МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2020 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ’ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ШЛЯХОМ ВИКОРИСТАННЯ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ.**

Виконав: студент 6 курсу, групи СЗДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Технічні системи інформаційного та
кібернетичного захисту»
(шифр і назва спеціальності)
Омельченко М.О.
(прізвище та ініціали)
Керівник Котенко А.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Гребенніков А.Б.

КИЇВ – 2021

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____к.т.н. Г.В.Шуклін

«_____»_____ 2021 р.

ЗАВДАННЯ

На магістерську роботу студента

Студент:Омельченко Микита Олегович

1.Тема роботи: Підвищення інформаційної безпеки об’єкту інформаційної діяльності шляхом використання інтегрованої системи безпеки.

Затверджена наказом по університету від « » _____ 2020р. №_____

2.Термін здачі: студентом оформленої роботи «21» грудня 2020 р.

3.Об’єкт дослідження: процес захисту інформації на ОІД.

4.Предмет дослідження: інтегровані системи безпеки.

5.Мета роботи: підвищення рівня захисту на об’єкті інформаційної діяльності за рахунок використання ІСБ та підвищення рівня інформаційної безпеки (ІБ).

6.Перелік питань, які мають бути розроблені:

- з’ясувати можливості і призначення ІСБ на ОІД;
- виявити особливості структури ІСБ;
- описати методику ефективності ІСБ для ОІД.

7.Перелік публікацій:

1. Омельченко М.О. ,“ХАРАКТЕРИСТИКА ТА ЗАГАЛЬНІ ВИМОГИ ДО СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ” // X Міжнародна науково-технічна конференція студентства «Світ інформації та телекомунікацій»
2. Омельченко М.О., **ХАРАКТЕРИСТИКА ТА ЗАГАЛЬНІ ВИМОГИ ДО СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ**. К Сучасний захист інформації № 4, 202 . - ТАК

8.Перелік ілюстративного матеріалу:

Презентація виконана для подання за допомогою оверхедів (світлопроекторів) та комп’ютерних засобів.

9.Дати видачі завдання «____»_____ 2020 р.

Науковий керівник _____ Котенко А.М.

Завдання прийняв до виконання _____ Омельченко М.О.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 10.09.20р.	виконано
2	Обґрунтування актуальності теми роботи	до 07.10.20р.	виконано
3	Написання першого розділу роботи	до 18.10.20р.	виконано
4	Написання другого розділу роботи	до 20.11.20р.	виконано
5	Написання третього розділу роботи	до 26.11.20р.	виконано
6	Написання четвертого та п’ятого розділу	до 28.11.20р.	виконано
7	Написання висновків по роботі	до 30.11.20р.	виконано
8	Підготовка демонстраційних матеріалів	до 18.12.20 р.	виконано
9	Захист у ДЕК	18.01.2021 р.	виконано

Студент групи СЗДМ-61 Омельченко Микита Олегович _____
(підпис)

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

РЕФЕРАТ

Дипломна робота містить 70 сторінок, 13 рисунків, 4 таблиці, 20 джерел.

Інтегрована система безпеки - це комплекс підсистем різного призначення пов'язаних в єдине ціле. ІСБ - це більше ніж сумафункціональних модулів які входять до неї, це єдина система безпеки, що забезпечує захист об'єкта на значно вищому рівні. Само за допомогою інтегрована система безпеки можна створити безперебійну систему захисту на підприємстві.

Мета роботи. підвищення рівня захисту на об’єкті інформаційної діяльності за рахунок використання ІСБта підвищення рівня інформаційної безпеки (ІБ).

Завдання дослідження:

- дослідити можливості і призначення ІСБ на ОІД;

- проаналізувати існуючі методи та засоби захисту інформаціїна ОІД за допомогою інтегрованої системи безпеки;

- визначити шляхи підвищення інформаційної безпеки об’єкту інформаційної діяльності шляхом використання інтегрованої системи безпеки.

Об’єкт дослідження. Процес забезпечення інформаційної безпеки на ОІД.

Предмет дослідження. Інтегрована система безпеки.

Методи дослідження. Методи системного аналізу, чисельні методи.

Галузь використання – інформаційна безпека.

Ключові слова:ІНТЕГРОВАНІ СИСТЕМИ БЕЗПЕКИ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ЗАХИСТ ІНФОРМАЦІЇ, СИСТЕМИ БЕЗПЕКИ.

ANNOTATION

Thesis contains 70 pages, 13 figures, 4 tables, 20 sources.

An integrated security system is a set of subsystems for different purposes connected into a single whole. ISB is more than the sum of the functional modules included in it, it is the only security system that provides protection of the object at a much higher level. Only with the help of an integrated security system you can create an uninterrupted security system in the enterprise.

The purpose of the work. Improving the effectiveness of information protection with an integrated security system.

Objectives of the study:

- to study the possibilities and purpose of ISB on OID;

- to analyze the existing methods and means of information protection at the OID with the help of an integrated security system;

- identify ways to improve the information security of the object of information activities through the use of an integrated security system.

Object of study. The process of ensuring information security at OID.

Subject of study. Integrated security system.

Research methods. Methods of system analysis, numerical methods.

Field of use - information security.

Keywords:INTEGRATED SECURITY SYSTEMS, OBJECT OF INFORMATION ACTIVITY, INFORMATION PROTECTION, SECURITY SYSTEMS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІСБ – інтегрована система безпеки

ОІД – об’єкт інформаційної діяльності

ІБ – інформаційна безпека

НСД – несанкціонований доступ

ПЕМВН – каналипобічних електромагнітних випромінювань і наводок

ВС – відеоспостереження

СКУД – система контролю управління доступом

БД – база даних

СТС – система тривожної сигналізації

СОС – система охоронної сигналізації

СВС – система відеоспостереження

ПЗ – програмне забезпечення

ППК – пристрої перегороджуючі керовані

ПВІО – пристрої введення ідентифікаційних ознак

ПК – пристрої керування

ВСТУП

З давніх часів питання забезпечення безпеки людського життя в її повсякденній діяльності було і залишається відкритим, фактори ризику різного роду року доповнюються новими загрозами - навколишнє середовище людини, житловий захист, захист від несприятливих природних явищ, безпека виробництв і виробництва, продукція для споживання і закінчується захистом людини від людини.

Розвиток суспільства не стоїть на місці, з кожним днем відкриваються нові і нові можливості для комфортного людського життя в соціальній, технологічній, промисловій та інших сферах життя і з кожним днем з 'являються нові види загроз. Що мотивує такі загрози і хто їх створює, чому це відбувається? Відповідь очевидна - розвиток продукції, технологій виробництва, створення інноваційних методів і методик призводить до значної конкуренції в умовах обмежень і чим більше один об'єкт інформаційної діяльності (ОІД) від іншого, тим більше конкуренція між ними, і так стають більш витонченими способи нашкодити ОІД і людині в цілому.

Однак створення загроз підштовхнуло світ до створення "галузь безпеки" - невелика або велика команда різних фахівців, які в свою чергу розробляють засоби нападу і оборони, включаючи такі області, як законодавство і способи ухилення від нього, засоби економічної розвідки, промислове шпигунство, електронна розвідка і захист інформації, фізичний вплив на людей, будівлі і споруди, пожежну та охоронну сигналізацію, відеоспостереження (ВС), системи контролю доступу (СКУД). Такі силові відомства можуть надавати охоронні послуги як через єдину автономну систему безпеки (пожежна, охоронна сигналізація, відеоспостереження, система контролю доступу тощо), так і створити абсолютно новий етап у будівництві систем безпеки - інтеграцію.

Більш складні умови захисту провокують використання і розвиток більш складних систем безпеки. На тлі розвитку ринку виникає необхідність інтеграції всіляких підсистем в єдину монолітну систему безпеки, здатну вирішувати весь спектр завдань - інтегровану систему безпеки.

Інтегрована система безпеки (ІСБ) - це спільне використання ресурсів підсистем (пожежна та охоронна сигналізація, відеоспостереження, системи контролю доступу тощо), в результаті чого система в цілому набуває нових якісних властивостей, на відміну від автономної роботи підсистем.

Незважаючи на те, що ринок пропонує широкий спектр охоронних моносистем, які працюють окремо від інших компонентів технічного захисту, жодна з них не здатна повною мірою захистити інтереси захищеного ОІД. Тому більш ефективними в захисті безпеки є інтегровані системи безпеки, які складаються не тільки з підсистем, але і з власних каналів зв 'язку, баз даних, алгоритмів і програмного забезпечення.

Основні напрями визначаються такими вимогами:

1. зниження ролі людини в процесі забезпечення безпеки шляхом підвищення інтелекту систем;

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

3. Вимога відкритості. Розробники ІСБ повинні надати замовнику за допомогою відкритих протоколів можливість підключати системи та обладнання інших виробників і гнучко підлаштовувати ІСБ під свої потреби.

Реалізація цих вимог з одного боку підвищить ефективність систем безпеки, знизить людський фактор, з іншого - зробить будівництво інтегрованих систем більш прозорим. [1]

Оскільки сучасність вимагає більш досконалих та ефективних засобів захисту інформації на ОІД, можна вважати, що тема магістерської роботи, яка фокусується на підвищенні рівня захисту на ОІД за рахунок використання ІСБ як високоефективного методу, є актуальним науковим завданням.

РОЗДІЛ 1

БЕЗПЕКА ТА НЕБЕЗПЕКА ЯК ОСНОВНІ ПОНЯТТЯ ПРИ КЛАСИФІКАЦІЯ ВИДІВ ЗАГРОЗ НА ОБ´ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Безпека — це умови, в яких знаходиться складна система, коли дія зовнішніх факторів і внутрішніх факторів не призводить до процесів, що вважаються негативними по відношенню до цієї складної системи відповідно до існуючих, на даному етапі, потреб, знань та ідей. Простіше кажучи, безпека - це стан захищеності, коли ніщо комусь або чомусь не загрожує.

Небезпека - можливість обставин, за яких матерія, поле, інформація або їх поєднання можуть таким чином вплинути на складну систему, що призведе до погіршення або неможливості її функціонування і розвитку. [2]

У сучасному світі з високим рівнем нестабільності зовнішнього і внутрішнього середовища будь-який об'єкт інформаційної діяльності (ОІД) - це будівлі, приміщення, транспортні засоби або інші інженерні споруди, функціональне призначення яких передбачає поширення інформації з обмеженим доступом [3], може піддаватися негативному впливу загроз.

Загроза - одна з ключових концепцій у сфері інформаційної безпеки. Загроза об'єкта інформаційної безпеки - сукупність факторів і умов, що виникають у процесі взаємодії різних об'єктів (їх елементів) і здатних зробити негативний вплив на конкретний об'єкт інформаційної діяльності. [4]

Для визначення засобів і методів захисту необхідно розібратися в класифікації типів загроз, а потім зважити всі наслідки для побудови і використання інтегрованої системи безпеки як одного з найсучасніших способів зниження вразливості до різних небезпек ОІД.

Класифікація загроз може бути проведена за безліччю ознак. Найбільш поширені з них наведені в Табл. 1.1 [4].

Таблиця 1.1.

Класифікація загроз

Критерії загроз	**Види загроз**
За видом властивості інформації, що порушується	загрози конфіденційності (витік, перехват, зняття, копіювання, викрадання, розголошення); загрози цілісності (втрата, знищення, модифікація); загрози доступності (блокування);
За характером порушення	порушення конфіденційності даних; порушення працездатності серверів, мережевого обладнання, робочих станцій; незаконне втручання у функціонування серверів, мережевого обладнання, робочих станцій, тощо;
За тяжкістю порушення	незначні помилки; дрібне хуліганство; серйозний злочин / природні і техногенні катастрофи;
За передбаченням наслідків порушника	умисне порушення; ненавмисне порушення;
За мотивацією	зловмисне порушення; незловмисне порушення;
За закінченістю	закінчені; незакінчені;
За об’єктом дії	загрози,націлені на всю інформаційну систему; загрози, націлені на окремі компоненти;
За причиною виникнення	загрози, які виникли через недостачу засобів технічного захисту; загрози, які виникли через недостачу організаційних заходів;

<table>
<tr><td>За походженням</td><td colspan="2">антропогенні;
техногенні;
природні;</td></tr>
<tr><td>За розміром нанесеної шкоди</td><td colspan="2">незначні;
значні;
критичні;</td></tr>
<tr><td>За типовими об’єктами інформатизації</td><td colspan="2">загрози безпеці інформації на базі автономної ЕОМ (без підключення до обчислювальної мережі);
загрози безпеці інформації на базі локальної обчислювальної мережі (без підключення до розподіленої обчислювальної мережі);
загрози безпеці інформації, підключеної до розподіленої обчислювальної мережі;</td></tr>
<tr><td rowspan="4">За способом реалізації загроз безпеці інформації</td><td colspan="2">1) загрози спеціальної дії на інформацію: механічної; хімічної; акустичної; біологічної; радіаційної; термічної; електромагнітної (електричні імпульси, електромагнітні випромінювання, магнітне поле);</td></tr>
<tr><td colspan="2">2) загрози несанкціонованого доступу (НСД)</td></tr>
<tr><td colspan="2">3) загрози витоку інформації технічними каналами:</td></tr>
<tr><td>по радіоканалу;
по електричному каналу;
по оптичному каналу;
по змішаним (параметричним) каналам;</td><td>загрози витоку по каналам побічних електромагнітних випромінювань і наводок(ПЕМВН);</td></tr>
<tr><td rowspan="2">За джерелом загрози</td><td colspan="2">1) створені порушником: внутрішнім;зовнішнім;</td></tr>
<tr><td colspan="2">2) створені апаратною закладкою:</td></tr>
</table>

	вбудованою; автономною;
	3) створені шкідливими програмами: програмні закладки типу «Троянський кінь»; програмні віруси; шкідливі програми, що поширюються мережею (мережеві черви); інші шкідливі програми для здійснення НСД;
За використаною вразливістю системи	з використанням вразливості програмного забезпечення; з використанням вразливості, викликаної наявністю апаратної вкладки; з використанням вразливості, пов'язаної з реалізацією протоколів мережевої взаємодії і каналів передачі даних; з використанням вразливості, викликаної недоліками організації технічного захисту інформації від НСД; з використанням вразливості системи захисту інформації; з використанням вразливості програмно-апаратних засобів при збоях і позаштатних ситуаціях;
За об'єктом взаємодії	1) НСД до інформації, яка обробляється на ЕОМ (вузли обчислювальної мережі): на відчужених носіях інформації; на вбудованих носіях довготривалого зберігання інформації; у засобах обробки і зберігання оперативної інформації; у засобах (портах) вводу (виводу) інформації;
	2) НСД до інформації залежно від її рівня

	мережевої взаємодії: на фізичному рівні; на канальному рівні; на мережевому рівні; на транспортному рівні; на сеансовому рівні; на презентаційному рівні; на прикладному рівні
	3) НСД до інформації користувачів або технологічної інформації залежно від способу доступу: загрози НСД до операційного середовища (до команд, інструкцій); загрози дії на технологічну інформацію, не пов’язані з допуском порушника до команд операційної системи (відмова в обслуговуванні при перевантаженні, збій операційної системи); загрози програмно-математичної дії;

Можлива шкода визначає величину небезпеки.

Державні служби, правоохоронні органи та силові структури деколи не в змозі забезпечити в повному обсязі необхідний рівень безпеки на ОІД одночасно використовуючи сучасні засоби захисту, тому власники ОІД були змушені шукати власні шляхи вирішення проблем безпеки. Одна з таких систем безпеки, що наразі ефективно вирішує одночасно декілька завдань – інтегрована система безпеки.

Виявлення загроз з різних причин виникнення і характеру прояву, автоматизоване реагування на виявлену загрозу, передача інформації про виявлену загрозу ці та інші функції і які завдання вирішує ІСБ на ОІД,розглянемо у наступних розділах.

РОЗДІЛ 2
ОСНОВНІ ПОНЯТТЯ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

Інтегрована система безпеки - це повноцінний програмно-апаратний комплекс високотехнологічних пристроїв, які функціонально взаємопов'язані на всіх рівнях побудови системи безпеки для ОІД.

Інтегрована системи безпеки - це комплекс безпеки об'єкта на єдиній основі. Інтегрована система безпеки (ІСБ) забезпечує захист об'єкта інформаційної діяльності відразу від декількох видів загроз, наприклад, пожежа, злом, крадіжка, проникнення і т.д. [5]

Інтегрована система безпеки - це сукупність функціонально та інформаційно пов'язаних один з одним підсистем безпеки, що працюють за єдиним алгоритмом і мають спільні канали зв'язку, програмне забезпечення, бази даних. [6]

Будь-яке з вищевказаних визначень чітко описує поняття ІСБ отже основною характеристикою цього поняття є багатозадачність, яка працює в комплексі.

ІСБ може бути застосована на найрізноманітніших об'єктах, таких як підприємства, офіси, фабрики чи заводи незалежно від їх сфери діяльності. Також такі системи встановлюють на охоронюваних об'єктах незалежно від їх розміру, чисельності людей або знаходження:

- невеликі об'єкти, такі як склади, магазини, офіси, супермаркети;
- великі промислові об'єкти, такі як заводи, фабрики, електростанції;
- великі адміністративні установи, такі як стадіони, банки, державні установи, вокзали, метро.

ІСБ встановлюються на об'єкті із заздалегідь спроектованою конфігурацією, яка і дозволяє системі виконувати конкретні завдання. Будь-яка система безпеки на об'єкті зі зміною будь-яких істотних параметрів об'єкта, може бути переобладнана або розширена.

Мета ІСБ достатньо проста і передбачає об'єднання всіх окремих підсистем безпеки в єдиний комплекс з підтриманням їх злагодженої та взаємної роботи.

ІСБ нового покоління - це сучасні мережеві системи безпеки з використанням ір-технологій. Такі системи дозволяють здійснювати контроль, управління і доступ до даних по мережі інтернет. Також сучасні ІСБ найчастіше включають в себе:

- пожежну систему, пожежну сигналізацію і систему пожежогасіння;
- охоронну і тривожну сигналізації;
- систему контролю та управління доступом (СКУД);
- систему оповіщення і гучного зв'язку;
- систему охоронного відеоспостереження;
- систему безперебійного живлення;
- систему контролю та моніторингу стану технологічного обладнання;
- систему передачі сповіщень;
- систему організації зв'язку та мережі інтернет, а також закритих конфіденційних телефонних ліній;
- систему обліку відвідувачів та ідентифікації людей;
- системи обліку робочого часу співробітників. [5]

2.1. Основних експлуатаційних можливостей ІСБ

ІСБ повинна відповідати наступним експлуатаційним вимогам:

- модульна структура, що дозволяє забезпечити безпеку як малих, так і дуже великих об'єктів, в тому числі територіально розподілених;

- контроль і управління доступом на охоронюваному об’єкті з урахуванням можливостей кожного співробітника;

- контроль охоронної та тривожної сигналізації на об'єкті;

- контроль пожежної сигналізації на об'єкті;

- відеоспостереження, відеоконтроль і відеореєстрація тривожних ситуацій з графічних планів об'єктів;

- відображення подій на графічних планах об'єктів;

- розробка сценаріїв дій (правил реакції) однієї системи у відповідь на події в іншій;

- управління установками пожежної безпеки;

- управління інженерними системами будівлі;

- імітo стійкість протоколу передачі даних в мережах;

- можливість передачі інформації побудь-яких каналах зв'язку;

- можливість взяття під охорону, зняття з охорони об'єктів за допомогою електронних карт, ключів;

- мовне попередження чергового про тривожні події, можливість запису і відтворення повідомлень;

- відображення стану зон, розділів, точок доступу, приймально-контрольних приладів, зчитувальних пристроїв, відеокамер на графічних планах приміщень з детальним текстовим поясненням;

- розмежування повноважень чергових операторів адміністраторів за рахунок багаторівневої системи паролів і можливого підключення біометричної систем обмеження доступу до програм автоматизованих робочих місць (АРМ);

- протоколювання всіх подій, що відбуваються в системі;

- ведення єдиної бази даних користувачів;

- розвинена діагностика працездатності всіх блоків і пристроїв системи;

- віддалене адміністрування системи;

- збереження загальної надійності системи при інтеграції підсистем;

- висока живучість системи, тобто зберігання її працездатності при виході з ладу окремих підсистем і блоків, а також збереження працездатності окремих підсистем (в рамках їх функцій) при виході з ладу сервера ІСБ або при втраті зв'язку з ним;

- автономна робота контролерів підсистем при порушенні зв'язку з сервером ІСБ. [7]

2.2. Вимоги функціонального призначення ІСБ

ІСБ повинен забезпечувати виконання таких обов 'язкових функцій:

- виявлення загроз, що мають різні причини і характер прояву, відповідно до функціонального призначення систем, що входять до складу ІСБ;

- автоматичне реагування ІСБ на виявлену загрозу здійснюється відповідно до заданої тактики кожної з входящих до його складу систем:

- передачу інформації про характер виявленої загрози на пристрій відображення, призначений для використання наступним оператором;

- забезпечення можливості ручного управління системами, що входять до складу ІСБ;

- ведення електронного протоколу роботи систем, що входять до складу ІСБ, з його реєстрацією в базі даних (БД);

- зміна складу та конфігурації ІСБ відповідно до зміни завдань, що вирішуються ІСБ.

2.3. Функціональний склад ІСБ та загальні вимоги до нього

1. ІСБ повинна включати в себе не менше трьох з таких базових систем: система тривожної сигналізації (СТС); система охоронної сигналізації (СОС);система відеоспостереження (СВ); система контролю управління доступом(СКУД).

2. Склад ІСБ може бути доповнено іншими системами безпеки за ГОСТ Р 53195.1.

3. Системи, що входять до складу ІСБ, повинні забезпечувати виконання своїх функцій як всередині ІСБ, так і автономно.

4. Стан роботи кожної з систем, що входять до складу ІСБ, не повинен заважати роботі інших систем.

5. Відмова (відмова) однієї з систем, що входять до складу ІСБ, не повинна впливати на роботу інших систем.

6. Зміна складу та конфігурації ІСБ шляхом збільшення числа транспортних засобів, що використовуються в кожній з його систем, не повинна призводити до відмови або погіршення функціональних параметрів ІСБ.

7. Пріоритет при передачі аварійних сигналів і відображенні інформації про виявлені загрози в ІСБ повинен віддаватися системам, робота яких спрямована на виявлення загроз, що займають більш високе положення в такому переліку:

• загроза життю і здоров 'ю людини:

• загроза крадіжки, пошкодження або знищення майна.

Виявлення загрози однієї з систем, що входять до складу ІСБ, при необхідності може призвести до автоматичного реагування та інших систем ІСБ. [8]

2.4. Інтеграційна та мережева побудова ІСБ

Способи інтеграції при побудові ІСБ:

• проектування - інтеграція компонентів на стадії проектування системи;

• програмне забезпечення - інтеграція обладнання з використанням програмного забезпечення, спеціально призначеного для інтеграції;

• апаратні та програмні засоби - інтеграція апаратних і програмних засобів, апаратні та програмні засоби працюють в єдиній системі;

• апаратне забезпечення - інтеграція на апаратному рівні. [5]

Інтеграція на рівні проектування (апаратна інтеграція). Інтеграція систем здійснюється на стадії проектування системи для кожного конкретного об 'єкта. Такі роботи виконують проектно-монтажні організації. Як правило, в

цьому випадку використовуються різнорідні підсистеми (системи) різних виробників. Об'єднання (інтеграція) цих підсистем (систем) здійснюється установкою обладнання управління підсистемами (системами) в загальному приміщенні. Взаємодія між підсистемами здійснюється на рівні операторів підсистем (систем), тобто без автоматизації. Очевидно, що це мінімальний рівень інтеграції, він має певні недоліки ("людський фактор", неоднорідність обладнання, складність технічного обслуговування, паралельний зв 'язок, відсутність автоматизації тощо) і його не можна вважати перспективним в даний час, хоча є ряд монтажних організацій, які пропонують свої готові і перевірені проектні рішення.

Варіантом такого типу інтеграції є інтеграція за допомогою релейних контактів, для передачі інформаційних повідомлень між окремими підсистемами (системами) ІСБ.

Переважає простота обладнання, низька вартість, можливість об 'єднання підсистем (систем) різних виробників.

Серед недоліків - обмежені види повідомлень, якими можна обмінюватися підсистемами (системами), проблеми з візуалізацією подій і станом системи в цілому; у міру збільшення числа ретрансляторів і ліній зв 'язку втрачається перевага низьких витрат на продаж. Загальна вартість релейної інтеграції може перевищувати вартість інших типів інтеграції.

Інтеграція на рівні програмного забезпечення (або точніше - на програмно-апаратному рівні з пріоритетом програмної підтримки). У цьому випадку роль об 'єднання підсистем являє собою програмний пакет, розроблений і поставлений як автономний продукт, призначений для роботи в апаратному середовищі, зазвичай в локальній обчислювальній мережі стандартних комп'ютерів, яка є верхнім рівнем ІСБ. Підключення до апаратних засобів підсистем нижнього рівня здійснюється за допомогою програм драйверів, розроблених спеціально для підтримки конкретних апаратних засобів інших виробників. Зв'язок з апаратними засобами здійснюється за допомогою стандартних комп'ютерних портів.

Існує два підходи до створення спеціалізованого програмного забезпечення (ПЗ) для ІСБ:

1) Програмне забезпечення розроблено для власного обладнання і не дозволяє працювати з технічними засобами інших виробників ("закритим" програмним забезпеченням);

2) Програмне забезпечення розробляється як "відкрита" програмна оболонка ("open" software), з можливістю підключення обладнання різних виробників.

Переваги - можливість на програмному рівні, використовуючи всі можливості сучасної комп'ютерної техніки, створювати якісні багатофункціональні програмні системи. Можливість інтеграції з апаратними засобами сторонніх виробників (з відповідним драйвером і відповідними інтерфейсами даних у найбільш часто використовуваних інструментах). Побудова ІСБ для даного типу вимагає меншої кількості ліній зв'язку між підсистемами (системами) порівняно з апаратною інтеграцією.

Недоліки - необхідність розробки драйверів для кожного обладнання, що використовується. Однак розробник апаратних засобів не завжди надає протоколи обміну даними. Навіть якщо протоколи відкриті і задокументовані, вони можуть мати обмежені можливості, які не дозволяють оптимально поєднувати. Крім того, фірма-розробник системи програмного забезпечення, що постачає тільки свій програмний продукт, не може в цьому випадку повністю гарантувати роботу всієї системи в цілому.

Інтеграція на рівні апаратного та програмного забезпечення. Найбільш поширений метод побудови ІСБ. У цьому випадку апаратне та програмне забезпечення розробляються в рамках єдиної системи. Це дозволяє досягти оптимальної продуктивності, так як вся розробка зосереджена, як правило, в одних руках і система як готовий продукт. Оптимальні економічні показники

Недоліком є те, що кожен виробник технічних засобів пропонує свою оригінальну систему, як правило, не сумісну з іншими засобами.[9]

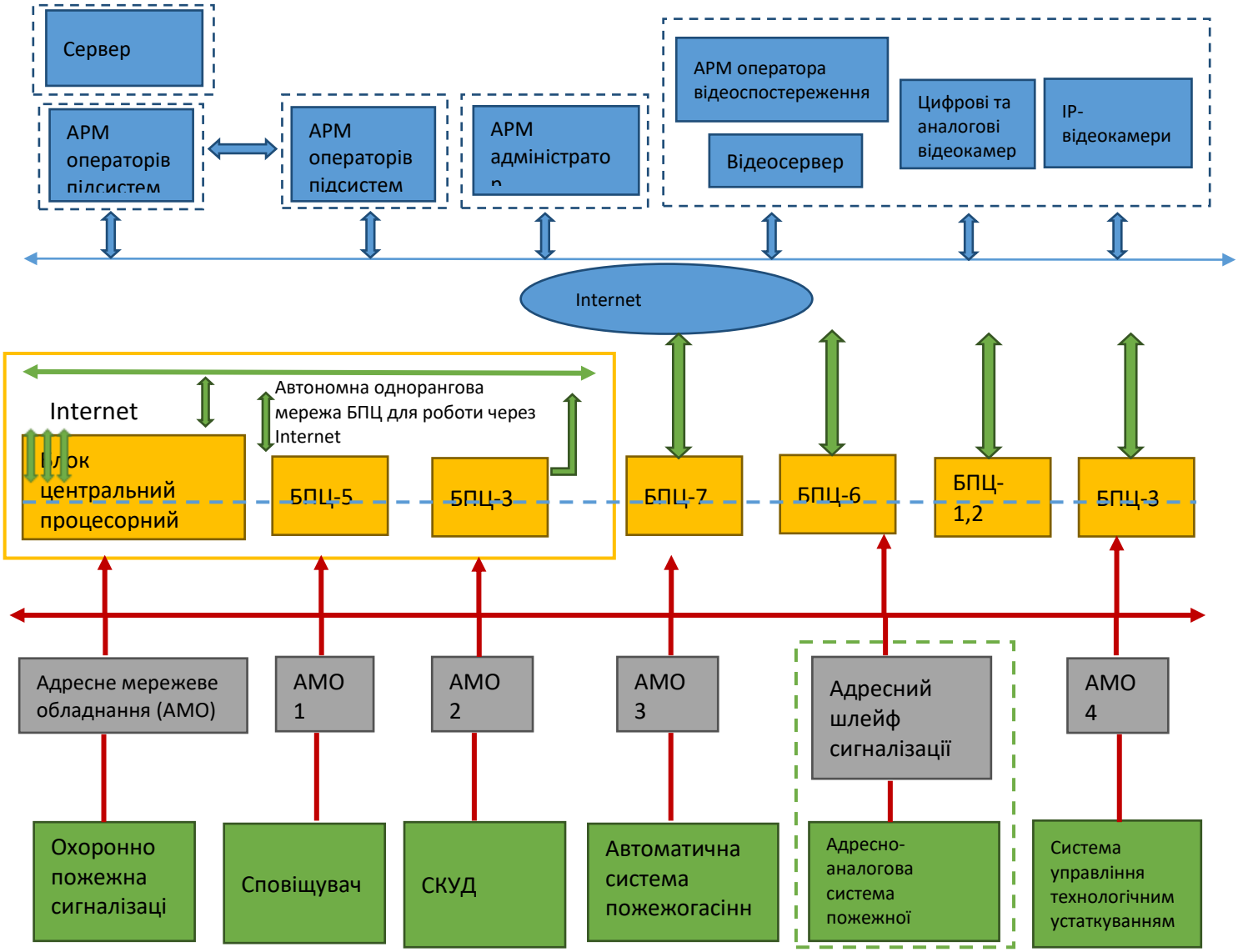

Рис. 1 Побудова ІСБ на мережевому рівні

Перший (верхній) рівень - клієнтсько-серверна комп'ютерна мережа, заснована на мережі Ethernet. Цей рівень забезпечує зв'язок між сервером і робочими станціями операторів. Управління ISB на вищому рівні забезпечується спеціалізованим програмним забезпеченням. Сучасні можливості комп'ютерних мереж дозволяють передавати інформацію по різних каналах зв'язку, таким чином на базі ІСБ можна створити системи моніторингу безпеки віддалених об'єктів.

Другий рівень - рівень локальних контролерів, основних компонентів управління ISB. Кожен контролер повинен забезпечувати виконання функцій у своїй зоні управління, навіть у разі порушення зв'язку з верхнім рівнем ІСБ.

Для зв'язку між однорідними контролерами (горизонтальний рівень зв'язку) використовується інтерфейс RS485 або інші інтерфейси, призначені для побудови мереж промислового рівня з хорошою помехостійкістю і достатньою швидкістю обміну даними.

Третій рівень - це рівень адресованих мережевих пристроїв, які підключаються до кожного контролера другого рівня. Кількість мережевих пристроїв, підключених до одного контролера, може досягати 256. Діапазон адресованих мережевих пристроїв досить різноманітний, від простих подовжувачів для підключення радіальних шлейфних кабелів до складних контролерів третього рівня, таких як пристрої управління пожежею або адресовані аналогові модулі підключення пожежної сигналізації.

Четвертий рівень - сповіщувачі і сповіщувачі, СКУД зчитувачів і виконавчих механізмів, датчики і пристрої управління технологічним обладнанням тощо. Тут, як правило, використовуються нестандартні спеціалізовані інтерфейси і протоколи.

Технічні можливості ІСБ дозволяють визначити подальші перспективи їх розвитку - інтеграції з іншими системами автоматизації та розширення типів і кількості загроз, від яких забезпечується захист за допомогою ІСБ. [10]

2.5. Приклад взаємодії складових ІСБ при виникненні загрози

У разі пожежі "спрацьовує" пожежна сигналізація системи пожежної сигналізації. Сигнал від них передається в ІСБ, який видає сигнал тривоги оператору.

Система відеоспостереження виводить зображення з камер, найближчих до джерела спалаху, на монітор оператора і аналізує зображення за допомогою алгоритмів розпізнавання зображень пожежі або диму.

У разі підтвердження пожежної загрози, за командою оператора або без його участі (за відсутності реакції або певних дій з боку оператора протягом певного часу) система реагує відповідно до зазначених поведінкових сценаріїв

Включається система звукового та світлового оповіщення. Системи контролю доступу розблокують виходи для евакуації людей. Система управління мікрокліматом відключає проточну систему вентиляції, яка обслуговує цю зону для запобігання потрапляння свіжого повітря в осередок загоряння.

Для видалення диму з коридорів, залів, сходів (уздовж шляхів евакуації) включається відповідна підсистема димовидалення (відкриваються заслінки, включаються вентилятори).

Система управління електропостачанням відключає ланцюга електроживлення поблизу зони пожежі.Автоматично включається система аварійного освітлення і так далі.

Ці дії можуть бути забезпечені тільки за рахунок взаємодії окремих систем складної та одноподібної логіки управління комплексом. Саме наявність таких відносин і подієвих моделей дозволяє говорити про дійсно інтегровану систему. При цьому не повинно бути абсолютно ніяких обмежень щодо опису логіки роботи системи - все, що може знадобитися на бетонному об'єкті в конкретних умовах, може бути описано за допомогою ІСБ. [6]

2.6. Переваги та недоліки ІСБ

Переваги ІСБ:

• Можливість інтеграції будь-якого обладнання. Інтеграція можлива як за наявності відкритого загальнодоступного програмного забезпечення, так і на апаратному або транспортному рівні, коли програмного забезпечення для обладнання не існує або воно з якихось причин недоступне.

• Великий набір можливостей взаємодії обладнання між собою.

• Можливість розробки спеціальних програмних функцій у процесі інтеграції.

Недоліки ІСБ:

• Необхідні додаткові ресурси для інтеграції нового обладнання та оновлення драйверів при зміні версій вбудованого ПЗ та обладнання. Це можливо тільки в тому випадку, якщо замовнику необхідно інтегрувати нове обладнання, яке не було інтегровано в нього.

• Іноді доводиться дублювати функціональність відразу в декількох місцях. Наприклад, ведення бази даних пропусків в інтегрованій системі і у вихідній базі підсистеми контролю і управління доступом.

РОЗДІЛ 3

ОСНОВНІ ВИМОГИ ТА ХАРАКТЕРИСТИКА СКЛАДОВИХ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

Інтеграція - це новий підступ до управління об'єктом і побудови систем безпеки.

Об 'єднання різних підсистем в рамках єдиної ІСБ дозволяє максимально ефективно вирішувати проблему комплексної безпеки об'єкта за рахунок їх взаємодії та обміну інформацією. Можна сказати по-різному: окремі підсистеми начебто доповнюють один одного, допомагаючи в кінцевому підсумку вирішити спільну задачу - безпеку.

Інтеграція системи в єдине рішення дозволяє забезпечити комплексний захист об'єктів, що дозволяє:

• мінімізувати витрати на оснащення об'єкта за рахунок інтеграції систем і використання існуючої інфраструктури;

• об'єднання всіх систем безпеки об'єкта в єдине інформаційне середовище, з єдиною базою даних і єдиним підходом до аналізу подій і прийняття рішень;

• встановлювати різні алгоритми взаємодії систем за сигналами один одного: включення камер і запису, закриття/розблокування дверей, включення систем пожежогасіння, сирен тощо, і забезпечувати тим самим значне збільшення функціональності комплексу;

• автоматизувати прийняття рішень у типових ситуаціях;

• провести комплексний автоматизований аналіз даних про події всього комплексу, включаючи порівняльний аналіз показань різних систем щодо обраних подій тощо (наприклад, системи відеоспостереження, охоронної сигналізації та контролю доступу);

• забезпечення оперативного надання достовірних даних керівництву;

• оперативно повідомляти співробітників служби безпеки та координувати їхні дії;

• зменшити обсяг отримуваної оператором інформації і зробити її більш помітною;

• значно знизити ймовірність помилкових дій оператора;

• мінімізувати залежність системи від конкретного виконавця і негативні наслідки людського фактора. [11]

Склад кожної конкретної інтегрованої системи безпеки може змінюватися - доповнюватися якимись новими підсистемами або, навпаки, виключатися із загального переліку. Це залежить від конкретних завдань, визначених на етапі проектування, виходячи з можливостей і потреб окремого ОІД. Базовий набір підсистем, що входять до складу інтегрованої системи безпеки, може бути представлений наступним чином:

- система пожежної сигналізації;
- система охоронної сигналізації;
- система охорони периметра.
- система контролю та управління доступом - СКУД;
- система відеоспостереження (більш продумана з точки зору інтелектуального відеоспостереження);

3.1. Загальні вимоги та характеристики до систем охоронної сигналізації

Система охоронної сигналізації - електрообладнання, що є складовою частиною системи тривожної сигналізації, призначене для виявлення та попередження про напад та/або вторгнення в охоронювані зони або об'єкти. [18]

Складається воно з панелі безпеки (пульта управління) - пристрою, який збирає і аналізує інформацію, отриману від датчиків безпеки. Той самий пульт керування виконує заздалегідь запрограмовані функції, які виконуються при спрацьовуванні датчиків. До складу обладнання також входить пульт управління, що відображає стан сигналізації, службовець для її програмування і здійснює установку та зняття об'єкта із захисту. Мінімальний комплект обладнання також має включати джерело безперебійного живлення (ДБЖ), кабельну мережу і, звичайно, датчики безпеки (рис. 2).

Рис. 2 Охоронні датчики

Датчики бувають декількох видів, залежно від того, на який чинник вони реагують. Найбільш поширені з них – об’ємні інфрачервоні (ІЧ-датчики), магнітоконтактні (геркони), акустичні, вібраційні, ультразвукові, променеві, ємнісні, а також датчики з направленою діаграмою виявлення.

Об’ємні датчики або датчики руху (Рис.3), це неточні назви ІЧ-датчиків, чутливих елементів яких є ПИР елемент. Це сенсор, який уловлює теплове випромінювання. Картинку він бачить як би розбиту на сектори, за допомогою лінзи Френеля. І якщо теплова пляма рухається, з сектора в сектор відбувається спрацювання. Серед таких датчиків є моделі, які можуть розрізняти людину і домашніх тварин за розміром теплового плями. Ці датчики не дуже дорогі і досить надійні. Охоронні сигналізації з такими датчиками часто використовуються для захисту квартир та житлових будинків.

Рис. 3 Об’ємні датчики

Магнітоконтактні (геркони) датчики (Рис.4)в основному застосовуються на першому рубежі охорони. Вони встановлюються на дверях і вікнах і відстежують їх відкриття або закриття. Два магніти встановлюються напроти один одного: один на рухомої частини дверей або вікна, а інший на нерухомій його частині. Коли контакт між двома магнітами втрачається, датчик негайно передає сигнал на контрольну панель. Цей тип датчиків найдешевший, дуже надійний і з мінімальним споживанням струму.

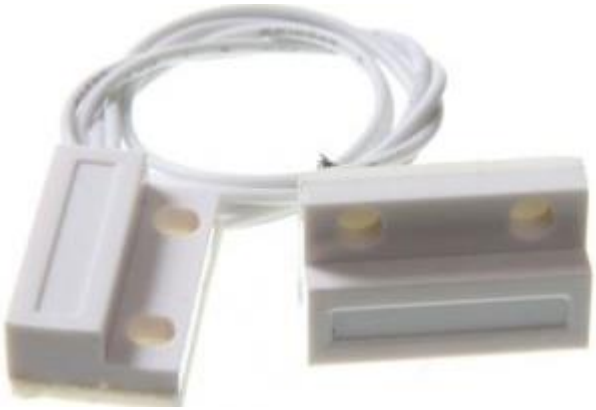

Рис. 4 Магнітоконтактні датчики

Акустичні датчики реагують на гучний звук - у тому числі на звук розбитого скла. Найсучасніший з них має мікропроцесор, який аналізує схему звуку і не плутає звук розбитого скла з іншим різким звуком. Крім того, пам 'ять таких датчиків містить звуки розбивання різних типів скла. Це може бути

звичайне скло, армоване скло, триплекс. Цей фактор значно знижує можливість випадкової роботи системи безпеки.

Датчики променя використовуються для покриття великих просторів і складаються з приймача і передавача. Коли невидимий промінь перетинається неозброєним оком, він запускається. Це досить дорогі і примхливі датчики використовуються в основному для захисту периметра. Вони розміщені вздовж паркану або паркану, і працюють постійно у всіх погодних умовах. [19]

3.2. Характеристики та загальні вимоги до систем пожежної сигналізації

Система пожежної сигналізації та оповіщення призначена для виявлення пожежі якомога раніше і подачі сигналу тривоги для вжиття необхідних заходів (наприклад, евакуація людей, виклик пожежної служби, запуск засобів пожежогасіння, управління пожежними дверима, арматурою і вентиляторами).

Система пожежної сигналізації може бути активована автоматично або вручну.

Система пожежної сигналізації та оповіщення повинна:

— надійно передавати сигнал виявлення пожежі у влаштування прийому та управління пожежею та, по можливості, до пункту спостереження за пожежею;

— швидко виявити ознаки пожежі для виконання свого цільового призначення;

— не реагувати на інші явища, за винятком тих, на які він повинен реагувати за призначенням;

—негайно і чітко сигналізує про виявлену несправність, яка може негативно позначитися на нормальній роботі системи;

— перетворити цей сигнал на чіткий сигнал тривоги, який відразу і безпомилково привертає увагу людей. [20]

3.3. Загальні вимоги та характеристики досистеми контролю і управління доступом

Система контролю та управління доступом (СКУД) - сукупність програмно-апаратних та організаційно-методичних засобів, що вирішують проблему контролю та управління приміщеннями та окремими приміщеннями ОІД, а також оперативного контролю за переміщенням осіб та їх перебуванням в ОІД. [12]

Сучасна СКУД являє собою об’єднані в комплекси електронні, механічні, електротехнічні, апаратно-програмні засоби, що забезпечують можливість доступу певних осіб в певні зони (територія, будівля, приміщення) або до певної апаратури, технічних засобів і предметів, і які обмежують доступ особам, які не мають такого права. Такі системи можуть здійснювати контроль переміщення осіб і транспорту по території об’єкту, що охороняється, забезпечувати безпеку персоналу і відвідувачів, а також збереження матеріальних та інформаційних ресурсів ОІД.

3.3.1. Основні можливості СКУД

Система контролю доступу об'єкту повинна забезпечувати:

– доступ до ОІД – по електронній карті-пропуску;

– доступ до ОІД– по електронній карті-пропуску і коду, що набирає на клавіатурі зчитувача;

– вихід з ОІД з використанням карти-пропуску або кнопки виходу;

– видачу сигналу тривоги в приміщення охорони (пультову) у разі несанкціонованого проникнення в зони доступу (злом, не закриття дверей; спроба підбору коду);

– примусове розблокування (з обов'язковим розбиванням захисного скла або автоматичне з пульта оператора) на випадок пожежі або іншій

екстреній ситуації дверей евакуаційних виходів, якщо вони оснащуються засобами контролю доступу з реєстрацією цих фактів на сервері СКУД;

– облік, реєстрацію і документування фактів проходу осіб в місцях установки пристроїв СКУД з вказівкою дати і часу проходу;

– створення і ведення бази даних на всіх осіб (співробітники/персонал), з введенням в неї паспортних і інших даних, кольорових фотографій, а також її оперативне коректування;

– доступ до бази даних і архіву, а також видачу довідок по ним з документуванням на принтері і екрані монітора оператора системи на вимогу користувача залежно від рівня доступу. Рівні доступу до бази даних і архіву системи визначаються власником ОІД і можуть змінюватися в ході експлуатації системи;

– облік, реєстрацію і документування дій оператора;

– резервування журналу подій і бази даних співробітників на накопичувачі на магнітній стрічці.[13]

3.3.2. Основні компоненти СКУД

На сьогоднішній день існує безліч типів СКУД від різних виробників, а також її компонентів. Незважаючи на унікальність кожної конкретної системи контролю доступу, вона містить 4 основні елементи:

- Ідентифікатор користувача (картка пропуск, ключ, біометричні дані);
- Контролер управління;
- Пристрій ідентифікації;
- Виконавчі механізми.

Ідентифікатор користувача - це пристрій або функція, що ідентифікує користувача. Для ідентифікації використовуються атрибути та біометричні ідентифікатори. Як ідентифікатори атрибутів використовуються автономні

носії знаків допуску: магнітні картки, безконтактні карти, клавіші TouchMemory, різні клавіші. Як біометричні ідентифікатори використовуються: зображення райдужки, відбитка пальця, відбитка долоні, риси обличчя та багато інших фізичних особливостей. Кожен ідентифікатор характеризується унікальним двійковим кодом. В СКУД кожен код співставляється з інформацією про права та привілеї власника ідентифікатора.

Пристрій зчитування карт (пристрій ідентифікації) передає інформацію в схему обробки сигналів контролера. Далі інформація в цифровому вигляді видається в схему прийняття рішення, яка вводить факт спроби переходу в схему буфера подій, запитує схему бази даних про законність проходження і в разі позитивної відповіді запускає виконавчий механізм.

Контролери - пристрої, призначені для обробки інформації від зчитувачів ID, прийняття рішень і управління виконавчими пристроями. Саме контролери дозволяють проходити через контрольні точки. Контролери розрізняються за ємністю бази даних і буферу подій, що обслуговується пристроями ідентифікації.

Виконавчі механізми - замки, турнікети, шлагбауми, ворота. Після зчитування інформації з карти (або іншого пристрою ідентифікації) контролер порівнює її зі своєю базою даних і вирішує: давати або не давати команду виконавчому пристрою.

"Датчик положення дверей" - для правильної роботи СКУД контролер повинен розуміти, що відбувається в "захищеній зоні": відкриті або закриті двері; якщо відкрито, то як довго; чи був турнікет повернутий після прочитання, і в якому напрямку був піднятий або опущений бар'єр і т.д. Наявність датчиків положення відрізняє показання, після яких нічого не відбувалося, від "фактичного проходження", і додає функції безпеки, оскільки будь-яке відкриття - як штатне, так і нестандартне - фіксується системою.

Допоміжне обладнання - джерела безперебійного живлення, датчики, кнопки, електропроводка тощо.

Програмне забезпечення - здійснює конфігурування та управління обладнанням, контроль його параметрів, систематизацію та архівування всієї системної інформації. Він також підтримує обмін даними між контролерами та комп'ютерним моніторингом, контроль доступу та моніторинг пунктів пропуску, роботу з базами даних та реєстрацію власників посвідчень особи, дозволяє візуально ідентифікувати власників "електронних перепусток" на пункті пропуску та для формування різних звітів, а також виконувати додатковий набір функцій. [12]

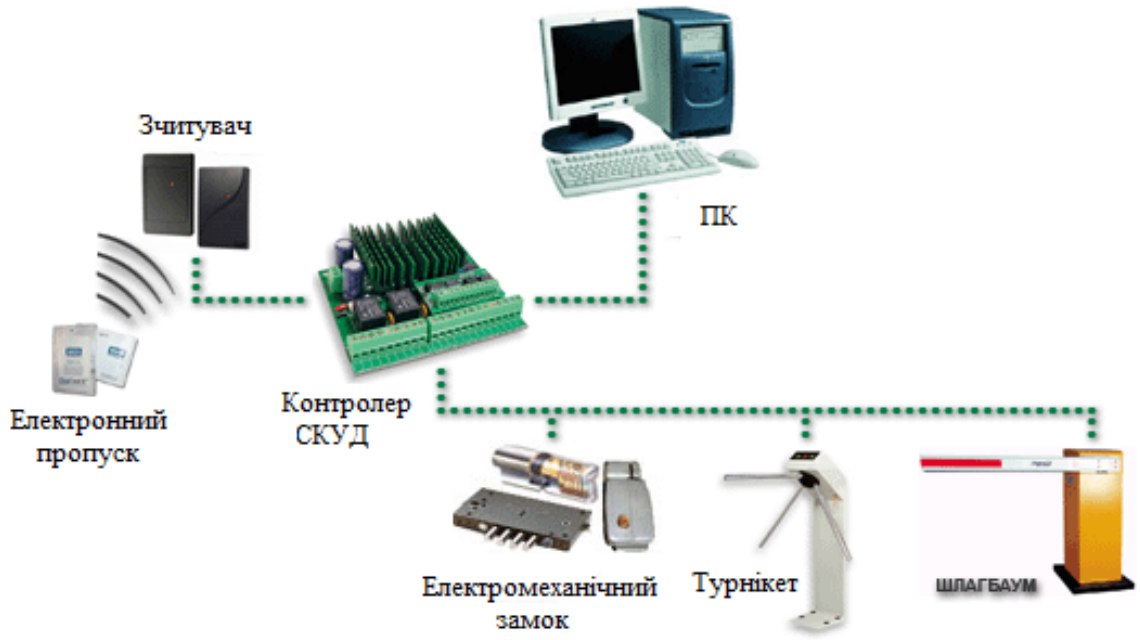

Рис. 5Схема найпростішої системи СКУД

3.3.3. Вимоги до систем контролю управління доступом

СКУД повинна складатися з пристроїв перегороджуючих керованих (ППК) у складі конструкцій перегородки і виконавчих механізмів; пристрої введення ідентифікаційних ознак (ПВІО) до складу зчитувачів та ідентифікаторів; пристрої керування (ПК) у складі апаратного та програмного забезпечення.

Зчитувачі та пульти управління обладнані: основними та службовими входами; контрольно-пропускні пункти; приміщення, в яких

безпосередньо зосереджені матеріальні цінності; приміщення для управління; інші приміщення. Допуск працівників і відвідувачів до ОІД через пункти контролю доступу повинен здійснюватися в будівлі та офісних приміщеннях - на одній основі; входи в зони обмеженого доступу (цінності, сейфи, приміщення для зберігання зброї) - не менше двох знаків упізнання.

СКУД повинна забезпечувати такі основні функції:

- відкриття ППК при зчитуванні розпізнавального ознаки, доступ до якого дозволений в даній зоні доступу (приміщеннях) в заданий інтервал часу або за командою оператора СКУД;
- авторизована зміна (додавання, видалення) ідентифікаційних ознак у ПК та їх зв'язок із зонами доступу (приміщеннями) та тимчасовими інтервалами доступу;
- заборона відкривати ППК при зчитуванні розпізнавальної ознаки, доступ до якого в даній зоні доступу (приміщенні) в заданий інтервал часу заборонений;
- захист від несанкціонованого доступу до програмного забезпечення ПК для зміни (додавання, видалення) функцій ідентифікації;
- збереження налаштувань і бази даних ідентифікаційних характеристик при відключенні живлення; ручне, напівавтоматичне або автоматичне відкриття пульта управління проходом при аварійних ситуаціях, пожежах, технічних несправностях відповідно до правил, встановлених режимом і правил пожежної безпеки;
- захист технічних засобів та програмного забезпечення від несанкціонованого доступу до органів управління, режимів та інформації;
- збереження налаштувань і бази даних ідентифікаційних характеристик при відключенні живлення; ручне, напівавтоматичне або автоматичне відкриття пульта управління проходом при аварійних ситуаціях, пожежах, технічних несправностях відповідно до правил, встановлених режимом і правил пожежної безпеки;

- автоматичне закриття ППК за відсутності факту проходу через певний час після зчитування дозволеної розпізнавальноїознаки;
- видача тривожного сигналу (або блокування ППК на певний час) при спробі вибору ідентифікаційних ознак (коду);
- протоколювання та реєстрація поточних і тривожних подій;
- автономна робота зчитувача з ППК в кожній точці доступу при відмові зв'язку з ПК.

На об'єктах підприємства, де потрібен контроль за збереженням виробів, необхідно встановити СКУД, що контролює несанкціоноване зняття цих виробів з ОІД на спеціальних розпізнавальних знаках.

ППК з виконавчими механізмами повинні забезпечувати:

– часткове або повне перекриття прохідного отвору;

– блокування людини всередині ППК (для замків, прохідних кабін);

– автоматичне і ручне (в аварійних ситуаціях) відкриття;

– необхідна пропускна здатність.

Зчитувачі ПВІО повинні забезпечувати:

– зчитування ідентифікаційної мітки з ідентифікаторів;

– порівняння введеної ідентифікаційної ознаки зі зберіганням у пам'яті або базі даних ПК;

– генерують сигнал для відкриття панелі керування при ідентифікації користувача;

– обмін інформацією з ПК.

ПВІО повинні бути захищені від підробки шляхом пошуку або ідентифікації.

Ідентифікатори ПВІО повинні забезпечувати збереження розпізнавальних знаків протягом усього терміну їх служби для ідентифікаторів без вбудованих батарей і не менше 3 років для ідентифікаторів з вбудованими батареями.

Оформлення, зовнішній вигляд і написи на ідентифікаторі та зчитувачів не повинні призводити до розкриття використовуваних кодів.

КП має забезпечувати:

– прийому інформації від ПВІО, її обробки, відображення в заданому вигляді та формування сигналів управління ППК;

– ведення електронного журналу реєстрації проїздів працівників та відвідувачів через пункти доступу;

– ведення баз даних співробітників та відвідувачів ОІД з можливістю зазначення характеристик їх доступу (код, інтервал часу доступу, рівень доступу тощо);

– пріоритетний висновок інформації про аварійні ситуації в точках доступу;

– контроль справності та стану ППК, ПВІО та ліній зв'язку з ними.[12]

3.4. Загальні вимоги та характеристика до системи відеоспостереження

Системи відеоспостереження (СВС) - програмно-апаратний комплекс (відеокамери, об'єктиви, монітори, реєстратори та інше обладнання), призначений для організації відеоспостереження як на місцевих, так і на географічно розподілених об'єктах. [14]

Система відеоспостереження призначена для візуального контролю обстановки по периметру об'єкта і в його інтер'єрі за допомогою телевізійного обладнання.

Система зазвичай включає в себе:

· внутрішні та зовнішні (поворотні та стаціонарні) відеокамери для прийому відеозображення;

· Пристрої обробки та перетворення відеозображення;

· Обладнання відеозапису та відтворення;

· Обладнання для управління та комутації відеосигналів.

Система повинна записувати візуальну і службову інформацію з відеокамер на відеомагнітофони і переглядати цю інформацію як на телевізійних моніторах. [13]

3.4.1. Основні компоненти системи відеоспостереження

1. Відеореєстратор

Основним пристроєм системи відеоспостереження можна назвати відеореєстратор (рис.6). Це обладнання підключено до відеокамер, органів управління, виконавчих механізмів і різних датчиків. Образ записується на жорсткий диск. Кількість можливих днів запису залежить від ємності цього диска. Зазвичай період запису становить від 5 до 21 дня. Можна записувати зображення з камер 24 годин на день або за розкладом або виявленням руху. Відеореєстратор може бути підключений до локальної комп'ютерної мережі або Інтернету за допомогою Інтернету.

Відеореєстратор має панель керування для відтворення та вилучення записаної інформації. Для зручності передбачені пульти дистанційного керування або USB-миші.

Рис. 6 Відеореєстратори

2. Відеокамери

Важливим елементом системи відеоспостереження є камери відеоспостереження (рис. 7). Вони показують кольорове або чорно-біле зображення вночі. Вони відрізняються за конструкцією. Є камери, які

призначені для роботи тільки при кімнатній температурі і, відповідно, для установки в приміщенні. А є зовнішні камери, які встановлені зовні і вони призначені для цілодобової роботи під дощем, снігом або сонцем. Для роботи в темряві випускаються камери з ІЧ-підсвічуванням. Є багато камер різного дизайну - від міні до великих роботизованих камер різного кольору і дизайну.

Однак їх слід розділити на аналогові та цифрові (IP-камери). Аналогові - це звичайні камери, які сьогодні поступаються за якістю зображення цифровим камерам і вже 5MP. 2592x1520 пікселів. IP-камери дозволяють підключати їх до комп'ютерної мережі і передавати зображення високої роздільної здатності в професійних камерах 6 Мп. 3072x2048 пікселів і є навіть 12 мегапіксельних камер.

Рис. 7 Відеокамери

3. Джерела живлення для системи відеоспостереження

Для того, щоб камера почала показувати зображення, необхідно подавати на неї харчування за допомогою спеціальних джерел живлення для відеоспостереження (рис.8). Вони можуть бути як змінним, так і постійним струмом, різним навантаженням і конструктивним виконанням. Є

трансформаторні та комутаційні джерела живлення, джерела безперебійного живлення з перезаряджуваною батареєю. Визначте тип і характеристики блоків живлення безпосередньо для підключення до певних моделей відеокамер. Багато в чому вибір правильного джерела живлення важливий, щоб уникнути проблем з перешкодами на екрані монітора і захистити систему відеоспостереження від стрибків.

Рис. 8 Джерела живлення для системи відеоспостереження

4. Кришки і кронштейни

Для установки і монтажу камер на вулиці передбачені герметичні кришки і кронштейни (рис. 9). При використанні при низьких температурах використовуються нагрівальні елементи, при високих - система охолодження. Щоб уникнути пошкоджень пропонується антивандальний герметик. За допомогою кронштейнів можна прикріпити відеокамеру до стелі, стіни або кута. Хоча це велика рідкість, сучасні камери вже оснащені стаціонарним кожухом, що відповідає всім вимогам стабільної роботи в суворих умовах. [15]

Рис. 9 Кожухи і кронштейни

5. Дротове і бездротове середовище передачі інформації

Дротові лінії передачі інформації

а.) Вита пара (Twistedpair) - інформаційний кабель, що являє собою віту пару мідних проводів (або кілька пар проводів), поміщених в екрановану оболонку. Пари проводів скручені разом для зменшення вигинів. Вітаючи пара досить шумостійка. Існує два типи цього кабелю: неекранована витая пара UTP і екранована витая пара STP. Кабель використовується для передачі даних зі швидкістю 10-100 Мбіт/с.

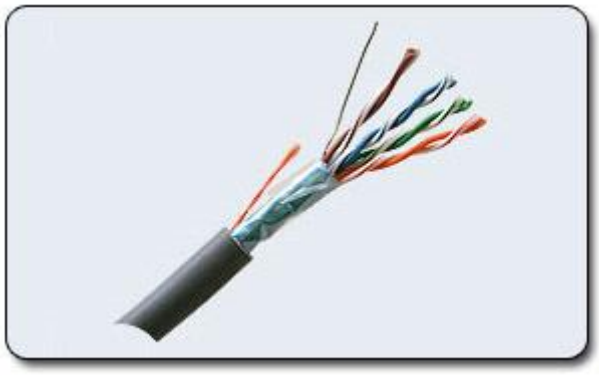

Рис. 10Графічне зображення кабелю типу «вита пара»

б.) Коаксіальний кабель(coaxialcable) - кабель з центральним мідним проводом, який оточений шаром ізоляційного матеріалу з метою відокремлення центрального провідника від зовнішнього екрану (мідної оплетки або шару алюмінієвої фольги). Існує два типи коаксіального кабелю: тонкий коаксіальний кабель діаметром 5 мм і товстий коаксіальний кабель діаметром 10 мм. Коаксіальний кабель більш екранований від перешкод, ніж витаючи пара, і зменшує власне випромінювання. Пропускна здатність - 50-100 Мбіт/с.

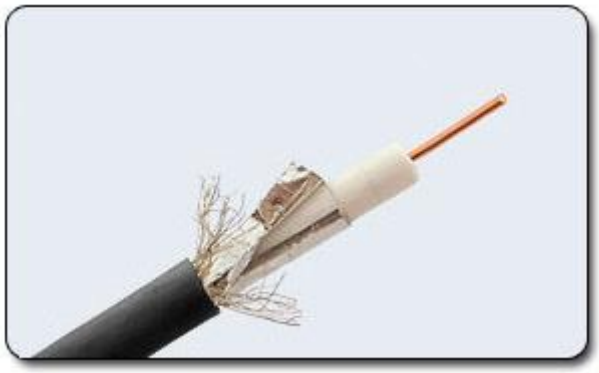

Рис. 11Графічне зображення коаксіального кабелю

в.) Волоконно-оптичний кабель (fiberoptic) - оптичне волокно на основі кремнію або пластику, розміщене в матеріалі з низьким показником заломлення, який закритий зовнішньою оболонкою. Оптичне волокно передає сигнали тільки в одному напрямку, тому кабель складається з двох волокон. На передавальному кінці волоконно-оптичного кабелю потрібне перетворення електричного сигналу на світло, а на приймальному кінці зворотне перетворення. 3Gbps швидкості передачі даних.

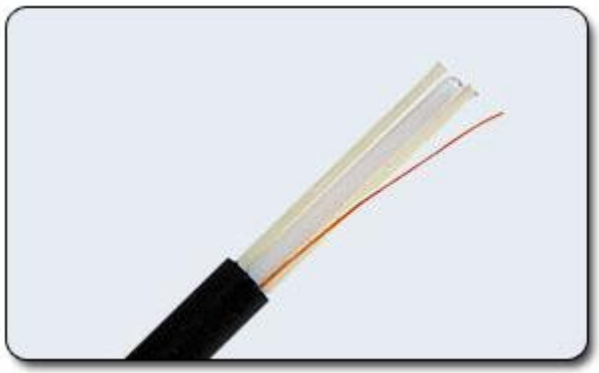

Рис. 12Графічне зображення оптоволоконного кабелю

Бездротові лінії передачі

Останнім часом для передачі відео широко використовуються локальні комп'ютерні мережі. Для цих цілей існують спеціальні мережеві цифрові камери з вбудованим модемом і внутрішнім мінісервером. Для створення цифрових файлів використовуються сучасні методи стиснення зображень JPEG та M-JPEG. Таким камерам можна призначити власну IP-адресу і реалізувати віддалений доступ для відеоспостереження по локальній комп'ютерній мережі. Для охоронних систем відеоспостереження існують спеціальні відеосервери, які не тільки забезпечують сигнали перемикання з різних камер, а й записують інформацію на вбудований жорсткий диск. За допомогою звичайного комп'ютера можна переглядати зображення однієї або декількох камер, як реальних, так і архівованих. [12]

7. Монітори відеоспостереження

Монітори відеоспостереження є інтерфейсним пристроєм для виведення відеосигналів з камер або відеомагнітофонів.

Монітори охоронного відеоспостереження забезпечують потокову передачу відео в реальному часі і відтворення архіву відео.

Очевидно, що при організації системи відеоспостереження охоронці приділяють велику увагу вибору камер відеоспостереження, а заодно і зовсім забувають, що важливі і характеристики моніторів відеоспостереження. Якість монітора для відеоспостереження має бути на високому рівні.

Для систем відеоспостереження використовуються спеціальні монітори. Монітори відеоспостереження відрізняються від неспеціалізованих телевізійних прийомників багатьма технічними характеристиками. Перш за все, це можливість цілодобової безперебійної роботи. У металевих корпусах також є монітори відеоспостереження для захисту від зовнішніх електромагнітних полів і зниження ризику загоряння.

Монітори відеоспостереження вважаються промисловими пристроями, і на відміну від домашніх телевізорів мають більше роз'ємів для підключення різних пристроїв, у тому числі пристроїв обробки відео.

Сучасні монітори відеоспостереження розраховані на безперебійну роботу 24 годин на добу, 7 днів на тиждень.

За колірними характеристиками зображення всі монітори для відеоспостереження можна розділити на:

• чорно-білі монітори відеоспостереження;

• кольорові монітори відеоспостереження.

Монохромні монітори відеоспостереження мають кращу роздільну здатність і контрастність, а також більш доступні за ціною.

Кольорові монітори для охоронного відеоспостереження дозволяють краще ідентифікувати різні об'єкти відеоспостереження, а також розрізняти кольори, тони і відтінки зображення. Вибір між цими двома типами відеомоніторів повністю залежить від завдань, що стоять перед системою відеоспостереження. [17]

8. Інфрачервоні прожектори

Сучасні вуличні камери доступні з вбудованим інфрачервоним підсвічуванням. Завдяки інфрачервоним світлодіодам зображення, яке практично непомітне для людського ока, захоплює чутлива електроніка камери. Ці світлодіоди, залежно від потужності, можуть світитися променем 10-100 м. Коли потрібно організувати освітлення в невидимому ІЧ-діапазоні для вирішення різних завдань, вони використовують окремі прилади - ІЧ-прожектори. Зазвичай вони встановлюються поруч з камерою і "освітлюють" зону спостереження. Чим вища потужність світлодіодів, тим далі і ширше може бути передбачено освітлення. [15]

Рис. 13 ІЧпрожектори

3.4.2. Вимоги до системи відеоспостереження

З практичної точки зору система відеоспостереження повинна відповідати наступним вимогам:

1. При монтажі та проектуванні елементів систем літака необхідно враховувати поле зору необхідної ділянки, тобто без об 'єктів і ділянок, що не представляють інтересу.

2. Камери ВС повинні бути встановлені попарно з датчиками руху так, щоб їх включення і включення в робочий відеозапис відбувалося як наявність рухомих об'єктів в полі їх зору.

3. При проектуванні бортової системи необхідно розрахувати необхідну кількість встановлених відеокамер в частині створення контролю якості території, що охороняється.

4. У встановлених системах ВС має бути забезпечена досить хороша якість запису, що має забезпечити безвідмовну ідентифікацію осіб, які незаконно проникли на об'єкт, а також впізнаваність дрібних деталей на об'єкті в будь-який момент.

5. Архівування даних відеозапису має бути достовірним, а також повністю виключати можливість пошкодження або втрати відеозйомки, знятої встановленими камерами.

6. Діюча система ВС повинна своєчасно обслуговуватися і проходити профілактичний огляд для виключення відмови його елементів, для якісного відображення знятого відео на моніторах системи.

7. Встановлення і відображення дати і часу відеозапису, і за яким він був виконаний, повинні постійно і надійно контролюватися в бортовій системі.

8. Бездротова система ВС, базована на використанні IP-камер або GSM-камер ВС, повинна бути оснащена системою шифрування і захисту конфіденційної відеоінформації від можливого перехоплення третіми особами.

9. Для забезпечення конфіденційності записаної відеоінформації доступ до її архіву і поточного перегляду повинен бути обмежений вузьким колом осіб.

3.5. Характеристики та загальні вимоги до системи охорони периметра

В даний час існує широкий спектр засобів виявлення периметра, які використовують різноманітні фізичні принципи і ймовірності для визначення факту проникнення людини в охоронювану зону.

Той чи інший тип сигналізації по периметру (і, можливо, поєднання декількох типів) вибирається залежно від типу огорожі, рослинності, рельєфу місцевості, кліматичних умов і різних інших факторів.

Найбільш часто використовувані системи, які використовують:

· ємнісні датчики;

· ультразвукові датчики;

· інфрачервоні датчики;

· датчики вібрації;

· мікрохвильові датчики;

· кабель датчика та датчики тиску;

РОЗДІЛ 4

МЕТОДИКА ОЦІНКИ РІВНЯ ЗАХИСТУ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ З ВИКОРИСТАННЯМ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

Для систематичного аналізу ІСБ та ефективності його роботи з ОІД, а також для розуміння необхідності вдосконалення його компонентів пропонується розробити методологію оцінки ефективності ІСБ в цілому. Як видно з практики, досі не було винайдено правильного підходу для оцінки ефективності безпеки на ОІД за рахунок будь-якої з систем, щоб дати повну картину функціональності процесів у системі. У зв'язку з цим пропонується провести оцінку ефективності ІСБ на основі процесу самооцінки, що допоможе охопити і описати всі аспекти безпеки на ОІД з різних сторін. Метод самооцінки допоможе скласти загальну картину безпеки і виявить недоліки, які потребують вдосконалення/вдосконалення.

Ця методика складається з восьми критеріїв: складність, функціональність, розмір, швидкість, відмовостійкість, масштабованість, взаємодія із зовнішніми системами, розширюваність, всі ці критерії оцінюються в таблиці 4.1.

У методиці пропонується використовувати математичний апарат, що використовує метод терезів. Цей метод заснований на наступному. Ці вісім критеріїв використовуються для оцінки кожного .

Для кожного з критеріїв вводяться ваги. Розраховується показник допомоги для кожного ІСБ, який визначається як сума множень значущості критеріїв на вагу обраного критерію:

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

де:

a_i – вага критерію.

Для побудови оптимальних варіантів системи на цьому морфологічному наборі будемо використовувати метод повного перебору. Суть методу полягає в тому, що розраховуються вигоди і витрати на реалізацію всіх варіантів ІСБ і вибирається необхідна кількість кращих з точки зору співвідношення витрат і доль. Всього таких варіантів в даному випадку:

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

де:

M_i – кількість альтернатив у даному критерії.

На основі отриманих даних методом повного перебору представлені кращі варіанти реалізації системи фізичної безпеки. Пошук виконується цільовою функцією:

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

Де:

f_i - показникІСБ:

C_i - вартість ІСБ.

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

Таблиця 4.1

Критерії оцінювання інтегрованих систем безпеки

Комплексність (середньозахищений ОІД має включати не менше 2 систем безпеки)		
Оцінка	Опис	
1	Об'єднує менше трьох систем	система пожежогасіння, система відеоспостереження
2	Об'єднує від 2 до 3 систем	система пожежогасіння, система відеоспостереження, СКУД, система охоронної сигналізації
3	Об'єднує більше 3 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 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	Присутня	ІСБ забезпечує можливість обміну інформацією на програмному рівні із зовнішніми системами інших виробників.
2	Відсутня	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 ефективності системи – менше 8 балів
- Середній рівень ефективності системи – від 9 до 15 балів
- Високийрівень ефективності системи – від 16 до 21 балів

Оцінка рівня захисту інформації наОІД за допомогою використання ІСБ шляхом визначення величини ризику для кожної пари вразливостей/загроз відіграє важливу роль у визначенні надійності ІСБ.

Створення переліку параметрів, перевірка яких дозволяє визначити ефективність підсистем ІСБ. Визначення проводиться на основі оцінки ймовірності реалізації загрози для ОІД, яка може використовувати вразливість і оцінку наслідків реалізації загрози ІСБ.

Оцінка ризиків складається з шести етапів:

1. Виявлення слабких місць у підсистемі - вразливостей, які можуть бути використані загрозою, і створення відповідних пар вразливостей/загроз для ІСБ;

2. Виявлення потенційних небезпек - загроз;

3. Виявлення існуючих ІСБ, які можуть знизити ризик загрози, що використовує певні вразливості в системах безпеки;

4. Визначення ймовірності загрози використання пов'язаної з нею вразливості з урахуванням існуючих підсистем ІСБ;

5. Визначення серйозності несприятливих наслідків або рівня впливу на ОІД у разі загрози, що використовує пов'язану з цим уразливість;

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

Крок 1-й - Визначеннявразливостей

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

Уразливості виявляються в таких областях:

• ОІД в цілому;

• Процеси і процедури;

• Фізичне середовище;

• Конфігурація програмно-апаратного забезпечення, апаратного забезпечення, програмного забезпечення або телекомунікаційного обладнання;

• Залежність від зовнішнього ОІД.

• Персонал;

Крок 2 - Виявлення загроз

Загрози можуть завдати шкоди ресурсам ОІД, включаючи інформацію, персонал, замовників, обладнання, процеси, програмне та апаратне забезпечення тощо. Загрози можуть бути природними і людськими джерелами і можуть бути випадковими або навмисними (класифікація загроз наведена в розділі 2).

На ОІД виявляються як випадкові, так і навмисні джерела погроз.

Для кожної вразливості, яка була виявлена на попередньому етапі і використання (експлуатація) якої може призвести до реалізації загрози, виявляються загрози.

Крок 3-й - ВизначенняіснуючихІСБ, 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 загрози полягає в тому, наскільки легко загроза може використовувати вразливість. Ймовірність реалізації загроз має оцінки ймовірності, наведені в Таблиці 3.

Таблиця 4.2

Ймовірність реалізації загрози

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 наОІД увипадку реалізації загрози, що експлуатує пов'язану вразливість

Визначаючи тяжкість негативних наслідків або рівень впливу у разі загрози (для кожної пари загроза/вразливість), необхідно оцінити вплив на такі властивості інформаційних ресурсів ОІД, наприклад - конфіденційність, цілісність, доступність;

Оцінка впливу на цілісність, доступність, конфіденційність і спостережливість наведена в Таблиці 4.

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:

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

$ВР_{з,в}$- 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.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

5.1. Основні поняття, терміни та визначення у галузі охорони праці

Однією зі специфічних форм людської діяльності є трудова діяльність, під якою розуміється не лише праця в класичному її розумінні, а будь-яка діяльність (наукова, творча, художня, надання послуг тощо), якщо вона здійснюється в рамках трудового законодавства.

Важкість та напруженість праці є одними з головних характеристик трудового процесу.

Під час виконання людиною трудових обов‘язків на неї діє сукупність фізичних, хімічних, біологічних та соціальних чинників. Ці чинники звуться виробничим середовищем.

Сукупність чинників трудового процесу і виробничого середовища, які впливають на здоров‘я і працездатність людини під час виконування нею трудових обов‘язків складають умови праці.

Під безпекою розуміється стан захищеності особи та суспільства від ризику зазнати шкоди.

Реальне виробництво супроводжується шкідливими та небезпечними чинниками (факторами) і має певний виробничий ризик. Виробничий ризик – це ймовірність ушкодження здоров‘я працівника під час виконання ним трудових обов‘язків, що зумовлена ступенем шкідливості та/або небезпечності умов праці та науково-технічним станом виробництва.

Поділення несприятливих чинників виробничого середовища на шкідливі та небезпечні зумовлене різним характером їх дії на людський організм, тим, що вони потребують різних заходів та засобів для боротьби з ними та профілактики викликаних ними ушкоджень, а також рядом причин організаційного характеру. В той же час між шкідливими та небезпечними виробничими факторами інколи важко провести чітку межу. Один і той же

чинник може викликати травму і профзахворювання (наприклад, високий рівень іонізуючого або теплового випромінювання може викликати опік або навіть призвести до миттєвої смерті, а довготривала дія порівняно невисокого рівня цих же факторів – до хвороби; пилинка, що потрапила в око, спричиняє травму, а пил, що осідає в легенях, – захворювання, що зветься пневмоконіоз). Через це всі несприятливі виробничі чинники часто розглядаються як єдине поняття – небезпечний та шкідливий виробничий фактор (НШВФ).

За походженням і характером дії НШВФ можна розділити на 5 груп: фізичну, хімічну, біологічну, психофізіологічну та соціальну.

Один і той же НШВФ за характером своєї дії може належати різним групам одночасно.

Однією з причин появи НШВФ є небезпечні речовини.

Безпека праці - стан умов праці, при якому виключається вплив на працівника небезпечних і шкідливих виробничих факторів.

Виходячи з того, що в житті, а тим більше у виробничому процесі, немає абсолютної безпеки, було б нерозумно вимагати від фактичного виробництва повного викорінення травм, виключення можливості будь-якого захворювання. Але реально і розумно ставити питання про мінімізацію впливу об'єктивно існуючих промислових небезпек. Дана проблема вирішується охороною праці - системою правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних та профілактичних заходів та інструментів, спрямованих на збереження життя, здоров'я та працездатності людини в процесі роботи.

Конструктивно модуль "Безпека праці" включає в себе такі компоненти:

- правові та організаційні засади;
- фізіологія, гігієна праці та промислова санітарія;
- промислової безпеки;
- пожежна безпека на виробництві.

Правові та організаційні засади охорони праці являють собою комплекс взаємопов'язаних законів і нормативних актів, соціально-економічні та організаційні заходи, спрямовані на правильну і безпечну організацію праці, забезпечення працівників засобами захисту, компенсації за працьовитість і роботу в небезпечних умовах, навчання працівників безпечній праці, регулювання відповідальності та компенсації працівникам у разі заподіяння шкоди їх здоров'ю.

Фізіологія, гігієна праці та промислова санітарія - комплекс організаційних, гігієнічних і санітарних заходів та інструментів, спрямованих на запобігання або зниження впливу на працівників шкідливих виробничих факторів.

Промислова безпека - безпека від аварій і аварій на виробничих об 'єктах та їх наслідки.

Пожежна безпека на виробництві - комплекс заходів та інструментів, спрямованих на запобігання пожежам, пожежам і вибухам у виробничому середовищі, а також на зниження негативного впливу небезпечних і шкідливих факторів, що виникають у разі їх виникнення.

5.2. Законодавство України в галузі охорони праці

Законодавство України про охорону праці являє собою систему взаємопов'язаних нормативних актів, що регулюють відносини в галузі державної політики з правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних та профілактичних заходів і засобів, спрямованих на підтримку здоров'я. і людський потенціал для роботи. Складається із Закону України "Про охорону праці", Кодексу законів України про працю, Закону України "Про обов'язкове державне соціальне страхування

від нещасних випадків на виробництві та професійних захворювань, що спричинили інвалідність" та нормативних актів, прийнятих відповідно до них.

Законодавство України про охорону праці засноване на конституційному праві всіх громадян України на належні, безпечні та здорові умови праці, гарантовані статтею 43 Конституції України.

Інші статті Конституції закріплюють право громадян на соціальний захист, включаючи право на її надання у разі повної, часткової або тимчасової непрацездатності (стаття 46); медичне обслуговування, медична допомога та медичне страхування (стаття 49); право знати свої права та обов'язки (стаття 57) та інші загальні права громадян, включаючи право на охорону праці.

Базовим документом у сфері охорони праці є Закон України "Про охорону праці", в якому визначаються основні положення про здійснення конституційного права трудящих на охорону життя і здоров'я на робочому місці, належні, безпечні і здорові умови праці, регулює відносини органів державної влади між роботодавцем і працівником з питань безпеки, гігієна праці та робоче середовище і встановлює єдиний порядок організації охорони праці в Україні. Інші нормативні акти повинні відповідати не тільки Конституції та іншим законам України, але, перш за все, цьому Закону.

Відповідно до Конституції України, Законом України "Про охорону праці" та Основами законодавства України про обов'язкове державне соціальне страхування у 1999 році був прийнятий Закон України "Про обов'язкове державне соціальне страхування від нещасних випадків на виробництві та професійних захворювань інвалідів. "Цей закон визначає правові засади, економічний механізм та організаційну структуру обов'язкового державного соціального страхування громадян від нещасних випадків на виробництві та професійних захворювань, що призвели до втрати працездатності або смерті застрахованого на виробництві. Основні законодавчі акти з охорони праці також повинні включати "Основи українського законодавства про охорону здоров'я", які регулюють суспільні відносини в цій сфері з метою забезпечення гармонійного розвитку фізичної і духовної сили, високої ефективності та

тривалого активного життя громадян, усунення факторів, що негативно впливають на їх здоров'я, профілактики та зниження захворюваності, інвалідності та смертності, поліпшення спадщини Основи законодавства України про охорону здоров'я передбачають встановлення єдиних санітарно-гігієнічних вимог до організації виробництва та інших процесів, пов'язаних з діяльністю людини, а також якості машин, устаткування, будівель і споруд, які можуть негативно позначитися на здоров'ї. "І народ (стаття 28); вимагати обов'язкового медичного огляду окремих категорій осіб, у тому числі працівників, зайнятих на роботах зі шкідливими та небезпечними умовами праці (стаття 31); закласти правову основу для проведення медико-соціальної експертизи інвалідності (стаття 69).

Крім вищевказаних законів, правовідносини в галузі охорони праці регулюються іншими національними законами, міжнародними договорами та угодами, до яких Україна приєдналася в установленому порядку, підзаконними актами: указами та розпорядженнями Президента України, постановою Уряду України, постановою міністерств та інших центральних органів державної влади. Сьогодні кілька десятків міжнародних нормативних актів і договорів, до яких приєдналася Україна, а також понад сто національних законів України безпосередньо стосуються або мають точки перетину зі сферою охорони праці. Відповідно до Закону про охорону праці прийнято майже 200 підзаконних актів, що регулюють деякі питання охорони праці. Всі ці документи створюють єдине правове поле охорони праці в країні.

5.3. Нормативно-правова база охорони праці

Конкретні вимоги охорони праці до виробничого середовища, обладнання, об'єктів, процедур, засобів захисту працівників, підготовки працівників тощо регулюються відповідними нормативними актами, які розробляються відповідно до законодавства про охорону праці та складають нормативну базу охорони праці.

Нормативний правовий акт - офіційний документ компетентного державного органу, що встановлює універсально обов'язкові правила (норми). Закон України "Про охорону праці" передбачає, що нормативними правовими актами з охорони праці (НПАОП) є правила, норми, регламенти, положення, стандарти, інструкції та інші документи, обов'язкові до виконання.

Стандарти, технічні умови та інші документи на засоби праці та технологічні процеси повинні включати вимоги до охорони праці та узгоджуватися з органами державного нагляду за охороною праці.

Серед нормативних правових актів про охорону праці важливе місце займають державні стандарти України (ДДТУ) та відповідні нормативні акти (правила, норми, інструкції тощо), в тому числі колишній Радянський Союз, що діють в даний час на Україні.

Починаючи з 1972 року в СРСР розроблялася і впроваджувалася Система стандартів охорони праці, а її стандарти були окремою - 12-ю групою Єдиної державної системи стандартів СРСР, яка отримала назву "Система стандартів охорони праці" (ССБТ). Відповідно до Угоди про співробітництво в галузі безпеки та гігієни праці, укладеної главами урядів СНД у грудні 1994 року, ця система продовжує розвиватися і вдосконалюватися на міждержавному рівні, і її стандарти визнаються Україною як міждержавні стандарти в узгодженому переліку. Дані стандарти включені до Держреєстру окремою групою під заголовком "Міждержавні стандарти системи стандартів безпеки праці".

Нормативні акти з охорони праці підприємств.

Власники підприємств, установ, організацій або уповноважені ними органи розробляють на основі нормативно-правових актів і затверджують власні нормативні акти з охорони праці, що діють в межах даного підприємства, установи, організації. Нормативні акти підприємства конкретизують вимоги нормативно-правових актів і не можуть містити вимоги з охорони праці менші або слабкіші ніж ті, що містяться в державних нормах.

До основних нормативних актів підприємства належать:

- Положення про систему управління охороною праці на підприємстві.
- Положення про службу охорони праці підприємства.
- Положення про комісію з питань охорони праці підприємства.
- Положення про навчання, інструктаж і перевірку знань працівників з питань охорони праці.
- Наказ про порядок атестації робочих місць щодо 'їх відповідності нормативних актів про охорону праці.
- Інструкції з охорони праці для працюючих за професіями і видами робіт.
- Інструкції про порядок зварювання і проведення інших вогневих робіт на підприємстві.
- Загальнооб'єктові та цехові інструкції про заходи пожежної безпеки.
- Перелік робіт з підвищеною небезпекою.
- Перелік посадових осіб підприємства, які зобов'язані проходити попередню і періодичну перевірку знань з охорони праці.
- Наказ про порядок забезпечення працівників підприємства спецодягом, спецвзуттям та іншими засобами індивідуального захисту.

Відповідальність за порушення законодавства про охорону праці.

Закон України "Про охорону праці" передбачає, що винні особи причетні до порушення законів та інших нормативних правових актів про охорону праці, створення перешкод у діяльності посадових осіб органів державного нагляду за охороною праці, а також представників профспілок, їх організацій та об 'єднань. дисциплінарної, адміністративної, матеріальної та кримінальної відповідальності.

Дисциплінарна відповідальність полягає в тому, що винний працівник підлягає дисциплінарному стягненню. ст. 147 Трудового кодексу встановлює два види дисциплінарних стягнень: догана і звільнення. Закони, нормативні акти та положення про дисципліну, які застосовуються в деяких галузях

(транспорт, гірничодобувна промисловість тощо), можуть передбачати інші дисциплінарні санкції для певних категорій працівників.

Адміністративна відповідальність виникає за будь-яке посягання на загальні умови праці. Згідно зі ст. 41 Кодексу України про адміністративні правопорушення Порушення законів і нормативних актів про охорону праці тягне адміністративну відповідальність у вигляді штрафів для працівників і, зокрема, посадових осіб підприємств, установ, організацій, а також громадян - власників підприємств або їх уповноважених осіб.

Відповідальність працівників і службовців регулюється Трудовим кодексом та іншими нормативними актами, що зачіпають цю відповідальність у трудових відносинах.

Загальними підставами накладення матеріальної відповідальності на працівника є:

- наявність прямої дійсної шкоди,
- провина працівника (у формі наміру чи необережності),
- протиправні дії (бездіяльність) працівника,
- наявність причинного зв'язку між винуватим та протиправними діями (бездіяльністю) працівника та заподіяною шкодою.

Працівник може бути притягнутий до відповідальності тільки за наявності всіх цих умов; відсутність хоча б одного з них виключає відповідальність працівника.

Притягнення працівника до кримінальної, адміністративної та дисциплінарної відповідальності за дії, що заподіюють шкоду, не звільняє його від відповідальності.

За наявності ознак кримінального злочину в діях працівника, який порушив правила охорони праці, його можуть притягнути до повної відповідальності, а за відсутності таких ознак - до відповідальності в межах свого середньомісячного заробітку.

Кримінальна відповідальність за порушення правил охорони праці передбачена ст. 271 - 275 Кримінального кодексу України, які об'єднані в розділі X "Злочини проти безпеки провадження".

Кримінальна відповідальність виникає не за будь-яке порушення, а за порушення вимог законів та інших нормативних актів про охорону праці, якщо це порушення створило загрозу смерті або інші тяжкі наслідки або заподіяло шкоду здоров'ю потерпілого або спричинило смерть людей або інших осіб. тяжкі наслідки.

Порушення вимог законодавчих та інших нормативних актів, передбачених вищевказаними статтями Кримінального кодексу України, карається штрафом у розмірі до п'ятдесяти неоподатковуваних податком мінімумів доходів або виправними роботами на строк до двох років, або обмеження волі на строк до п'яти років або позбавлення волі на строк до дванадцяти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

ВИСНОВОК

Інтеграція - система безпеки об'єкта, що охороняється, об'єднує всі підсистеми за принципом програмно-апаратного симбіозу.

Інтегровані системи допомагають вирішити відразу ряд важливих питань:

Зниження витрат на забезпечення систем і підсистем безпеки за рахунок скорочення апаратних коштів;

Систематизація та уточнення інформації, що надходить на центральний пульт управління;

При частому виникненні однорідних ситуацій запрограмувати систему на прийняття стандартних рішень;

Зменшіть ймовірність помилок, внісши зміни у налаштування програмного забезпечення та системи.

Забезпечити більш надійний захист самої системи. Це простіше реалізувати, ніж використовувати окремі автономні системи безпеки.

Варто відзначити, що на даний момент використання інтегрованих систем безпеки не так поширено. І для цього є ряд причин. Багато об 'єктів вже давно встановлюють системи безпеки і не хочуть витрачатися на переоснащення. Нові користувачі здебільшого також хочуть мати моносистеми (відеоспостереження окремо, сигналізація окремо), побоюючись зв'язати все обладнання в моноліт. Але ви також можете бачити прогрес, коли ви можете бачити як автономні, так і інтегровані системи безпеки на одному об'єкті. Наприклад, відеоспостереження інтегровано з системою контролю доступу, але система охоронної та пожежної сигналізації роздільна. І інші варіації.

Перевагою використання інтегрованих систем безпеки є їх модульна система. Завжди можна підключити нову підсистему. Загалом таке обладнання - майбутнє галузі технічного захисту.

Варто відзначити перспективи розвитку ІСБ. Їх основні напрямки визначаються вимогами часу. Насамперед необхідно скоротити кількість помилкових спрацьовувань. Це може бути досягнуто за рахунок більш тісної

взаємодії всіх систем. Також - зниження ролі людського фактора і підвищення "інтелекту". Це реалізується в ускладненні детекторів руху, алгоритмів розпізнавання і створенні сценаріїв взаємодії систем. Тут допоможе тільки потужне програмне забезпечення.

Тому, беручи до уваги цю роботу, можна наочно побачити всі переваги переходу на ІСБ для власних ОІД, в яких система розглядається в майбутньому, проаналізувати за допомогою методології оцінки вдосконалення ІСБ вже використовуваних ІСБ за ОІД і зрозуміти, на якому етапі вона потребує вдосконалення.

В результаті розробленої методики було досягнуто задане призначення дипломної роботи.

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. [Електроннийресурс]https://xn--80adgeboqrpy5j.com.ua

6. [Електроннийресурс]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. / [Електроннийресурс]http://oksim.com.ua

17. Монітори відеоспостереження. / [Електроннийресурс]http://xn--80adgeboqrpy5j.com.ua

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

19. [Електронний ресурс]http://ukrtekbezpeka.com/ua/sistema-ohrannoj-signalizatsii/

20. ДСТУ ISO 7240-1:2007.НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ СИСТЕМИ ПОЖЕЖНОЇ СИГНАЛІЗАЦІЇ ТА ОПОВІЩУВАННЯ Частина 1. Загальні положення, терміни та визначення понять (ISO 7240-1:2005, IDT)