

Міністерство надзвичайних ситуацій України

Національний університет цивільного захисту України
Кафедра автоматичних систем безпеки та інформаційних технологій

ЗАТВЕРДЖУЮ
Начальник кафедри
полковник сл. цив. захисту
О.А. Дерев'янка
“ ____ ” _____ 2018 р.

Лекція № 8
з дисципліни "Автоматичні системи забезпечення протипожежного захисту"

Розділ 2
Принципи побудови автоматичних систем протипожежного захисту

Тема 2
Принципи побудови автоматичних систем протипожежного захисту

Тема лекції
СУЧАСНІ КОМПЛЕКСНІ СИСТЕМИ БЕЗПЕКИ ОБ'ЄКТІВ

Лекція обговорена на засіданні кафедри
Протокол № ____ від _____ 2018 р.

ХАРКІВ - 2018

План лекції.

1. Загальні вимоги до створення комплексних систем безпеки об'єктів.
2. Принципи організації інтегрованих систем і комплексів безпеки
3. Приклади технічної реалізації КСБ.

Питання 1. Загальні вимоги до створення комплексних систем безпеки об'єктів

Для створення необхідного рівня безпеки об'єкта і його персоналу нормативні документи допускають застосування для його захисту комплексних систем безпеки (КСБ). У цьому випадку функції спільно діючих різних систем повинні доповнювати один одного, не роблячи взаємного впливу на працездатність своїх складових частин. У спільно діючих системах повинні забезпечуватися алгоритмічна сумісність і роздільна реєстрація вступників від них службових і тривожних сигналів. Створення сучасних комплексів безпеки різних об'єктів, як правило, вимагає використання інтегрованих систем, до складу яких входять наступні основні системи:

- охоронно-тривожної сигналізації;
- пожежної сигналізації;
- контролю і керування доступом;
- охоронного телебачення;
- збору, обробки і відображення інформації;
- пожежогасіння і димовидалення;
- оповіщення і управління евакуацією;
- оперативного зв'язку;
- гарантованого електроживлення.

Структура КСБ виконується за класичною схемою. Як правило, вона складається з наступних елементів:

- сервер або головний комп'ютер, де зберігаються і обробляються всі бази даних системи;
- робочі станції окремих систем (при необхідності), що здійснюють обмін даними і командами з периферійними пристроями своїх підсистем і виконуючу попередню обробку одержуваної інформації;
- периферійні пристрої (контролери, розширники, пульти керування і т.п.), безпосередньо на апаратному рівні взаємодіючі зі своїми сповіщувачами, датчиками або виконавчими пристроями, а на інформаційному рівні об'єднуються по локальному інтерфейсу (RS-485, RS-232) з робочими станціями або з головним комп'ютером;
- сповіщувачі охоронної, тривожної, пожежної сигналізації, клавіатури, телекамери, світлові і звукові оповіщувачі і т.п.;

- локальна мережа ethernet, що інформаційно зв'язує в єдиний інтегрований комплекс окремі системи, кожна з яких може функціонувати окремо і незалежно;

- мережне, системне і прикладне програмне забезпечення сервера і робочих станцій, а також мікропрограмне забезпечення системних контролерів, контрольних панелей і модулів;

- система гарантованого електроживлення, що містить у собі: електрощитові КСБ, підключену до мережі 220 В першої категорії, що містить весь необхідний набір вхідних і вихідних силових автоматів;

- джерела безперебійного живлення (ИБП), що забезпечують безперервне і якісне електроживлення всієї апаратури КСБ протягом заданого часу;

розгалужену по всьому об'єкті окрему мережу живлення з розміщенням при необхідності окремих ІБП у спеціально виділених приміщеннях, нішах або шафах, що перебувають під охороною.

При проектуванні систем комплексної безпеки об'єктів доводиться вирішувати ряд послідовних завдань. Насамперед, необхідно виділити конкретні аспекти в організації безпеки з урахуванням потреб і специфіки об'єкта. Далі, виходячи з оцінки ймовірного збитку у випадку здійснення злочинної акції треба визначити значимість виділених аспектів. Це найбільш складне завдання, і у більшості випадків оцінка ймовірного збитку не може бути виражена точним кількісним значенням. Потім необхідно провести ретельне обстеження об'єкта з метою виявлення його найбільш уразливих для проникнення місць. Для цього вивчаються і аналізуються місця і порядок зберігання матеріальних і інших цінностей, розташування телефонних, комп'ютерних і інших ліній зв'язку, електричних, водопровідних, вентиляційних і інших інженерних комунікацій. Іншими словами, повинні бути виявлені місця і шляхи досить «простого», неконтрольованого доступу як на сам об'єкт, так і до його матеріальних і інших цінностей. Таке обстеження дозволяє змодельовати можливе поведіння зловмисника і сценарій його передбачуваних дій.

Основним підсумком обстеження на даному етапі повинне стати визначення зон і точок захисту об'єкта і встановлення ступенів їхньої значимості. При побудові КСБ об'єкта і аналізі її ефективності обрані зони і точки захисту розглядаються як первинні структурні елементи. На практиці зонами і точками захисту можуть бути як окремі будівельні елементи об'єкта (вікна, двері, ворота, входи, паркан і т.д.), так і його територія, її периметр, будинки і спорудження, окремі приміщення, зони на території і в будівлі і т.д.

Коли структура КСБ об'єкта обрана, важливо визначити можливі засоби для її побудови. У першу чергу, розглядаються кадрові ресурси. При протидії злочинним зазіханням вони відіграють основну роль, несучи охоронну службу, проводячи профілактичні заходи, організовуючи і підтримуючи заданий режим роботи КСБ і об'єкта в цілому.

Крім визначення складу необхідних кадрових ресурсів потрібно намітити набір технічних засобів, які будуть використані при побудові КСБ об'єкта. За допомогою технічних засобів забезпечення безпеки відбувається блокування загроз, автоматичний контроль цілісності границь зон захисту, ведеться дистанційний візуальний контроль, оперативно змінюється ступінь захищеності охоронюваних зон і об'єкта (наприклад, блокування дверей при проникненні злоумисників або, навпаки, їхнє розблокування у випадку пожежі). Крім того, автоматично протоколюються несанкціоновані зміни в точках і зонах захисту, а у випадку порушення або проникнення в зону захисту порушників фіксуються події і дії охорони по їхньому знешкодженню.

Обсяг і состав устаткування, використовуваного в кожній із систем, що входить в КСБ об'єкта, залежать від його призначення і значимості. Критерієм оцінки при виборі варіанта спільного використання декількох систем на об'єкті є компроміс між вартістю можливих втрат і витратами на його реалізацію.

Пріоритетними для виконання є вимоги, що забезпечують безпеку для життя людей і пожежну безпеку об'єкта. КСБ повинна, насамперед, забезпечувати необхідну функціональну і апаратну надійність, пожежну безпеку і завадостійкість.

Технічні засоби управління і контролю функціонування, спільно діючих систем повинні визначатися цільовим їх призначенням. Кращі автоматичні засоби управління і контролю, але в якості дублюючих допускаються і ручні. Доцільність дублювання визначається вимогами забезпечення експлуатаційної надійності систем.

Засоби управління і контролю повинні мати захист від можливих помилкових дій персоналу.

Аварійні, тривожні сигнали від різних спільно діючих систем об'єкта, передані для реєстрації автоматично, варто фіксувати приладами управління роздільно. Дотримання даної умови дозволяє запобігти можливості реагування однієї служби об'єкта на сигнали, призначених для іншої служби, або прийняти персоналу охорони об'єкта рішень і дій, неадекватні сформовані ситуації, що виникла обставині.

У спільно діючих об'єктових системах різного функціонального призначення, що вимагають різного реагування на видавані ними сигнали і повідомлення, види і інтенсивність таких сигналів повинні бути різними.

Всі складені елементи системи технічних засобів забезпечення безпеки об'єкта можуть і повинні поєднуватися в єдиний комплекс із можливістю взаємного обміну інформацією. Комплекс, що складається із сучасного встаткування, дозволяє включити у свій арсенал комп'ютер, не просто здатний програмно управляти КСБ, але і надавати безліч додаткових переваг. Сучасний персональний комп'ютер (ПК) з його розвиненими можливостями є ідеальним засобом для рішення завдань забезпечення безпеки будь-якого об'єкта. Його відкрита конфігурація дозволяє вбудовувати або підключати до нього спеціалізовані контролери для обробки будь-якої цифрової і аналогової

інформації. Гнучкість архітектури і високорозвинене інструментальне математичне забезпечення ПК дозволяє створювати програмно-апаратні комплекси охорони об'єктів, що багаторазово перевищують по можливості спеціалізовані прилади.

Іншим достоїнством сучасних ПК і програмного забезпечення є можливість використання ергономічного, інтуїтивно зрозумілого інтерфейсу, розрахованого на непідготовленого користувача. Такий інтерфейс спрощує використання можливостей КСБ і фактично може сховати від користувача внутрішню складність.

Персонал охорони одержує в користування надзвичайно зручну і функціональну інтегровану систему безпеки, не потребує глибоких спеціальних знань. Автоматизовані КСБ забезпечують найбільшу ефективність безпеки охоронюваних об'єктів і повинні задовольняти наступним основним вимогам:

- забезпечувати об'єктивною оперативною інформацією оператора системи про стан об'єкта в зручній для нього формі;
- давати можливість операторові системи на основі цієї інформації приймати правильне рішення про реагування на тривожні і аварійні ситуації і задіяти відповідні служби реагування;
- фіксувати в протоколі системи всі події, що представляють інтерес для служби безпеки, для їхньої наступної аналізу.

Слід зазначити, що будь-яка автоматизована КСБ представляє лише набір засобів, що дозволяють особам, відповідальним за безпеку об'єкта, установити якийсь порядок і забезпечити його виконання.

Сама ж безпека залежить від набору функціональних можливостей системи і компетентності осіб, відповідальних за безпеку. Основне завдання автоматизованих комплексів охорони - підвищити ефективність роботи системи безпеки і знизити вплив людського фактора.

Питання 2. Принципи організації інтегрованих систем і комплексів безпеки

Проблема безпеки будь-якого об'єкта вимагає для свого рішення певного підходу. Так, для забезпечення безпеки невеликих об'єктів, як правило, досить використання технічних засобів охоронної сигналізації. У той же час очевидно, що вирішити проблему безпеки об'єктів, несанкціоноване проникнення на які може привести до особливо великого або непоправного збитку, погрози здоров'ю або життю великої кількості людей, за допомогою одних лише технічних засобів сигналізації неможливо. Тому в нас у країні і за рубежом в охороні таких об'єктів стали широко застосовуватися охоронні системи і комплекси, що включають у себе крім технічних засобів охоронної сигналізації засобу телевізійного спостереження, контролю і управління доступом, пожежної сигналізації, а також інших технічних засобів безпеки. Перші комплекси являли собою, як правило, симбіоз із декількох незалежних, не зв'язаних між собою підсистем і не могли вирішити

поставлене завдання, тому що збільшений обсяг продубльованої кожною підсистемою інформації практично не піддавався обробці і не дозволяв операторові прийняти правильне рішення. Останнім часом загальновизнаним став комплексний підхід до забезпечення безпеки важливих об'єктів, одним з основних напрямків якого є створення інтегрованих систем охорони.

Цілями інтегрування є одержання ІСКБ нових функцій при збереженні в повному обсязі можливостей її окремих складових частин, економія необхідних для реалізації цих функцій засобів, максимальна автоматизація дій в усіх напрямках захисту об'єкта. Інформація операторові видається після її аналізу і обробки в самій системі, що дозволяє підвищити її вірогідність і оперативно прийняти рішення відповідно до виниклої ситуації.

Керуючою і обов'язковою ланкою будь-якої ІСКБ є система збору і обробки інформації (ССОІ). Залежно від значимості об'єкта і пропонованих до рівня його безпеки вимог окремі підсистеми можуть входити або не входити до складу ІСКБ такого об'єкта. До складу ІСКБ при необхідності можуть входити і інші підсистеми, що забезпечують, наприклад, нормальне функціонування систем життєзабезпечення об'єкта, його інформаційну безпеку і т.п. Вхідні до складу ІСКБ технічні засоби, окремі підсистеми, складові частини, елементи в тім або іншому ступені функціонально перетинаються між собою і мають крім загального і своє локальне керування. Формалізоване визначення ІСКБ ще не цілком склалося, однак можна вважати, що інтегрована система охорони - сукупність об'єднаних загальним управлінням систем і технічних засобів безпеки, що володіють технічним, інформаційною, програмною і експлуатаційною сумісністю і призначених для рішення завдань охорони об'єкта.

Більшість ІСКБ будується за принципом дворівневого інтегрування.

Перший рівень - системний. ССОІ або центральний процесор (сервер) поєднує всі підсистеми ІСКБ і забезпечує їхню взаємодію. Кожна з підсистем автоматично виконує які-небудь дії при надходженні певного сигналу від будь-якої іншої.

Другий рівень - модульний. Контролери «місцевого» значення управляють невеликою групою сповіщувачів, телевізійних камер, считувачів, виконавчих пристроїв і т.п.

Така побудова ІСКБ має ряд переваг. Завдяки гнучкій архітектурі система легко конструюється з певного набору модулів і блоків практично для будь-яких об'єктів. У процесі експлуатації досить просто нарощувати і вдосконалювати функції системи шляхом підключення різних типів виконавчих пристроїв і пристроїв, що реєструють. ІСКБ будуються на базі комп'ютерних технологій, структурно вони можуть бути розбиті на наступні складові частини:

- пристрою прийому, передачі і обробки сигналів, що дозволяють одержувати максимально повну інформацію і відтворювати на центральному пульті керування всебічну і об'єктивну картину стану приміщень і території об'єкта, працездатності апаратури і встаткування;

- виконавчі пристрої, здатні при необхідності діяти автоматично або по команді оператора;
- пункт (або пункти) контролю і управління системою відображення інформації, через які оператори можуть стежити за роботою всієї ІСКБ;
- центральний процесор, що наочно представляє і накопичує інформацію для її наступної обробки;
- комунікації, за допомогою яких здійснюється обмін інформацією між елементами ІСКБ і операторами.

Така структура побудови ІСКБ забезпечує ним наступні функціональні можливості:

- контроль за більшою кількістю приміщень і територій з організацією декількох рубежів охорони;
- багаторівневий доступ співробітників і відвідувачів із чітким розмежуванням повноважень по праву доступу в певні охоронювані зони, за часом доби і дням тижня;
- ідентифікацію об'єкта, що перетинає певний рубіж;
- розпізнавання порушника, що дозволяє персоналу охорони приймати найбільш раціональні міри протидії;
- взаємодія постів охорони і органів правопорядку при несенні охорони і у випадках локалізації подій;
- нагромадження документальних матеріалів для використання їх при розслідуванні і аналізі подій.

Можливість гнучкого програмування ІСКБ і окремих підсистем дозволяє активно протидіяти таким несанкціонованим діям, як переривання каналів передачі тривожної інформації, часткова нейтралізація системи особами, що мають доступ до окремих її елементів і підсистем, знищення інформації про подію, порушення персоналом охорони встановленого порядку несення служби і т.п.

Завдання на самопідготовку:

1. Дерев'янка А.А. и др. Применение и эксплуатация приборов пожарной автоматики. –Х.: УЦЗУ, 2008, 245 с.
2. Системи пожежної та охоронної сигналізації. Бондаренко С.М., Христич В.В., Дерев'янка О.А., Антошкін О.А. Текст лекцій. Харків: УЦЗУ МНС України, 2007.- 136 с.