DOI: https://doi.org/10.37129/2313-7509.2020.14.1.112-122
УДК 623.45: 623.486

В.Г. Головань[1], к.т.н., проф. https://orcid.org/0000-0002-4451-4703
С.М. Тарасенко[1] https://orcid.org/0000-0002-8779-5621
О.М. Будур[1] https://orcid.org/0000-0003-4193-2616
К.М. Дехтяренко[1]
Р.В. Бубенщиков[2] https://orcid.org/0000-0001-6610-0360
[1]*Військова академія (м. Одеса),Україна*
[2]*Національна академія Сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів, Україна*

ОБҐРУНТУВАННЯ ПРИНЦИПІВ БУДОВИ ТА ОЦІНКИ ЕФЕКТИВНОСТІ ПЕРИМЕТРОВИХ СИСТЕМ ОХОРОНИ АРСЕНАЛІВ, БАЗ ТА СКЛАДІВ

Сучасний стан організації охорони об'єктів зберігання ракет і боєприпасів вказує на недосконаліть встановлених систем периметрової сигналізації та як наслідок на неефективний механізм реагування у разі виникнення надзвичайних подій. Події останніх років, а саме вибухи на арсеналах у м. Балаклея Харківської області та м. Калинівка Вінницької області, польових складах поблизу м. Сватове Луганської області, с. Малоянісоль Донецької області та м. Ічня Чернігівської області вказують на недосконалу систему охорони і оборони місць зберігання.

Мають місце системні упущення в організації систем виявлення проникнення диверсійних груп на територію арсеналів, баз та складів, що показали навчання із залученням Спецназу у серпні-вересні 2018 році.

Ці чинники напряму пов'язані з недостатнім фінансуванням програм по забезпеченню безпечного зберігання ракет і боєприпасів у місцях зберігання, та як наслідок, призводять до виникнення надзвичайних ситуацій.

У всіх випадках розглядалися версії надзвичайних подій, які стали причиною вибухів. До основних версій відносяться умисний підпал, службова недбалість і диверсія, при цьому основною версією була диверсія.

Варто відзначити, що в основі розробки різних систем захисту лежить принцип створення замкнутих, послідовних рубежів, що починаються за межами контрольованої зони і концентрично стягуються до особливо важливих приміщень. На кожному рубежі загрози порушення безпеки повинні бути виявлені за мінімальний час. При цьому периметр – перший і найбільш відповідальний рубіж охорони. Основне завдання охорони периметра території – виявлення порушника під час підходу і подолання лінії периметра.

Саме принцип превентивності є найбільш важливим критерієм системи безпеки об'єкта критичної інфраструктури, що дає можливість отримати інформацію про інцидент до вторгнення порушника, тим самим отримати додатковий час на реакцію і запобігання загрози.

***Ключові слова**: сигналізація, система охорони, арсенал, база, склад, периметр.*

Іноді для захисту рубежу №1 застосовуються системи відеоспостереження (охоронного телебачення) – як найбільш поширене рішення серед технічних засобів охорони. Але варто пам'ятати – відеоспостереження часто не захищає від протиправних дій. Інциденти, які фіксуються відеокамерами, розслідуються набагато пізніше після їх здійснення. Звичайно, якщо система відеоспостереження працездатна, обслуговується і інцидент зафіксований в архіві системи відеоспостереження. Але, за статистикою, це не завжди так. При цьому, незалежно від бюджету рішення і застосовуваної технології, часто саме «людський фактор» нівелює всі переваги і знижує ефективність системи безпеки.

Системи охорони периметра мають ряд якісних особливостей, які відрізняють їх від інших систем охорони. Так, системи охорони периметру (СОП) відрізняються за принципами дії, конструктивним виконанням і варіантами конфігурації. При цьому більшість периметральних систем використовуються для охорони відкритих територій в умовах безперервного впливу несприятливих природних факторів.

При різноманітті технологій, способів реалізації, особливостей проектування, монтажу та обслуговування систем охорони периметра обґрунтування вибору повинно базуватися на критерії вибору оптимальних рішень. Як зазначає у своїй роботі Ю. Тарасов, «вибір оптимального варіанта побудови системи охорони периметру (СОП) здійснюється на основі порівняльного аналізу їх основних характеристик, в першу чергу, таких, як ефективність і вартість.

Постановка проблеми

Говорячи про ефективність, приймається, що ймовірність виявлення порушника системою охорони повинна бути максимальною, а ймовірність помилкових спрацьовувань – мінімальною. Зручно використовувати якісні оцінки (бали) показників надійності виявлення і стійкості до помилкових тривог, які прийнято називати потенціалом виявлення і потенціалом помилкових тривог. Так, згідно з даною методикою, ймовірність виявлення порушника оцінюється в діапазоні від низької (нижче 0,7) до дуже високої (0,98 і вище). Всього в даній моделі застосовується 5 етапів оцінки ймовірності. При оцінці показників виявлення порушника розглядаються різні способи подолання порушником периметра. Так, крім стандартної ходьби і бігу, в оцінці задіяні такі способи пересування порушника, як підкоп, перелаз через огорожу, розрізання загородження, стрибки, перекати тощо.

Аналіз останніх досліджень і публікацій

Автоматизована система охорони об’єкта складається з комплексу інженерно-технічних засобів охорони об’єкта та особового складу охорони.

Комплекс інженерно-технічних засобів охорони об’єкта включає в себе інженерні засоби охорони (фізичні огорожі, проїзні ворота и шлагбауми, контрольно-пропускні пункти і т.п.), комплекс технічних засобів охорони.

У комплекс технічних засобів охорони, в загальному випадку, входять технічні засоби охоронної сигналізації, технічні засоби спостереження, засоби і системи управління доступом та допоміжні пристрої.

Зазвичай виділяються наступні характеристики периметральних сповіщувачів.

1. Вразливість. Даний параметр визначає можливість подолання рубежу без виникнення сигналу тривоги, в тому числі з використанням спеціальних методів і засобів або пристроїв блокування системи.

2. Ймовірність виявлення, тобто ймовірність видачі сигналу тривоги при перетині людиною зони дії датчика. Цим параметром характеризується «тактична надійність» рубежу охорони, тому його величина повинна складати не менше 90-95%. Однак при різних умовах експлуатації він може варіюватися в досить великих межах.

3. Частота помилкових спрацьовувань. Від цього показника багато в чому залежить загальна ефективність всього комплексу безпеки. Прийнятна частота помилкових спрацьовувань для сучасних систем - не більше одного за 10 діб роботи на ділянці довжиною 250 м. Однак слід враховувати, що значний вплив на величину цього параметра надають кліматичні і індустріальні перешкоди, тому при проектуванні периметрової системи охорони в сильно «шумній» зоні необхідно систему сигналізації дублювати (використовувати системи сигналізації з різним принципом дії).

4. Універсальність і гнучкість засобів виявлення. Визначає можливість роботи системи в різних кліматичних умовах і на різноманітних об’єктах.

5. Надійність, довговічність, простота монтажу і експлуатації. Важливі параметри системи, що визначають не тільки витрати на організацію самого периметра, але і на відновлення і експлуатаційне обслуговування.

6. Вартість погонного метра кордону охорони, тобто сумарна вартість апаратури, чутливих елементів, їх монтажу та наладки, що припадають на 1 м довжини периметра.

Існують різні способи побудови системи охорони периметра в залежності від категорії та місця розташування об’єкта:

– із застосуванням одного рубежу охорони;

– із застосуванням двох і більше рубежів охорони.

Однак, при побудові системи охорони периметра із застосуванням двох і більше рубежів охорони необхідно враховувати, що принцип роботи датчиків в системі повинен бути обов’язково різним. Застосування датчиків, робота яких заснована на різних принципах дії дозволяє зменшити ризик подолання порушником периметра об’єкта прихованим способом [2].

Для побудови периметральної системи охорони насамперед потрібно визначити необхідний ступінь захисту об’єкта, проаналізувати можливі дії потенційного порушника і можливість тих чи інших загроз. До

початку проектних робіт слід пройти уздовж передбачуваного розташування основного контуру периметра, оглянути місцевість і особливості ландшафту (пагорби, яри, болота і т.д.). Крім того, необхідно мати дані метеоспостережень, в тому числі про можливість сильних вітрів, снігових заметів, різкої зміни температури, ймовірності туманів і їх щільності. При виборі системи сигналізації слід враховувати розташування поблизу від об'єкту який охороняється індустріальні точки (промислові підприємства, магістралі та інші), які можуть мати значний вплив на кількість помилкових спрацьовувань системи. Остаточний вибір системи організації захисту периметра повинен бути заснований не тільки на обліку початкових витрат на обладнання, але також виходячи з вартості її подальшої експлуатації, підтримки її в робочому стані.

Постановка завдання

Метою статті є розгляд принципів побудови та оцінки ефективності периметрових систем охорони арсеналів, баз та складів:

– проаналізувати можливі загрози і способи подолання рубежу і розглянути модель потенційного порушника;

– провести аналіз кліматичних і погодних умов, можливість утворення снігових заметів, їх можливу висоту (перш за все, у сигналізаційного огорожі), дізнатися діапазон зміни температур та ймовірність сильних вітрів зі швидкістю понад 25 м/с;

– з'ясувати відомості про перетин периметра підземними та надземними магістралями (трубопроводами, естакадами, каналізаційними та кабельними лініями і т. д.);

– визначити вимоги до маскування системи сигналізації та естетичні вимоги.

Виклад основного матеріалу дослідження

Для аналізу технічних засобів забезпечення охорони периметра об'єкту, що входять до складу комплексу КС-200, необхідно розглядати розріз перетину ділянки периметра об'єкта, на якому він розташований.

Радіотехнічні засоби контролю розташовуються між зоною патрулювання і зоною протидії. Це дозволяє забезпечити контроль порушення периметра об'єкту за умови подолання їм зовнішньої фізичної огорожі та контрольної смуги, що знаходиться в зоні патрулювання [5].

Радіотехнічні засоби, які застосовуються в системі радіотехнічного контролю комплексу КС-200, дозволяють забезпечити досить високий рівень технічних параметрів.

Існує кілька підходів до вирішення питання про оцінку ефективності системи охорони периметра (СОП). Один з основних методів, який використовується в даний час, базується на принципах імовірнісно-часового аналізу взаємодії елементів системи охорони периметра (СОП), об'єднаних загальним цільовим призначенням – запобігання несанкціонованого проникнення на об'єкт, що охороняється [3].

Систему охорони периметра (СОП) можна вважати ефективною, якщо сумарний час затримання порушника інженерними засобами охорони буде не більше часу, необхідного для запобігання порушенню:

$$ТЗі - ТП, I=1 \quad (1)$$

де ТЗі – час затримання порушника і-тим інженерним засобом охорони; і – кількість інженерних засобів охорони в забороненій зоні об'єкта (після першого рубежу виявлення); ТП – час, необхідний для запобігання порушенню.

Час подолання порушником периметра об'єкту, що охороняється багато в чому буде залежати від кількості і якості інженерних засобів охорони.

Крім того, ефективність системи охорони периметру (СОП) залежить від імовірності виявлення порушника засобами охоронної сигналізації та спрацювання сигналу тривоги. З моменту спрацювання сигналу тривоги починається виконання функції по запобіганню порушення силами охорони. Периметрова система охоронної сигналізації об'єкту в загальному вигляді складається з засобів виявлення, об'єднаної системи збору та обробки інформації в єдине інформаційне поле.

В ідеальному випадку при всій різноманітності чинників які впливають на систему охорони периметру (СОП), вона повинна забезпечувати нейтралізацію всіх спроб несанкціонованого проникнення на об'єкт. Тому ефективність системи охорони можна оцінити показником ймовірності запобігання будь-яких спроб подолання периметра за розглянутий проміжок часу:

$$Ф = P\ (N>0,\ n = 0,\ t> 0) \qquad (2)$$

де N – кількість спроб подолання периметра за проміжок часу t;

n – кількість випадків які не запобігли порушення за проміжок часу t;

t – розглянутий проміжок часу (наприклад, один рік).

Кожна ділянка системи охорони має певний набір елементів, які характеризуються різними властивостями: надійністю елементів комплексу інженерно-технічних засобів охорони; ймовірністю виявлення порушника; здатністю затримання порушника на заданий час; здатністю оповіщення про спробу порушення; підготовленістю особового складу.

В даний час в інтегрованих системах, при надходженні сигналу тривоги з об'єкту, що охороняється на пульт централізованої охорони (ПЦО) оперативний черговий (оператор) зобов'язаний направити на даний об'єкт групу затримання, яка повинна забезпечити затримання порушника. Виконання даної процедури залежить від часу знаходження порушника на об'єкті охорони, яке може бути, наприклад, оцінено з використанням підходів.

Разом з тим слід зазначити, що даний методологічний підхід не повною мірою може бути застосований до ситуації, коли ставиться завдання не допустити проникнення порушника на об'єкт охорони. Дане завдання актуальна, наприклад, при забезпеченні безпеки підприємств енергетичного комплексу. При цьому для забезпечення безпеки об'єкта необхідно передбачити ряд систем:

- технічних засобів охорони;
- фізичного захисту;
- інженерно-технічного оснащення;
- управління системою охорони об'єкта.

Слід зазначити, що захист об'єкта будується за багаторівневою структурою, в якій можуть бути, наприклад, виділені кілька рівнів захисту, утворені наявністю в загальному випадку декількох незалежних «зон». До таких зон відносяться: контрольована – служить для контролю доступу на територію об'єкта; захищена – прилегла до об'єкта область, оснащена фізичними загородженнями, електронними системами; особлива зона – всередині захищеної зони, оснащена додатковими системами.

Наявність ешелонованої охорони направлено на збільшення часу, що витрачається порушником до його потрапляння на об'єкт захисту. Отже, головним показником виступає фактор часу. В цьому випадку при побудові системи охорони повинен бути реалізований принцип, заснований на ідеї протиборства між протиправною стороною і системою захисту при обмежених ресурсних витратах.

Тому виникає проблема вибору функції-моделі оцінки ефективності системи охорони об'єктів даного типу і формулювання задачі оптимізації.

Завдання функції-моделі оцінки ефективності системи охорони «система розпізнавання + система реагування» і формулювання задачі оптимізації при обмежених ресурсних витратах.

Постановка задачі. Нехай є дві сторони конфлікту: А – протиправна сторона (порушник), Б – сторона, що створює систему охорони за принципом «система розпізнавання + система реагування» з часом, що витрачається на виконання завдання з використанням j-го варіанта побудови системи охорони, (j = 1, ... N).

Сторона А представлена і-м порушником з фіксованим часом, що витрачається їм до досягнення об'єкта захисту (i = 1, ... M).

В цьому випадку для якісного виконання завдання з охорони об'єкта стороні Б необхідно мати часовий ресурс безпеки, величина якого може бути оцінена з виразу:

$$\Delta t_i^{A,Б} = t_i^A - t_j^Б \qquad (3)$$

$$C = \sum_{j=1}^{N} C_j \le C_{доп},$$

За умови обмежень на допустимі фінансові витрати може виступати в якості показника ефективності системи охорони при забезпеченні завдань які виконуються в реальному масштабі часу.

На практиці стратегія сторони А полягає в прагненні мінімізації величини, а сторона Б – до його максимізації, що відповідає тимчасовому ресурсу. Отже, в рамках протиборства сторін А і Б з урахуванням відмінностей варіантів побудови систем, що обумовлює необхідність внесення додаткового часу $\Delta\tau_{ij}$ в умовах обмеженого часового ресурсу безпеки, необхідне виконання співвідношення виду:

$$\Delta t_i^{А,Б} > t_{доп\,\min}^{А} + \Delta\tau_{ij} \tag{4}$$

Виконання співвідношення забезпечує стороні Б в реальному масштабі часу гарантований результат, і в цьому випадку вираз є умовою, при якому об'єкту охорони не завдається шкоди. Слід зазначити, що виконання умови залежить від часів $t_i^{А}$ і $t_j^{Б}$. Приймаючи той факт, що складова часу, продиктована стороною А в даній стратегії, покладається наперед заданої. Тому можна розглянути складову часу $t_j^{Б}$ в «системі розпізнавання + система реагування». Для подальшого міркування опустимо індекси при складових часу. Виходячи з принципів побудови охорони об'єкта і характеру завдань, які вирішуються, величину можна представити у вигляді двох складових:

$$\Delta t^{Б} = t_ч + t_m \tag{5}$$

де $t_ч$ – тимчасові витрати в «системі розпізнавання + система реагування», обумовлені «людським фактором»; t_m – тимчасові витрати в «системі розпізнавання + система реагування», обумовлені використанням комплексу технічних засобів (КТС).

Виходячи з традиційного підходу до побудови системи охорони об'єкта слід врахувати те, що складова часу (другий доданок) у натуральному вираженні обумовлена затримками реагування: оперативного чергового, виходом тривожної групи (сил реагування) з вартового приміщення, рухом тривожної групи від вартового приміщення до об'єкта охорони. З огляду на, що дані операції виконуються послідовно, загальний час обумовлений «людським фактором», визначається як:

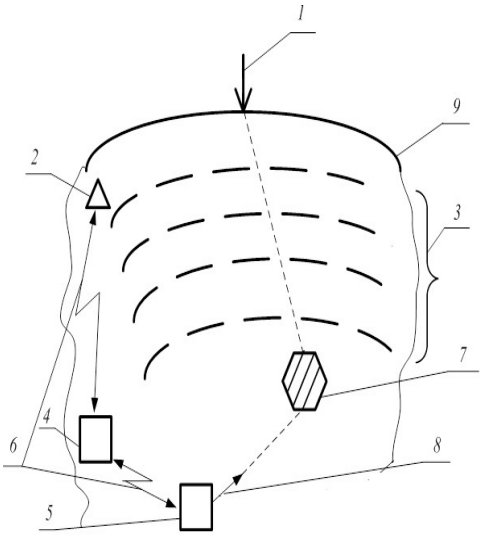
$$t_ч = \tilde{t}_1 + \tilde{t}_2 + \tilde{t}_3 \tag{6}$$

Складові часу, що відображають фактори $t_ч$ (перший доданок) вираження, обумовлені затримками при формуванні інформаційного сигналу: з сповіщувача при передачі інформації від сповіщувача на пульт центральної охорони ПЦО (при передачі інформації від оперативного чергового – групі затримання). З огляду на що дані операції виконуються послідовно в часі, то загальний час, обумовлене використанням технічних коштів, приймає вигляд:

$$t_т = \tilde{t}_1 + \tilde{t}_2 + \tilde{t}_3 \tag{7}$$

Слід зазначити, що в даний час в інтересах ефективності прийняття управлінських рішень використовуються в комплексі технічних засобів сповіщувачі поряд з вирішенням завдання виявлення об'єкта (людина, тварина, транспортний засіб) повинні здійснювати їх класифікацію. В цьому випадку сповіщувач необхідно розглядати як об'єкт автоматизованої інформаційної системи, де здійснюється поетапна обробка даних, носієм яких можуть виступати різні датчики: відеозображення, інфрачервоні і радіолокаційні. Причому радіолокаційні датчики мають перевагу, так як їх робота не пов'язана з часом доби, погодними умовами, освітленням і обмеженими

дальностями дії. Крім того, при використанні широкосмугових сигналів (з внутрішньо-імпульсною модуляцією або без неї) об'єкти локації стають просторово розподіленими цілями. При цьому сигнал містить ряд інформативних ознак, які можуть бути використані в інтересах класифікації об'єктів.



1 – порушник (сторона А); 2 – сповіщувач; 3 – «зони» охорони; 4 – ПЦО; 5 – вартове приміщення; 6 – канали зв'язку; 7 – об'єкт охорони; 8 – група реагування; 9 – зовнішня межа зони, що охороняється.

Рис. 1. Фрагмент топології системи охорони за участю протиборчих сторін А і Б

Виходячи з принципу побудови даного типу сповіщувача, в його склад входить передавальний та приймальний тракти. Передавальний тракт не вносить затримку в величину, а приймальний навпаки вносить, і його величина залежить від схеми побудови приймача обробки сигналу (рис. 1). З аналізу (рис. 1) видно, що рішення про формування сигналу «тривога» приймається за результатами перебування об'єкта в зоні виявлення сповіщувача і обробки сигналу трактом виявлення. Рішення про клас об'єкту виноситься на підставі вимірювання інформативних ознак в тракті сигнального розпізнавання. Отже, час реакції сповіщувача можна представити у вигляді:

$$\hat{t}_1 = t_{обн} + t_{кл} \tag{8}$$

Де $t_{обн}$ – час, що витрачається на виявлення об'єкта;

$t_{кл}$ –час, що витрачається на класифікацію об'єкта.

Слід зазначити, що час залежить від методу розпізнавання і включає дві складові, що витрачаються в тракті сигнального розпізнавання на отримання оцінок інформативних параметрів і на прийняття рішення про клас об'єкту.

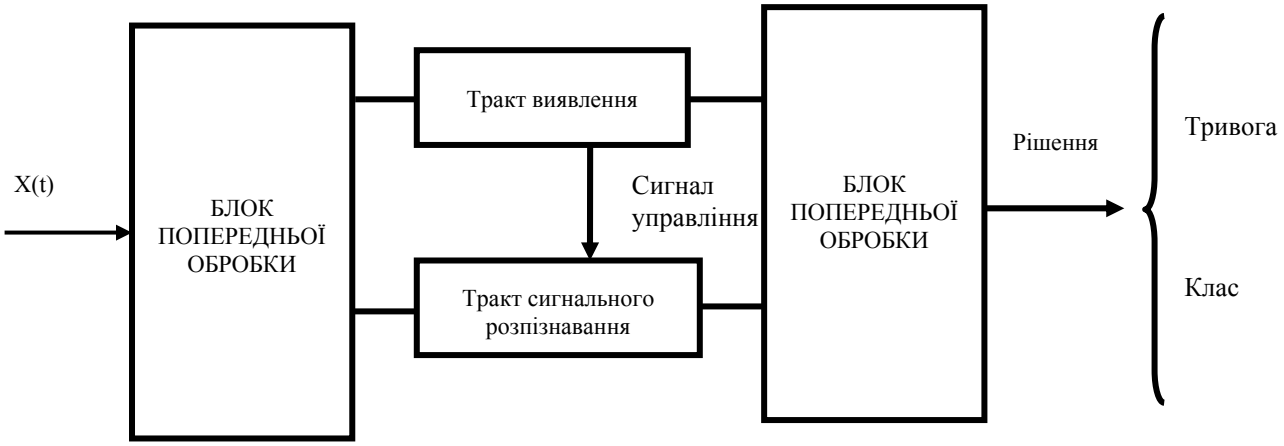


Рис. 2. Узагальнена схема приймача обробки сигналу сповіщувача

Отже, час реакції сповіщувача приводиться до вигляду:

$$\hat{t}_1 = t_{обн} + t_1 + t_2 \tag{9}$$

Складові часу залежать від лінії зв'язку: фізичної (по дротах) або радіоканальної. В результаті цього сумарний час передачі інформації (друга і третя складова у виразі може бути представлено у вигляді:

$$t_{\Sigma}^{n(p)} = \hat{t}_2^n + \hat{t}_3^n + t_2, \quad або \quad \hat{t}_2^n + \hat{t}_3^n \tag{10}$$

$$\hat{t}_2^p + \hat{t}_3^n, \quad або \quad \hat{t}_2^n + \hat{t}_3^n$$

В цьому випадку загальний час, обумовлений використанням комплексу технічних засобів (КТС) в «системі розпізнавання + система реагування», з урахуванням виразів набуває вигляду:

$$t_{\text{т}} = t_{обн} + t_1 + t_2 + t_{\Sigma}^{n(p)} \tag{11}$$

Таким чином, на виконання співвідношення, що характеризує показник часового ресурсу вираження, впливають складові, обумовлені можливостями технічних засобів передачі інформації і складові, обумовлені людським фактором (затримки реагування). В цьому випадку показник часового ресурсу з урахуванням введених раніше індексів набирає вигляду:

$$\Delta t_{\text{і}}^{\text{АБ}} = t_i^A - (\tilde{t}_1 + \tilde{t}_2 + \tilde{t}_3 + t_{\Sigma}^{n(p)} + t_1 + t_2) \tag{12}$$

Разом з тим ефективність системи охорони, яка випливає з виразу, визначається, в основному, затримками при використанні комплексу технічних засобів (КТС) і людським фактором. Оскільки система охорони об'єкта є інформаційною автоматизованою системою комбінованого типу, то інформаційні елементи можуть бути представлені показниками якості, а для оцінки ефективності необхідно вводити узагальнені показники і критерії. Слід зазначити, що при практичній реалізації системи охорони «система розпізнавання + система реагування» необхідно виходити з того факту, що системі даного типу з урахуванням характеру вирішуваних завдань властива дилема. Для оцінки даного судження необхідно ввести в розгляд величину збитку, який би оцінював з точки зору кількісних характеристик можливості системи, синтезованої стороною Б, при наміри сторони А в умовах ресурсних обмежень, що відповідають режиму реального масштабу часу.

Однак аналіз науково-технічної літератури показує, що єдиного підходу до оцінки збитку такого виду автоматизованих інформаційних систем не існує. У відомій літературі описуються підходи до розробки різних видів критеріїв ефективності. Однак їх застосування обмежена, як внаслідок своєї різнотипності, вони розроблялися стосовно до вузького кола поставлених практичних завдань і не можуть бути застосовані в повній мірі до автоматичних систем охорони комбінованого типу, якими є розглянуті системи «система розпізнавання + система реагування». Разом з тим для аналізу можливостей даної системи «система розпізнавання + система реагування» можна ввести узагальнений показник, який буде виступати в якості критерію ефективності. З урахуванням загальновідомого підходу до синтезу інформаційних систем «досягнення максимуму ефективності при мінімумі витрат» і за аналогією в якості такого узагальненого показника може бути використаний в системі «система розпізнавання + система реагування», який визначається наступним чином:

$$E_{\text{ср}+\text{ср}_\text{j}} = K_{об}^{A} \cdot E_{об} (1 - (1 - П_\text{j}^{T^o} П_\text{j}^{ч}) П_\text{у}) \tag{13}$$

де $K_{об}$ – важливість об'єкта, в відносних одиницях;

$E_{об}$ – завданий збиток, що наноситься об'єкту охорони порушником, при відсутності системи охорони, в відносних одиницях (без прив'язки до грошових одиниць);

$П_j^Т$ – показник якості, що характеризує КТС;

$П_j^ч$ – показник якості, обумовлений людським фактором;

$П_у$ – показник, що характеризує фактор виникнення загрози, зумовленої стратегічним вибором сторони А;

^{o} – знак об'єднання, який вказує на арифметичну операцію між елементами множин. $Ц_0 = К_{об}$, $Е_{об}$ – цінність об'єкта охорони

$$E_{\text{ср+ср}_j} = Ц_o \cdot (1 - П_y(1 - П_j^{T\,o} П_j^{ч})) \tag{14}$$

Отже, структура охорони «система розпізнавання + система реагування» в умовах фіксованого часу, що витрачається порушником, відповідна критерієм ефективності «відвернений збиток», може бути знайдена із співвідношення при обмеженнях виду:

$$\begin{aligned} &\xi^* = \arg\max E_{ср+ср,j} \\ &C_j \le C_{доп} \qquad \Delta t_{ij}^{АБ} > 0 \end{aligned} \tag{15}$$

Аналіз виразу показує, що в системі величина збитку безпосередньо залежить від показників якості, а саме, чим вони вищі, тим більш гарантований результат досягається стороною Б. Між тим величину показників необхідно оцінювати. Для цього показники повинні мати явний фізичний зміст, який відображає можливості комплексу технічних засобів (КТС), так і обумовлений впливом людського фактора. Однак дана постановка завдання є предметом подальших досліджень.

В системі може бути передбачений апарат реакцій на спрацювання сигналізації на ділянках периметра – включення освітлення; включення сирени; поворот відеокамер в сторону ділянки, звідки надійшов сигнал тривоги; включення запису з відеокамер на спрацьованій ділянці і т.д.

При виборі обладнання для прийому і обробки сигналів (концентратора) також необхідно передбачити резервні промені, так як в подальшому можливе розширення системи охорони і при додатковій установці будь-яких датчиків буде можливість підключити ці датчики до вже існуючої приймально-контрольної апаратури [1].

Приймальне обладнання периметральної системи обов'язково повинно мати електронний журнал подій (протокол подій) – це пов'язано в першу чергу з великою кількістю потенційних перешкод і мінливим навколишнім середовищем, яке викликає ці перешкоди. Наявність цього журналу допоможе виявити джерела помилкових тривог на етапі налагодження і під час експлуатації.

В умовах протяжного периметра промислових об'єктів, приймально-контрольне обладнання також повинно мати можливість графічного відображення спрацювання ділянки, що дозволить оператору наочно побачити на якій ділянці відбулося спрацьовування датчика (рис. 3).

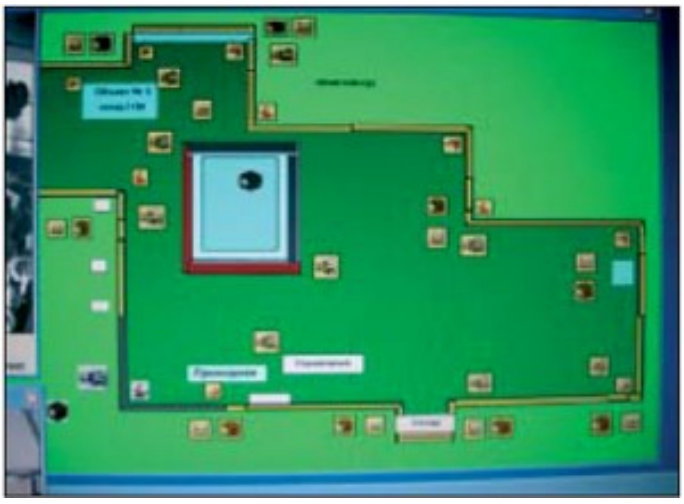


Рис. 3. Графічне зображення периметра на моніторі

На даному етапі проводиться обстеження і вивчення функціонування об'єкта з точки зору його безпеки (особливості функціонування об'єкта, його місце розташування, рельєф місцевості, кліматичні умови, навколишнє оточення, наявність існуючої системи безпеки, характеристика системи електропостачання, перешкоджаючі обставини і т. ін.). А також аналітичні роботи з оцінки загроз, виділення за ступенем важливості окремих зон, розробці моделі порушника і вибору схеми взаємодії технічних засобів захисту і особистого складу охорони. На цьому ж етапі проводиться розробка техніко-економічного обґрунтування або технічного завдання на проектування, в якому детально описується структурна схема комплексу, вибір номенклатури, кількості апаратури, допоміжного обладнання, підбір типів кабелів, способів прокладки, укрупнені кошторисні розрахунки витрат з урахуванням робіт з проектування, придбання і виготовлення, монтажу і налагодження обладнання [4].

Для того щоб система контролю служила якомога довше, необхідна грамотна технічна і оперативна експлуатація комплексу. Обов'язково слід передбачити проведення поточного технічного обслуговування відповідно до вимог експлуатаційної документації на апаратуру. Планово-попереджувальні роботи зазвичай здійснюються в режимі перевірок, вимірювань і регулювань встановленого обладнання. Вони дозволяють виявити будь-яке погіршення параметрів системи і можуть передбачати проведення відновлювальних робіт, які доводять систему до прийнятного стану. Процедури планово-попереджувального обслуговування розробляються постачальником обладнання і включають в себе перелік перевірок, методику перевірок, склад використовуваного для проведення перевірок обладнання, критерії відмов і заходи щодо їх усунення.

Висновки

Таким чином, розглянута автоматизована комбінована система охорони об'єктів, побудована за принципом «система розпізнавання + система реагування», розроблена математична модель і введений критерій ефективності дозволяють пред'явити обґрунтовані вимоги до елементів системи охорони периметрів і підвищити ефективність прийняття управлінських рішень.

Список використаних джерел

1. Дворський М.М., Палатченко С.М. Технічна безпека об'єктів підприємництва, І том: Київ: Видавництво «А-ДЕПТ», 2006. – 302 с.

2. Рувинова Э. Охрана периметров. Средства обнаружения и сигнализации: / Э. Рувинова. // Электроника: Наука, технология, бизнес. – 2001. – С. 48–51.

3. Варнеев Н. Системы охраны периметра – задачи и проблема выбора / Н. Варнеев, В. Никитин. // БДИ(Безопасность, достоверность, информция).№2(65) – 2006. – С. 40–47.

4. Тарасов Ю. Моделирование систем охраны периметра / Ю. Тарасов. // Алгоритм безопасности. – 1/2012. – С. 60–62.

5. Петровский Н.П., Пинчук Г.Н. Периметровые технические средства обнаружения нарушителей: особенности выбора // Системы безопасности средств связи. - 2000. - № 1. - С. 50-55.

References

1. Dvorsky, M.M., & Palatchenko, S.M. (2006). *Tekhnichna bezpeka obyektiv pidpryyemnytstva [Technical safety of business facilities],* (Vol.1). Kyiv: A-DEPT [in Ukrainian].

2. Ruvinova, E.V. (2001). Okhrana perimetrov. Sredstva obnaruzheniya i signalizatsii [Perimeter protection. Means of detection and signalling]. *Elektronika: Nauka, tekhnologiya, biznes, 1,* 48-51 [in Russian].

3. Varneyev, N., & Nikitin V. (2006). Cistemy okhrany perimetra – zadachi i problema vybora [Perimeter security systems – tasks and the problem of choice]. *BDI (Bezopasnost', dostovernost', informtsiya), 2(65),* 40-47 [in Russian].

4. Tarasov, U.A. (2012). Modelirovaniye sistem okhrany perimetra [Modeling of perimeter security systems]. *Algoritm bezopasnosti, 1,* 60–62 [in Russian].

5. Petrovsky, N.P., & Pinchuk, G.N. (2000). Perimetrovyye tekhnicheskiye sredstva obnaruzheniya narushiteley: osobennosti vybora [Perimeter technical means of detecting intruders: features of the choice]. *Sistemy bezopasnosti sredstv svyazi, 1,* 50-55 [in Russian].

Рецензент: Петрушенко М.М., доктор технічних наук, професор, Військова академія (м. Одеса), Україна

ОБОСНОВАНИЕ ПРИНЦИПОВ СТРОЕНИЯ И ОЦЕНКИ ЭФФЕКТИВНОСТИ ПЕРИМЕТРОВ СИСТЕМ ОХРАНЫ АРСЕНАЛОВ, БАЗ И СКЛАДОВ

В. Головань, С. Тарасенко, О. Будур, К. Дехтяренко, Р. Бубенщиков

Современное состояние организации охраны объектов хранения ракет и боеприпасов показывает несовершенство установленных систем периметров сигнализации и как следствие неэффективный механизм реагирования в случае возникновения чрезвычайных событий. События последних лет, а именно взрывы на арсеналах в г. Балаклея Харьковской области и Калиновка Винницкой области, полевых складах вблизи Сватово Луганской области, с. Малоянисоль Донецкой области и г. Ичня Черниговской области указывают на несовершенную систему охраны и обороны мест хранения. Имеют место системные упущения в организации систем обнаружения проникновения диверсионных групп на территорию арсеналов, баз и складов, показали учения с привлечением спецназа в августе, сентябре 2018 года. Эти факторы напрямую связаны с недостаточным финансированием программ по обеспечению безопасного хранения ракет и боеприпасов в местах хранения, и, как следствие, приводят к возникновению чрезвычайных ситуаций. Во всех случаях рассматривались версии чрезвычайных событий, которые стали причиной взрывов. К основным версиям относятся умышленный поджог, служебная халатность и диверсия, при этом основной версией была диверсия. Стоит отметить, что в основе разработки различных систем защиты лежит принцип создания замкнутых, последовательных рубежей, начинающиеся за пределами контролируемой зоны и концентрически взымаемых в особо важных помещениях. На каждом рубеже угрозы нарушения безопасности должны быть выявлены за минимальное время. При этом периметр – первый и самый ответственный рубеж охраны. Основная задача охраны периметра территории – выявление нарушителя во время подхода и преодоление линии периметра. Именно принцип превентивности является наиболее важным критерием системы безопасности объекта критической инфраструктуры, что позволяет получить информацию об инциденте в вторжения нарушителя, тем самым получая дополнительное время на реакцию и предотвращения угрозы.

Ключевые слова: *сигнализация, система охраны, арсенал, база, склад, периметр.*

SUBSTANTIATION OF PRINCIPLES OF STRUCTURE AND EVALUATION OF EFFICIENCY OF PERIMETER SYSTEMS OF PROTECTION OF ARSENALS, BASES AND WAREHOUSES

V. Golovan, S. Tarasenko, O. Budur, K. Dekhtyarenko, R. Bubenshchikov

The current state of organization of protection of missile and ammunition storage facilities shows the imperfection of the installed perimeter alarm systems and, as a result, an ineffective response mechanism in case of emergencies. Events of recent years, namely explosions at arsenals in Balakleya, Kharkiv region and Kalynivka, Vinnytsia region, field depots near Svatove, Luhansk region, Maloyanisol, Donetsk region, and Ichnia, Chernihiv region, point to an imperfect system of protection and defense of storage sites. There are systemic omissions in the organization of systems for detecting the penetration of sabotage groups into the territory of arsenals, bases and warehouses, which showed training with the involvement of Special Forces in August, September 2018. These factors are directly related to the lack of funding for programs to ensure the safe storage of missiles and ammunition in storage, and, as a result, lead to emergencies. In all cases, versions of the emergencies that caused the explosions were considered. The main versions include arson, negligence and sabotage, with the main version being sabotage. It should be noted that the development of various protection systems is based on the principle of creating closed, consistent boundaries that begin outside the controlled area and are concentrically tightened to particularly important premises. At each border, threats of security

breaches must be identified in a minimum amount of time. The perimeter is the first and most responsible line of protection. The main task of protecting the perimeter of the territory is to detect the violator during the approach and to overcome the perimeter line. The principle of prevention is the most important criterion of the security system of the critical infrastructure, which makes it possible to obtain information about the incident before the intruder, thus gaining additional time to respond and prevent the threat.

Sometimes video surveillance systems (security television) are used to protect the border №1 – as the most common solution among technical means of protection. But it is worth remembering – video surveillance often does not protect against illegal actions. Incidents recorded by video cameras are investigated much later after they are committed. Of course, if the video surveillance system is operational, the incident is serviced and the incident is recorded in the archives of the video surveillance system. But, according to statistics, this is not always the case. In this case, regardless of the budget of the solution and the technology used, it is often the «human factor» eliminates all the benefits and reduces the effectiveness of the security system. Perimeter security systems have a number of qualitative features that distinguish them from other security systems. Thus, perimeter security systems differ in the principles of operation, design and configuration options. At the same time, most perimeter systems are used to protect open areas in the face of continuous exposure to adverse natural factors. With a variety of technologies, methods of implementation, features of design, installation and maintenance of perimeter security systems, the rationale for the choice should be based on the criteria for selecting optimal solutions. As Yu. Tarasov notes in his work, «the choice of the optimal option for building a perimeter security system is based on a comparative analysis of their main characteristics, primarily such as efficiency and cost».

Keywords: *alarm system, security system, arsenal, base, warehouse, perimeter.*