УДК 654.1
DOI: 10.31673/2409-7292.2022.016769

Котенко А.М., Калініченко О.Г., Цимбалістий В.І.

ТЕХНОЛОГІЯ ПОБУДОВИ ЕФЕКТИВНОЇ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

У статті проаналізовано існуючі підходи до побудови систем безпеки об'єктів інформаційної діяльності. Запропонована методика побудови ефективної інтегрованої системи безпеки ОІД. Методика ґрунтується на положеннях методу динамічного програмування, теорії оптимізації.

Ключові слова: інтегрована система безпеки, канал витоку інформації, інформація з обмеженим доступом, технічна система охорони, критерій, об'єкт інформаційної діяльності.

Вступ

Об'єкт інформаційної діяльності являє собою приміщення де здійснюється обіг інформації з обмеженим доступом. Це фізичне середовище як у випадку побудови комплексної системи захисту інформації або у інших випадках. Із поняттям фізичного середовища пов'язане поняття технічного каналу витоку інформації. Саме для забезпечення безпеки інформації на ОІД і створюються різноманітні системи охорони ОІД.

Основна частина.

Відомо, що для забезпечення безпеки,або охорони об'єктів інформаційної діяльності використовуються: технічна система охорони, система відеоспостереження, система контролю та управління доступом [1]. Вони забезпечують захист інформації від витоку матеріально-речовим каналом. Але більш ефективним та перспективним є поєднання таких систем з метою побудови інтегрованої системи безпеки. На сьогодні під час створення інтегрованих систем наукові підходи не застосовуються. При їх створенні лише суб'єктивно оцінюється вартість складових, їх характеристики.

Метою даної статті є запропонування наукового підходу для побудови ефективної інтегрованої системи безпеки.

Детальніше про інтегровані системи безпеки (ІСБ). ІСБ це поєднання функціонально та інформаційно пов'язаних одна з одною технічних підсистем безпеки, які працюють за єдиним алгоритмом і мають спільні комунікації, програмне забезпечення, бази даних. [1]. Метою ІСБ являється об'єднання окремих технічних підсистем безпеки в єдиний комплекс з підтриманням їх злагодженої та взаємної роботи. ІСБ повинна забезпечувати наступні експлуатаційні вимоги:

мати модульну структуру, для забезпечення безпеки малих і великих територіально розподілених об'єктів;

відображати події на графічних планах об'єктів;

мати можливість передавати інформацію по будь-яких каналах зв'язку;

відображати стан зон, точок доступу, зчитувальних пристроїв, відеокамер на графічних зображеннях приміщень з текстовим поясненням;

розмежовувати повноваження чергових операторів адміністраторів використанням багаторівневої системи паролів і застосування біометричної систем обмеження доступу до програм автоматизованих робочих місць;

протоколювати всі події, що відбуваються у системі;

діагностувати працездатність блоків і пристроїв системи;

забезпечити віддалене адміністрування системи;

зберегти загальну надійність системи при інтеграції підсистем;

мати високу живучість, тобто зберігати працездатність при виході з ладу окремих підсистем, зберігати працездатність окремих підсистем (їх функцій) при поломці сервера ІСБ або при втраті інформаційного обміну з ним;

забезпечити автономну роботу контролерів підсистем при втраті зв'язку з сервером ІСБ.

До складу ІСБ повинні входити не менше трьох із зазначених базових систем: технічна система охорони; система тривожної сигналізації;система відеоспостереження; система

контролю управління доступом. У ГОСТ Р 53195.1 зазначається, що до складу ІСБ можуть входити інші системи забезпечення безпеки.

Розрізняють три типи інтеграції при побудові ІСБ:

проектна - це інтеграція складових під час проектування системи;

програмна – коли для інтеграції обладнання використовується спеціально розроблене програмне забезпечення;

апаратно-програмна - інтеграція апаратури та програмного забезпечення, при цьому апаратні і програмні засоби працюють в єдиній системі;

апаратна – інтеграція на апаратному рівні.

Кожен тип має переваги та недоліки. Так перевагами проектної є простота обладнання, невисока вартість, можливість об'єднання систем різних виробників. Як недоліки: обмеженість видів повідомлень якими обмінюються підсистеми; труднощі з візуалізацією подій і стану системи в цілому; при зростанні кількості реле і комунікаційних ліній втрачається перевага низької вартості реалізації. Серед переваг програмної: використовуючи всю функціональність сучасних комп'ютерних технологій, створювати високоефективні багатофункціональні програмні системи. Можливість інтегруватися з апаратними засобами інших виробників. Розробка ІСБ за програмною інтеграцією вимагає меншої кількості ліній зв'язку між підсистемами порівняно з проектною інтеграцією. Недолік те, що необхідно розробляти драйвери для кожного апаратного засобу. Не завжди розробник апаратного засобу надає протоколи обміну даними. Інтеграція на апаратно-програмному рівні є найбільш поширеним методом побудови ІСБ. Оскільки апаратні і програмні засоби розробляються в рамках єдиної системи і вся розробка зконцентрована як правило, в одних руках, можливо досягти оптимальних характеристик. Недоліком даної інтеграції те, що кожен виробник технічних підсистем пропонує свою оригінальну версію виробу, як правило, не сумісну з іншими.

По функціональності кожної зі складових. Технічна система охорони призначена для виявляння та попереджування про вторгнення в охороняєму зону об'єкту. Вона складається з охоронних сповіщувачів – чутливих елементів системи. Прилад прийомо-контрольний який отримує і аналізує інформацію що надійшла від охоронних сповіщувачів. З’єднувальні канали зв’язку – шлейфи. Оповіщувачі – засоби створення звукового сигналу тривоги.

Система пожежної сигналізації - призначена для виявлення ознак пожежі та подавання сигналу тривоги для вживання необхідних заходів протидії пожежі. Система оповіщування про пожежу приводиться у дію автоматично або вручну.

Системи відеоспостереження - це комплекс програмно-апаратних засобів призначений для відеоконтролю та відеохорони на невеликих і територіально-розподілених об'єктах, у приміщеннях і на вулиці. Складається з поворотних і стаціонарних відеокамер для перетворення візуального зображення у електричні сигнали; пристроїв зберігання зображення, ліній зв’язку, пристроїв відтворення зображення. Функцію відеохорони забезпечує програмний відеотектор руху. Його реакція на появу руху у визначеній зоні контролю – початок запису відео і видача звукового сигналу тривоги.

Система контролю і управління доступом (СКУД) – це сукупність програмних та технічних засобів які вирішують завдання контролю і управління доступом до окремих приміщень ОІД, а також оперативний контроль за пересуванням осіб та часу їх знаходження на території ОІД.СКУД поєднує у комплекс апаратно-програмні,механічні, електротехнічні та інші засоби які забороняють доступ до приміщень ОІД особам які такого права не мають. Така їх функціональність дозволяє забезпечувати безпеку персоналу, відвідувачів, а також зберігати матеріальні та інформаційні ресурси ОІД.

В основі даного наукового апаратузастосовується метод динамічного програмування.

Динамічне програмування використовується в теорії управління як спосіб вирішення складних завдань за рахунок розбиття їх на більш прості підзадачі. Такий метод використовується до задач з оптимальною підструктурою. Вона являє собою набір під задач

що перетинаються, складність яких менша вихідної складнощі. У загальному випадку алгоритм вирішення таких задач виглядає наступним чином [2].

1. Загальна задача розбивається на менші підзадачі.
2. Знаходиться оптимальне рішения підзадач, за таким же трьох кроковим алгоритмом.
3. Використовуються отримані рішення підзадач для вирішения вихідної задачі.

Припустимо інтегрована система безпеки побудована з наступних підсистем: відеоспостереження, технічної системи охорони, системи контролю управління доступом. Виходячи з цього у математичному вигляді постановка завдання на вибір оптимального варіанту системи буде виглядати наступним чином:

Дано: (система відеоспостереження, технічна система охорони, системи контролю управління доступом) – інтегрована система безпеки ***M.***

Знайти: $\frac{F}{I}$ –критерієм ефективність/вартість для кожної з реалізацій та обрати варіант з найбільшим значенням серед усіх варіантів:

$$\max\left(\frac{F}{I}\right) = \max\left(\frac{\sum_i f_i}{\sum_i I_i}\right)$$

де:

F – показник корисності i – ої реалізації ІСБ;

I – вартість i – ої реалізації ІСБ.

Виходячи з цього знайдемо оптимальний склад ІСБ який задовольняє показнику якості виконання своїх функцій при мінімальній вартості системи.

У відповідності з даним методом необхідно прорахувати показник корисності кожного з елементів системи M (система відеоспостереження, технічна система охорони, системи контролю управління доступом). Далі застосовуючи метод повного перебору необхідно прорахувати значення цільової функції для кожної реалізації ІСБ. Всіх таких реалізацій ІСБ буде:

$$N = \prod_{i=1}^{n} K_i$$

де:

n – число елементів що входять до ІСБ;

K – число альтернативних варіантів кожної зі складової ІСБ.

Обрахування вартості кожної з підсистем ІСБ не викликає складнощів. Постає питання обрахунку якості кожної з підсистем.

Пропонується використовувати запропонований метод також і до кожної з підсистем. У [3] показано застосування методу динамічного програмування при побудові ефективної системи відеоспостереження. Для розрахунку показника $\frac{F}{I}$ СКУД застосовується такий же самий метод. Тобто потрібно визначитись с обладнанням для кожного варіанту СКУД. Для коректності порівняння варіанти СКУД повинні мати однакову функціональність. Йдеться про наступне.

Відомо що СКУД, в залежності від розмірів об’єкту, його масштабності, діляться на дві велику групи: централізовані та розгалужені. Обладнання буде різне. Далі визначаємось яким чином буде здійснюватись ідентифікація особи. Існують статичні та динамічні методи ідентифікації. У кожному з них використовуються свої засоби. Серед статичних поширені засоби: біометричної та атрибутивної ідентифікації. До біометричних відносяться різні особисті ознаки людини і відповідно обладнання теж буде різне. Біометричні ознаки це: зображення райдужної оболонки ока, відбиток пальця, відбиток долоні та інші фізичні ознаки.

Атрибутивні це автономні носії ознак ідентифікації, наприклад: магнітні картки, безконтактні проксіміті-карти, брелоки «тач-меморі», RFID ідентифікатори та інші.

Серед динамічних методів ідентифікації відомі: ідентифікація по почерку, динаміці роботи на клавіатурі, по голосу та особливостям мови.

Після того як визначились з методом ідентифікації необхідно обрати другу невідємну складову СКУД – контролер (пристрій що аналізує сигнал з засобу ідентифікації). Контролери розрізняються за способом управління (можливості об'єднання): автономні, мережні (централізовані) і комбіновані. Автономні - повністю закінчені пристрої, призначені для обслуговування однієї точки проходу. Можливість об'єднання з іншими аналогічними контролерами не передбачається. Мережеві контролери можуть працювати в мережі під управлінням комп'ютера. У цьому випадку рішення приймає персональний комп'ютер з встановленим спеціалізованим програмним забезпеченням. Мережеві контролери призначені для створення СКУД любого ступеня складності. Кількість мережевих контролерів у системі може бути від двох до сотень. Інформація виводиться на центральний пункт охорони.

Третій елемент СКУД – виконавчі пристрої. Це електромеханічні пристрої, що керуються контролером і фізично дозволяють чи забороняють доступ людині до ОІД.

Для порівняння засобів СКУД у кожній з цих трьох груп визначаються найбільш важливі їх показники якості функціонування. Далі, для порівняння засобів між собою необхідно ці показники пронормувати (привести до безрозмірного вигляду).

Нормування здійснюється за виразами лінійної трансформації [4]. Це виглядає наступним чином. Якщо для показника якості приладу,x_1,більш якісній роботі відповідає зростання величини показника, то вираз переходу від його ненормованого значення до нормованого x_n буде:

$$X_n = \frac{x_1 - f_1^{min}}{f_1^{max} - f_1^{min}} \quad (1)$$

де:

f_1^{min}і f_1^{max} – абсолютні мінімальне (найгірше) й максимальне (найкраще) значення показника якості роботи приладу;

x_1 – абсолютне значення показника,що нормується.

Якщо навпаки для показника x_1 абсолютне мінімальне значення визначає більш якісне функціонування, то вираз трансформації наступний:

$$X_n = \frac{f_1^{max} - x_1}{f_1^{max} - f_1^{min}}. \quad (2)$$

Далі визначаємо вагові коефіцієнти показників якості роботи кожного приладу. У найпростішому випадку можна використовувати метод експертного оцінювання, або математичні методи як то метод попарних порівнянь, метод Сааті та інші. Результатом є деяке числове значення: показник який має певну перевагу над іншим показником отримує більш високий відповідний бал.

За наступним виразом розраховується показник корисності f_iдля кожного елементу підсистеми СКУД, як сума перемножень значимості показника якості на вагу цього показника:

$$f_i = \sum a_i Kc_i$$

де:

a_i – вага показника якості елементу СКУД;

Kc_i – нормоване значення показника якості цього ж елементу СКУД (за виразом (1) або (2)).

Методом повного перебору складаються усі можливу варіанти СКУД. Розраховується вартість кожного з варіантів системи.

У результаті таких розрахунків отримуємо значення $\frac{F}{I}$ для кожної з СКУД. У подальшому потрібно обрати варіанти кожної з підсистем ІСБ які мають найвищі значення показника $\frac{F}{I}$. З них і буде складатися ІСБ побудована за найвищим показником ефективність/вартість.

Вищевикладений матеріал зводиться до методики побудови ефективної ІСБ за критерієм ефективність/вартість.

1. Визначити склад ІСБ.
2. Обрати обладнання яке планується використовувати у кожній підсистемі ІСБ.
3. По кожному обладнанню обрати для порівняння найбільш важливі параметри.
4. Пронормувати ці параметри.
5. Визначити вагові коефіцієнти цих параметрів для кожного обладнання кожної підсистеми ІСБ.
6. Розрахувати показник корисності кожного з елементів підсистеми по кожній категорії обладнання.
7. Використовуючи метод повного перебору скласти всі варіанти підсистем ІСБ.
8. Розрахувати показник корисності для кожного варіанту підсистеми ІСБ та вартість кожного варіанту підсистеми.
9. Обрати найкращий варіант підсистеми по максимальному значенню відношення показника корисності системи до її вартості.
10. Найкращим варіантом ІСБ за критерієм ефективність/вартість буде ІСБ сформована з цих підсистем.

Висновок.

У статті проаналізовано склад ІСБ та принцип її побудови. Розроблена методика побудови ефективної ІСБ за показником ефективність/вартість з використанням наукових підходів.

Перелік посилань

1. https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/security-systems-review

2. Кулич И.Л. Глава 4. Задачи динамического программирования // Математическое программирование в примерах и задачах. — М.: Высшая школа, 1986. — 319 с. — ISBN 5-06-002663-9.

3. Котенко А.М., Кітіченко Н.С. Застосування методу динамічного програмування для побудови ефективної системи відеоспостереження. Сучасний захист інформації. Київ: ДУТ, 2020. №1(41) 2020. С.31 – 36.

4. https://psytest.wordpress.com/data_treatment/normalization_indicator/

Надійшла: 11.01.2022 Рецензент: д.т.н., професор Гайдур Г.І.