УДК 004.934:681.391 DOI: 10.46972/2076-1546.2023.25.03

О. Ф. Дубина, С. О. Соболенко, І. В. Пулеко, О. В. Андреєв, А. Ю. Денисюк

ПІДХІД ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ КОМПЛЕКСНОЇ СИСТЕМИ ОХОРОНИ

Захист й охорона здоров'я, життя, місця проживання, матеріальної та інтелектуальної власності людини є важливим завданням на сучасному етапі розвитку суспільства. Для розв'язання цієї проблеми використовують системи безпеки й охорони, в основі яких юридичні, організаційні, морально-етичні, апаратно-програмні методи та засоби. Вони повинні відповідати правовим нормам і вимогам, що висуваються до кожної категорії об'єктів захисту. Одним із важливих апаратно-програмних засобів охорони є елементи та пристрої електронної техніки, зокрема сенсорні пристрої. В основу їх функціонування покладено досягнення фізики твердого тіла, оптики, електрооптики, електроакустики та інше. Сучасні електронні технології дають можливість створювати ефективні мікроелектронні сенсорні пристрої для систем безпеки й охорони, функціонування яких полягає у використанні оптичних, механічних, магнітних, п'єзоелектричних, тензометричних, ємнісних та інших типів сигнальних перетворювачів. У процесі побудови сучасних систем безпеки й охорони необхідно, з одного боку, володіти інформацією про можливості та особливості функціонування окремих складових елементів, які забезпечують виконання завдання з охорони об'єкта, а з іншого – необхідно мати оцінку ефективності розробленої системи, яка повинна включати як показники надійності усіх елементів і каналів передачі інформації, так і показники ефективності виконання функціонального завдання.

Розроблена математична модель ефективності застосування системи охорони надасть можливість правильно вибрати елементи системи, параметри яких найповніше забезпечать виконання завдання. Такий підхід сприяє організації взаємодії систем охоронної сигналізації, пожежної сигналізації, системи контролю доступу, системи відеоспостереження та пультів централізованої охорони.

Ключові слова: *комплекс технічних засобів; датчик системи охорони; пульт централізованої охорони; ефективність системи охорони.*

Постановка проблеми в загальному вигляді. У сучасних умовах системи охорони об'єктів є невід'ємною частиною будь-якого офісу, підприємства, приватного домогосподарства тощо. У цілому така система є комплексною і включає в себе: відеоспостереження, охоронну та пожежну сигналізації, систему контролю доступу [9]. Відповідно до сучасних вимог з безпеки об'єктів система охорони складається із певної кількості рівнів залежно від значущості об'єкта. При цьому засоби комплексної охоронної системи, які можуть бути використані для оснащення рівнів, повинні відповідати широкому колу вимог, серед яких на перший план виступає необхідність виконання завдання не лише прийняття рішення про виявлені або невиявлені об'єкти, але й проведення їх класифікації залежно від призначення.

Ця інформація може надходити як на пультову системи охорони, так і на засоби власника (комп'ютер або мобільний телефон), як дротовими, так і бездротовими каналами зв'язку. Це дозволить здійснювати управлінські дії, спрямовані на вжиття адекватних заходів, пов'язаних із процесом постановки завдань силам реагування, зокрема групі затримання. Разом із тим така постановка завдання потребує вдосконалення датчиків охоронних систем у частині розширення функціональних можливостей, пов'язаних із формуванням розширеного формату даних про об'єкт.

Цей підхід вимагає уточнення приватних, узагальнених та комплексних показників для застосування комплексу технічних засобів (КТЗ) в охоронних системах відповідно до покладених завдань. Тому виникає проблема вибору функції-моделі оцінки ефективності автоматизованих систем охорони об'єктів даного типу.

Аналіз останніх досліджень і публікацій. На сьогоднішній день тематика охоронних систем є досить актуальною як у виробництві, так і в наукових дослідженнях. Так, у [2] визначено фактори успіху управління інформаційною безпекою, у [3] показано зниження продуктивності праці співробітників під час впровадження механізмів контролю доступу технологій інформаційної безпеки. У [1, 4, 10] описано теперішній рівень автоматизації для забезпечення роботи домашніх (приватних) систем безпеки. У [8] проаналізовано значну кількість факторів, що визначають якісні й кількісні показники комплексної системи охорони об'єкта. Однак слід зауважити, що мало досліджено питання моделювання системи охорони щодо її ефективності.

Формулювання завдання дослідження. Метою статті є розроблення математичної моделі оцінювання ефективності системи охорони об'єкта.

Виклад основного матеріалу. У загальному випадку показники ефективності автоматизованої охоронної системи можуть включати, з одного боку, ті, що характеризують КТЗ систем охорони, з іншого – показники, які враховують людський чинник. З огляду на те, що технічна складова КТЗ систем охорони є визначальною у надійності їх структур, надалі обмежимося першою групою показників.

Для визначення ефективності системи охорони скористаємося підходом, за якого процес оцінювання ефективності систем охорони об'єкта складається з низки етапів, що включають, по-перше, поетапне перетворення структур систем окремих показників, по-друге, їх узагальнення в показник, що містить моделі об'єднання нижнього рівня, а саме комплексний (інтегральний) показник ефективності. Під час аналізу КТЗ варто розглянути інформаційні елементи (ІЕ), під якими розумітимемо найпростіші елементи охорони об'єкта, що відображають джерела (канали) інформації.

Кожен ІЕ (датчик, канал зв'язку) характеризується такими показниками ефективності, як $K_{Д}$, $K_{ЛЗ}$, що мають сенс узагальнювальних показників ефективності як за рахунок застосування датчиків охорони, що виконують завдання типу «виявлення – розпізнавання» об'єктів, так і завдяки застосуванню ліній зв'язку (проводових або радіозв'язку) відповідно.

З іншого боку, кожен ІЕ характеризується показниками ефективності, а саме $K_{НД}$, $K_{НЛЗ}$, що мають узагальнювальний сенс і визначають надійнісні характеристики сповіщувачів комбінованого типу та ліній зв'язку відповідно.

Виявлені та розпізнані властивості КТЗ системи охорони пов'язані з рішеннями щодо видачі інформації з необхідними показниками про об'єкт на пультову систему охорони, вони можуть бути описані ймовірностями: правильного виявлення сигналу датчиками, помилкової або правильної класифікації об'єктів, своєчасності обробки інформації в тракті сигнального розпізнавання.

Надійнісні характеристики КТЗ пов'язані з раптовими відмовами, що виникають у процесі експлуатації охоронних систем і характеризуються набором показників, серед яких можуть бути виділені, наприклад, імовірності безвідмовної роботи, своєчасної видачі інформації каналами зв'язку, ефективності виконуваного завдання в них.

Викладене дозволяє уявити якість функціонування КТЗ системи охорони об'єкта на основі ефективності та надійності КТЗ у такому вигляді:

$$V_e = \|V_1, V_2, V_3, V_4, V_5\|. \quad (1)$$

У виразі (1) компоненти V_1, V_2, V_3, V_4, V_5 – показники ефективності, що характеризують виявлення об'єкта датчиками, правильність його класифікації, своєчасність надання інформації каналами зв'язку, надійнісні характеристики датчиків та ліній зв'язку відповідно.

У загальному випадку в ході побудови систем охорони для оцінювання складових компонентів V_1 і V_2, що входять у вираз (1), можна ввести ймовірнісні показники:

P_O – імовірність виявлення об'єкта датчиками;

$P_{КЛ}$ – імовірність правильної класифікації об'єктів датчиками;

$P_{СВ}$ – імовірність, що характеризує своєчасність обробки інформації в тракті сигнального розпізнавання.

Слід зауважити, що для аналізу охоронних систем необхідно враховувати два фактори: по-перше, елементна база в ході створення датчиків і каналів зв'язку характеризується раптовими відмовами, тобто вказані вище ІЕ в процесі експлуатації мають зрештою напрацювання на відмову; по-друге, необхідно забезпечити видачу інформації протягом часу, що не перевищує встановленої нормативної вимоги. У цьому разі для оцінювання елементів структур системи охорони об'єктів доцільно компоненти векторного показника подати ймовірнісними показниками та доповнити такими характеристиками надійності: імовірність безвідмовної роботи датчика $P_Н^Д$, імовірність безвідмовної роботи каналу зв'язку $P_Н^{КЗ}$ та ймовірність виконання, що характеризує своєчасність видачі інформації каналом зв'язку $P_{СВ}^{КЗ}$.

З урахуванням викладеного векторний показник, описаний виразом (1), матиме такий вигляд:

$$V_e = \left\| P_O, P_{КЛ}, P_{СВ}, P_Н^Д, P_Н^{КЗ}, P_{СВ}^{КЗ} \right\|. \quad (2)$$

На первинному етапі роботи системи охорони відбувається процес виявлення об'єкта з імовірністю P_O засобами виявлення (ЗВ). Це практично визначає наступні етапи

обробки й виконання завдання системою охорони в цілому. Багаторівнева система охорони утворюється, як правило, на основі застосування ЗВ, що працюють на різних принципах.

Аналіз схем побудови комбінованих засобів виявлення (КЗВ) показав, що в наш час серед розроблюваних і розроблених систем (комплексів) найбільшого поширення набули схеми логічної обробки (бінарних сигналів тривоги з окремих ЗВ) *K* з *N*, наприклад: 2 з 3 ($N = 3,\ K = 2$). Для цієї схеми ймовірність виявлення складається з імовірностей тих комбінацій, у яких присутні дві або три одиниці [11]:

$$P_{2/3} = \sum_{j=1}^{4} \Delta P_j .$$

За аналогією до засобів радіолокації, розпізнавання об'єктів, що належать до кінцевого алфавіту, наприклад *k* класам, відбувається на тлі різноманітних непередбачуваних перешкод різного виду. Причому найчастіше йдеться про вплив флуктуаційних шумів. Даний факт вказує на ймовірнісний характер процесу класифікації об'єктів і може характеризуватися як розгорнутим критерієм ефективності, що містить елементи матриці ймовірностей правильних і помилкових рішень, так й усіченим, описаним, наприклад, лише ймовірностями правильної класифікації $P_{\text{пр}}$. Однак у разі зіставлення ефективності різних алгоритмів розпізнавання в умовах багатоальтернативної класифікації об'єктів вважають за краще оперувати величиною ймовірності помилки класифікації $P_{\text{пом}}$, яка може бути оцінена з матриці альтернативних рішень, що виносяться за *k* класами об'єктів. Матриця альтернативних рішень, що містить рядки та стовпці, відповідні *k* класам об'єктів, що розпізнаються, має такий вигляд:

$$P = \begin{vmatrix} P_{11} & \dots & P_{1k} \\ \dots & \dots & \dots \\ P_{k1} & \dots & P_{kk} \end{vmatrix}.$$

Отже, виходячи з розгорнутого критерію ефективності, величина ймовірності помилки класифікації об'єктів може бути визначена як

$$P_{ПОМ} = 1 - \frac{1}{k} \sum\nolimits_{i=1}^{k} P_{ii} .$$

Елементи $P_{ij}, i = j$ під знаком суми – вірогідності правильного розпізнавання з матриці альтернативних рішень.

У виразі (1) показники V_1, V_2, що враховують достовірність та своєчасність обробки інформації сповіщувачами комбінованого типу, з огляду на їх об'єднання в аналітичному вигляді, можуть бути подані в такий спосіб:

$$V_{12} = P_O \left(1 - P_{ПОМ}\right) P_{СВ} . \qquad (3)$$

У процесі оцінювання складових компонентів V_3 і V_4, що входять у вираз (2), необхідно враховувати той факт, що раптова відмова будь-якого типу ІЕ системи охорони

веде до порушення її працездатності. Це свідчить про послідовну схему надійності ІЕ в системі охорони. Враховуючи, що надійність у системі ототожнюється з властивістю КТЗ нормально функціонувати протягом певного часу, замість введених імовірностей безвідмовної роботи сповіщувачів комбінованого типу та ймовірностей безвідмовної роботи каналу зв'язку слід ввести імовірність безвідмовної роботи КТ $P_{БР}$, яку можна описати таким виразом:

$$P_{БР} = e^{-\Delta t \sum_n a_n}, \tag{4}$$

де індекс вказує на належність до *n*-го типу ІЕ, а саме:

n = 1 – сповіщувач комбінованого типу;

n = 2 – канал зв'язку дротовою лінією зв'язку;

n = 3 – канал зв'язку бездротовою лінією зв'язку;

Δt – тимчасовий інтервал безвідмовної роботи КТЗ системи охорони на інтервалі часу від 0 до *t*;

$\sum_n a_n$ – сумарна інтенсивність відмов типів ІЕ.

Враховуючи, що в даний час у системах охорони під час виготовлення ІЕ використовують останні досягнення мікроелектроніки, а саме інтегральні технології, наведені типи ІЕ приблизно рівнонадійні. У цьому разі з практичного погляду у виразі (2) можна оперувати величиною середньої інтенсивності відмов, яку визначимо як

$$a_{сер} = \frac{\sum_n a_n}{n}. \tag{5}$$

Тоді у виразі (2) поряд із величинами $P_H^Д$, $P_H^{КЗ}$ можна оперувати величиною середньої інтенсивності відмов $P_H^{сер}$ [11].

Відповідно до цього підходу компоненти V_3 і V_4 перетворюються на показник V_{34}, який з урахуванням виразу (5) може бути поданий у вигляді середньої ймовірності безвідмовної роботи КТЗ на інтервалі часу

$$P_H^{сер} = e^{-\Delta t a_{сер}}. \tag{6}$$

Для оцінювання компонента V_5 необхідно враховувати той факт, що для фізично справного каналу зв'язку потрібно забезпечити своєчасність видачі інформації з імовірністю виконання $P_{СВ}^{КЗ}$. Оцінка даної ймовірності практично труднощів не викликає, тому що нормативний час у разі використання каналу зв'язку вказується в керівних документах.

Враховуючи мультиплікативний підхід до об'єднання узагальнювальних показників, можна отримати з (2) показник ефективності та надійності КТЗ системи охорони й записати його в аналітичному вигляді як

$$V_e = P_O(1 - P_{ПОМ})P_{СВ}, P_H^{сер}, P_{СВ}^{КЗ}. \tag{7}$$

Аналіз відомих методик показав, що цілком оптимально оцінювати ефективність КТЗ як складну інформаційну систему і характеризувати декількома частковими показниками, на підставі яких формується загальний критерій [7].

Отримані аналітичні вирази дозволяють сформулювати оптимізаційну задачу визначення найкращої структури КТЗ інтегрованої системи охорони у вигляді такого співвідношення:

$$s^*_{c,l} = arg\ max\, V_e\left(s_{c,l}\right), \tag{8}$$

де

$$s_{m,n} \in C,\ C \in \left\{s_1, s_2 \ldots s_c;\ s_1, s_2 \ldots s_l\right\}, m = 1, \ldots c;\ n = 1, \ldots l. \tag{9}$$

У виразі (8) індекс c означає кількість датчиків, l – кількість каналів зв'язку, що входять до складу КТС системи охорони об'єктів, які відповідають вимогам надійності, за обмежених ресурсних витрат.

Сучасні системи охорони об'єктів можуть застосовувати декілька каналів передачі інформації для підвищення надійності. Це може бути дротовий або Wi-Fi канал, один або декілька каналів мобільного зв'язку із залученням різних операторів. Крім того, для бездротового зв'язку може передбачатися основний і додатковий канали передачі даних на різних частотних діапазонах із використанням приватних (закритих) захищених протоколів.

Висновки. Розглянутий підхід до оцінювання якості функціонування технічної складової в автоматизованих системах охорони на основі використання імовірнісних показників дозволяє провести аналіз пристроїв КТЗ із позиції елемента автоматизованої інформаційної системи. За допомогою запропонованих аналітичних виразів можна оцінювати ефективність роботи КТЗ у рамках виконання поставлених завдань з урахуванням надійності їх структур та ймовірнісних показників інформаційних елементів.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Design and Construction of an Automatic Home Security System Based on GSM Technology and Embedded Microcontroller Unit / I. K. Olarewaju, O. E. Ayodele, F. O. Michael et al. // American Journal of Electrical and Computer Engineering. 2017. Vol. 1, No. 1. P. 25–32. http://dx.doi.org/10.11648/j.ajece.20170101.14

2. Ključnikov A., Mura L., Sklenár D. Information security management in SMEs: factors of success // Entrepreneurship and Sustainability. 2019. Iss. 6 (4). P. 2081–2094. http://doi.org/10.9770/jesi.2019.6.4(37)

3. Zeng W., Koutny M. Modelling and analysis of corporate efficiency and productivity loss associated with enterprise information security technologies // Journal of Information Security and Applications. 2019. No. 49. http://dx.doi.org/10.1016/j.jisa.2019.102385

4. Nwalozie G. C., Aniedu A. N., Nwokoye C. S. & Abazuonu I. E. Enhancing Home Security Using SMS-based Intruder Detection System // International Journal of Computer Science and Mobile Computing. June 2015. Vol. 4, Iss. 6. P. 1177–1184.

5. Грицунов О. В. Інформаційні системи та технології : навч. посіб. Харків : ХНАМГ, 2010. 222 с.
6. Інформаційні системи і технології : навч. посіб. / [П. М. Павленко, С. Ф. Філоненко, К. С. Бабіч та ін.]. Київ : НАУ, 2013. 324 с.
7. Толюпа С. В., Самохвалов Ю. Я., Цьопа Н. В. Комплексні системи захисту інформації спеціальних об'єктів та методика їх оцінки // Сучасний захист інформації. 2014. № 1. С. 81–88.
8. Єніна І. І. Обробка сигналів при несанкціонованих проникненнях на охороняємий об'єкт // Наукові записки. 2016. Вип. 19. С. 158–162.
9. Електронні елементи та пристрої систем безпеки й охорони : навч. посіб. / Г. І. Барило, М. В. Вісьтак, З. Ю. Готра та ін. ; за ред. З. Ю. Готри. Чернівці : Рута, 2017. 216 с.
10. Kaur S., Singh R., Khairwal N., & Jain P. Home Automation and Security System // Advanced Computational Intelligence: An International Journal (ASCII). July 2016. Vol. 3, No. 3. P. 17–23.
11. Niels Richard Hansen. Probability Theory and Statistics. Department of Mathematical Sciences University of Copenhagen, November 2010. 296 p.

Стаття надійшла до редакції 21.09.2023.

REFERENCES

1. Olarewaju, I. K., Ayodele, O. E., & Michael, F. O. et al. (2017). Design and Construction of an Automatic Home Security System Based on GSM Technology and Embedded Microcontroller Unit. *American Journal of Electrical and Computer Engineering, Vol. 1,* No. 1, 25–32. http://dx.doi.org/10.11648/j.ajece.20170101.14
2. Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information Security Management in SMEs: Factors of Success. *Entrepreneurship and Sustainability, Iss. 6* (4), 2081–2094. http://dx.doi.org/10.9770/jesi.2019.6.4(37)
3. Zeng, W., & Koutny, M. (2019). Modelling and Analysis of Corporate Efficiency and Productivity Loss Associated with Enterprise Information Security Technologies. *Journal of Information Security and Applications, 49.* http://dx.doi.org/10.1016/j.jisa.2019.102385
4. Nwalozie, G. C., Aniedu, A. N., Nwokoye, C. S., & Abazuonu, I. E. (June 2015). Enhancing Home Security Using SMS-based Intruder Detection System. *International Journal of Computer Science and Mobile Computing, Vol. 4,* Iss. 6, 1177–1184.
5. Hrytsunov, O. V. (2010). *Informatsiini systemy ta tekhnolohii : navch. posib. [Information Systems and Technologies: academic. manual]*. Kharkiv [in Ukrainian].
6. Pavlenko, P. M., Filonenko, S. F., & Babich, K. S. et al. (2013). *Informatsiini systemy i tekhnolohii : navch. posib. [Information Systems and Technologies: education. manual]*. Kyiv [in Ukrainian].
7. Toliupa, S. V., Samokhvalov, Iu. Ia., & Tsopa, N. V. (2014). Kompleksni systemy zakhystu informatsii spetsialnykh ob'iektiv ta metodyka yikh otsinky [Complex Information Protection Systems of Special Objects and Their Assessment Methods]. *Suchasnyi zakhyst informatsii [Modern Information Protection], 1,* 81–88 [in Ukrainian].
8. Ienina, I. I. (2016). Obrobka syhnaliv pry nesanktsionovanykh pronyknenniakh na okhoroniaiemyi ob'iekt [Signal Processing During Unauthorized Intrusions into a Protected Object]. *Naukovi zapysky [Scientific Notes], 19,* 158–162 [in Ukrainian].

9. Barylo, H. I., Vistak, M. V., & Hotra, Z. Iu. et al. (2017). *Elektronni elementy ta prystroi system bezpeky y okhorony : navch. posib. [Electronic Elements and Devices of Safety and Security Systems: teaching. manual]*. Chernivtsi [in Ukrainian].
10. Kaur, S., Singh, R., Khairwal, N., & Jain, P. (July 2016). Home Automation and Security System. *Advanced Computational Intelligence: An International Journal (ASCII), Vol. 3,* No. 3, 17–23. http://dx.doi.org/10.5121/acii.2016.3303
11. Niels, R. H. (November 2010). *Probability Theory and Statistics.* Department of Mathematical Sciences University of Copenhagen.

O. F. Dubyna, S. O. Sobolenko, I. V. Puleko, O. V. Andreiev, A. Y. Denysiuk

APPROACH TO EVALUATING THE EFFICIENCY OF A COMPLEX SECURITY SYSTEM

Protection and protection of human health, life, habitat, material and intellectual property is an important task at the current stage of society's development. Security and protection systems based on legal, organizational, moral and ethical, hardware and software methods and tools are used to solve this problem. They must meet the legal norms and requirements that are put forward for each category of protection objects. One of the important hardware and software means of protection are elements and devices of electronic equipment, including sensor devices. Their functioning is based on the achievements of solid-state physics, optics, electro-optics, electro-acoustics, etc. Modern electronic technologies make it possible to create effective microelectronic sensor devices for security and protection systems, the functioning of which consists in the use of optical, mechanical, magnetic, piezoelectric, strainometric, capacitive and other types of signal transducers. In the process of building modern safety and security systems, it is necessary, on the one hand, to have information about the capabilities and peculiarities of the functioning of individual components that ensure the fulfillment of the task of protecting the object. On the other hand, it is necessary to have an assessment of the effectiveness of the developed system, which should include both reliability indicators of all elements and channels of information transmission, as well as indicators of the performance of the functional task.

The developed mathematical model of the efficiency of the application of the protection system will provide an opportunity to make the correct choice of the constituent elements of the system, the parameters of which most fully ensure the performance of the protection task. This approach ensures the organization of the interaction of security alarm systems, fire alarm systems, access control systems, video surveillance systems and centralized security consoles.

Keywords: *complex of technical means; security system sensor; centralized security control panel; security system efficiency.*