МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна інженерія»

Група: 2БКС-26

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

здобувача освіти денної форми навчання

БКС.26.10.000.КРБ

Николюк Олександри Степанівни

м. Одеса
2022 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: **«Комп'ютерна інженерія»**

Група: **2БКС-26**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему:_____

_____**«Дослідження методів інженерно-технічної безпеки об'єктів»**_____

_____

Проектний матеріал складається з пояснювальної записки на _____ сторінках та графічного (презентаційного) матеріалу на _____ аркушах (слайдах)

Виконавець _____ (Николюк О.С.)
Керівник проекту____ _____ (Кільдішев В.Й.)

Консультанти:

з охорони праці_____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ _____ (Петрашова В.І.)

старший консультант _____ (Кільдішев В.Й.)

До захисту допущений

Завідувачка кафедри _____ (Іванова Л.В.)

Завідувач відділення _____ _____ (Суліма Ю.Ю.)

Захист «____»_____ 202____ р. Протокол ДКК №_____

Оцінка ДКК _____

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Кафедра *комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР_____

_____

"_____"_____202____р.

З А В Д А Н Н Я

на кваліфікаційну роботу бакалавра

Здобувачеві (здобувачці) освіти Николюк Олександрі Степанівні

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи
Дослідження методів інженерно-технічної безпеки об'єктів

затверджена наказом по коледжу від "____"_____202____р. №_____

2. Термін здачі кваліфікаційної роботи_____

3. Вихідні дані до роботи ____Об'єкт аналізу – компоненти базової IT- інфраструктури: фізична мережа, сервіси, служба каталогу, захищене з'єднання, файлові сервіси. Кількість складових ТСО - 15. Моделі життєвого циклу – каскадна, спіральна. Етапи оптимізації ЖЦ – аудит, інвентаризація, пентестінг, програмні засоби, WLAN.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Вступ. 1. Розглянути склад, компоненти, класифікацію щодо IT – інфраструктури підприємства. 2. Навести загрози та ризики кіберсередовища підприємства. 3. Дослідити життєвий цикл інформаційних систем та засобів. 4. Обрати та впровадити етапи оптимізації життєвого циклу інформаційної системи підприємства. 5. Охорона праці. Висновки. Перелік використаних джерел. Додаток

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Лист 1 – _____

Лист 2 – _____

Лист 3 – _____

Лист 4 – _____

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів роботи, що стосується їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний	*Кільдішев В.Й.*		
Охорона праці	*Черновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кільдішев В.Й.*		

7. Дата видачі завдання Кільдішев В.Й. _____

Керівник роботи _____

(підпис)

Завдання прийняв до виконання _____

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів кваліфікаційної роботи	Термін виконання етапів кваліфікаційної роботи	Примітка
1	Вступ. Базові відомості про ІТ-інфраструктуру сучасного підприємства	**24.05.2022 р.**	
2	Загрози та ризики кіберсередовища підприємства	**27.05.2022 р.**	
3	Дослідження «життєвого» циклу інформаційних засобів та систем	**02.06.2022 р.**	
4	Оптимізація життєвого циклу ІТ - системи підприємства з позиції кібербезпеки	**04.06.2022 р.**	
5	Виконання розділу «Охорона праці»	**08.06.2022 р.**	
6	Виконання графічної частини роботи	**13.06.2022 р.**	
7	Чистове оформлення пояснювальної записки кваліфікаційної роботи	**15.06.2022 р.**	
8	Підготовка доповіді та презентації для захисту	**17.06.2022 р.**	
9	Отримання рецензії, відповіді на зауваження рецензента	**21.06.2022 р.**	
10	Захист роботи	**24.06.2022 р.**	

Виконавець _____

(підпис)

Керівник роботи _____

(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 26.10.000.00 КРБ	*Кваліфікаційна робота*		
А4			БКС 26.10.000.00 КРБ ПЗ	*Пояснювальна*	*1*	
				записка		
			БКС 26.10.000.00 КРБ МП	*Мультимедійна*		
				презентація		

Ізм.	Арк.	№ докум.	Підпис	Дата	*БКС 26.10.000.00 КРБ ПЗ*		
Розробив		Николюк О.С.			Дослідження методів інженерно-технічної безпеки об'єктів	Літ.	Аркуш
Перевірив		Кільдішев В.Й.				*Н Д П*	*3*
						ОТФК ОНТУ гр.БКС-26	
Н. Контр.		Петрашова В.І.					
Затверд.		Іванова Л.В.					

ЗМІСТ

ВСТУП

Питання наявності охоронної сигналізації стають все більш актуальними. Щорічна статистика міністерства внутрішніх справ говорить про збільшення кількості грабежів в різних регіонах України. Наприклад, у середньому, тільки в столиці сьогодні здійснюється близько 40 квартирних крадіжок на добу. В цілому, розкриття даного виду злочинів складає 30%.

Аналіз крадіжок, що сталися останнім часом, показує, що зловмисники проникають, насамперед, у ті приміщення та будівлі, де технічна укріпленість слабка – пустотілі дерев'яні двері, замки низької секретності, дешеві і низькоякісні елементи захисту. Особливо вразливими об'єктами посягання є перші поверхи житлових будинків. Популярні металопластикові вікна давно не є бар'єром для зловмисника. Залізні двері з хитромудрими замками, грати на вікнах – це перепони серйозніше, але також не зупиняти кваліфікованого зловмисника.

Найбільш надійно захищені від крадіжки ті приміщення, де окрім надійних дверей і решіток доданий ще один елемент – охоронна сигналізація з виведенням сигналу тривоги на ПЦС МВС або приватної охоронної компанії. Як то кажуть – охоронна сигналізація – не розкіш, а необхідність.

Експерти кажуть, що встановлена в квартирі охоронна сигналізація з підключенням до ПЦС в 95% зупиняє зловмисника, навіть якщо він відкрив замки і проник в квартиру. Звук тривоги в 100 дБ зверне увагу всіх сусідів і всього кварталу. До того ж, час реакції групи швидкого реагування складає період 3-5 хвилин. Все це допоможе надійно захистися від злочинців та спростити розкриття злочинів.

1 БАЗОВІ ВІДОМОСТІ ЩОДО ПІДХОДІВ ДО ПОБУДОВИ ІНЖЕРЕНО-ТЕХНІЧНОГО ЗАХИСТУ

Під інженерним захистом мають на увазі фізичне зміцнення всіх елементів та будівельних конструкцій об'єкта з метою запобігти несанкціонованому проникненню зловмисників на територію об'єкту та/або всередину приміщень. Система інженерного захисту має протистояти простому подоланню, злому (пролому, тарану), підриву, підпалу. Гарантований час протистояння має бути таким, щоб служби безпеки могли встигнути зафіксувати факт спроби силового проникнення, оцінити рівень потенційної небезпеки та вжити адекватних заходів протидії.

Інженерно-технічна укріпленість - сукупність заходів, що спрямовані на посилення конструктивних елементів будівель і приміщень, а також огородження об'єктів з метою запобігання проникненню в зону, що охороняється.

Варто відзначити, що головну роль при побудові комплексної безпеки об'єкта грають технічні засоби та засоби технічного укріплення. Правильний вибір та застосування ТСО та засобів технічного укріплення на об'єкті дозволить забезпечити високу надійність захисту об'єкта від усіх можливих внутрішніх та зовнішніх загроз. Вибір варіанта обладнання об'єкта ТЗ та засобами технічної укріпленості об'єкта визначається характеристиками значущості приміщень об'єкта, його будівельними та архітектурними рішеннями, умовами експлуатації та обслуговування, режимом роботи, перешкодами та багатьма факторами, що детально описують об'єкт.

1.1 Концептуальні питання забезпечення безпеки

Нормальне, планове функціонування підприємства, підприємства, банку, магазину та інших організацій (далі - фірм, об'єктів) - одне з головних турбот їхніх керівників. Стійка робота будь-якої фірми неможлива без забезпечення належного рівня її безпеки - здатності функціонувати без шкоди та при цьому постійно протистояти всіляким загрозам.

Для створення оптимальної ефективної системи безпеки об'єкта необхідно насамперед розробити обґрунтовану концепцію, яка визначає цілі захисту, характер можливих загроз та ймовірність їх

появи, основні напрями вирішення завдань захисту тих чи інших цінностей від аварій, стихійних лих та неправомірних дій потенційних порушників.

Предмет захисту – конкретні цінності фірми, які підлягають захисту за допомогою тієї чи іншої системи.

До таких цінностей відносяться:

• люди – персонал об'єкта, відвідувачі та клієнти фірми;

• матеріальні та фінансові цінності (гроші, цінні папери, документи, обладнання);

• інформація про конфіденційний характер.

Пріоритети зазначених цінностей великою мірою обумовлені характером діяльності фірми.

Об'єкт захисту - фізичний простір, де зосереджені ті чи інші цінності, багато в чому визначає можливі дії порушника безпеки та заходи щодо запобігання загрозам безпеки фірми.

Шляхи формування технічної системи охорони значною мірою залежать від характеристик огороджувальних конструкцій приміщень та інженерно-технічних систем об'єкта, їх відповідності вимогам нормативно-технічної

документації щодо будівництва, забезпечення безпеки, протипожежних правил. Великий вплив на характеристики ТСО має також стан, в якому знаходиться об'єкт - стадія розробки проекту, будівництва, реконструкції або постійної експлуатації.

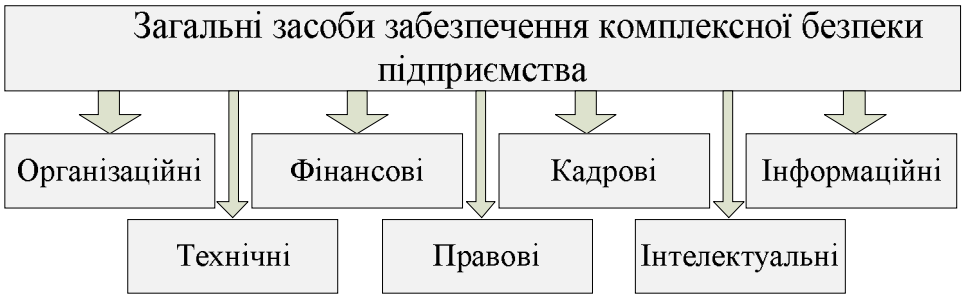

Рисунок 1.1 - Основні засоби забезпечення комплексної безпеки підприємства

У кожній фірмі існують приміщення, що вимагають особливого підходу до забезпечення їхньої охорони. До таких приміщень насамперед відносяться:

• кабінети керівництва фірми;

• переговорні кімнати;

• касові приміщення;

• центр обчислювальної та телекомунікаційної мережі – "серверна";

• базові приміщення систем інженерного забезпечення (СІБ) - вентиляційна камера, електрощитова кімната, приміщення резервного електроживлення та диспетчерської служби;

• приміщення служби безпеки фірми та пожежної охорони;

• архів паперових та електронних копій;

• найважливіші технологічні приміщення, з характеру бізнес-процесу у фірмі.

Загрози безпеки фірми можна класифікувати так: за природою виникнення - загрози випадкового характеру та спричинені навмисними діями порушників; по відношенню до об'єкта, що захищається: зовнішні і внутрішні.

До загроз випадкового характеру (зовнішнім та внутрішнім) відносяться стихійні лиха та катастрофи природного та техногенного характеру, аварії або порушення у роботі систем життєзабезпечення об'єкта, а також помилкові дії персоналу та відмови обладнання.

До зовнішніх загроз входять також криміногенні загрози, недобросовісна конкуренція, промисловий шпигунство навмисно діючих зловмисників. Загрози, викликані навмисними діями порушників безпеки об'єкта (як зовнішніх, і внутрішніх), виявляються як розкрадань матеріальних цінностей, вандалізму, шкідництва, саботажу, диверсій і терору. Основними

мотивами таких загроз можуть бути невдоволення конкретним керівником, бажання самоствердитись, марнославство, корисливе прагнення отримати матеріальну чи іншу вигоду, а також намір реалізувати свої політичні, релігійні та ідеологічні устремління.

Внутрішні загрози - це зловмисні дії персоналу (зазвичай із соціально-психологічними та моральними проблемами). Ініціаторами такого виду загроз виступають, як правило, самі співробітники або зовнішні структури, які діють шляхом підкупу персоналу.

Оцінка загроз, аналіз ризику реалізації та прогнозування можливої шкоди в кожному виду загроз - найважливіший напрям забезпечення безпеки фірми.

1.2 Категорування об'єктів, що охороняються

Як відзначалося вище, інженерно-технічна укріпленість об'єкта - сукупність заходів, спрямованих на посилення конструктивних елементів

будівель, приміщень і територій, що охороняються, що забезпечують необхідну протидію несанкціонованому проникненню в зону, зламу та іншим злочинним посяганням. Не дивно, що застосування засобів інженерного захисту веде до основної мети - затримати або зупинити на кожному з потенційних рубежів потенційного порушника. Основні компоненти для цього – стіни та перекриття, вентиляційні короби, люки та технологічні отвори, двері, вікна, замки та запірні механізми, сейфи для зберігання матеріальних та інших цінностей.

Вибір засобів захисту залежить від категорії приміщення.

Категорії об'єктів, що охороняються:

1. Об'єкти, що не охороняються, з вільним допуском персоналу та відвідувачів.

2. Об'єкти з простими (пасивними) обмеженнями і огорожами типу загород, що не охороняються (огорожі, стіни, грати тощо).

3. Об'єкти з загородженнями, що охороняються, які контролюються охоронцями, з постовими нарядами, патрульними службами та співробітниками пропускної системи.

4. Об'єкти з особливим режимом, допуск на які забезпечується спеціально підготовленими та розставленими по території та периферії охоронцями. Використовуються складні інтегровані технічні системи санкціориванного допуску, телеспостереження та охоронно-пожежної сигналізації, об'єднані в єдиний комплекс, який управляється комп'ютером та контролюється на центральному пульті охорони.

За результатами аналізу української та зарубіжної статистики спроб несанкціонованого проникнення в приміщення комерційних структур (офіси, виробничі та складські приміщення) зроблено такі висновки щодо ефективності різних систем безпеки:

- на об'єкти першої категорії – до 50% від загальної кількості спроб проникнення;

- на об'єкти другої категорії – близько 25%;

- на об'єкти третьої категорії – близько 20%;

- на об'єкти четвертої категорії – менше 5%.

Існують інші підходи до категоріювання приміщень. Так, галузевий документ ДСТУ 78.11.001-98 запроваджує таке категорування.

Залежно від значимості, виду та концентрації матеріальних, історичних, культурних та інших цінностей, що зберігаються на об’єктах та в приміщеннях, що охороняються, ці об’єкти та приміщення розподіляються на три категорії (А, Б, В):

1. Обєкти категорії «А»:

а) об’єкти життєзабезпечення населених пунктів;

б) фабрики та центральні сховища грошових знаків та цінних паперів;

в) об’єкти Державного комітету по телебаченню та радіомовленню;

г) державні центральні статистичні управління;

д) сховища державних архівів;

е) особливо важливі приміщення, в яких зберігаються:

– кошти;

– зброя, боєприпаси;

– наркотичні та психотропні речовини, прекурсори, отрути;

– дорогоцінні метали та каміння, ювелірні вироби з них;

– історичні та культурні цінності державного значення.

2. Обєкти та приміщення категорії «Б»:

а) комп’ютерна техніка;

б) малогабаритна техніка;

в) відео- та аудіотехніка;

г) кіно-, фототехніка;

д) хутра натуральні та штучні вироби з неї

е) шкіра натуральна та вироби з неї;

є) автомобілі та запасні частини до них;

ж) промислові та продовольчі товари повсякденного попиту;

з) технологічне та господарське обладнання;

к) технічна та конструкторська документація.

3. Обєкти та приміщення категорії «В»: особисте майно громадян (квартири, садиби, гаражі, дачі, автомобільні стоянки та ін.).

Рисунок 1.2 - Категорування об'єктів за стандартом ГСТУ 78.11.001-98

1.3 Аналіз галузевого стандарту ГСТУ 78.11.001-98

Базові відомості про стандарт ГСТУ 78.11.001-98.

ГСТУ встановлює порядок та спосіб забезпечення засобами механічного захисту об`єктів різних форм власності з метою протидії злочинним посяганням (несанкціонованому проникненню) під час їх проектування, будівництва, реконструкції та технічного переозброєння об`єктів, що підлягають передачі під охорону управлінням, відділам та відділенням Державної служби охорони при МВС України (далі - підрозділи ДСО).

СТУ мають рекомендовані вимоги та є обов`язковими для виконання, якщо:

-це передбачено чинними актами законодавства;

-ці вимоги включено до договорів на об’єкти, що підлягають охороні.

Вимоги ГСТУ діють на території України і стосуються громадян, а також підприємств, установ та організацій усіх форм власності, що уклали відповідні договори(контракти) на охорону з підрозділами ДСО. Питання технічної укріпленості засобами механічного захисту банків та підпорядкованих їм об`єктів цим ГСТУ не регламентується. Вимоги до таких об`єктів установлюються окремими нормативними документами, погодженими (введеними) Національним банком України та МВС України.

Забезпечення об`єктів заходами ТУК під час їх проектування, будівництва, реконструкції та технічного переозброєння, до яких неможливо застосувати типові рішення (типові проекти) згідно з ДБН А.2.2-3, проектуються за чинними в Україні нормативними документами та узгоджуються з підрозділами ДСО.

Під час проектування складних та унікальних (ДБН А.2.2-3) об`єктів, що підлягають взяттю під охорону підрозділами ДСО, замовнику спільно з

проектувальниками слід розробляти спеціальні технічні умови, що відображають специфіку його охорони, та узгоджувати з підрозділами ДСО.

Засоби механічного захисту (запірні пристрої, замки, ґрати, броньовані та ударотривкі засклення, віконниці та ін.) повинні бути спрямовані на ускладнення процесу проникнення на об'єкт, що охороняється, та узгоджені з підрозділами ДСО.

Під час добору засобів захисту слід застосовувати оптимальні та раціонально з'єднані механічні та технічні засоби.

Приміщення об'єктів, що охороняються, мають бути обладнані автоматичними установками пожежної сигналізації та пожежогасіння відповідно до галузевих нормативних документів, затверджених в установленому порядку.

Загальні вимоги щодо технічної укріпленості елементів будівель та приміщень.

Стіни, перекриття, підлога.

Об`єкти та приміщення, де зберігаються матеріальні цінності категорій А та Б, повинні мати по периметру капітальні (щодо охорони) стіни. Капітальними (щодо охорони) стінами, перегородками та перекриттями можуть бути такі, що виготовляються за чинними в Україні нормативними документами з повнотілої цегляної або кам'яної кладки завтовшки не менше 500 мм, бетонних стінових блоків товщиною не менше 180 мм, бетонних каменів товщиною 90 мм у два шари, залізобетонних панелей товщиною не менше 180 мм. Стіни, виготовлені з каміння "ракушнику", можуть бути капітальними, якщо їх товщина не менше 500 мм (окрім стін приміщень категорії А, де такі стіни мають бути обов'язково укріплені сталевими ґратами з арматури діаметром не менше 16 мм та розміром вічка не більше 150 мм х 150 мм).

Внутрішні приміщення об'єктів категорій А, які призначені для зберігання безпосередньо зброї, ювелірних виробів, наркотичних та психотропних речовин,

отрут, інформації, що містить комерційну, технологічну, господарську та інші таємниці, не повинні мати віконних прорізів та межувати з приміщеннями інших інших організацій, що не охороняються, технічними приміщеннями, коридорами та ін.

Двері сховищ мають бути броньованими, рівноміцними щодо стін сховища, обладнуватися не менш як двома спеціальними замками (з кількістю сугальдних пластин не менше як 8) та двоборідковим ключем.

Можливе обладнання захисних оболонок сховищ із рівноміцних щодо означеної залізобетонної оболонки збираних панельних конструкцій. Відповідність панельних конструкцій та бронедверей вимогам міцності можуть підтверджуватися сертифікатом відповідності, виданим органом сертифікації, акредитованим на ці види робіт Держстандартом України. Сертифікаційні випробування проводяться за чинними НД чи методиками, затвердженими в установленому порядку. Фундаменти під сховищами, що розташовані в підвалах чи на першому поверсі, мають бути виготовлені з монолітного бетону або кам'яної кладки завтовшки не менше 600 мм. Між фундаментом та залізобетонною оболонкою слід передбачати подвійну гідроізоляцію.

Двері.

У будинках та приміщеннях сучасної будови двері повинні відповідати вимогам ДСТУ Б В.2.6-11, ГОСТ 6629, ГОСТ 24698, ГОСТ 24584, ГОСТ 14624 та бути міцними відповідно до вимог за ДСТУ Б В.2.6-12.

Вхідні двері мають бути виготовлені за діючими стандартами, мати не менше двох урізних замків (що не замикаються самі) із встановленням їх на відстані не менше 300 мм між центрами регелів. Дерев’яні двері мають бути повнотілими, товщиною не менше 40 мм.

У разі наявності в приміщеннях, що охороняються, двостулкових дверей вони обладнуються двома внутрішніми стопорними шпінгалетами або засувами,

що встановлюються у верхній та нижній частинах дверного полотна. Перетин стопорних шпінгалетів або засувів має бути не менше 100 кв. мм, глибина фіксуючих оттворів - не менше 30 мм.

З метою захисту двостулкових дверей можуть використовуватись спеціальні двосторонні шпінгалетні запори, що у разі замикання можуть фіксуватися врізними або навісними замками.

Двері, що виходять у двір, провулки, а також запасні двері та двері входу до підвальних приміщень, вхідні двері до приміщень, де зберігаються цінності, та вхідні двері об'єктів охорони категорій А, Б мають бути повнотілими, завтовшки не менше 40 мм.

Вхідні двері приміщень категорії А (окрім прохідних до суміжних аналогічних приміщень), вхідні двері головних кас підприємств, установ та організацій, вхідні скляні двері з вітринного скла, металопластикові двері мають бути додатково захищені зсередини ґратчастими металевими дверима або розсувними металевими ґратами, що замикаються на навісний замок за допомогою вушок із внутрішнього боку за п.7.5.12. Ґратчасті металеві двері виготовляються із металопрокату, що має поперечний переріз менше 100 мм2 , і мають вічка не більше 150 мм х 150 мм, які зварюються на кожному перетині. Вподовж периметра ґратчасті двері обрамляються сталевим кутником 25 мм х 25 мм х 3 мм за ГОСТ 8509.

Вхідні двері чи одна з внутрішніх стін каси обладнуються спеціальним віконцем із дверцятами для операцій з клієнтами. Розмір віконця має бути не більше 200 мм х 300 мм. Якщо розмір віконця більший зазначеного, то зовні його слід укріпити металевими ґратами. Вимоги до дверцят та їх обрамлення аналогічні вимогам до дверей, оббитих цільнолистовим металом із вушками для навісного замка та двома шпінгалетами (угорі і внизу) з внутрішнього боку.

Двері сховища мають бути броньовані, виготовлені згідно з чинними нормативними документами. В дверному прорізі, крім броньованих дверей, встановлюють внутрішні ґратчасті металеві двері, що відкриваються всередину сховища

Люки, вентиляційні шахти та конструкції елементів будинків та приміщень

Двері люків за конструкцією мають бути аналогічні вхідним дверям, зсередини замикатися на запори, зовні на навісні замки амбарного типу.

Дерев'яне обплетення люка має кріпитися до капітальних конструкцій сталевими дугами з внутрішнього боку або йоржами зі сталі діаметром не менше 10 мм і забиватися в будівельні конструкції на глибину не менше 80 мм.

Двері та коробки люків горищ та виходів для покриття плоских крівель мають бути аналогічними, відповідно до п.7.2.4 - повнотілі, оббиті цільнолистовим металом унапуск та замикатися зсередини на замки, засувки, накладки та ін.

Вентиляційні шахти, короби та димарі, а також вікна горищ будинків, у яких розташовані приміщення, що охороняються, мають вихід на дах або в суміжні приміщення, своїм перетином входять до приміщення, де знаходяться матеріальні цінності, обладнуються на вході до цих приміщень металевими ґратами з металопрокату поперечним перерізом не менше 100 мм2, вічком не більше 150 мм х 150 мм.

У разі проходження вентиляційних коробів, шахт, каналів та димарів перерізом більше як 400 мм х 400 мм у стінах приміщень, де розміщуються матеріальні цінності категорії А, стіни таких приміщень із внутрішнього боку мають бути зміцнені вподовж площини, межуючої із коробом, ґратами або канали мають “перерізатися” з внутрішнього боку на входах до приміщення з установленням трубоарматурних касет.

У конструкціях елементів будинків та приміщень (підлоги, стіни тощо) слід передбачати кріплення сейфів, вагою упорожні менше 200 кг, де зберігаються предмети, зазначені в п.5.1.1, до цих конструкцій за допомогою металевих йоржів або болтів (крізь дно, стінки сейфа).

Замки, елементи кріплення замикаючих пристроїв

Для замикання вхідних дверей об'єктів, що охороняються, а також внутрішніх дверей приміщень, де розміщуються матеріальні цінності категорій А (окрім банківських сховищ), слід використовувати замки підвищеної секретності, сугальдні з двоборідковим ключем, циліндрові штифтові дво- та багаторядні.

Примітка. Для категорії А відповідність замикаючих пристроїв вимогам НД має підтверджуватися сертифікатом відповідності. Сертифікаційні випробування проводяться згідно з чинними нормативними документами чи методиками, затвердженими в установленому порядку.

Показником надійності замка є спосіб кріплення запобіжних накладок, розеток, щитків до полотна дверей, тобто кріплення їх за допомогою гвинтів або шурупів. У замках, що призначені для замикання вхідних дверей, кріплення накладок, розеток, щитків має здійснюватися лише за допомогою гвинтів.

Завіси для дверей мають бути виготовлені зі сталі. Кріплення завісів до дверного полотна має здійснюватися за допомогою шурупів. На об'єктах категорії А дверні завіси приварюються до металевого кутника дверної коробки назустріч один одному.

Якщо двері відчиняються "назовні", на дверних завісах мають бути встановлені торцеві гаки. Торцеві гаки в разі зачинення дверей входять до встановлених у дверній коробці анкерних пластинок або аналогічних елементів. Якщо двері металеві, то торцеві гаки приварюються, якщо ж двері дерев'яні, то вони встановлюються за допомогою шурупів. Двері ліфтових шахт мають блокуватися навісними замками, розпорками, засувами.

Рисунок 1.3 – СОСТАВ СТАНДАРТА ГСТУ 78.11.001-98

2 СИСТЕМИ ФІЗИЧНОГО ЗАХИСТУ ЯК ВДОСКОНАЛЕННЯ НАПРЯМУ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ОБЄЕКТІВ

Система фізичного захисту (СФЗ) об'єднує людей, процедури та обладнання для захисту майна від об'єктів розкрадань, диверсій та інших неправомірних дій. Проектування ефективної СФЗ вимагає певного методологічного підходу, при якому розробник знаходить баланс між цілями СФЗ і існуючими ресурсами. Після відбувається оцінка запропонованого проекту для визначення відповідності поставленим цілям. Без оцінки системи фізичного захисту можна витратити цінні ресурси на організацію непотрібної захисту або не забезпечити адекватний рівень захисту в критичних точках об'єкта.

Алгоритм проектування систем фізичного захисту складається з ряду етапів, послідовне виконання яких дозволяє отримати оптимальну і ефективну СФЗ. На етапі визначення цілей відбувається визначення характеристик об'єкта, виявлення загроз і цілей нападу. На етапі безпосереднього проектування СФЗ відбувається робота з 3-ма основними параметрами - виявленням, затримкою і реагуванням. Відбувається вибір датчиків, методів оцінювання сигналу тривоги, збір даних, моделювання дій сил реагування та вибір засобів зв'язку.

Важливим етапом при підготовці проекту СФЗ є аналіз і оцінка проекту. На зазначеному етапі застосовуються якісні і кількісні моделі оцінки, складаються діаграми послідовності дій порушника діаграми, відбувається оцінка ризиків.

Якісне проведення проектування системи фізичного захисту, виконання всіх необхідних етапів, оцінка ризиків і т.д. дозволяють побудувати і ввести в експлуатацію ефективну СФЗ, що позитивно позначиться на загальній системі

безпеки об'єкта інформаційної діяльності. На рис.2.1 представлено склад системи фізичного захисту обєкту.

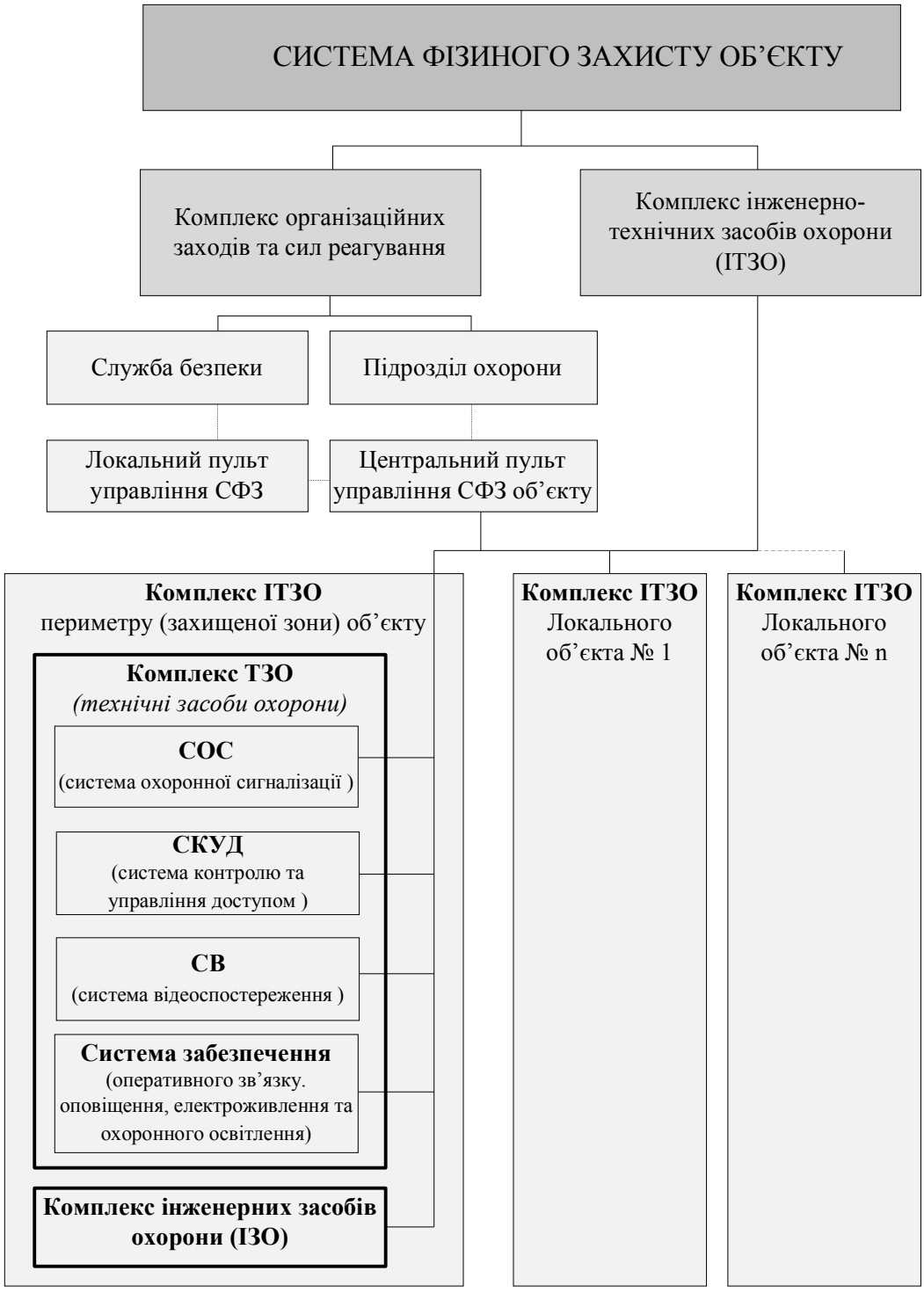

Рисунок 2.1 - Склад системи фізичного захисту обєкту

2.1 Формулювання цілей та аналіз етапів створення СФЗ

Графічне представлення методології СФЗ дано на рис. 2.2. Як зазначено вище, перший крок в процесі - визначити цілі системи фізичного захисту. Для того щоб їх сформулювати, розробник повинен визначити характер і умови функціонування об'єкта, виявити загрози і цілі нападу.

Процес починається з визначення завдань, потім проектується система, вирішальна ці завдання, і нарешті, оцінюється, наскільки добре система їх виконує. Для визначення характеру і умов функціонування об'єкта потрібне ретельне опис самого об'єкта (знаходження меж об'єкта і будівель, плани поверхів будівель, вказівку входів). Необхідні також характеристики робочих процесів на об'єкті та виявлення існуючих заходів захисту. Ця інформація може бути отримана з декількох джерел, включаючи проектну документацію об'єктів, описи технологічних процесів, звіти з охорони праці та оцінки щодо впливу об'єкта на навколишнє середовище. Крім збору і вивчення подібної документації необхідні також відвідування досліджуваного об'єкта і опитування працюючого на ньому персоналу, тобто обстеження об'єкту з метою проектування СФЗ. Це допоможе краще зрозуміти вимоги щодо фізичного захисту об'єкта, а також обмеження, пов'язані з його функціонуванням і аварійної безпекою, які повинні бути прийняті до уваги. Будь-який об'єкт унікальний, тому процес повинен виконуватися кожного разу, коли виникає в цьому потреба. Для того щоб робота могла тривати ефективно, безпечно і при цьому здійснювалася фізичний захист, зазвичай доводиться йти на компроміси. Крім того, слід розглянути питання відповідальності, а також діючі юридичні та інші нормативні вимоги.

Потім треба визначити загрози для об'єкта. Інформація може бути отримана при відповідях на три питання про порушника:

1. Який тип порушника слід розглядати?

2. Який діапазон його тактичних прийомів?

3. Які можливості порушника?

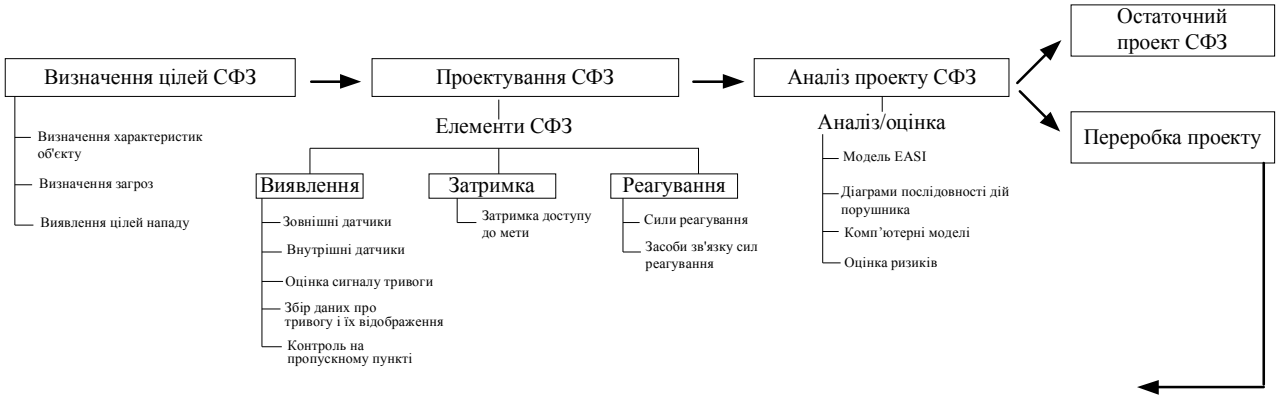

Рисунок 2.2 - Процес проектування та оцінки ефективності систем фізичного

2.2 Завдання та функції СФЗ

Загалом, до основних завдань систем фізичного захисту (СФЗ) відносяться

- попередження несанкціонованого доступу,
- своєчасне виявлення несанкціонованих дій,
- затримка (уповільнення) проникнення порушника,
- припинення несанкціонованих дій,
- затримання осіб, причетних до підготовки або вчинення диверсії.

Систему можна визначити як інтегровану сукупність компонентів, призначену для вирішення завдань відповідно до плану. Розробник будь-якої системи повинен тримати в голові її кінцеву мету. Кінцева мета СФЗ полягає в тому, щоб запобігти успішне виконання (особливо потенційним кваліфікованим порушником) відкритих або таємних зловмисних акцій. Типові завдання системи - запобігання диверсії спрямованої на виведення з ладу обладнання, розкрадання матеріального майна або інформації з об'єкта, а також захист службовців

(адміністративна або від насильства на робочому місці). Система повинна виконувати зазначені завдання або шляхом стримування, або шляхом поєднання дій по виявленню, затримки і реагування.

Функція утримання і стримування СФЗ можуть бути реалізовані за допомогою використання обладнання і охоронців. Функцію реагування зазвичай виконує охорона об'єкта. Для різних умов і додатків існує певний баланс між використанням обладнання і охоронців. У міру розвитку технологій баланс між обладнанням і охоронцями може змінюватися. Ключем до створення ефективної СФЗ є інтеграція людей, процедур і обладнання в систему, яка захищає майно від зловмисних порушників.

Ефективна СФЗ повинна виконувати всі три функції: виявлення, затримки і реагування. Вони повинні реалізовуватися в зазначеному порядку протягом меншого інтервалу часу, ніж час, необхідний порушнику для виконання свого завдання. Добре спроектована система забезпечує надійну і збалансовану захист, а також зводить до мінімуму наслідки відмов компонентів. Крім того, в процесі проектування, заснованому на критеріях ефективності, а не на умовах необхідних коштів, процедури і елементи вибираються на основі їх внеску в загальну ефективність системи. Критерії ефективності є вимірюваними, тому вони допомагають аналізувати розроблену систему.

Виявлення.

Виявлення є виявлення акції порушника, яка може носити як прихований, так і відкритий характер. Показники ефективності опції визначення - це ймовірність виявлення акції порушника і час, необхідний для повідомлення про напад і його оцінки. Ймовірність виявлення для певного датчика охоплює обидва цих показника. У функцію виявлення СФЗ входить також контроль на вході, т. Е. Дозвіл проходу особам, яким це дозволено, і виявлення несанкціонованого проходу або виносу матеріалів. Показниками ефективності контролю на вході є

пропускна здатність, частота помилкових проходів, частота помилкових відмов. Пропускна здатність визначається кількістю персоналу, який проходить в одиницю часу за умови, що всім, хто намагається пройти, це дозволено. Частота помилкових проходів - це частота, з якою дозволяється прохід особам з підробленими документами або невірно ідентифікованих (упізнаних), а частота помилкових відмов - це частота відмов у доступі особам, яким це дозволено.

Сили реагування також можуть виконувати функцію виявлення. Охоронці, що знаходяться на постах або здійснюють патрулювання, можуть зіграти важливу роль у виявленні проникнення. Однак таке рішення повинно бути ретельно продумано. Якщо поданий сигнал тривоги або отримано повідомлення про неї, починається оцінка. Ефективна система оцінки забезпечує два типу даних, пов'язаних з виявленням:

1) є тривога істинною або помилковою;

2) яка причина тривоги (що, хто, де і в якій кількості).

Затримка.

Затримка - друга функція СФЗ, яка уповільнює просування порушника до мети. Вона досягається шляхом використання бар'єрів, замків, а також залучення персоналу і може бути активована. Персонал сил реагування також можна розглядати як засіб затримки, якщо він розміщений на добре захищених позиціях. Показником ефективності затримки є час, який буде потрібно порушнику (після виявлення) для того, щоб обійти кожен елемент затримки. Хоча нападник може бути затриманий ще до виявлення, така затримка не грає ролі при оцінці ефективності СФЗ так як не надає додаткового часу для реагування на дії порушника. Затримка до виявлення по суті є стримуванням.

Реагування.

Функція реагування складається з дій, що вживаються силами реагування для перешкоджання успіху порушника. Реагування - як воно тут трактується -

полягає в перериванні дій. Переривання визначається як прибуття достатньої кількості персоналу сил реагування до відповідного місце для зупинки порушника і передбачає передачу їм точної про порушника, а також їх розгортання. Показником ефективності реагування є тривалість інтервалу часу між отриманням інформації про акцію порушника і її перериванням.

Розгортання включає в себе дії сил реагування між моментом отримання ними повідомлення і часом їх появи на позиціях з метою переривання акції порушника. Показники ефективності для цієї функції - ймовірність своєчасного розгортання сил реагування в районі розташування порушника і час, необхідний для цього.

Рисунок 2.3 - Функції системи фізичного захисту

2.3 Проектування систем фізичного захисту

2.3.1 Підсистеми і функції СФЗ

Після етапів, що визначають, кого і як варто захищати, настає етап проектування нової системи або визначення характеристик вже існуючої.

При проектуванні нової системи слід вирішити, як найкращим чином інтегрувати людей, процедури і технічні засоби для вирішення завдань СФЗ. Після того як система спроектована або визначені її характеристики, необхідно проаналізувати і оцінити її щоб бути впевненим, що вона забезпечує вирішення

всіх завдань фізичного захисту. Проект СФЗ повинен бути заснований на спільній роботі елементів захисту, що гарантує вирішення відповідних завдань, а не на індивідуальному використанні захисних засобів. У цьому випадку реалізація проекту СФЗ дозволить забезпечити системний інтегрований захист майна від передбачуваних нападів порушників, а не просто реакцію на що відбуваються напади.

При проектуванні нової СФЗ розробник повинен визначити, як оптимальним чином поєднати перешкоди, бар'єри, датчики, процедури і засоби зв'язку і персонал служби безпеки в СФЗ, яка може вирішувати завдання захисту. Остаточний проект системи повинен вирішувати ці завдання в рамках обмежень, пов'язаних з робочими процесами на об'єкті, аварійної безпекою, а також економічними та юридичними питаннями. Як згадувалося вище, первинними функціями СФЗ є виявлення порушника, його затримка, а також реагування персоналу служби безпеки (рис. 2.4).

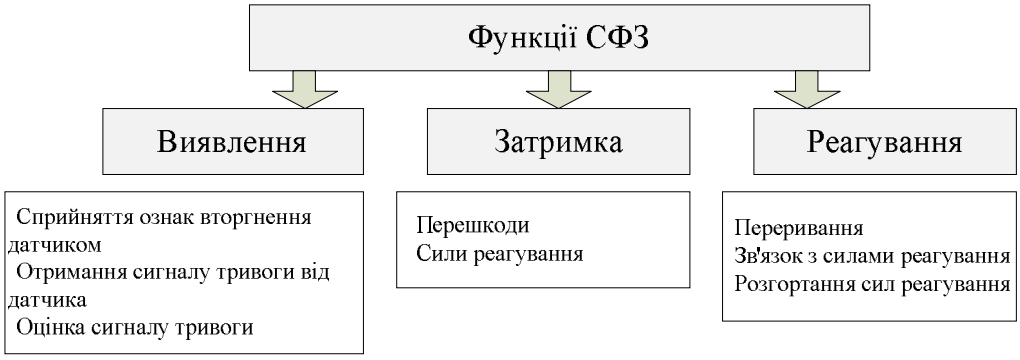

Рисунок 2.4 - Функції безпеки

При проектуванні СФЗ слід дотримуватися певних принципів. Система працює краще, якщо виявлення відбувається на якомога більшій відстані від мети нападу, а елементи затримки наближені до неї. Крім того, є тісний зв'язок між

виявленням (з використанням зовнішніх і внутрішніх датчиків) і оцінкою. Те, що виявлення без оцінки - це не виявлення, - базовий принцип проектування СФЗ, так як без оцінки оператор не буде знати причину сигналу тривоги. Якщо причиною сигналу тривоги стали стерпний вітром легкий сміття або вимикання світла всередині приміщень, реагування не потрібно, так як це - не вторгнення порушника.

Проектування починається з огляду завдань СФЗ і їх ретельного вивчення. Це легко можна зробити, перебравши наступні сфери застосування засобів фізичного захисту: виявлення вторгнення, контроль на пропускному пункті, затримка доступу, зв'язок з силами реагування та самі сили реагування. Однак не можна очікувати, що проект СФЗ, заснований на використанні необхідних коштів, дозволить створити високоефективну систему доти, поки ці кошти, які вживаються спільно, чи не будуть достатніми для забезпечення необхідного рівня захисту. У проектах, заснованих на використанні необхідних коштів, просто передбачається застосування конкретного числа або типів компонентів без аналізу ефективності їх роботи під час нападу порушника. Надійну СФЗ отримують, якщо використовують компоненти з перевіреними показниками ефективності.

Показники ефективності компонентів перетворюються в показники ефективності системи в цілому за допомогою методів системного моделювання.

2.3.2 Підсистеми фізичного захисту

Система фізичного захисту може бути визначена як сукупність елементів або компонентів, призначених для досягнення будь-якої мети відповідно до плану. Кінцева мета СФЗ - запобігти явні і скритні ворожі дії. Типові завдання полягають в тому, щоб не допустити диверсію по відношенню до найбільш важливого (критичного) обладнання, розкрадання майна або інформації з об'єкта і захистити

людей. Система фізичного захисту повинна вирішувати свої завдання шляхом стримування або комбінації функцій виявлення, затримки і реагування. Нижче перераховані підсистеми, що виконують ці функції:

Функції і підсистеми:

1. Виявлення

Зовнішні / внутрішні датчики

Оцінка сигналів тривоги

Збір даних про тривогу і їх відображення

Системи контролю на пропускному пункті

2. Затримка

Затримка доступу до мети

3. Реагування

Сили реагування

Засоби зв'язку сил реагування

Системні функції виявлення і затримки можуть виконуватися з використанням технічних засобів і (або) охоронців.

Ключем успішної реалізації СФЗ є інтеграція людей, процедур і технічних засобів в систему, яка захищає цілі від нападу від загроз. Така інтеграція вимагає аналізу співвідношення витрати - ефективність.

Виявлення, затримка і реагування - необхідні функції ефективної системи фізичного захисту. Вони повинні виконуватися в зазначеному порядку протягом часу меншого, ніж час досягнення зловмисником своїх цілей.

Добре спроектована система забезпечує надійний і збалансований захист, а також мінімізує наслідки відмов технічних засобів. Крім того, процес проектування, заснований на критеріях ефективності, а не на умовах необхідних коштів, призводить до вибору технічних засобів на основі їх внеску в загальну

ефективність системи. Критерії ефективності також є вимірюваними, тому вони допоможуть при аналізі проектованої системи.

2.3.3 Первинні функції СФЗ

Первинні функції системи фізичного захисту - виявлення, затримка і реагування. Варто зазначити, що для ефективної затримки має відбутися виявлення. Пріоритетна мета системи - захистити критичні ресурси від розкрадань і диверсій з боку зловмисного особи.

Для того щоб система ефективно виконувала це завдання, має мати місце оповіщення про напад (виявлення), потім просування порушника необхідно уповільнити (затримка), що дозволить силам реагування перервати або зупинити дії порушника.

Виявлення - це виявлення дій порушника. Воно включає спостереження укритті або відкритих дій. Щоб дії порушника було виявлено, повинні відбутися наступні події:

1. Датчик реагує на дії і видає сигнал тривоги.

2. Інформація від датчика і підсистем оцінки збирається і відображається.

3. Людина оцінює інформацію і вирішує, чи є сигнал тривоги істинним. Якщо він оцінюється як помилкова тривога, то виявлення не відбувається. Отже, виявлення без оцінки не може розглядатися як виявлення. Оцінка - це процес визначення того, чи є причиною сигналу тривоги напад, або тривога помилкова.

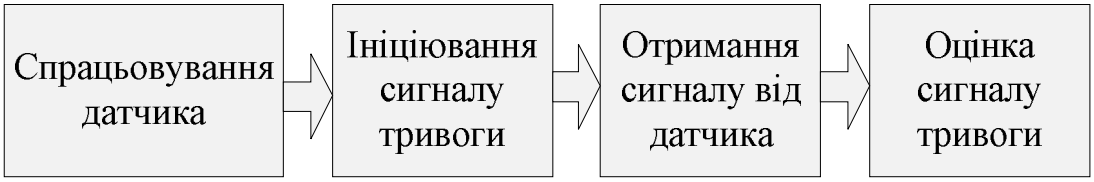

Рисунок 2.5- Функція виявлення у СФЗ

Виявлення починається після спрацьовування датчика та закінчується оцінкою сигналу тривоги з метою визначення його причини.

Показники ефективності опції визначення наступні: ймовірність виявлення дій порушника; час, необхідний для отримання та оцінки сигналу тривоги; частота помилкових тривог. Датчик спрацьовує в момент часу T_0, потім в більш пізній момент людина отримує інформацію від датчика і підсистем оцінки. Якщо час затримки між спрацьовуванням датчика і оцінкою сигналу тривоги мало, то ймовірність виявлення P_D близька до ймовірності P_S спрацьовування датчика від несанкціонованої дії. Ймовірність виявлення знижується в міру збільшення часу оцінки. На рис. 2.6 показано, що значна затримка між спрацьовуванням датчика і виконанням оцінки знижує ймовірність виявлення, оскільки, чим більше час, необхідний для виконання точної оцінки, тим менше ймовірність, що причина спрацьовування все ще буде мати місце.

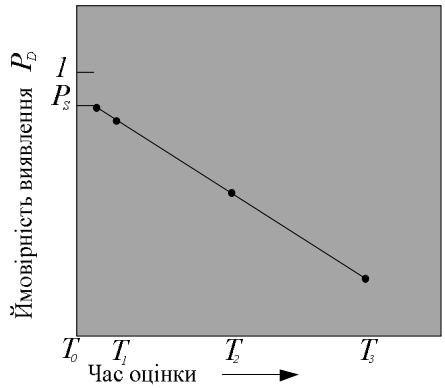

Рисунок 2.6 - Зв'язок між часом оцінки ймовірністю виявлення

Затримка - друга функція СФЗ. Вона уповільнює просування порушника. Ця функція може бути реалізована за допомогою людей, бар'єрів, замків і засобів активованої затримки. Сили реагування можуть розглядатися як елемент затримки, якщо вони знаходяться на фіксованих, добре захищених позиціях.

Показником ефективності затримки служить час, необхідне виявленому порушнику для того, щоб обійти кожен елемент затримки. Хоча порушник може відчувати затримку ще до виявлення.

Реагування - включає дії, що вживаються силами реагування для того, Щоб перешкодити успіху дій порушника. Реагування, так як воно тут розуміється, - це переривання.

Переривання визначається як прибуття достатнього числа персоналу в відповідне місце для зупинки послідовності дій порушника. Воно включає повідомлення сил реагування точної інформації про дії порушника і розгортання сил реагування. Показник ефективності дій сил розгортання - час між отриманням повідомлення про дії порушника і перериванням цих дій (час дії сил реагування). На рис. 2.7 показана виконувана СФЗ функція реагування. При захисті особливо важливих об'єктів застосовується додатковий захід ефективності дій сил реагування - нейтралізація.

Нейтралізація - це міра, яка визначає результат протиборства сил реагування та порушників. Такий тип реагування рідко використовується при захисті промислових об'єктів.

Рисунок 2.7 – Функція реагування у СФЗ

2.4 Оцінка ефективності технічної частини СФЗ

Для інженерної оцінки ефективності роботи елементів ТЗО застосований метод найслабшого елемента, суть якого полягає у виборі в послідовного ланцюга самого ненадійного елемента і проведенні по ньому оцінки всього ланцюга. Вважаємо, що таким елементом є оповіщувач. Для більшості оповіщувачів охоронної сигналізації периметра $T_0 \approx 10000$ годину закон розподілу відмов приймається експонентний, режим роботи ТЗО цілодобовий. За рахунок проведення планового ТО вважається, що деградація параметрів ТЗО щодо природного старіння знижується, а коефіцієнт старіння тракту доставки тривожного повідомлення складає близько 1% в рік.

При оцінці ймовірності виявлення $P_{вияв.}$ прийнято, що ймовірність виявлення залежить від підготовки порушника і способу установки сповіщувача. Останній може бути маскований і не маскований. При вторгненні порушника, який застосовує способи обходу, ймовірність його виявлення істотно знижується. Значення імовірності виявлення підготовленого порушника, застосовує способи обходу, розрізняється залежно від способу установки сповіщувача: 0,6 - для не замаскованого 0,8 - для замаскованого. Ймовірність виявлення «нормального» порушника не залежить від способу установки і приймається рівною 0,95.

Рисунок 2.8 – Схема роботи охоронної системи

де T_0 – середній час напрацювання на відмову, годин;

$P_{спов.}$ – ймовірність безвідмовної роботи;

$P_{кан.}$ – ймовірність безвідмовної роботи каналу (умовно приймаємо за 1);

БОС (ПКП) – блок обробки сигналу (приймально-контрольний прилад);

ПА ЦПУ – пультова апаратура ЦПУ.

На підставі викладеного проведені розрахунки та складена таблиця значень ймовірності виявлення в залежності від терміну експлуатації, моделі порушника і кількості сигналізаційних рубежів. Варіанти комбінацій та розрахункові формули наведено в табл. 2.1.

Таблиця 2.1 - Варіанти побудови сигналізаційного рубежу і вихідні формули для оцінки ймовірності виявлення порушника

Порушник	Сповіщувач	Кількість рубежів	Термін служби ТЗО (років)						
			1	2	3	4	5	6	7
Порушник підго-товлений	Маскуємий	1	$0,8(1-0,009n)$						
		1-маскуємий 2-не маскуємих	$1,4(1-0,009n)-0,48(1-0,009n)^2$						
		2	$1,6(1-0,009n)-0,64(1-0,009n)^2$						
		3	$2,4(1-0,009n)-1,92(1-0,009n)^2+0,512(1-0,009n)^3$						
	Не маскуємий	1	$0,6(1-0,009n)$						
		2	$1,2(1-0,009n)-0,36(1-0,009n)^2$						
		3	$1,8(1-0,009n)-1,08(1-0,009n)^2+0,216(1-0,009n)^3$						
Сповіщувач – Не маскуємий Порушник – Не підготовлений		1	$0,95(1-0,009n)$						
		2	$1,9(1-0,009n)-0,9(1-0,009n)^2$						
		3	$2,85(1-0,009n)-2,71(1-0,009n)^2+0,857(1-0,009n)^3$						

В основу створення СФЗ має бути покладений принцип превентивності, який може бути реалізований по-різному. Стосовно до СФЗ об'єкта це означає наступне: чим раніше буде виявлено вторгнення (порушення) і проведена оцінка його масштабу, тим успішніше виявиться відбиття або локалізація загрози, тобто тим СФЗ ефективніше.

2.5 Модель оператора в системі фізичного захисту

Місце і роль оператора в контурі системи фізичного захисту для всіх фахівців-проектувальників очевидна. Так само, як і у порушника, у СФЗ є центр координації її дій, іменований часто як ПЦО.

Передбачається, що у порушника є координатор, який не бере участь безпосередньо в атаці, його роль - координація дій, забезпечення та реалізація плану терористичної атаки. На об'єкті атаки є ПЦО, де чергова зміна (оператор) також забезпечує і координує дії з відбиття атаки. Різниця полягає в тому, що у порушника завжди є перевага - раптовість. У зв'язку з цим оператор ПЦО СФЗ, на відміну від оператора центру терористичної атаки (або бандитського нападу), володіє значно меншим резервом часу, для того щоб включити в протидія порушнику наявні сили реагування і, оцінивши масштаб вторгнення, запросити додатковий ресурс для його відображення. Тому від точності його дій фактично залежить безпека об'єкта.

Надалі під «оператором» будемо розуміти не тільки окремої людини, а й всю чергову зміну ПЦО. Контролер-охоронець на посту поза ПЦО не може вважатися повноцінним оператором, він скоріше підходить під визначення «інтелектуального сповіщувача».

Роль і значення оператора можна оцінити виходячи з постановки задачі: чи зможе система фізичного захисту протистояти організованому нападу на об'єкт групи порушників протягом заданого часу.

Моделювання оператора проводиться при певних припущеннях і обмеженнях:

–основним з них - оператор не є внутрішнім порушником.

–оператор підготовлений, має на робочому місці необхідні інструкції (плани дій), які наказують йому алгоритм дій в залежності від масштабу та

напрямки вторгнення порушника.

–приймальня апаратура (засоби відображення) оператора технічно справна.

–канали оперативного зв'язку з силами реагування та силовими структурами справні.

–санітарні умови чергування оператора - нормальні.

При таких припущеннях оператор розглядається як людина, фізичний стан якого підпорядковується біологічним залежностям. Рівень підготовки, ступінь відповідь-ності мало впливають на його біологічні параметри. Оцінка повинна бути спроможною і адекватною. Таким чином, модель оператора є складова частина моделі СФЗ. Основною вимогою до моделі оцінки ефективності СФЗ і оператора, в тому числі є счетності. Модель повинна базуватися на відомих і зрозумілих математичних чи інших залежностях, що дозволяють провести розрахунок без застосування складного програмного забезпечення. Моделювання діяльності оператора базується на методах інженерної психології:

– психологічних;
– фізіологічних;
– імітаційних.

За допомогою психологічних методів проводиться аналіз діяльності оператора в реальних умовах обстановки, проводиться оцінка впливу надходять факторів на його діяльність і на її результати.

Фізіологічні методи застосовуються для оцінки функціонального стану оператора в процесі чергування для визначення часу і якості (вірно / не вірно або ін.) реакції організму на виконання даної діяльності.

Використання математичних методів проводиться при знаходженні залежностей і при побудові моделей діяльності оператора.

Різновидом математичних методів є імітаційні методи. Суть їх зводиться до моделювання за допомогою ЕОМ досліджуваних процесів. В інженерній

психології ці методи використовуються для моделювання діяльності оператора за допомогою ЕОМ. Ефективне моделювання діяльності оператора може бути проведено лише при розумному поєднанні різних методів. Це випливає з вимог системного підходу.

Не применшуючи переваг всіх перерахованих методів, при проектуванні СФЗ, особливо на ранній стадії, при оцінці ефективності системи повинна бути врахована модель діяльності оператора, для чого найбільш доцільне застосування математичних методів. З їх допомогою можна оцінити в загальному вигляді вплив оператора, розрахувати основні показники його діяльності, пред'явити вимоги до технічних пристроїв. При цьому може виникнути необхідність отримання додаткових вихідних даних. Можливості застосування математичних методів в інженерній психології:

- теорія інформації;
- теорія масового обслуговування;
- теорія автоматичного управління;
- теорія автоматів;
- теорія статистичних рішень.

Найбільш широке використання для опису діяльності оператора в даний час знайшли методи теорії автоматичного управління, теорії інформації і теорії масового обслуговування.

Час реакції людини - це час від початку подачі сигналу до відповідної реакції організму, яке ділиться на 3 фази:

–час проходження нервових імпульсів від рецептора до кори головного мозку;

–час, необхідний для переробки нервових імпульсів та організації відповідної реакції в центральній нервовій системі;

–час відповідного дії організму.

Час реакції людини залежить від виду сигналу-подразника, інтенсивності подразника, тренованості, налаштованості на сприйняття сигналу, віку і статі, складності реакції (проста чи виборча).

Час реакції людини на дискретні незалежні подразники змінюється в широких межах. Для простої реакції середній час в найсприятливіших випадках становить не менше 0,15 с (розпізнавання зорових образів - не менше 0,4 с).

Даний показник - один з найважливіших факторів професійного відбору оператора, що має вирішальне значення при визначенні психофізіологічних можливостей людини виконувати операторську роботу.

За основу при моделюванні оператора ПЦО СФЗ прийнятий 24-годинний біоритм людського організму. Він визначає фізіологічну готовність людини до роботи в залежності від часу доби. Періодичні коливання працездатності виникають внаслідок різної установки організму по черзі то на працю, то на відпочинок. Для людини в нормальних умовах життя неможливо довільне зміна біоритму. Звідси - проблеми з організацією праці при багатозмінної роботі. На рис. 2.9 приведена крива зміни фізіологічної готовності до роботи протягом доби (24-годинний біоритм).

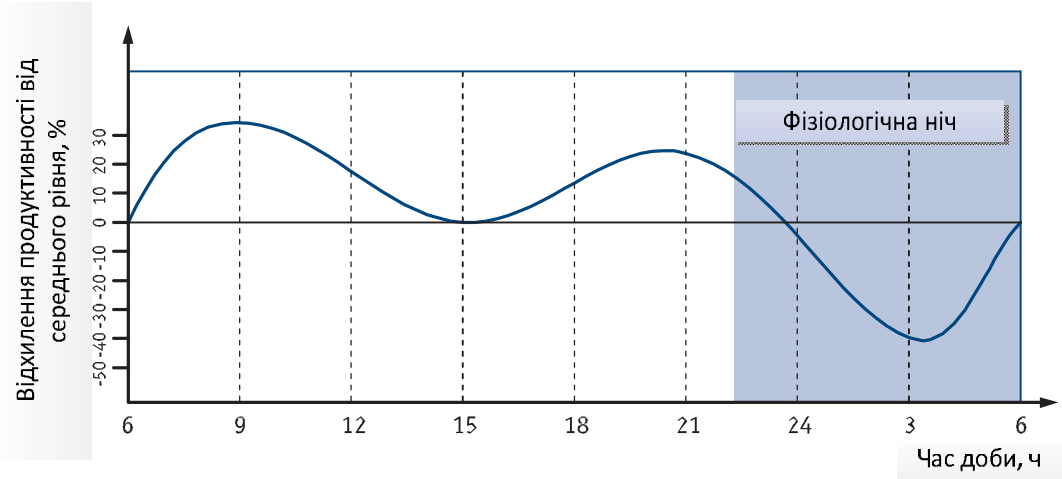

Рисунок 2.9 - Крива зміни фізіологічної готовності до роботи протягом доби (24-годинний біоритм)

На підставі цієї залежності побудована тимчасова функція ймовірності сприйняття сигналу тривожного сповіщення та прийняття рішення оператором пульта (рис. 2.10).

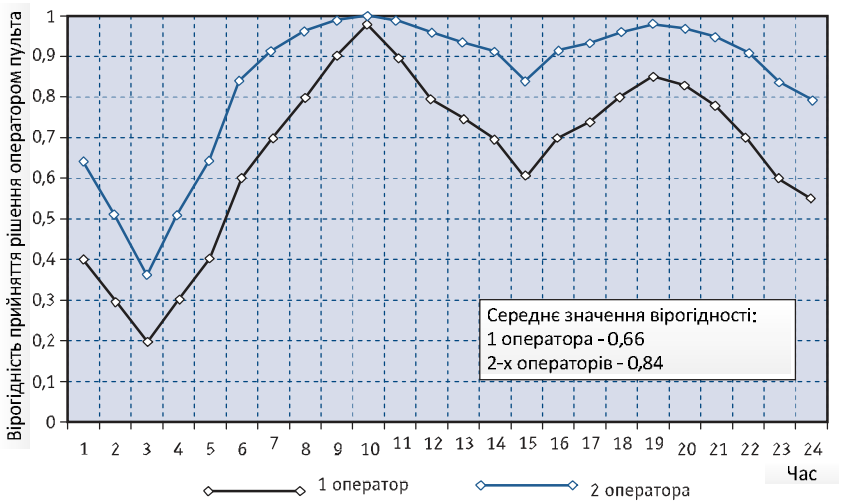

Рисунок 2.10 - Тимчасова функція ймовірності сприйняття сигналу тривожного сповіщення та прийняття рішення оператором пульта

Весь діапазон відхилення продуктивності від середнього рівня в діапазоні від мінус 50% до плюс 40% розбитий на інтервали з ціною поділки 0,1.

Сума поділок дорівнює 1. Для визначення ймовірності прийняття рішення за наявності двох операторів застосована формула логічного складання ймовірностей (схема «АБО»):

$$P_0 = P_1 + P_2 - P_1 P_2 , \qquad (2.1)$$

де P_0 – ймовірність прийняття рішення за наявності двох операторів;

$P_1 = P_2$ – ймовірність сприйняття сигналу та прийняття рішення кожним оператором. При наявності двох операторів на ПЦО їх імовірності сприйняття одних і тих же сигналів тривожного сповіщення прийняті однаковими.

Оцінка цього значення проведена за формулою:

$$P_{cp} = \frac{1}{24}\sum_{i=1}^{n} P_{0i}\,, \tag{2.2}$$

де P_{0i} - значення ймовірності при 24-годинному циклі роботи оператора.

Середнє значення сприйняття сигналу тривожного сповіщення та прийняття рішення в залежності від кількості операторів ПЦО:

– для одного оператора: 0,64;

– для двох операторів: 0,84.

У разі чергування двох операторів оцінка сприйняття сигналу тривожного сповіщення та прийняття рішення підвищується в 1,3 рази. Говорячи про оператора і його ролі при оцінці ефективності системи, неможливо не враховувати ту обставину, що сучасні системи дають можливість оператору не тільки почути сигнал тривожного сповіщення, а й побачити місце виникнення цього сигналу. Це їх корисна властивість дозволяє оператору проводити оцінку масштабу порушення і приймати відповідне рішення.

Останнім часом все більше журнальних публікацій присвячено системам відеоспостереження. Замовники вимагають, проектувальники збільшують число телекамер, встановлюють складні системи управління, відеореєстратори і т. п. Пульт централізованої охорони все більше стає схожим на центр управління польотом космічних апаратів. При цьому часом забувається, що всі ці принади виводяться на екран для ока оператора, кількість яких не збільшується з метою економії. В результаті може вийти, що на одного оператора буде припадати кілька моніторів з мультикартинним зображенням (8-16) і декілька моніторів з зображенням обстановки в реальному часі. Виникає ситуація, коли система охоронного телебачення в загальному комплексі безпеки з додаткової стає домінуючою. З цього можна зробити тільки один висновок.

3 ФОРМУВАННЯ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ОБ'ЄКТІВ

Побудова ІТЗ на об'єкті включає комплекс заходів, який включає в себе:

1. Інженерно-технічне зміцнення.

2. Технічні засоби охорони та сигналізації (ТСОО).

3. Сили охорони.

4. Технічні засоби захисту інформації.

Склад інженерно-технічного захисту об'єктів представлений на рис. 3.1 Розглянемо деякі з блоків докладніше.

Рисунок 3.1 - Детализация состава инженерно-технической защиты объектов

3.1 Застосування технічних засобів охорони

Як елемент загальної картини інженерно-технічного захисту, для захисту приміщень обєкту можливе використання технічних засобів охорони. В нашому випадку до системи безпеки будуть входити такі модулі:

- Модуль автоматичної системи пожежної сигналізації
- Модуль охоронної сигналізації
- Модуль системи охоронного відеоспостереження
- Модуль автоматизації
- Модуль системи контролю та керування доступом

Модуль автоматичної системи пожежної сигналізації.

Згідно вимог пожежної безпеки - ГОСТ 12.1.004-91 ССБТ, об'єкти повинні бути забезпечені системами протипожежного захисту. Автоматична система пожежної сигналізації спрацьовує при виявленні вогнища загоряння. Центральна станція в цьому випадку повинна чітко виконувати приписані дії, що стосуються управління системами автоматики будівлі: відключаються вентиляційні системи, включаються системи оповіщення, димовидалення та пожежогасіння.

Встановлення сучасних систем пожежної сигналізації дає можливість локальної пожежної частини і людям, що знаходяться в приміщенні почати дії з ліквідації пожежі ще на стадії зародження даної небезпеки. На рис. 3.2 на плані приміщення представлена схема АСПС.

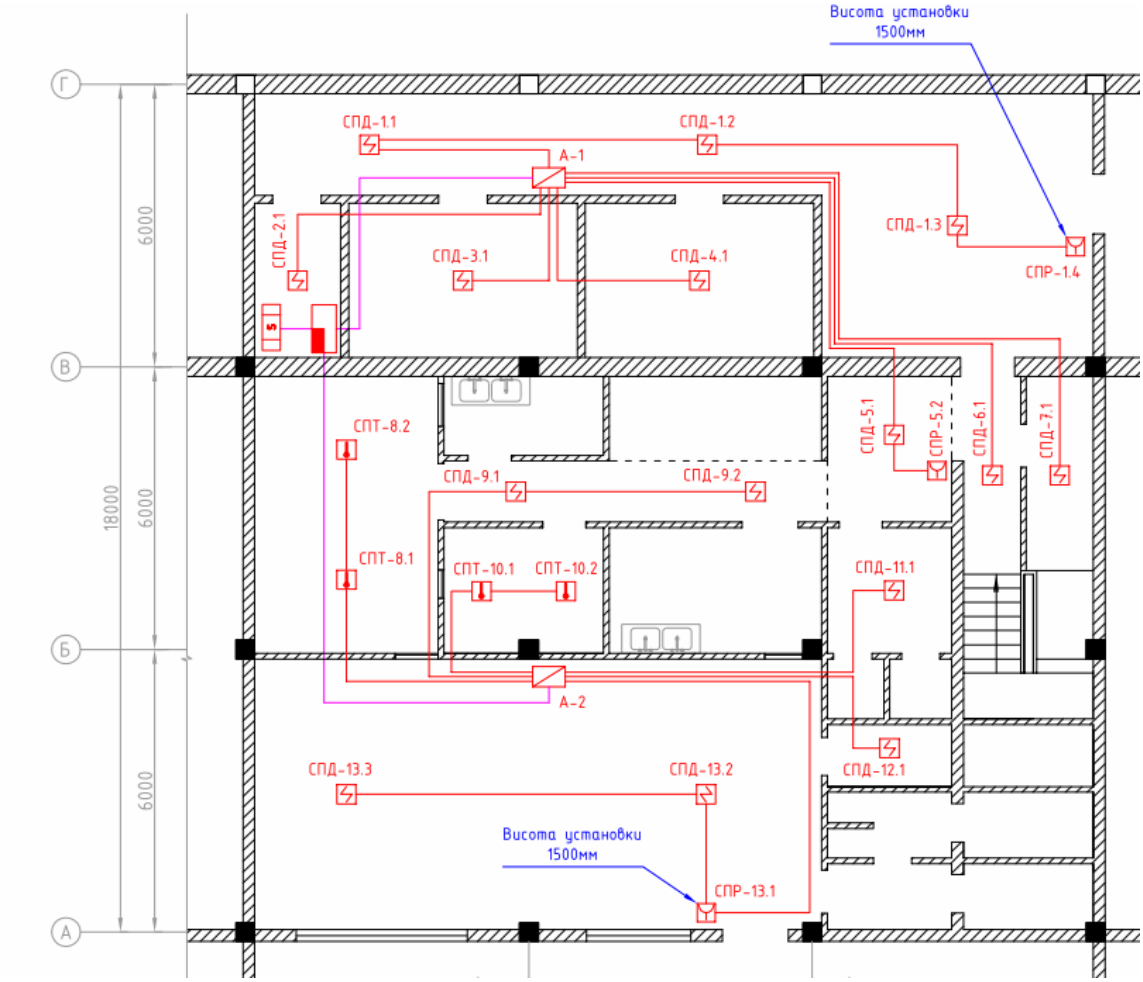

Рисунок 3.2 – Схема розташування облананяя АСПС на плані приміщення

Модуль автоматичної системи пожежної сигналізації.

Згідно зі статистикою, близько 84% всіх злочинних намірів залишаються на рівні задуму за наявності на об'єкті сигналізації. Абсолютна більшість злочинців не володіє достатніми знаннями для відключення і грамотної нейтралізації системи. У той же час і виробники профільного обладнання постійно впроваджують нові розробки, використовують передові технології, що дозволяють звести до мінімуму можливість відключення охоронної сигналізації.

Досить часто останнім часом зустрічаються оголошення з пропозиціями встановлення охоронної сигналізації ремонтними бригадами, а то і взагалі

самостійно. У даному випадку фактично йдеться про бутафорії, яка буде тільки візуально настращати зловмисників.

Як і в будь-який інший технічній галузі питаннями проектування системи, вибору обладнання, його розташування, установкою, інсталяцією повинні виконуватися виключно професіонали. Існує досить багато типів приміщень, у кожному окремому випадку вони мають різне призначення, планування, свою специфіку. На кожному з підприємств встановлено свій власний порядок виконання робіт, по-різному організовано допуск персоналу на об'єкт, відрізняється графік роботи в цілому.

У кожному окремому випадку для грамотної організації ефективної охоронної сигналізації обов'язково повинен бути вивчений об'єкт, його структура, принцип роботи, план будівлі, призначення приміщень і т.д. далі згідно з цими даними виконується проектування, а потім і вибір необхідного обладнання, його встановлення. Загальна структура системи охоронної сигналізації наведена на рис. 3.3.

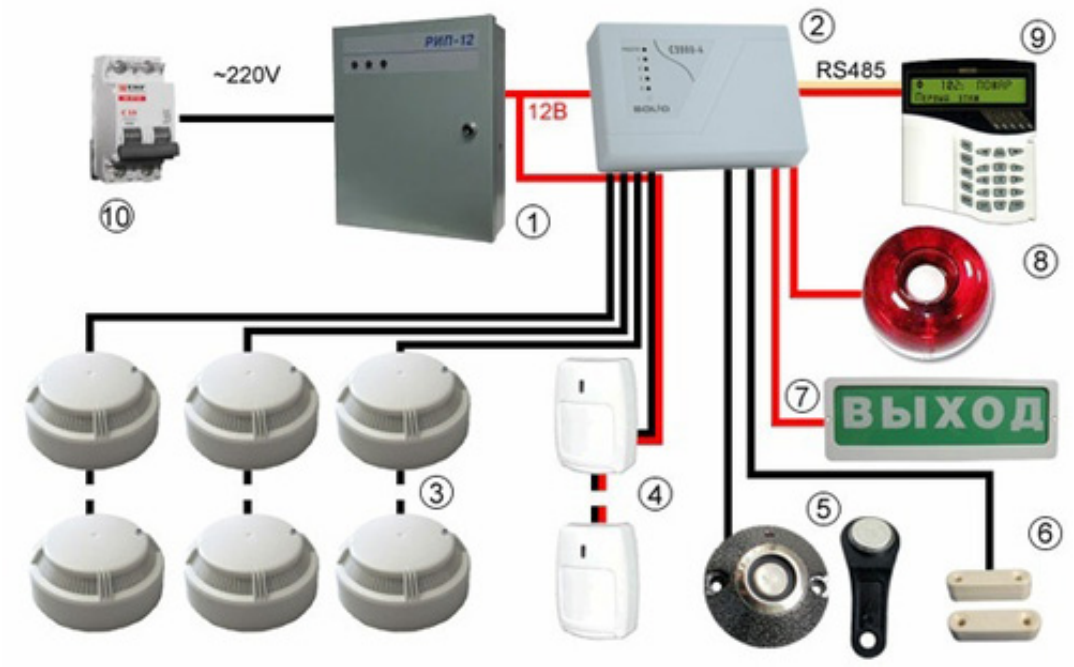

Рисунок 3.3 – Загальна структура системи охоронної сигналізації

При побудові системи охоронної сигналізації в ролі виконуючих пристроїв застосовна датчики охоронної сигналізації. Наприклад, як видно из таблиці, в ролі датчика розбиття скла застосовано датчик INDIGO.

Розрахуємо струм споживання системи $I_{ч}$ від резервного джерела живлення в черговому режимі:

$$I_{Ч} = I_{П.Ч} + K \times \sum_{j=1}^{r} I_{шj}, \tag{3.1}$$

де $I_{п.ч}$ – початковий струм приймально-контрольного приладу в черговому режимі;

$I_{шj}$ – струм, що проходить в j-му шлейфі сигналізації;

r – кількість використовуваних шлейфів сигналізації;

K – коефіцієнт заряд/розряд, К = 1,24.

$$I_{шj} = I_{пшj} + I_{навшj}, \tag{3.2}$$

де $I_{пшj}$ – початковий струм в шлейфі без сповіщувачів з підключеним кінцевим елементом;

$I_{навшj}$ – струм навантаження шлейфу з охоронними енергоспоживаючими сповіщувачами різних видів.

Струм споживання системи в режимі «Тривога» $I_{с.т}$:

$$I_{С.Т} = I_{П.Т} + K \times \left(\sum_{j=1}^{S} I_{шj} + \sum_{l=1}^{Z} I_{шml} \right), \tag{3.3}$$

де s – загальна кількість шлейфів в черговому режимі;

z – загальна кількість шлейфів у режимі «тривога»;

$I_{шт/}$ – струм, що проходить в *l*-му шлейфі сигналізації зі сповіщувачами в режимі «Тривога».

Згідно формули 4.11 знайдемо струм споживання системи $I_ч$ від резервного джерела живлення в черговому режимі на кожному поверсі. При цьому будемо користуватись тим, що $I_{п.ч}$ для цього ПКП та блоків розширення дорівнює 250 та 120 мА відповідно:

$I_{ч0}$=120+1,25×302,5=498,125 мА

$I_{ч1}$=120+250+1,25×302,5=770,625 мА

$I_{ч2}$=120+1,25×213=386,25 мА

В режимі «тривога»:

$I_{ст0}$=120+1,25×177,5=341,875 мА

$I_{ст1}$=120+250+1,25×225,5=651,875 мА

$I_{ст2}$=120+1,25×260=445 мА

Час роботи системи охоронної сигналізації *T* в автономному режимі (від резервного джерела постійного струму - акумулятора) визначається за допомогою виразів:

В черговому режимі :

$$T = M \times C / I_ч, \tag{3.4}$$

В режимі «тривога»:

$$T = M \times C / I_{C.T}, \tag{3.5}$$

де *C* - ємність акумуляторної батареї, *C*=7,2 А.г.;

M - поправочний коефіцієнт:

M = 1,1 при $C / I_{ч\ (с.т.)} > 10$;

M = 1 при $10 > C / I_{ч\ (с.т)} > 4$;

M = 0,75 при $4 > C / I_{ч\ (с.т)} > 1$;

M = 0,5 при $C / I_{ч\ (с.т)} < 1$.

Всі розрахунки зведемо в табл. 3.1.

Таблиця 3.1 – Ємність акумуляторної батареї та час роботи системи черговому режимі та в режимі «тривога»

Поверх	*T*, годин	
	Черговий	«Тривога»
Цокольний	15,9	23,2
Перший	9,3	12,15
Другий	20,5	17,8

Загальна ємність акумуляторних батарей повинна відповідати умові тривалості роботи системи охоронної сигналізації в черговому режимі не менше 24 годин, в режимі "тривога" - не менше 4 годин. На рис. 3.4 зображено схему розташування елементів охоронної сигналізації на плані приміщення кафе.

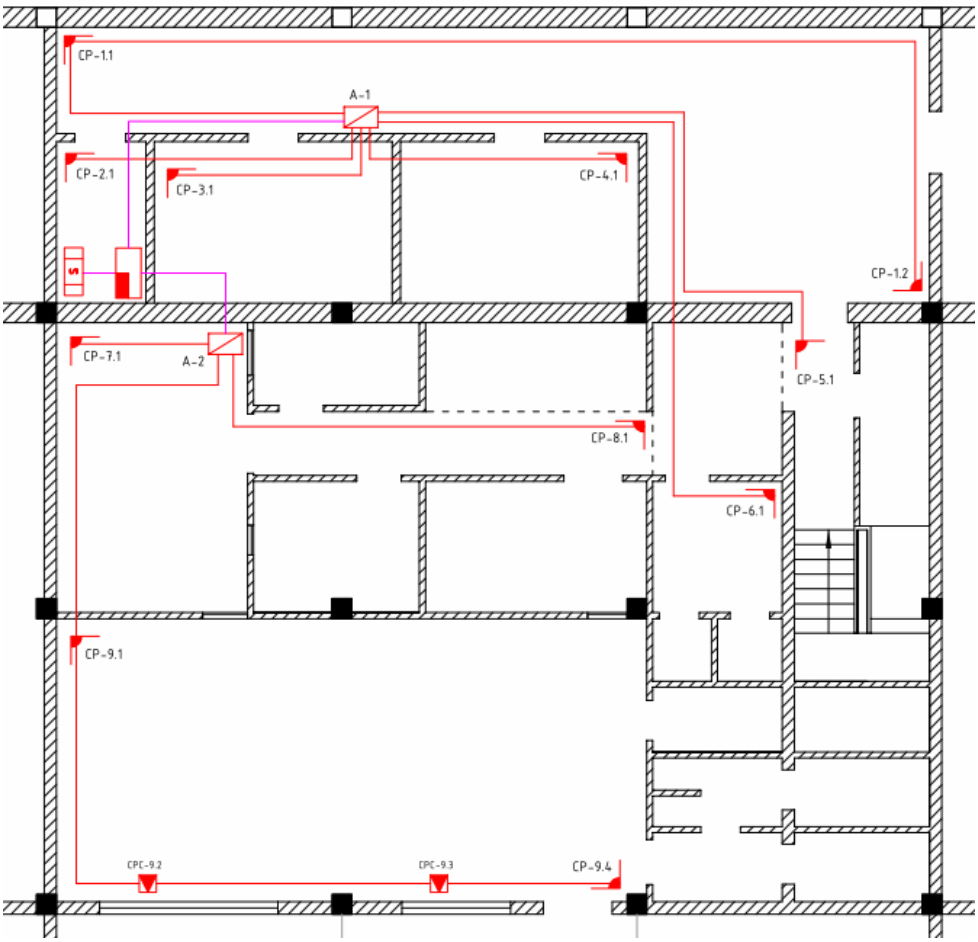

Рисунок 3.4 – Розташування елементів охоронної сигналізації

Модуль охоронного відеоспостереження.

Система відеоспостереження в кафе - запорука успіху бізнесу.

Як показує практика, після установки відеоспостереження в офісі компанії, співробітники починають працювати більш ефективно, ростуть якість і загальний темп роботи. Крім цього, наявність аудіозаписи допомагає розібратися в конфліктних ситуаціях, які можуть виникати як між співробітниками фірми, так і між співробітниками і клієнтами.

Переваги встановлення відеоспостереження в кафе:

– Запобігання розкрадань;

– Контроль і облік робочого часу співробітників;

– Поліпшення якості обслуговування;

– Можливість визначити винуватця псування майна;

– Можливість об'єктивно розібрати конфліктну ситуацію між обслуговуючим персоналом та відвідувачами кафе.

Камери відеоспостереження в першу чергу встановлюються в зонах, найбільш небезпечних з точки зору безпеки. Як правило, "левова" частка розкрадань та інших порушень відбувається в таких місцях, як барна стійка (співробітники кафе можуть бути у змові з відвідувачами), на складі та в інших зонах кафе. Вхід в кафе, також рекомендується перекривати однією з камер. Завдяки такому підходу зацікавлені особи зможуть контролювати реальну кількість відвідувачів, що дозволяє звірити кількість замовлень, проведених по касі з кількістю фактичних відвідувачів за певний проміжок часу (за зміну). Також, встановлення камер відеоспостереження в цих місцях дозволить звести до мінімуму можливість протиправних дій з боку відвідувачів і підвищить дисципліну співробітників. Система відеоспостереження в кафе дозволяє контролювати обстановку як в режимі "реального" часу, так і переглядати архів відеозапису. Причому обладнання дозволяє налаштувати процес запису по руху,

тобто запис буде вестися тільки в ті моменти, коли в поле зору відеокамери відбувається який-небудь рух, що істотно заощаджує Ваш час, що витрачається на перегляд архіву.

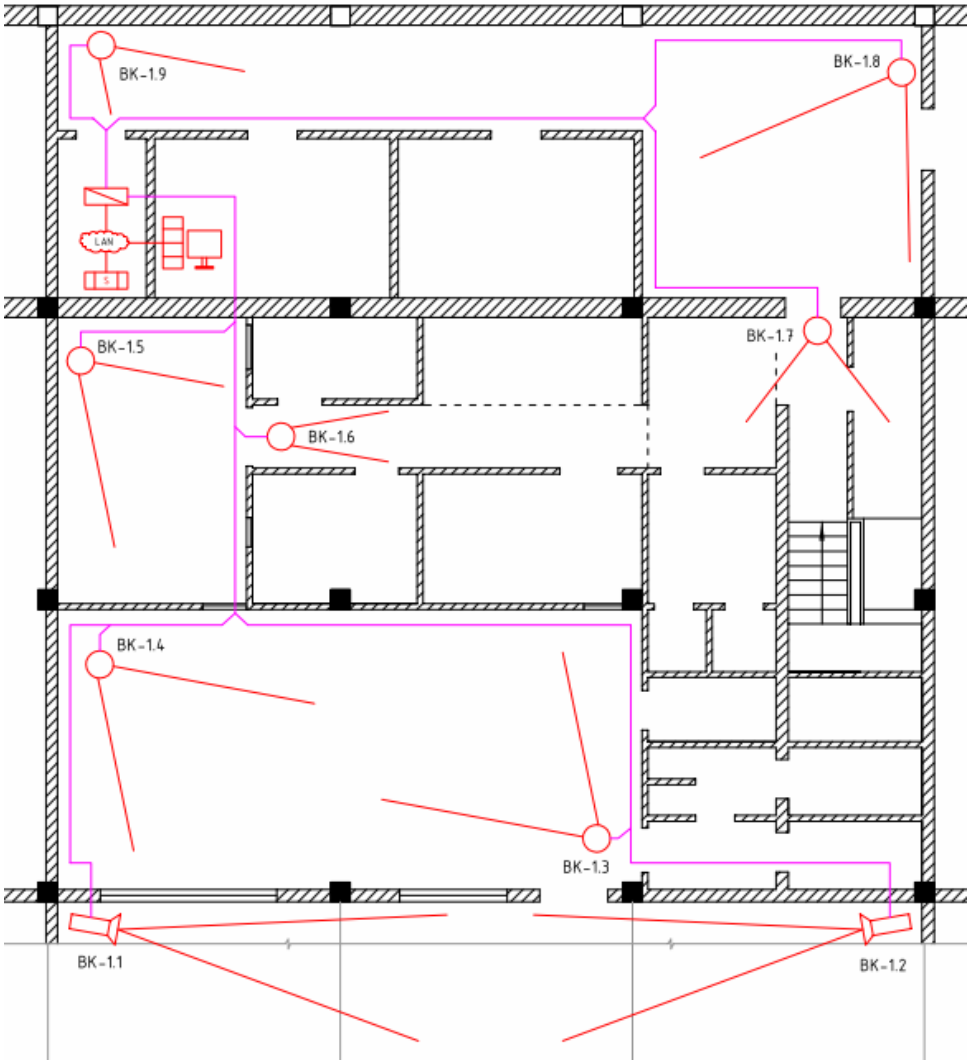

Рисунок 3.5 – Схема розташування СОТ

Припустимо, що підприємство працює з 10.00 до 22.00. Змоделюємо ситуацію, коли в першому випадку система пише постійно, тобто протягом 12-ти годин. У такому випадку параметр% руху складає 100%. Другий випадок - запис

по детектору руху камери. Припустимо, що з огляду внутренню активність усередині приміщень, активність детектора буде составалять 40%. При цьому в розрахунку будуть брати участь тільки камери, встановлені внутр. приміщень у кількості рівній 7. Результати порівняння варіантів використання повного запису і запису з реакції детектора руху показані на рис. 3.6.

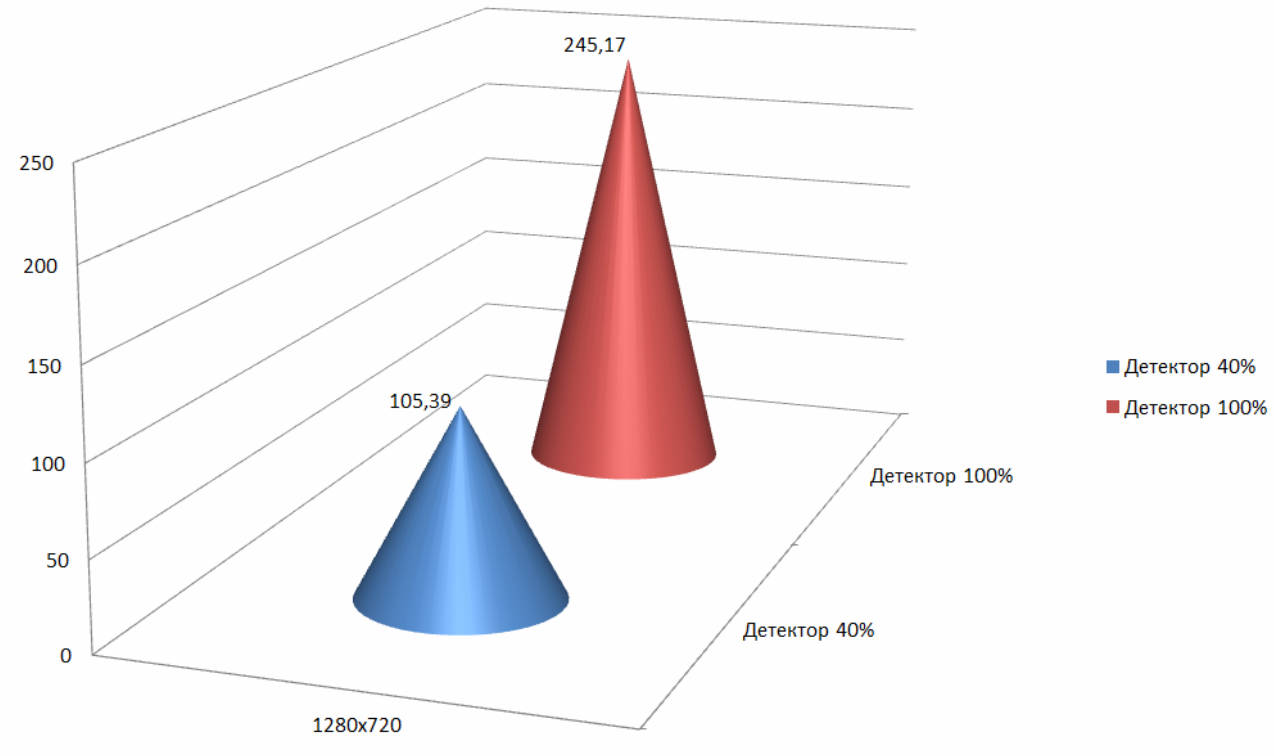

Рисунок 3.6 – Залежність параметрів СОТ від кількості роботи детектора

Розрахунок проводився за рядом параметрів:

1. Кодек – H.264.
2. Кадрів за секунду – 25.
3. Годин запису на добу – 12.
4. Кількість камер – 7.
5. Розподільча здатність камер – HD (1280× 720).

Як бачимо, застосування детектора на відеокамері підвищує ефективність використання модулю охоронного відеоспостереження в 2,3 рази, що досить доцільно при виборі обладнання та його оптимального використання.

Також досить ефективним фактором застосування підсистеми безпеки є систем контролю та керування доступом.

Система контролю і управління доступом являє собою інтелектуальний замок, який дуже часто використовується в багатьох офісах. В якості виконавчого пристрою в даному випадку може виступати безпосередньо сам замок (електромагнітний або електромеханічний), турнікет, електромеханічна клямка, шлагбаум і т.д. Основним призначенням даної системи є пропуск на територію або в будівлю, офіс тільки тих, хто має доступ і заборона в доступі тим, кому не належить проходити в кабінет.

3.2 Застосування обладнання технічного захисту інформації

Блокіратор радіомікрофонів та відео передавачів.

Рисунок 3.7 - Блокіратор радіомікрофонів, відеопередавачів

ФУНКЦІЇ:

– блокування (придушення) несанкціонованої роботи пристроїв, що працюють в стандартах Bluetooth, Wifi, 3g, Dect і частотах 400-450мгц, 1100-1300мгц і 2400мгц;

– блокування роботи пристроїв несанкціонованого прослуховування, несанкціонованої передачі даних, а також, для блокування роботи радіовиконавчих пристроїв, аудіо і відео передавачів, створених з використанням стандартів Bluetooth, Wifi, 3g, Dect.

Пристрій може використовуватися як для одночасного блокування вищеперелічених каналів, так і з можливістю відключення будь-якого з них.

Включення і виключення генератора здійснюється вимикачем, який розташований на його передньою панеле. Включеному стану генератора відповідає свічення світлодіода.

При включенні пристрою відбувається втрата зв'язку призначеним для користувача терміналом, а після його виключення пользовальський термінал повертається в нормальний режим роботи.

У випадку з аудіо-відео передавачами, здійснюється придушення або самого передавача або помеховий сигнал "забиває" вхідний тракт приймача.

Обладнання блокування стільникового зв'язку.

Рисунок 3.8 - БАРХАН-3 / DS-BARHAN-3.

Радіус дії - 40 метрів. Блокує всі стандарти стільникового зв'язку.

У базового виконання пристроєм BARHAN є функціонально закінчений блок, без зовнішніх антен.

BARHAN:

1. Цілодобовий режим роботи в широкому діапазоні температур навколишнього середовища.

2. Відсутність зовнішніх антен, дозволяє вибрати оптимальне місце установки.

3. 2 року гарантії.

4. Плавне регулювання радіусу дії.

5. Управління EGSM.

6. Управління DAMPS.

7. Блокування всіх відомих стандартів стільникового зв'язку.

8. Чотири незалежні канали зі своїми антенними системами.

9. Наявність санітарно-епідеміологічного висновку.

10. Простота установки і використання.

Придавлювач диктофонів ШТОРМ-1С.

ФУНКЦІЇ:

– запобігає просочуванню інформації за рахунок несанкціонованого (скритного) застосування диктофонів і інших портативних засобів звукозапису в стаціонарних умовах.

– Дозволяє боротися з будь-якими типами диктофонів (цифрові і кінематичні). Встановлюється в місцях передбачуваного використання засобів звукозапису.

ДАЛЬНІСТЬ ПРИДУШЕННЯ:

– цифрові диктофони: до 2 метрів;

– кінематичні диктофони: до 3,5 метрів.

Подавлювач складається з генератора сигналу перешкоди і зовнішньої направленої випромінюючої антени. З одним генератором застосовується як правило одна антена.

ШТОРМ-2С - стаціонарний пристрій придушення цифрових і кінематичних диктофонів. Дальність придушення - до 4м (залежно від типу диктофона). Можливість обхвату більшої площі придушення. 2 пульти управління по радіоканалу. Пульт управління по дротяному каналу. Антени виносні направлені 2шт. Живлення 220 В.

Пристрій захисту телефонних переговорів від прослуховування.

Для захисту міської телефонної лінії до АТС методом постановки активної перешкоди, що пригнічує дію практично будь-яких, що існують на сьогоднішній день, телефонних закладок під час розмови. У приладі реалізовано запатентоване рішення, що дозволяє гарантовано запобігати зніманню і передачі інформації по телефонній лінії в проміжках між телефонними переговорами. Прилад дозволяє здійснювати виявлення підключених телефонних закладок і контролювати постійну складову напруги в телефонній лінії.

Захисний модуль простий в експлуатації, практично не вимагає налаштування користувачем, включення захисту при переговорах здійснюється натисненням однієї кнопки на приладі або пульті ДУ. При необхідності можна відрегулювати рівень перешкоди і напруги на лінії, контроль напруги на лінії здійснюється за допомогою вбудованого вольтметра. Модуль забезпечує світлову індикацію режимів роботи і стану телефонної лінії, а також світлову індикацію піратського використання лінії в проміжках між переговорами. Документування телефонних переговорів забезпечується підключенням звукозаписного пристрою.

ОСОБЛИВОСТІ:

– Телефонна лінія під час розмови захищається на всьому протязі лінії від модуля до АТС, а для гарантованого захисту лінії в проміжках між переговорами організована ділянка телефонної лінії підвищеної захищеності, який розташовується між захисним модулем і виносним блокує. Спосіб організації ділянки лінії підвищеної захищеності і його пристрій запатентовані.

– Придушення нормальної роботи телефонних закладок будь-яких типів підключення під час переговорів здійснюється шляхом перевантаження вхідних ланцюгів двома активними перешкодами з разнимі фізичними характеристиками.

– Гарантується блокування роботи комбінованих (телефон/акустика) радіопередавачів в режимі «акустика» (лінія у відбої), як що харчуються від лінії, так і з автономним живленням, підключених на ділянці лінії підвищеної захищеності. Також гарантується блокування проникнення сигналів від апаратури ВЧ-НАВ'ЯЗУВАННЯ на телефонний апарат.

– Вбудований стробуючий пристрій управління напругою і струмом на телефонній лінії блокує нормальну роботу комбінованих радіопередавачів в режимі «телефон».

– Модулем забезпечується помилкове спрацьовування звукозаписною апаратуру системи VOX (VOR), підключеної на телефонну лінію в будь-якому місці, від модуля до АТС. Забезпечується помилкове спрацьовування звукозаписної апаратури, забезпеченої датчиком на перепад напруги, якщо вона підключена на ділянці лінії підвищеної захищеності. При помилковому спрацьовуванні відбувається непродуктивна витрата плівки і батареї живлення звукозаписної апаратури.

Пристрої віброакустичного захисту переговорів.

Модель 2Б апаратури «Соната-АВ».

Система акустичного та віброакустичного захисту "СОНАТА-АВ" модель 2б призначена для захисту мовної інформації, циркулюючої у виділених приміщеннях до першої категорії включно, від витоку по акустичним і віброакустичними каналам.

До складу моделі 2б апаратури "СОНАТА-АВ" входять базові елементи, вказані у табл.4.2.

Генератор-випромінювач "Соната СА-65М" є технічним засобом захисту акустичної мовної інформації, циркулюючої у виділених приміщеннях до 1 категорії включно, від витоку по акустичному каналу шляхом формування шумового сигналу мовного діапазону частот відповідно до вимог “Збірки нормативно-методичних документів по протидії акустичній мовній розвідці”.

Таблиця 3.2 – Базовий склад обладнання віброакустичного захисту

Базовий елемент	Тип базового елементу
Генератор-вібровипромінювач («важкий»)	«Соната-СВ-45М»
Генератор-вібровипромінювач («легкий»)	«Соната-СП-45М»
Генератор-аудіовипромінювач	«Соната-СА-65М»
Мережевий блок електроживлення	«Соната-ИП1», «Соната-ИП2»

Генератор-випромінювач "Соната СА-65М" не утворює каналів просочування інформації за рахунок акустоелектріческих перетворень, може встановлюватися у виділених приміщеннях до 1 категорії включно і відповідає вимогам технічних умов.

Генератор-випромінювач "Соната СВ-45М" є технічним засобом захисту акустичної мовної інформації, циркулюючої у виділених приміщеннях до 1 категорії включно, від витоку по вібраційному каналу шляхом формування шумового сигналу мовного діапазону частот відповідно до вимог “Збірки нормативно-методичних документів по протидії акустичній мовній розвідці”. Генератор-випромінювач "Соната СВ-45М" не утворює каналів просочування інформації за рахунок акустоелектричних перетворень, може встановлюватися у виділених приміщеннях до 1 категорії включно і відповідає вимогам технічних умов.

Генератор-випромінювач "Соната СП-45М" є технічним засобом захисту акустичної мовної інформації, циркулюючої у виділених приміщеннях до 1

категорії включно, від витоку по вібраційному каналу шляхом формування шумового сигналу мовного діапазону частот відповідно до вимог “Збірки нормативно-методичних документів по протидії акустичній мовній розвідці”.

Універсальний блок живлення "Соната-ИП1" не утворює каналів просочування інформації за рахунок у перетворень, може встановлюватися у виділених приміщеннях до 1 категорії включно і відповідає вимогам технічних умов.

Універсальний блок живлення "Соната-ИП2" у складі системи "СОНАТА-АВ" модель 2б є технічним засобом захисту акустичної мовної інформації, циркулюючої у виділених приміщеннях до 1 категорії включно, від витоку по вібраційному каналу шляхом формування шумового сигналу мовного діапазону частот відповідно до вимог “Збірки нормативно-методичних документів по протидії акустичній мовній розвідці”. Універсальний блок живлення "Соната-ИП2" не утворює каналів просочування інформації за рахунок акустоелектріческих перетворень, може встановлюватися у виділених приміщеннях до 1 категорії включно і відповідає вимогам технічних умов.

Рисунок 3.9 - Зовнішній вигляд базових елементів моделі 2б - випромінювача СВ-45М.

Рисунок 3.10 - Зовнішній вигляд базових елементів моделі 2Б Соната-ПРГ1

Ознакою моделі 2Б апаратури "СОНАТА-АВ" є побудова за принципом «єдине джерело електроживлення + генератори-випромінювачі» (рис. 3.11).

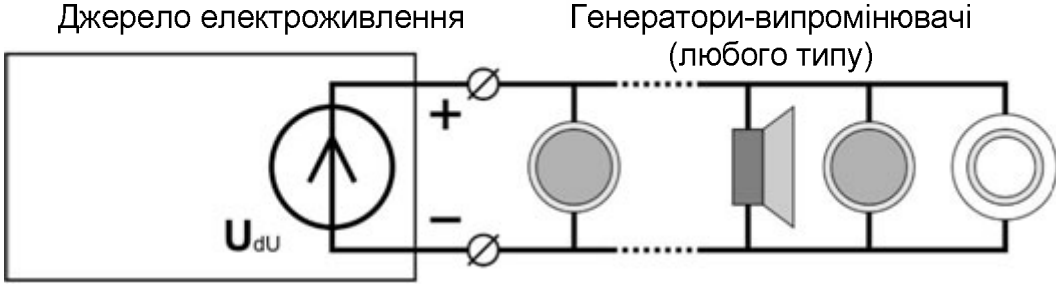

Рисунок 3.11 - Побудова обладнання віброакустичного захисту переговорів за принципом «єдине джерело електроживлення + генератори-випромінювачі

Основними позитивними наслідками такої побудови є:

– відносно невисока вартість системи, а також простота її проектування і монтажу при малій кількості і/або великій різноманітності типів навантажень (можливе підключення до одного живлячого шлейфу будь-яких поєднань генераторів-випромінювачів);

– потенційно вища стійкість захисту мовної інформації унаслідок статистично незалежного збудження маскуючого шуму у всіх каналах витоку;

– потенційна менша дія системи, що заважає, унаслідок можливості регулювання інтегрального рівня і коректування спектру кожного випромінювача.

ОХОРОНА ПРАЦІ

При організації праці, що пов'язана з використанням персональних комп'ютерів, для збереження здоров'я працюючих, запобігання професійним захворювання і підтримки працездатності слід передбачити внутрішньозмінні регламентовані перерви для відпочинку.

Внутрішньозмінні режими праці і відпочинку мають передбачати додаткові нетривалі перерви в періоди, що передують появі об'єктивних і суб'єктивних ознак стомлення і зниження працездатності.

За основну роботу з персональним комп'ютером слід вважати таку, що займає не менше 50% часу впродовж робочої зміни.

Протягом дня мають передбачатися:

- перерви для відпочинку і вживання їжі (обідні перерви);
- перерви для відпочинку і особистих потреб (згідно з нормами);
- додаткові перерви, що вводяться для окремих професій з урахуванням особливостей трудової діяльності.

Тривалість обідньої перерви визначається чинним законодавством про працю і Правилами внутрішнього трудового розпорядку.

Встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

- для розробників програм слід призначати регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи за персональним комп'ютером;
- для операторів персональних комп'ютерів слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години;

– для операторів комп’ютерного набора слід призначати регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи за персональним комп’ютером.

У всіх випадках, коли виробничі обставини не дозволяють застосувати регламентовані перерви, тривалість безперервної роботи з персональним комп’ютером не повинна перевищувати 4 години.

При 12-годинній робочій зміні регламентовані перерви повинні встановлюватися в перші 8 годин роботи аналогічно перервам при 8-годинній робочій зміні, а протягом останніх 4-х годин роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хвилин.

ВИСНОВОК

Захист інформаційного середовища комерційного підприємства – край актуальна багатоетапна задача, в рамках якої необхідно вирішувати проблематику в різних площинах. До того ж, для кожного підприємства система захисту буде різною, бо маємо різні вихідні дані, специфіку роботи, сферу діяльності, соціально-психологічну складову, тощо. У магістерській роботі проведений аналіз методів та рішень захисту інформаційного середовища комерційного підприємства

Результати роботи такі:

1. Розглянуто роль та значення інформації у діяльності комерційного підприємства.

2. Проведено аналіз етапів формування системи управління ризиками, розглянуто методику картографування, індивідуалізації радарів і матриць управління ризиками.

3. Досліджено методологію раціонального вибору технічних засобів забезпечення інформаційної безпеки підприємства.

4. Проведено аналіз оптимальних варіантів застосування технічних засобів охорони інформаційного середовища.

5. Проведено дослідження ефективності функціонування технічних засобів охорони на прикладі комерційного підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Дворский М.М., Палатченко С.М. Технічна безпека об’єктів підприємництва, І том. - Київ: Видавництво "А-ДЕПТ", 2006. – 302 с.

2. Магауренов Р. Г. Системы охранной сигнализации: основы теории и принципы построения / Учебное пособие. М.: Горячая линия-Телеком, 2004.

3. Волхонский В. В. Системы охранной сигнализации / 2-е изд., доп. и перераб. СПб: Экополис и культура, 2005

4. Волонский В. В., Малышкин С. Л.К вопросу единства терминологии в задачах физической защиты объектов / В. В. Волхонский // Информационно-управляющие системы. - 2013. - С. 61-68.

5. Синилов В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации : учебник для нач. проф. образования/ В. Г. Синилов. — 5-е изд., перераб. и доп. — М.: Академия, 2010. — 512 с.

6. Гарсія М. Проектування і оцінка систем фізичного захисту. Пер. з англ. - ТОВ «Издательство АСТ», 2002. - 386 с.

7. Муляр В. Л., Кириллов И. А., Пантелеев В. А., Сумской С. И., Мешалкин Е. А., Глебов С. Н. Комплексное обеспечение безопасности и антитеррористической защищенности зданий и сооружений. Термины и определения. НП СРО "Объединение организаций-разработчиков систем комплексной безопасности", 2010.

8. Петров Н. В. Модель оператора. Роль, место и значение в системе физической защиты / Н. В. Петров. // INSIDE. Защита информации. – 2006. – С. 69–73.

9. Петров Н.В. Проектирование и оценка систем физической защиты / Петров Н.В. // Защита информации. INSIDE №5(11), 2006 - С.58-64.

10. Петров Н.В. Обоснование выбора технических средств обнаружения для систем охранной сигнализации / Петров Н.В. // Защита информации. INSIDE №4(10), 2010 - С.64-70.

11. Гонта А. Проектування охоронних систем з врахуванням вимог безпеки об’єкта //Алгоритм безпеки. № 1, 2008.

12. ГОСТ Р 52860-2007. "Технические средства физической защиты. Общие технические требования". — Введ. 27.12.2007. — М.: Стандартинформ, 2008.

13. ГСТУ 78.11.001-98 Укріпленість об’єктів, що охороняються за допомогою пультів централізованого спостереження державної служби охорони - Київ, 1998 р. - 19 с.

14. ВБН.В.2.5.-78.11.01 – 2003 Інженерне обладнання будинків і споруд. Системи сигналізації охоронного призначення - Київ, 2003 р. - 56 с.

15. Теоретический минимум проектировщика ОПС, 2014 - 87 с.

16. Роль и место технических средств охраны в защите информации [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: http://5fan.ru/wievjob.php?id=63441.

17. Халяпин Д.Б., Ярочкин В.И. Основы защиты информации. М.: ИПКИР, 1994.

18. Каргашин В. Л. Проблемы активной защиты виброакустических каналов//Специальная техника.