюється. Сигнал передається в аналоговому вигляді від сповіщувача спеціальну контрольну панель, яка дозволяє визначати відстань до перегрітої ділянки. Такі сповіщувачі можуть ефективно застосовуватися для контролю об'єктів з електричним обладнанням, приміщень з фальшпотолками, кабельних трас та каналів.

Відповідно до виявлених первинних ознак пожежі сповішувачі бувають: теплові, димові, сповіщувачі полум'я, газові та комбіновані. Комбіновані сповіщувачі реагують на два та більше параметри, що характеризують появу вогнища пожежі.

Теплові пожежні сповіщувачі бувають:

- з використанням плавких матеріалів, що руйнуються під впливом підвищеної температури;

- використанням залежності електричного опору елементів від температури;

- використанням залежності магнітної індукції від температури;

- комбіновані.

Теплові сповіщувачі можуть реагувати не тільки на збільшення абсолютного значення температури вище над максимально визначений поріг, але і на перевищення швидкості наростання її граничного значення. Тому відповідно до характеру реакцію зміну контрольованого ознаки вони поділяються на максимальні, диференціальні і максимально-диференціальні.

Димові пожежні сповіщувачі за принципом дії поділяються на оптико-електронні та іонізаційні. За способом електроживлення пожежні сповіщувачі поділяються на:

- такі що живляться по шлейфу сигналізації від приладу приймально-контрольного або контрольної панелі;

- що живляться від окремого зовнішнього джерела живлення;

- що живляться від вбудованого внутрішнього джерела живлення (автономні пожежні сповіщувачі).

Пожежні сповіщувачі полум'я є засобами виявлення електромагнітного випромінювання полум'я або вогнища, що тліє, пожежі. Полум'я супроводжується процесом виникнення електромагнітного випромінювання в оптичному діапазоні, який залежно від довжини хвилі поділяється на ультрафіолетовий (УФ), видимий та інфрачервоний. Випромінювання вогнища пожежі в залежності від температури та виду хімічної реакції має різний спектральний склад. Гарячі матеріали, полум'я яких має відносно низьку температуру і, як правило, пофарбоване в червоний колір, активно випромінюють сигнал в інфрачервоному діапазоні. Високотемпературне полум'я має більшу інтенсивність випромінювання в УФ діапазоні. Чутливий елемент сповіщувача полум'я є перетворювачем електромагнітного випромінювання в електричний сигнал і реагує на випромінювання полум'я в одному або декількох діапазонах хвиль. Залежно від діапазону довжин хвиль випромінювання, що реєструється, сповіщувачі поділяються на сповіщувачі полум'я ІЧ або УФ діапазону. Перетворювачі видимого випромінювання практично не використовуються у зв'язку з суттєвими труднощами у забезпеченні прийнятної перешкоди.

Газові сповіщувачі є засобами виявлення невидимих газоподібних продуктів термічного розкладання; вони реагують на гази, що виділяються при тлінні та горінні матеріалів. У якості чутливого елементу в них в основному застосовуються напівпровідникові газові датчики (сенсори) на основі електрохімічних перетворювачів. Найбільш поширені горючі речовини та матеріали, що звертаються як у виробництві, так і в побуті, являють собою органічні сполуки. Основними газами, що утворюються при згорянні таких горючих речовин, є вуглекислий та чадний. Чутливим елементом, що реєструє наявність в атмосфері підвищеного вмісту недоокислених газів є так званий датчик Тагучі. При попаданні чадного газу на поверхню датчика відбувається його доокислення, датчик змінює свою електричну характеристику, що реєструється схемою обробки.

Ручні пожежні сповіщувачі призначені для ручного увімкнення сигналу пожежної тривоги в системах пожежної сигналізації та пожежогасіння. Вони забезпечують передачу в шлейф пожежної сигналізації тривожного сповіщення при ручному включенні приводного елемента (важеля, кнопки, крихкого)

елемента або іншого пристрою), призначеного для переведення сповіщувача з чергового режиму в режим видачі тривожного сповіщення за допомогою механічного впливу

Комбіновані сповіщувачі бувають теплодимовими, світлодимовими, теплосвітловими та ін. Найбільшого поширення набули теплодимові сповіщувачі: їх конструкція проста, вони мають низьку інерційність. При спрацьовуванні комбінованих сповіщувачів велике значення має процес тепломасоперенесення. Комбіновані сповіщувачі забезпечують більш надійне виявлення пожежі, оскільки дозволяють виявляти горіння широкого класу речовин. Однак при проектуванні слід враховувати, що зона захисту комбінованого сповіщувача розраховується за якоюсь однією ознакою пожежі, інша ознака є додатковою. Деякі виробники випускають і так звані комбіновані триканальні сповіщувачі, в яких в одному корпусі об'єднані димовий оптичний, димовий іонізаційний і тепловий принципи виявлення. Однак випадки використання подібних приладів дуже рідкісні через

їхню велику вартість. В даний час з'явилися ефективніші пожежні сповіщувачі навіть з чотирма каналами виявлення факторів пожежі: дим, тепло, газ і полум'я.

3.3. Система контролю та управління доступом

На сьогодня система контролю та управління доступом є невід'ємним елементом інфраструктури сучасного офісу подібно до системи кондиціонування або системи електронного документообігу [12]. Крім того, система контролю доступу є обов'язковим елементом багатьох комплексних систем безпеки. І цілком виправдано, адже система контролю та управління доступом дозволяє автоматично контролювати не лише вхід людей до будівлі чи приміщення, а й вихід із неї, будучи ефективним засобом захисту від проникнення сторонніх осіб на територію об'єкта. У результаті контроль доступу допомагає забезпечувати як збереження матеріальних цінностей, а й безпеку персоналу організації. Окрім запобігання доступу сторонніх на територію офісу, встановлення систем контролю доступу дозволяє розмежувати прохід співробітників та відвідувачів у відповідальні приміщення організації. Також встановлення СКУД на прохідній підприємстві дозволяє автоматизувати роботу пункту охорони в бюро перепусток, виключаючи вплив людського чинника. Тим самим контроль управління доступом дозволяє впорядкувати прохід відвідувачів до приймальної організації.

Основні елементи такої системи безпеки: контролер управління, зчитувачі персональних ідентифікаторів, персональні ідентифікатори, апаратура узгодження, апаратура, що блокує доступ).

Персональні ідентифікатори навидаються персоналу організації та використовуються як перепустки на територією офісу чи підприємства. Кожен такий ідентифікатор містить унікальний код, який витягується зчитувачем при контакті з кодоносієм. Персональний код ідентифікатора проходить аналіз бази даних контролера СКУД. Якщо код картки відповідає критеріям допуску, автоматика подає сигнал на блокуючий пристрій і робиться відкриття дверей, підйом шлагбауму і т.п. Персональні ідентифікатори розрізняються за

протоколами зв'язку зі зчитувачами, тому при проектуванні СКУД необхідно, щоб зчитувач та ідентифікатор підтримували один і той самий протокол зв'язку.

Зчитувачі СКУД, необхідні для вилучення інформації з кодоносія та її подальшу передачу контролеру системи. Вибір зчитувача, крім технічних характеристик, визначається ще й вимогами, які накладає інтер'єр приміщення, де встановлюється сам зчитувач (рис.3.2).

Контролери СКД – дуже важливий елемент контролю доступу. Надійність та продуктивність контролерів СКУД сильно позначається на подальшій роботі всієї системи. У випадку необхідності вибору контролера без його подальшого зв'язку з керуючим комп'ютером, потрібно приділити пильну увагу характеристикам: максимальна кількість користувачів, наявність внутрішніх годин, кількість подій, що реєструються, підтримка програмованих правил і т.п.

Апаратура узгодження використовуються для підключення одного або кількох контролерів системи до офісного комп'ютера чи сервера. У деяких випадках апаратура узгодження вже вбудована у контролер доступу.

Блокуючі пристрої - шлагбауми, турнікети, електромеханічні, електромагнітні замки, хвіртки, шлюзи. При виборі блокуючого пристрою аналізують вимоги конкретного об'єкта.

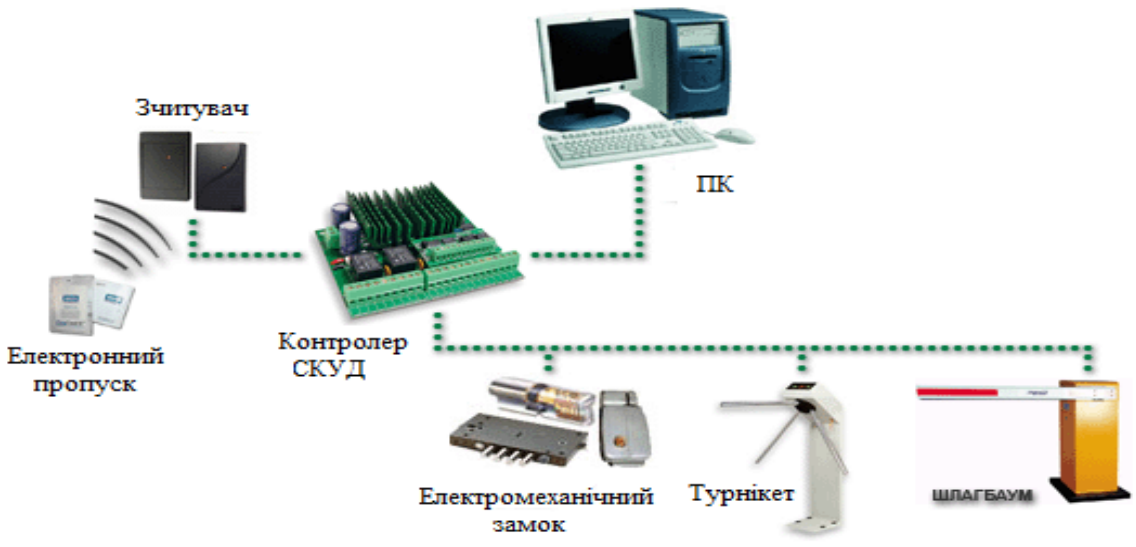

Рис. 3.2. Склад типової СКУД

Принцип роботи системи контролю та управління доступом. На прохідній підприємства, при вході у відповідальні приміщення встановлюються засоби контролю доступу: електромеханічні турнікети, електромеханічні або електромагнітні замки, зчитувачі безконтактних карток. Ці пристрої підключаються до контролерів системи управління доступом. Контролери приймають та аналізують інформацію про карти доступу, що пред'являються, а також управляють різними виконавчими пристроями. До складу обладнання системи контролю доступу можуть входити два типи контролерів: контролери замку та контролери турнікету, кожен із яких відповідає за контроль роботи власного вузла. Кожному співробітнику надається персональний ідентифікатор, найчастіше це безконтактна карта доступу - пластикова картка з унікальним електронним кодом. Але можливе застосування магнітних карт або т.зв. Touch memory пристроїв. Цей ідентифікатор одночасно є перепусткою на прохідній організації та ключем від тих приміщень, куди співробітнику дозволено доступ. Для проходу через турнікет або входу у відповідальне приміщення працівники підприємства повинні піднести свою карту доступу до зчитувача, після чого зчитувач передає код пред'явленої картки до контролера, а контролер доступу приймає рішення про дозвіл або заборону проходу на підставі закладеної в нього інформації. Якщо доступ дозволено, СКУД автоматично розблокує турнікет або замок на дверях.

За своїм типом СКУД класифікуються на *мережеві та автономні* [12].

Автономні СКУД ідеально підходять для невеликих будівель та малих офісів. Автономні СКУД не мають постійного каналу зв'язку з комп'ютером, а керування такою системою здійснюється за допомогою майстер-карток або за допомогою перемичок на самому контролері. На середніх і великих об'єктах, що охороняються, автономні СКУД використовуються в поодиноких випадках, за винятком контролю доступу у віддалені приміщення або ж у ролі резервної системи. Встановлення автономних систем контролю доступу зазвичай здійснюється на центральних дверях або запасних виходах. На дверях із

пропускною спроможністю в районі 1000 осіб автономні СКУД зазвичай оснащуються зчитувачем карт доступу або кодовим замком, крім того, зустрічаються реалізації автономних СКУД у вигляді прохідних з турнікетом або шлагбаумом. В умовах невеликого офісу з єдиними вхідними дверима автономна система виконується у вигляді автономного контролера, підключеного до електромагнітного/електромеханічного замку, поєднаного зі зчитувачем Proximity карт.

Мережеві СКУД обов'язково мають один або кілька комп'ютерів як керуючі елементи. Завдяки комп'ютеру у складі мережевий СКУД здійснюється моніторинг подій на об'єкті та здійснюється керування параметрами системи контролю. У порівнянні з автономною системою доводиться мати справу з більш гнучкою та функціональною моделлю системи безпеки. Недарма мережеві системи контролю доступом користуються найбільшою популярністю під час встановлення на об'єктах будь-якої складності. Часто при інсталяції мережеві системи інтегруються з охоронною сигналізацією, що дозволяє провести комплексний захист об'єкта, що охороняється, без додаткових витрат.

Основні можливості системи контролю та управління доступом:

- контроль та керування доступом;
- збір та предоставлення статистики;
- доступ співробітника лише за особистим ідентифікатором;
- облік робочого часу;
- автономність роботи системи;
- дистанційне керування системою через інтернет або з мобільного телефону;
- інтеграція СКУД з іншими системами безпеки та охорони.

3.4. Система відеоспостереження

Аналогова СВС - це класична система на базі аналогових, і передачею сигналу зображення по коаксіальному кабелю.

Всі аналогові відеокамери мають матрицю ПЗС. Ці відеокамери є оптичними пристроями, ПЗЗ-матриці яких формують відеосигнал з світлового потоку, що проходить через об’єктив і групу лінз потрапляє на цю матрицю. Об’єктиви для камер відеоспостереження встановлюються на відеокамери з метою збільшення дальності її роботи, поліпшення технічних параметрів і пристосування відеокамер до конкретних умов роботи. Для відеоспостереження за рухомими об’єктами використовують об’єктиви зі змінною фокусною відстанню-трансфокатори. В умовах мінливої освітленості застосовують об’єктиви з автодіафрагмою. На приховані камери прихованої ситеми відеоспостереження встановлюють об’єктиви типу Pin-Hole. Поворотні пристрої для камер відеоспостереження. Для розширення кута огляду відеокамери і стеження за рухомими відеоспостереження, камери встановлюють на поворотні пристрої об’єктами. Механізм поворотного пристрою переміщує її в горизонтальному і вертикальному напрямках, та дозволяє оператору системи відеоспостереження переглядати однієї відеокамерою досить великі площі території, що охороняється. Базовий блок виробляє постійний контроль наявності та справності всіх модулів і клавіатур в системі. В міру необхідності в будь-який момент часу в систему може бути додано або видалено будь модуль (рис. 3.3).

Рис. 3.3. Аналогова система відеоспостереження

Пристрої запису відеоінформації (відеомагнітофони, відеореєстратори, відео рекордери – DVR, відеосервери) призначені для запису, зберігання і подальшого відтворення зображень, що надходять від камер. Пристрої цифрового запису (відеорекодер, відеонакопичувач або відеореєстратор) здійснюють запис відеоінформації в цифровому форматі безпосередньо на жорсткий диск. Як правило, цифрові відеореєстратори останніх моделей оснащені системою, що реагує на рух в кадрі - детектори руху, і автоматично записуючої це відео, а так само мають мережеву плату для підключення відеореєстратора до системи відеоспостереження по LAN/WAN мережі. Розрізняють одноканальні відеореєстратори і багатоканальні 4, 6, 8, 16. Монітори виводу зображення і перегляду архіву запису. Можуть бути побудовані на базі променевої трубки. Джерело вторинного живлення 12 в або 24 В.

З кінця 1950-х років, камери відеоспостереження стали встановлювати на дорогах, в людних місцях та на критично важливих об'єктах. 1960 року, поліція Лондону встановила дві камери на Трафальгар-сквер. Це було зумовлено офіційним візитом тайської королівської сім'ї. Після візиту камери було знято через їх велику вартість. До кінця десятиліття було винайдено дистанційно керовані поворотні механізми для камер, що дозволило ставити одну камеру там, де раніше було потрібно кілька. Однак, основною проблемою систем відеоспостереження була потреба у використанні безлічі моніторів для передавання відеосигналу. На кожен монітор можна було вивести тільки одну камеру системи відеоспостереження. Операторам доводилося постійно пробігати очима по усій кількості моніторів, що призводило до розсіювання уваги оператора. Перший пристрій, що забезпечує можливістю телефонного відеозв'язку, було представлено лише 20 квітня 1964 року.

У 1969 році було видано патент на домашню систему безпеки (нині — відеодомофон), що дозволяв бачити на екрані телевізора, тих хто знаходиться за дверима, і дистанційно відмикати замок. Нова епоха відеоспостереження почалася з винаходом на початку 1970-х років, побутових відеомагнітофонів. Відеозапис став доступним, як приватним особам, так і малому й середньому бізнесу. Це

призвело до потужного розвитку систем відеоспостереження - камери почали з'являтися майже всюди: у будинках, крамницях, банках, навчальних закладах, просто на вулицях і проїжджих частинах міст. Свідку не треба було в суді пред'являти доказову базу з очевидців, достатньо долучити до судової справи VHS - касету з записом неправомірної пригоди, для обвинувачення підсудного у справі, злочинця. Згодом з'явилися мультиплексори, що дозволяли показувати зображення з декількох камер на одному моніторі та записувати його на одну касету.

У 1980-х роках, відбулася значна зміна конструкції найголовнішого елементу будь-якої системі відеоспостереження - відеокамер. Застосування електронно-променевої трубки було змінено на прилади із зарядовим зв'язком. Роздільна здатність світлочутливих матриць перших CCD-камер була вкрай низькою, однак вони були меншими та в рази світлочутливішими за старі камери.

Системи цифрового відеоспостереження.

Для людей, хто ніколи не стикався з установкою системи відеоспостереження, фраза - цифрове відеоспостереження просте поєднання двох сучасних слів. Цифрове телебачення, відеокамери і цифрові фотоапарати знайомі всім, але чим цифрова техніка краще і чому установка систем відеоспостереження з цифровим якістю, є такою популярною. Постараємося зрозуміло розповісти про те, що таке цифрове відеоспостереження, які переваги і недоліки має встановлення системи відеоспостереження цифрового формату.

За кілька десятків років, наш світ якісно змінився. Багато хто пам'ятає вінілові платівки з характерним потріскуванням при відтворенні, а зараз у нас в розпорядженні лазерні диски. Різниця між цими двома носіями інформації у тому, що вініл - це аналоговий формат, а компакт-диск - цифровий. Відповідно різні розміри і колосальна різниця в обсязі збереженої інформації, крім того цифровий носій стійкий до впливу часу і зчитування з нього інформації. Ось в принципі і загальний відповідь. Якщо провести паралель і взяти за основу цифрове відеоспостереження, то вийде приблизно така картина. Аналоговий потік обмежений реальним часом, таким чином по одному дроту можна передати тільки

один сигнал від однієї відеокамери, що виходить. Установка системи відеоспостереження аналогового типу передбачає індивідуальне підключення для кожної камери.

Цифрові системи також як і аналогові ведуть послідовну передачу даних, але швидкість передачі незрівнянно вище. Завдяки існуючих протоколів (правилами) дані можна розділяти, для того щоб було зрозуміло можна провести таку аналогію: аналоговий сигнал порівняємо з рідиною, що якщо змішати, то складно розділити, цифровий формат можна порівняти з кольоровими кульками, які можна перемішувати і розділяти. Таким чином, цифрове відеоспостереження дозволяє підключати велику кількість камер, керувати ними, швидко зберігати інформацію і паралельно працювати з нею. Установка системи відеоспостереження цифрового формату дозволяє уникнути втрат при передачі даних, це пов'язано з тим, що цифровий сигнал складається з послідовності одиниць і нулів, а аналоговий на амплітуді коливань. Як це позначається на виборі установки системи відеоспостереження? Ніяк, просто у випадку перешкод в аналоговій системі ви побачите шуми і спотворення на екрані, а цифрова передача даних, намагаючись виправити помилку «заморозить» кадр чи встигне виправити і збої будуть непомітними. Цифрове відеоспостереження відрізняється високою роздільною здатністю, так можна збільшувати зображення, розглядати окремі деталі, такий ефект досягається за рахунок зменшення розміру комірок матриці, і отже їх кількості, яка вимірюється в мегапікселях. Для порівняння, аналогова камера 0,4 Мрх, цифрові камери в кілька разів більше. Але якість зображення для звичайного відеоспостереження не приносить істотної користі.

Цифрове відеоспостереження обґрунтовано у разі охорони великих об'єктів, або якщо потрібен високий рівень безпеки, наприклад в Банках. Багато хто наші клієнти використовують повністю цифрове відеоспостереження, але застосування цифрових камер повинно бути обґрунтованим, для економічної доцільності проекту відеоспостереження.

IP відеоспостереження - один з поширених методів з сучасних системах спостереження та охорони. Всі великі виробники електроніки намагаються

зробити свою техніку ip сумісною. IP - це протокол (Internet Protocol) міжмережевої взаємодії. Він дозволяє пристроям підключатися до мережі і взаємодіяти за допомогою програм з комп'ютером.

Саме IP відеоспостереження використовується в сучасних системах охорони, нових системах виявлення та аналізу предметів, для автоматичного розпізнавання номерних знаків автомобілів. Монтаж відеоспостереження на основі IP дозволяє об'єднати відеокамери допомогою існуючої мережі, звернення до камери можливо безпосередньо з комп'ютера, достатньо просто ввести ip адресу камери. Монтаж відеоспостереження займає мінімум часу, камери швидко інсталюються. IP відеоспостереження підходить як для роботи всередині приміщень, так і зовні. Для вуличного спостереження використовується спеціальний кожух і об'єктив. Камери для ip відеоспостереження мають функцію пре-і пост запису (за сигналом тривоги), для цього використовується карта пам'яті.

IP відеокамери бувають декількох типів, високочутливі, панорамні, купольні, з високою роздільною здатністю 1280x1024 пікселів. І швидкістю до 30 к/с. Всі вони розроблені для організації систем охорони і спостереження. Для ip відеоспостереження випускаються спеціальні кожухи до камер, для роботи в умовах підвищеної вологості, низьких температур і навіть антивандальний кожух для міського ip відеоспостереження. Монтаж відеоспостереження з використанням IP, зазвичай здійснюється спільно з організацією локальних мереж. Наша компанія розробляє проекти пов'язані не тільки з IP відеоспостереженням, а комплексні рішення організації безпеки. Такі як, системи контролю доступу, автоматизовані паркування або АТС, телефонія.

Висновок по розділу. Розглянуто склад, принцип функціонування, призначення технічної системи охорони, системи відеоспостереження, системи контролю та управління доступом. Ці всі системи дозволяють, з використанням принципу комплексування, створити інтегровану систему безпеки.

РОЗДІЛ 4
МЕТОДИКА ОЦІНКИ РІВНЯ ЗАХИСТУ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗА РАХУНОК ВИКОРИСТАННЯ ІНТЕГРОВАНИХ СИСТЕМ БЕЗПЕКИ

Для систематичного аналізу ІСБ та ефективності її роботи на ОІД, а також для розуміння необхідності удосконалення її складових пропонується розробка методики оцінки ефективності ІСБ в цілому [8]. Як видно з практики на даний час не було винайдено правильного підходу до оцінки результативності по забезпеченню безпеки на ОІД за рахунок будь-якої з систем, щоб давало повну картину функціональності процесів в системі. У зв'язку з цим пропонується проводити оцінку ефективності ІСБ на основі процесу самооцінки, яка допоможе охватити і описати всі аспекти забезпечення безпеки на ОІД з різних сторін. Метод самооцінки допоможе скласти загальну картину захищеності та вкаже на слабкі сторони, які потребують удостоналення/поліпшення.

Така методика складається з восьми критеріїв: комплексність, функціональність, розмір, швидкодія, відмовостійкість, масштабованість, взаємодія із зовнішніми системами, можливість розширення, всі ці критерії сведено у таблицю 4.1.

У методиці пропонується використовувати математичний апарат із застосуванням методу вагових коефіцієнтів. Даний метод базується на наступному. Для оцінки кожної ІСБ використовуються означені вісім критеріїв.

Для кожного з критеріїв вводяться вагові коефіцієнти. Розраховується показник вигоди для кожної ІСБ, який визначається як сума перемножень значущості критеріїв на вагу обраного критерію:

$$f_i = \sum_{i=1}^{8} a_i,$$

де:

a_i – вага критерію.

Для побудови оптимальних варіантів системи по даній морфологічній множині скористаємося методом повного перебору. Суть методу полягає в тому, що прораховуються вигоди і витрати від реалізації всіх варіантів ІСБ і вибирається необхідне число кращих з точки зору ставлення вигод до витрат. Всього таких варіантів у даному випадку:

$$N = \prod_{i=1}^{8} M_i$$

де:

M_i – кількість альтернатив у даному критерії.

На підставі отриманих даних методом повного перебору знаходяться кращі варіанти реалізації системи фізичної безпеки. Пошук здійснюється по цільовій функції:

$$max\left(\frac{f_i}{C_i}\right) = \frac{\sum_{i=1}^{8} a_i}{C_i}$$

де:

f_i - показник ІСБ:

C_i - вартість ІСБ.

Та альтернатива, яка має найвище значення функції і буде найкращою.

Таблиця 4.1. Оцінка ІСБ

Комплексність (середньозахищений ОІД має включати не менше 4 систем безпеки)		
Оцінка	Опис	
1	Об’єднує менше трьох систем	система протипожежна, система відеоспостереження
2	Об’єднує від 3 до 5 систем	система протипожежна, система відеоспостереження, СКУД, система охоронної сигналізації
3	Об’єднує більше 5 систем	
Функціональність (набір основних функціональних характеристик ІСБ за обміном інформацією і управлінням складовими ІСБ)		
Оцінка	Опис	
1	Малофункціональна ІСБ	передача інформації між системами відбувається тільки при виникненні тривоги в якій-небудь одній системі. Відсутня можливість управління всіма системами одночасно з одного робочого місця. Бази даних систем не синхронізовано.
2	Середньофункціональна ІСБ	передача інформації між системами відбувається тільки при виникненні тривоги в якій-небудь одній системі. Є можливість управління всіма системами одночасно з одного або декількох робочих місць. Бази даних окремих систем не синхронізовано.
3	Високофункціональна ІСБ	передача інформації між системами відбувається не тільки при виникненні тривоги в одній з систем, але і при виконанні системою своїх штатних функцій. Є можливість управління всіма системами одночасно з одного або декількох робочих місць, що мають загальну програмну оболонку з широким набором функцій. Бази даних систем синхронізовані.
Розмір (розмір ІСБ залежить від розміру складових, що входять в кожну з систем безпеки)		
Оцінка	Опис	
1	Мала	складається з систем, в кожній з яких до 50 точок (адресних елементів/адресних датчиків/зчитувачів/відеоканалів)
2	Середня	складається з систем, в кожній з яких від

Продовження табл. 4.1

		50 до 500 точок
3	Велика	складається з систем, в кожній з яких більше 500 точок
Швидкодія (визначення проміжку часу між подією в одній системі безпеки і відповідної реакцією в іншій /інших системах безпеки, що входять в ІСБ)		
Оцінка	Опис	
1	Низька	час реакції перевищує 2 секунди.
2	Середня	час реакції знаходиться в межах від 1 до 2 секунд.
3	Висока	час реакції між системами становить менше 1 секунди.
Відмовостійкість/живучість		
Оцінка	Опис	
1	Низька	ІСБ має один нерезервованої сервер управління або нерезервованої процесорний модуль. Лінії зв'язку не резервовані. Збій в роботі сервера, процесора або обрив лінії зв'язку відразу призводять до порушення обміну інформації в ІСБ і розсипання її на окремі системи безпеки.
2	Середня	ІСБ має резервний сервер або процесор, що працюють в "гарячому" режимі. Лінії зв'язку резервовані. У такій ІСБ одноразовий збій в роботі сервера або обрив лінії зв'язку не призводять до порушення роботи систем ІСБ.
3	Висока	ІСБ має резервний сервер або процесор, що працюють в "гарячому" режимі. Лінії зв'язку резервовані. Інтеграція між системами виконана не тільки на програмному, а й на апаратному рівні.
Масштабованість (збільшення розміру систем, з яких складається ІСБ в процесі експлуатації)		
Оцінка	Опис	
1	Фіксована	ІСБ не може збільшувати свій розмір.
2	Масштабна	ІСБ може значно збільшувати існуючий розмір за рахунок додавання, закінчених модулів або нових окремих систем.
Взаємодія із зовнішніми системами		
Оцінка	Опис	
1	Відкрита	ІСБ забезпечує можливість обміну інформацією на програмному рівні із зовнішніми системами інших виробників.

Продовження табл. 4.1

2	Закрита	ІСБ не забезпечує можливості обміну інформацією на програмному рівні з зовнішніми системами інших виробників.
Можливість розширення		
Оцінка	Опис	
1	Розширювана	ІСБ дозволяє додавати в існуючий склад ІСБ системи нових виробників.
2	Нерозширювана	ІСБ включає до свого складу тільки жорсткий перелік обладнання вже певних виробників. Додати устаткування інших виробників неможливо.

Низький рівень захищеності – менше 8 балів

Середній рівень захищеності – від 9 до 15 балів

Високий рівень захищеності – від 16 до 21 балів

Оцінка рівня захисту інформації на ОІД за рахунок використання ІСБ через визначення величини ризику для кожної пари вразливість/загроза відіграє не малу важливу роль у визначеній надійності ІСБ.

Створення переліку параметрів, перевірка яких дозволяє визначити дієвість підсистем ІСБ. Визначення проводиться на підставі оцінки ймовірності реалізації загрози на ОІД, що може використати вразливість і оцінки наслідків реалізації загрози ІСБ.

Оцінка ризиків складається з шести кроків:

1. Визначення підсистемних слабкостей - вразливостей, якими може скористатися загроза та створення відповідних пар вразливість/загроза для ІСБ;

2. Виявлення потенційних небезпек - загроз;

3. Визначення існуючих ІСБ, що можуть знизити ризик загрози, яка використовує певні вразливості систем безпеки;

4. Визначення ймовірності реалізації загрози, що експлуатує пов'язану вразливість враховуючи існуючі підсистеми ІСБ;

5. Визначення тяжкості негативних наслідків або рівня впливу наОІД у випадку реалізації загрози, що експлуатує пов’язану вразливість;

6. Визначення величини ризику для пари вразливість/загроза (з врахуванням існуючого механізму безпеки), шляхом перемноження ймовірності реалізації загрози на рівень впливу на ОІД при реалізації загрози.

Крок 1-й - Визначення вразливостей

Вразливість є слабістю систем безпеки, яка може бути використана однією або кількома загрозами. Використання (експлуатація) вразливості приводить до реалізації загрози, що в свою чергу, породжує негативні наслідки, наприклад - у вигляді порушення таких властивостей як конфіденційність, цілісність, доступність інформації, що зберігається на ОІД. Вразливість не може заподіяти ніякої шкоди сама по собі, повинні існувати загрози, які можуть її використовувати.

Вразливості ідентифікуються в таких областях:

- ОІД у цілому;
- Процеси та процедури;
- Конфігурація програмно-технічних комплексів, обладнання, програмне забезпечення або телекомунікаційне обладнання;
- Персонал;
- Фізичне середовище;
- Залежність від зовнішніх ОІД.

Крок 2-й - Визначення загроз

Загрози потенційно можуть завдати шкоди ресурсам ОІД, зокрема інформації, персоналу, клієнтам, обладнанню, процесам і програмно-технічним комплексам та ін. Загрози можуть мати природні та людськід жерела і можуть бути випадковими або навмисними (класифікація загроз наведена у розділі 2).

На ОІД проводиться ідентифікація як випадкових, так і навмисних джерел загроз.

До кожної вразливості, яка була ідентифікована на попередньому кроці і використання (експлуатація) яких може привести до реалізації загрози проводиться ідентифікація загроз.

Крок 3-й - Визначення існуючих ІСБ, що можуть знизити ризик загрози, яка використовує певні вразливостісистем безпеки

Існуючі ІСБ зменшують ймовірність реалізації загрози щодо використання пов'язаної уразливості підсистем та/або зменшують величину впливу при реалізації пари загроза/експлуатована уразливість.

Крок 4-й - Оцінка ймовірності реалізації загроз

Ймовірність реалізації загроз - це те, як легко загроза може використовувати вразливість. Ймовірність реалізації загроз має оцінки ймовірності, що наведені в таблиці 4.2.

Таблиця 4.2. Ймовірність реалізації загроз

Оцінка ймовірності	Опис
1	Реалізація загрози практично неможлива
2	Реалізація загрози малоймовірна (не частіше ніж 1 раз на 1 рік)
3	Реалізація загрози ймовірна до 1 разу на 3 місяці
4	Реалізація загрози ймовірна до 1 разу на тиждень
5	Реалізація загрози ймовірна до 1 разу на добу

Крок 5 - Визначення тяжкості негативних наслідків або рівня впливу на ОІД увипадку реалізації загрози, що експлуатує пов'язану вразливість

Визначення тяжкості негативних наслідків або рівня впливу у випадку реалізації загрози (для кожної пари загроза / вразливості), необхідно проводити оцінюючи вплив на такі властивості інформаційних ресурсів ОІД, наприклад - конфіденційність, цілісність, доступність;

Оцінка впливу на цілісність, доступність, конфіденційність, спостережність, наведені у таблиці 4.3

Таблиця 4.3. Оцінка впливу на основні складові ІБ

Оцінка рівня наслідків	Опис
1	Практично не призводить до наслідків з фінансовими втратами (до 1 тис.грн.)
2	Призводить до незначних фінансових втрат (до 10 тис. грн.) та має незначний вплив на репутаціюОІД
3	Призводить до значних фінансових втрат (від 10 до 50 тис. грн.) та має значний вплив на репутаціюОІД
4	Призводить до великих фінансових втрат (більше 50 тис. грн), має значний вплив на репутаціюОІД і може призвести до зупинки роботи процесів ОІД
5	Призводить до зупинки процесів ОІД і порушує законодавство України

Максимальна з оцінок впливу на конфіденційність, цілісність, доступність для кожної пари загроза/ вразливість використовується потім при визначенні (розрахунку) величини ризику.

Крок 6-й – Визначення величини ризику

Для кожної пари загроза/вразливість, величина ризику визначається за наступною формулою:

$$\mathbf{ВР_{з,в} = Й_{з,в} * РВ_{з,в}},$$

де**:**

$ВР_{з,в}$- величина ризику для пари загроза -з, вразливість –в;

$Й_{з,в}$ - ймовірності реалізації загрози -з, що експлуатує пов'язану вразливість - в;

РВ $_{з,в}$ - рівень впливу на ОІД при реалізації загрози – з , що експлуатує пов’язану вразливість – в.

Таким чином, використавши метод самооцінки та метод оцінки рівня захисту інформації на ОІД за рахунок використання ІСБ через визначення величини ризику для кожної пари вразливість/загроза можна скласти чітке уявлення щодо рівня ефективності ОІД за рахунок ІСБ.

Висновок по розділу. Розроблена методика оцінки якості функціонування ІСБ. Розроблена методика дозволяє серед варіантів ІСБ обрати найкращий за показником якість-вартість методом повного перебору. За рахунок такого перебору можна підвищити ефективність функціонування ІСБ.

ВИСНОВОК

У роботі досліджено призначення, способи побудови, склад інтегрованих систем безпеки. Встановлено, що застосування інтегрованих систем безпеки дозволяє вирішити ряд питань, а саме: зменшити витратну частину об'єкта на забезпечення системами і підсистемами охорони за рахунок зменшення апаратної частини; систематизувати і зробити більш зрозумілою інформацію, яка надходить на центральний пульт управління. Це легше втілити в життя, ніж у разі застосування розрізнених автономних систем безпеки. Перевагою у використанні інтегрованих систем безпеки є їх модульна система.

Розроблено методику оцінки ефективності інтегрованих систем безпеки яка дозволить раціонально будувати найбільш ефективну інтегровану систему на об'єкті інформаційної діяльності з урахуванням таких чинників як вартість системи та її ефективність до протидії відповідним загрозам інформації.

В результаті поставлена мета дипломної роботи досягнута.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Интеграция как новый подход к построению систем безопасности. [Електронний ресурс] / Журавлев С.П. //Журнал научных публикаций аспирантов и докторантов. - 2006 – 1с.

2. БЕЗПЕКА // Юридична енциклопедія : [в 6-ти т.] / ред. кол. Ю. С. Шемшученко (відп. ред.) [та ін.]. — К.: Українська енциклопедія, 1998.

3. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення /НД ТЗІ 1.1-005-07 / Держспецзв’язок - 2007

4. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури / ДержНДІ Спецзв’язку УДК 004.056 /– 2015 –58-60с.

5. [Електронний ресурс]https://xn--80adgeboqrpy5j.com.ua

6. [Електронний ресурс]http://bezpeka.ck.ua/article-21.html

7. Дурденко В.А. Разработка классификация и архитетуры построения интегрированых систем безопасности / Дурденко В.А. Рогожин А.А. – К.: Информационно-вычеслительные управляющие и сетевые системы – 2012 – 62 с.

8. Интегрированные системы безопасности. Общие положения./ ГОСТ Р 57674 – 2017 – 3-4с.

9. Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности / [Електроннийресурс] Р-78.36.018–2011

10. [Електроннийресурс]http://www.sigma-is.ru/integration.html

11. [Електронний ресурс] https://www.electronika.ru/products-solutions/solutions/integrated/

12. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом.- М.: Горячая линия- Телеком, 2010. - 272 е.: ил. – 5с., 16-24с., 27-30

13. [Електронний ресурс]http://studopedia.com.ua/1_30311_sistema-kontrolyu-dostupu.html

14. [Електронний ресурс] https://guard-lviv.com.ua/uk/sistemi-videonablyudeniya/index.html

15. [Електронний ресурс] https://asisvok.com.ua/blog/item/z-choho-skladaietsia-systema-videosposterezhennia

16. Лінії зв’язку передачі даних./ [Електронний ресурс]http://oksim.com.ua

17. ДСТУ 3960-2000. Системи тривожної сигналізації. Системи охоронної і охоронно-пожежної сигналізації. Терміни та визначення.