УДК 654:94

# ПОБУДОВА КОМПЛЕКСНОЇ СИСТЕМИ ОХОРОНИ ПЕРИМЕТРА СТРАТЕГІЧНОГО ОБ'ЄКТУ

А. М. Лузан[1], В. М. Степаненко[1]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

## Анотація

В роботі розглянуто рішення для захисту периметра стратегічних об'єктів. Сформульовано основні вимоги до комплексів безпеки таких об'єктів. Дане питання є важливим, оскільки до системи безпеки стратегічних об'єктів пред'являються найвищі вимоги.

*Ключові слова*: система захисту периметра, система контролю доступу, системи виявлення, інтегровані комплекси безпеки

## Вступ

До системи безпеки стратегічних об'єктів пред'являються високі вимоги. Порушення їх нормального функціонування призведе до численних людських жертв, екологічних лих або серйозних економічних втрат, а тому не тільки спланований теракт, а й проста недбалість може призвести до непоправних наслідків. До класу стратегічних об'єктів в першу чергу відносяться:

- атомні, теплові та гідроелектростанції;
- газо- і нафтопроводи;
- військові бази;
- великі продуктохраніліща;
- сховища радіоактивних і хімічних речовин;
- закриті лабораторії та науково дослідні центри.

Незважаючи на різноманітність і різні призначення перерахованих вище об'єктів, їх об'єднують найвищі вимоги до питань безпеки.

## 1. Основні завданнями комплексу безпеки стратегічного об'єкту

Інтегрований комплекс безпеки (ІКБ) призначений для забезпечення комплексної безпеки об'єктів різного масштабу і призначення. Основні завданнями комплексу безпеки стратегічного об'єкту є:

- захист периметра об'єкта;
- захист від несанкціонованого доступу на територію об'єкта;
- розмежування прав доступу персоналу залежно від рівня секретності приміщення;
- забезпечення розподіленого відеоконтролю за всіма процесами на об'єкті, що охороняється;
- організація єдиного центру моніторингу та управління всіма системами комплексу;
- забезпечення інформаційної взаємодії підсистем, тобто будь-яка ситуація (прохід людини через турнікет, спрацювання охоронного датчика, поява людей в зоні видимості відеокамер), зафіксована однією з підсистем, обробляється єдиним аналізатором і може змінювати параметри роботи інших підсистем;
- забезпечення гнучкої логіки програмування алгоритмів дії у відповідності до специфічних вимог до охорони об'єктів;
- забезпечення інформаційної безпеки
- автоматичне включення системи оповіщення персоналу про пожежу й системи пожежогасіння в разі виникнення пожежі;
- організація автоматичного пожежогасіння для окремих приміщень і територій залежно від їх категорійності вибухо-, пожежонебезпеки;
- можливість використання автоматизованої (за участю оператора) і автоматичної (без участі оператора) тактики охорони.

Типовий інтегрований комплекс безпеки стратегічного об'єкту включає такі системи:

- захисту периметра;
- інтелектуального відеоконтролю;
- управління та контролю доступу;
- охоронної сигналізації;
- пожежної сигналізації;
- автоматичного пожежогасіння.

Система захисту периметра є першим рубежем охорони і призначена для запобігання несанкціонованому проникненню небажаних осіб на територію стратегічно важливого об'єкта. Як правило, така система багаторівнева і складається з [1]:

- фізичного бар'єру, що запобігає прямому проникненню і перетину контрольованої зони (паркани);
- контрольної смуги, що констатує факт вторгнення на територію, що охороняється;
- активної зони, що забезпечена датчиками сповіщення про порушення в контрольованій зоні (мікрохвильові, радіопроменеві, радіохвильові, ємнісні, вібраційні та інфрачервоні);
- другого фізичного бар'єру із застосуванням активного впливу на порушника (колючий дріт,

провідно-натяжна система під високою напругою);

Паралельно з вищезгаданою системою найбільш вразливі місця периметра обладнуються засобами інтелектуального відеоконтролю, інтегрованими в єдиний комплекс безпеки (стаціонарні та роботизовані відеокамери високої роздільної здатності з функцією день/ніч та інфрачервоним підсвічуванням). Наприклад, у випадку спрацювання периметральної сигналізації, включається відеоконтроль з відповідної камери спостереження і оператор має можливість оперативно відреагувати на позаштатну ситуацію.

## 2. Система інтелектуального відеоконтролю

Одним з елементів інтегрованого комплексу безпеки є система інтелектуального відеоконтролю, що виконує наступні функції:

- цілодобовий відеоконтроль на об'єкті, реєстрація всього, що відбувається в реальному часі з одночасним записом відеоінформації в архів, що дає можливість здійснювати перегляд і подальший аналіз подій, що відбулися;
- контроль внутрішніх приміщень і зовнішньої території на об'єкті, з автоматичним виявленням несанкціонованого переміщення в зонах, що охороняються (використовується інтелектуальний детектор руху);

Система відеоконтролю також реалізує функцію віддаленого контролю технологічних процесів, що відбуваються на об'єкті, дозволяючи персоналу об'єкта постійно вести спостереження за процесами, що відбуваються в реальному часі, і в той же час знаходитись на безпечній відстані від об'єкта спостереження. Ця функція є незамінною для забезпечення безпеки радіоактивно і хімічно небезпечних об'єктів (АЕС, військові лабораторії, сховища радіоактивних та токсичних відходів тощо).

Система автоматизованого контролю автотранспортом дозволяє:

- розпізнавати номери всіх в'їжджаючих/виїжджаючих машин і залізничних вагонів;
- отримувати інформацію про вагу автомобіля і автоматично порівнювати з офіційно заявленою вагою;
- отримувати інформацію про вагу залізничних вагонів в динаміці і автоматично порівнювати з вагою до і після завантаження;
- видавати звіт про кількість залитого пального.

## 3. Система контролю доступу

Система контролю доступу інтегрована в комплекс безпеки об'єкта дозволяє побудувати кілька ліній захисту від несанкціонованого доступу з розмежуванням прав на відвідування приміщень різного ступеня важливості [2].

На перших рубежах розмежування контролю доступу здійснюється, як правило, за допомогою Proximity карток. Для дозволу доступу в особливо важливі приміщення доцільно використовувати біометричні системи розмежування доступу (зчитувачі відбитків пальців, модулі розпізнавання по райдужній оболонці ока, модуль розпізнавання осіб Face-ID), які максимально гарантують захист від доступу сторонніх осіб і повністю усувають небезпеку підробки засобів особистої ідентифікації.

Вимоги до системи контролю доступу стратегічних об'єктів:

- запис в базу даних інформації про персонал і складання звітів про переміщення персоналу по території об'єкта;
- забезпечення алгоритму анти пас-бек (один раз пройшовши через точку контролю доступу, її не можна перетнути вдруге, не вийшовши через цю або аналогічну за рівнем точку;
- контроль працездатності системи, а також можливість інформування охорони про вихід з ладу обладнання або каналу зв'язку;
- відстеження стану охоронної та пожежної сигналізації та можливість блокування/розблокування дверей за заздалегідь визначеним алгоритмом;
- реєстрація всіх подій в системі і зберігання їх у протоколі;
- повноцінна автономна працездатність системи у випадку повного відключення електроживлення на протязі як мінімум 30 хв.

## 4. Система охоронної сигналізації

Система охоронної сигналізації, що входить до складу комплексної системи безпеки, забезпечує роботу спеціалізованих охоронних панелей, широкого спектра сенсорів, "тривожних" кнопок, засобів оповіщення і т. П. Всі елементи охоронної сигналізації знаходяться під управлінням програмного ядра комплексу і мають єдину логіку роботи. Переваги такого підходу очевидні - користувач отримує не набір розрізнених датчиків і сенсорів, а потужну систему, компоненти якої ефективно взаємодіють один з одним.

Система охоронної сигналізації стратегічного об'єкта реалізує наступні функціональні можливості:

- будь тривожна подія ініціює графічне і звукове повідомлення на робочих місцях охоронців із зазначенням адреси тривоги;
- реєструє всі тривожні подій з негайним виведенням про них графічних і звукових повідомлень, контролює їх отримання охоронцями і зберігає їх у протоколах;
- підтримує різні типи сповіщувачів (ІЧ пасивні або активні, ІЧ + НВЧ, акустичні розбиття скла, магніто-контактні, вібраційні, ультразвукові і т.д.).
- здійснює повноцінну автономну працездатність у разі відключення електроживлення.

## 5. Система пожежної сигналізації та пожежогасіння

Система пожежної сигналізації та пожежогасіння дозволяє:

- реалізувати можливість графічного та звукового сповіщення про виникнення загрози пожежі;
- здійснити підключення датчиків контролю хімічного зараження;
- керувати системами вентиляції, кондиціонування, знезараження (у разі хімічного зараження проводити автоматичну вентиляцію зараженого приміщення);
- інтегруватися з системою контролю доступу та здійснювати можливість блокування (у разі хімічної або радіаційного забруднення) або розблокування (в разі пожежі) окремих зон об'єкта;
- забезпечувати видачу сигналу пожежної тривоги на пульт позавідомчої охорони;
- створити систему захисту від помилкового спрацьовування;
- зберігати дані в незалежній пам'яті і відображати в графічному вигляді на дисплеї ППК;
- здійснювати локалізацію та ліквідацію загорянь;

## 6. Аналіз ефективності інтегрованих систем безпеки

Ефективність будь-якої складної технічної системи (СТС) відображає її пристосованість до виконання своєї цільової функції [3]. Так, ГОСТ 34.003-99 визначає ефективність автоматизованої системи як "властивість, що характеризується ступенем досягнення цілей, поставлених при створенні системи". Зокрема, ефективність ІСБ можна охарактеризувати як здатність системи протистояти несанкціонованим діям порушника в рамках проектної загрози. Таким чином, ефективність ІСБ і характеризує рівень захищеності об'єкта.

Існують якісні та кількісні методи аналізу. У багатьох випадках якісних оцінок бінарного типу (відповідає/не відповідає вимогам) цілком достатньо, щоб відповісти на питання, наскільки захищений об'єкт. Для того, щоб "виміряти" ефективність кількісним методом, необхідно мати обґрунтований критерій. Критерій ефективності (критерій оптимальності) - ознака, що дозволяє дати порівняльну оцінку запропонованих альтернатив і вибрати оптимальне рішення. На практиці застосовують такі типи критеріїв:

- критерії типу "ефект-витрати", що дозволяють оцінювати досягнення цілей функціонування СТС при заданих витратах (так звана економічна ефективність);
- елімінуючі критерії, що дозволяють оцінити якість СТС за заданими показниками і виключити ті варіанти, які не задовольняють заданим обмеженням;
- зважуючі критерії - штучно сконструйовані критерії, що дозволяють оцінювати інтегральний ефек.

Інтегрована система безпеки являє собою збалансовану сукупність елементів виявлення порушника, затримки просування порушника по шляху прямування, а також елементів реагування сил охорони на дії порушника. Ці елементи є цільовими функціями системи. Кожна з них характеризується рядом показників (ймовірність виявлення датчика виявлення, напрацювання на помилкове спрацювання, ймовірність відмови датчика, способи подолання фізичних бар'єрів, час збору та розгортання сил охорони і т.д.). Оцінивши наведені характеристики тим чи іншим способом, можна зробити судження про ефективність ІСБ в цілому. Існують наступні методи аналізу:

- детерміністичний підхід;
- методи багатокритеріальної оптимізації;
- логіко-імовірнісне моделювання;
- імітаційне моделювання.

Детерміністичний підхід пов'язаний із завданням і подальшою перевіркою вимог, що містяться в НТД, ТЗ на проектування, в робочому проекті обладнання об'єкта засобами охоронно-тривожної сигналізації. Перевагою детерміністичного підходу є те, що в руки проектувальника даються чіткі і ясні критерії того, як обладнати об'єкт технічними засобами охорони. Основна проблема - спосіб отримання інтегрального показника.

Основою методів багатокритеріальної оптимізації є агрегування інформації про окремы показники якості. Серед них виділяють методи лексикографічного упорядкування, ітераційні методи кращого вибору, аксіоматичний підхід з використанням теорії корисності та ін.

Логіко-імовірнісні методи дозволяють отримати кількісну оцінку ризику як міри небезпеки. Вони давно застосовуються у вітчизняній практиці для аналізу надійності та безпеки СТС. В основі лежать два поняття: ступінь ризику і рівень захищеності. Ступінь ризику - ймовірність невиконання ІСБ своєї цільової функції. Зворотній величина характеризує рівень захищеності.

Логіко-імовірнісне моделювання дозволяє побудувати модель безпечного функціонування ІСБ, визначити "вразливі місця" системи і оцінити "внесок" кожного з них, ранжуючи їх за ступенем небезпеки. Як недолік тут можна відзначити трудомісткість логічних перетворень при аналізі складних сценаріїв (перехід від функції небезпечного стану до ймовірнісної функції).

Імовірнісний підхід до аналізу базується на припущеннях про випадковість та незалежність часових параметрів в системі "охорона-порушник". Ефективність тут розуміється як ймовірність припинення несанкціонованих дій порушника. Один з методів оцінки цієї вероятності- імітаційне моделювання. Це обчислювальний експеримент, заснований на тому відомому факті, що при збільшенні числа випробувань n відносна частота появи випадкової події A в серії випробувань прямує до його ймовірності в одиничному випробуванні. Перевагою імітаційного моделювання є фізично обгрунтований критерій ефективності (ймовірність). Недолік - труднощі його інтерпретації та нормування. Наприклад, в результаті аналізу отримано значення $P = 0.9$. Не зрозуміло, чи достатній рівень захисту об'єкта при такому коефіцієнті чи ні?

## Висновки

Забезпечити надійний захист об'єкту неможливо без використання комплексних систем безпеки, що включають в себе системи контролю доступу, оповіщення, охоронно-пожежну сигналізацію і т.д. Можна виділити наступні переваги впровадження інтегрованих комплексів безпеки:

- підвищення рівня безпеки об'єкта в цілому (запобігання аварій, забезпечення безперервності процесів контролю та управління);
- організацію мережевої структури управління з реалізацією функцій автоматичного контролю, обробки, аналізу та зберігання інформації про стан систем і дій оператора системи з єдиного диспетчерського пульта управління;
- можливість інтеграції на інформаційному рівні (протокол обміну) з системами різних підрозділів підприємства;
- забезпечення своєчасної локалізації аварійних ситуацій;
- підвищення економічної ефективності діяльності підприємства.

В результаті роботи було проаналізовано системи, що входять до складу інтегрованого комплексу безпеки, та сформульовано основні вимоги до таких систем. Було наведено критерії та методи оцінки ефективності інтегрованих комплексів безпеки.

## Перелік використаних джерел


1. Введенский Б. С. Современные системы охраны периметра — К. : Специальная техника, 1999. — №4
2. Ерошин Р., Глебовский Алгоритм Безопасности. — 2006. — № 4.
3. Панин О.А. С. Системы безопасности. — 2006. — № 2.