DOI:**10.33099/2311-7249/2019-34-1-111-114**

УДК: 004.94.355

Валерій Олександрович Крайнов *(кандидат технічних наук, доцент)*
Роман Іванович Грозовський

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ОБГРУНТУВАННЯ ПОКАЗНИКА ЯКОСТІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНУ ВІЙСЬКОВОГО УПРАВЛІННЯ

Темпи розвитку інформаційних технологій за останні роки спонукали впровадженню засобів обчислювальної техніки в процеси управління військами. Це в свою чергу відобразилось і на зворотній стороні цього процесу, а саме, виріс інтерес до інформації, яка циркулює всередині інформаційних систем не тільки зі сторони користувачів, а в значній ступені зі сторони противника. На сьогоднішній день існує велика кількість каналів витоку та спотворення інформації.

Система інформаційної безпеки виконує функцію повної або часткової компенсації загроз для інформаційної системи. Основною характеристикою системи інформаційної безпеки є імовірність усунення кожної загрози. За рахунок функціонування системи інформаційної безпеки забезпечується зменшення втрат, які наносяться інформаційній системі під дією загроз. Таким чином, метою статті є обґрунтування показника якості системи інформаційної безпеки автоматизованої інформаційної системи органу військового управління.

Ключові слова: *система інформаційної безпеки; автоматизована інформаційна система; орган військового управління; загроза.*

Вступ

Постановка проблеми. Процеси, що відбуваються в сучасному світі, все більше демонструють взаємозв'язок і взаємозалежність глобалізації та розвиток інформаційно-телекомунікаційних технологій. Інформаційні, технологічні інновації та інновації управління істотно розширюють можливість управління збройними силами, розвитку інформаційного обміну, а також підвищують цінність інформації [1].

Заходи щодо забезпечення інформаційної безпеки автоматизованої інформаційної системи є основою для конструктивної взаємодії органів військового управління для захисту інформації в інтересах виконання покладених завдань.

Аналіз останніх досліджень і публікацій. Головна причина значного приділення уваги до інформаційної безпеки є значне спрощення методів за засобів добування та використання інформації. Інформація, яка обробляється та передається в автоматизованих інформаційних системах є достатньо вразлива як з точки зору небезпеки її спотворення або знищення.

На сьогоднішній день є велика кількість підходів щодо оцінки функціонування системи інформаційної безпеки [1-4]. Поряд з цим, в різних підходах використовуються різні показники щодо її оцінювання. Одним із основних показників, який впливає на ефективність функціонування системи інформаційної безпеки є показник якості системи інформаційної безпеки автоматизованої системи управління.

Метою статті є обґрунтування показника якості системи інформаційної безпеки автоматизованої інформаційної системи органу військового управління.

Виклад основного матеріалу дослідження

Система інформаційної безпеки автоматизованої інформаційної системи органу військового управління – це спеціалізована система, що має на меті зменшення або ліквідування чинників загроз, умов, які приють прояву кожного з них, і зниженню вірогідності виникнення ситуації загрози об'єкту безпеки.

Таким чином, функціонування системи інформаційної безпеки автоматизованої інформаційної системи органу військового управління можна представити структурною схемою (рис. 1).

Виходячи з цього, у загальному вигляді модель функціонування системи інформаційної безпеки автоматизованої інформаційної системи органу військового управління може бути представлена загальною моделлю (рис. 2).

Противник, за допомогою деякого джерела загроз, генерує сукупність загроз функціонування автоматизованої інформаційної системи органу військового управління (обираємо обмеження $i = \overline{1,n}$). Кожна i-та загроза характеризується імовірністю появи $P_{i\,загр}$ та втратою $\Delta g_{i_{загр}}$, яку вона завдає інформаційний системі. Види втрат та їх показники, структурна схема механізму виникнення втрат від противника описана роботі Домарова В.В. [2].

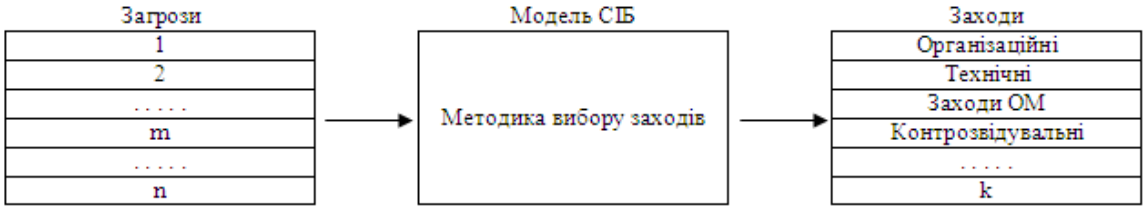

Рис. 1. Структурна схема функціонування системи інформаційної безпеки автоматизованої інформаційної системи органу військового управління

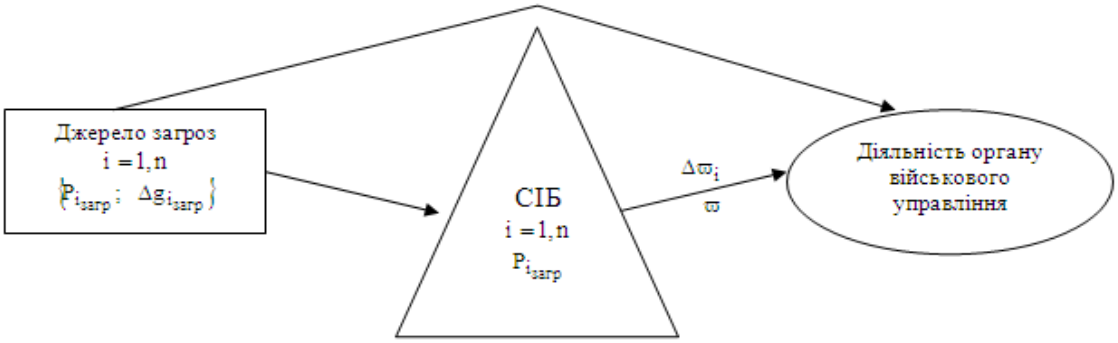

Рис. 2. Загальна модель функціонування системи інформаційної безпеки автоматизованої інформаційної системи органу військового управління

Противник, за допомогою деякого джерела загроз, генерує сукупність загроз функціонування автоматизованої інформаційної системи органу військового управління (обираємо обмеження $i = 1, n$). Кожна i-та загроза характеризується імовірністю появи $P_{i_{загр}}$ та втратою $\Delta g_{i_{загр}}$, яку вона завдає інформаційний системі. Види втрат та їх показники, структурна схема механізму виникнення втрат від противника описана роботі Домарова В.В. [2].

Система інформаційної безпеки виконує функцію повної або часткової компенсації загроз для інформаційної системи. Основною характеристикою системи інформаційної безпеки є імовірність усунення кожної i-тої загрози $P^{ус}_{i_{загр}}$. За рахунок функціонування системи інформаційної безпеки забезпечується зменшення втрат W, які наносяться інформаційній системі під дією загроз. Позначимо загальний показник ефективності процесів організації та ведення заходів інформаційної безпеки $\overline{W}$, а попереджені втрати за рахунок ліквідації впливу i-тої загрози через ϖ_i.

Сформулюємо в загальному вигляді завдання створення системи інформаційної безпеки в інформаційних системах. Необхідно обрати такий варіант реалізації системи інформаційної безпеки, який би забезпечував максимум попереджених втрат від дій розвідувальної системи противника при допустимих витратах на неї. Формально постановка завдання має вигляд:

$$T^0 = \arg\max \overline{W}(T) \qquad (1)$$

Знайти

$$T^0 \in T^+ \text{ при } C(T^0) \le C_{доп} \qquad (2)$$

де: T – деякий вектор, який характеризує варіант організаційно-технічної реалізації системи інформаційної безпеки;

T^0, T^+ – допустиме та оптимальне значення вектору T;

$C_{доп}$ – допустимі витрати на систему інформаційної безпеки.

Для вирішення завдання необхідно сформувати показник якості функціонування системи інформаційної безпеки $\overline{W}(T)$.

Попереджені втрати у загальному вигляді виражаються співвідношенням:

$$\overline{W} = F\left(P_{i_{ззаг}}; \Delta g_{i_{загр}}; P^{ус}_{i_{ззаг}}; i = 1, n\right) \qquad (3)$$

Попереджені втрати за рахунок ліквідації дії i-ої загрози описується виразом:

$$\varpi_i = P_{i_{ззаг}} * \Delta g_{i_{загр}} * P^{ус}_{i_{ззаг}}; i = 1, n \qquad (4)$$

Таким чином, при умові незалежності загроз і адитивності їх наслідків з урахуванням виразу (4) вираз розрахунку попереджених втрат запишемо як:

$$\overline{W} = \sum_{i=1}^{n} P_{i_{загр}} * \Delta g_{i_{загр}} * P^{ус}_{i_{загр}} \qquad (5)$$

Розглянемо детально множники виразу (5).

Імовірність появи i-тої загрози визначається $P_{i_{загр}}$ статистично і відповідає відносній частоті її появи

$$P_{i_{загр}} = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} = \overline{\lambda}_i \qquad (6)$$

де: λ_i – частота появи i-тої загрози.

Втрати, які завдаються i-тою загрозою $\Delta g_{i_{загр}}$, можуть бути визначені в абсолютних одиницях: людських стратах, витратах ресурсів, витратах часу, знищеній або викривленій інформації і т.д.. Поряд з цим, більш доцільно, замість абсолютних втрат використовувати відносні втрати, які представляють ступінь небезпеки i-тої загрози для інформаційних систем. Ступінь небезпеки може бути визначена експертним шляхом в припущенні, що всі загрози для інформаційних систем

складають повну групу подій, тобто $0 \le \Delta g_{i_{загр}} \le 1;\ \sum_{i=1}^{n} \Delta g_{i_{загр}} = 1$.

Найбільш важким питанням є визначення імовірності усунення і-тої загрози $P_{i_{загр}}^{ус}$ при створенні системи інформаційної безпеки. Робиться припущення, що ця імовірність визначається тим, наскільки повно враховані якісні та кількісні вимоги до системи інформаційної безпеки при її створенні, тобто

$$P_{i_{загр}}^{ус} = f_i\left(x_{i1,} K, x_{ij,} K, x_{im}\right) \quad (7)$$

де: x_{ij} – ступінь виконання j-тої вимоги до системи інформаційної безпеки для усунення і-тої загрози, $i \equiv \overline{1,n},\ j = 1,m$.

Нехай перші "k" вимог будуть кількісними $\left(j = \overline{1,k}\right)$, а інші "m-k" – якісними $\left(j = \overline{k+1,m}\right)$.

Ступінь виконання j-тої кількісної вимоги визначається її близькістю до вимагає мого (оптимального) значення. Для оцінки ступеня виконання j-тої кількісної вимоги до системи інформаційної безпеки найбільш доречно використовувати її нормоване значення $x_{ij}\left(j = 1,k\right), 0 \le x_{ij} \le 1$.

Для нормування є зручною у використанні функція у вигляді:

$$x_{ij} = \frac{x_{ij} - x_{ij}^{нк}}{x_{ij}^{нг} - x_{ij}} \quad (8)$$

де: x_{ij} – значення j-тої вимоги;

$x_{ij}^{нк}$, $x_{ij}^{нг}$ – найгірше та найкраще значення.

З урахуванням виразу (7) отримаємо наступне співвідношення:

$$\text{при } x_{ij}^{нк} = x_{ij\max};\ x_{ij}^{нг} = x_{ij\min};\ x_{ij} = \frac{x_{ij} - x_{ij\min}}{x_{ij\max} - x_{ij\min}} \quad (9)$$

$$\text{при } x_{ij}^{нк} = x_{ij\min};\ x_{ij}^{нг} = x_{ij\max} \quad (10)$$

$$\text{при } \bar{x}_{ij} = \frac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\min}} \quad (11)$$

$$\bar{x}_{ij} = \begin{cases} 0 \quad \text{при} \quad x_{ij} > x_{ij\min};\ x_{ij} < x_{ij\max} \\ 1 \quad \text{при} \quad x_{ij} = x_{ij\_opt} \\ \dfrac{x_{ij} - x_{ij\min}}{x_{ij\_opt} - x_{ij\min}} \quad \text{при} \quad x_{ij\min} \le x_{ij} \le x_{ij\_opt} \\ \dfrac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\_opt}} \quad \text{при} \quad x_{ij\_opt} \le x_{ij} \le x_{ij\max} \end{cases}$$

Ступінь виконання j-тої якісної вимоги визначається функцією придатності до найкращого значення $\mu\left(x_{ij}\right)$.

Розклавши функцію (7) у ряд Макларена і обмеживши лише першими членами ряду, отримаємо:

$$P_{i_{загр}}^{ус} = P_{i_{загр}}^{ус}(0) + \sum_{\gamma=1}^{m} \frac{\partial P_{i_{загр}}^{ус}}{\partial x_{ij}} x_{ij} \quad (12)$$

де: $P_{i_{загр}}^{ус}(0) = 0$ – ймовірність усунення і-тої загрози при невиконанні вимог;

$\frac{\partial P_{i_{загр}}^{ус}}{\partial x_{ij}} = \alpha_{ij}$ – величина, що характеризує ступінь впливу вимоги на імовірність усунення і-тої загрози (важливість виконання j-тої вимоги для усунення і-тої загрози).

Очевидно, що $0 \le \alpha_{ij} \le 1;\ \sum_{\gamma=1}^{m} \alpha_{ij} = 1$ для $i = 1,n$.

Після підстановки у вираз (12) відповідних значень отримаємо

$$P_{i_{загр}}^{ус} = \sum_{j=1}^{k} \alpha_{ij} \bar{x}_{ij} + \sum_{j=k+1}^{m} \alpha_{ij} \mu\left(x_{ij}\right) \quad (13)$$

Остаточно, вираз (5) для оцінки величини $\overline{W}$ попереджених втрат приймає вигляд

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \bar{\lambda}_i \Delta g_i \alpha_{ij} \bar{x}_{ij} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \bar{\lambda}_i \Delta g_i \alpha_{ij} \mu\left(x_{ij}\right) \quad (15)$$

де: $\bar{\lambda}_i$ – відносна частота появи і-тої загрози, $i = 1,n$;

Δg_i – відносний збиток (ступінь небезпеки) від і-тої загрози, $0 \le \Delta g_i \le 1;\ \sum_{i=1}^{n} \Delta g_i = 1$;

α_{ij} – важливість j-го показника для усунення і-тої загрози, $j = 1,m$;

$\bar{x}_{ij}$ – нормоване значення j-го кількісного показника для усунення і-тої загрози, $\bar{x}_{ij} \le 1;\ j = 1,k$;

$\mu\left(x_{ij}\right)$ – функція належності j-го якісного показника необхідному рівню для усунення j-тої загрози $0 \le \mu\left(x_{ij}\right) \le 1;\ j = k+1,m$.

Комплексний показник ефективності пропонується визначати методом експертних оцінок, використовуючи положення теорії нечіткої логіки і нечітких тверджень. Величина часткових показників кожного з елементів матриці визначається на основі використання відповідних функцій приналежності.

Обґрунтовано узагальнений показник ефективності процесів організації та ведення заходів інформаційної боротьби $\overline{W}$, що враховує характеристики інформаційних загроз і часткові показники на основі матриці оцінок (14).

Висновки й перспективи подальших досліджень

Задачі формулювання раціональних рішень щодо проведення заходів інформаційної безпеки зведені до вибору варіанта, що забезпечує максимальне значення показника W при припустимих витратах на реалізацію.

Необхідні вихідні дані доцільно одержувати на основі збору і відпрацьовування експертної інформації з використанням теорії нечітких множин.

Результат впровадження запропонованої моделі системи інформаційної безпеки

автоматизованої інформаційної системи органу військового управління, що розглядає питання оцінки організації та проведення заходів інформаційної безпеки дає можливість розробки рекомендацій щодо створення ефективної системи інформаційної безпеки автоматизованої інформаційної системи органу військового управління, яка забезпечує максимум попереджених втрат від дій розвідувальної системи противника при допустимих витратах на систему інформаційної безпеки.

Література

1. Довгий С.О., Воробієнко П.П., Гуляєв К.Д. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання.-К.: "Азимут-України". 2013.-608с. **2. Домарев В.В.** Безопасность информационных технологий. Методология создания систем защиты. К.: ТИД ДиаСофт, 2002. – 688 с. URL: https://www.twirpx.com/file/26250/. **3. Есин В.И., Кузнецов А.А., Сорока Л.С.** Безопасность информационных систем и технологий.-Х.:ООО "ЭДЭНА", 2010. – 656 с. **4. Домарев В.В.** Безопасность информационных технологий. Системный подход - К.:ООО ТИД «Диасофт», 2004.-992 с. URL:http://library.univer.kharkov.ua.

ОБОСНОВАНИЕ ПОКАЗАТЕЛЯ КАЧЕСТВА СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНОВ ВОЕННОГО УПРАВЛЕНИЯ

Валерий Александрович Крайнов *(кандидат технических наук, доцент)*
Роман Иванович Грозовский

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Темпы развития информационных технологий за последние годы побудили внедрению средств вычислительной техники в процессы управления войсками. Это в свою очередь отразилось и на обратной стороне этого процесса, а именно, вырос интерес к информации, циркулирующей внутри информационных систем не только со стороны пользователей, а в значительной степени из стороны противника. На сегодняшний день существует большое количество каналов утечки и искажения информации.

Система информационной безопасности выполняет функцию полной или частичной компенсации угроз информационной системы. Основной характеристикой системы информационной безопасности является вероятность устранения каждой угрозы. За счет функционирования системы информационной безопасности обеспечивается уменьшение потерь, которые наносятся информационной системе под действием угроз. Таким образом, целью статьи является обоснование показателя качества системы информационной безопасности автоматизированной информационной системы органа военного управления.

Ключевые слова: *исистема информационной безопасности; автоматизированная информационная система; орган военного управления; угроза.*

SUBSTANTIATION OF THE QUALITY INDICATOR OF THE SYSTEM OF INFORMATION SECURITY OF THE AUTOMATED INFORMATION SYSTEM OF MILITARY MANAGEMENT BODIES

Valerii Krainov *(Candidate of technical sciences, associate professor)*
Roman Hrozovskyi

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The pace of development of information technology in recent years has prompted the introduction of computer technology in the processes of command and control. This, in turn, was reflected in the reverse side of this process, namely, interest grew in information circulating inside information systems not only from the users, but largely from the side of the enemy. To date, there are a large number of channels of leakage and distortion of information.

The information security system performs the function of fully or partially compensating threats to the information system. The main characteristic of the information security system is the probability of eliminating each threat. Due to the functioning of the information security system, losses are reduced, which are inflicted on the information system under the influence of threats. Thus, the purpose of the article is to substantiate the quality index of the information security system of the automated information system of the military command body.

Keywords: *information security system; automated information system; military management body; threat.*

References

1. Dovgiy SO, Vorobienko PP, Gulyaev KD. Suchasni telekomunikatsiyi: Merezhi, tehnologiyi, bezpeka, ekonomika, regulyuvannya.-K .: "Azimut-UkraYini". 2013-608s. **2. Domarev VV**. Bezopasnost informatsionnyih tehnologiy. Metodologiya sozdaniya sistem zaschityi. K .: TID DiaSoft, 2002. - 688 s. URL: https://www.twirpx.com/file/26250/**. 3. Esin VI, Kuznetsov AA, Soroka LS**. Bezopasnost informatsionnyih sistem i tehnologiy.-H.:OOO "EDENA", 2010. - 656 s. **4. Domarev VV** Bezopasnost informatsionnyih tehnologiy. Sistemnyiy podhod - K.:OOO TID «Diasoft», 2004.-992 s. URL: http: //library.univer.kharkov.ua.