УДК 004.056

к.т.н., с.н.с. **Буяло О.В.** (ВДА)

ОБГРУНТУВАННЯ ВИМОГ ДЛЯ АНАЛІЗУ І СИНТЕЗУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, ЯК СКЛАДНОЇ ТЕХНІЧНОЇ СИСТЕМИ

У статті проведено обґрунтування вимог для аналізу і синтезу системи захисту інформації інформаційної системи. Система захисту інформації при цьому представлена у вигляді складної технічної системи. В результаті отримано у явному вигляді аналітичних залежностей для обраних показників ефективності: ймовірності усунення загрози та загальну успішної попередженої шкоду інформаційній системі. Отримані результати дозволяють науково-обгрунтовано формулювати вимоги до архітектури система захисту інформації, здійснювати кількісну оцінку якості функціонування системи захисту інформації на етапі розробки, а також дозволяють здійснювати управління її компонентами на етапі експлуатації.

Ключові слова: інформаційна система, загрози, система захисту інформації, складна технічна система.

Постановка проблеми у загальному вигляді. Стрімкий розвиток науково-технічного прогресу призводить до широкого впровадження в усі сфери діяльності сучасного суспільства інформаційних систем. Сьогодні інформація – це один з основних активів, який забезпечує усе: від життєдіяльності окремої людини до держави у цілому. Широка доступність інформаційних систем і технологій робить їх об’єктами постійної посиленої уваги з боку злочинних угруповань. У зв’язку з цим останнім часом зростає роль кіберпростору у питаннях забезпечення національної безпеки у інформаційній сфері. Це в свою чергу спонукає до удосконалення та перегляду діючих вимог (концепцій) щодо розробки і побудови систем захисту інформації (СЗІ) та стратегій їх раціонального застосування і управління їхніми складовими (компонентами) з метою швидкого реагування на сучасні загрози [1-11].

Важкість вирішення питань забезпечення безпеки інформаційних систем (ІС) посилюється великою невизначеністю умов їх функціонування. Вирішення завдання забезпечення безпеки ІС, як правило, не володіє властивістю єдиного рішення, а раціональні рішення визначаються саме ступенем врахування обмежень, які характерні для конкретних загроз. Для підвищення ступеню коректності постановки задачі забезпечення безпеки інформаційної системи необхідно підвищувати знання про ІС в сучасних умовах, що безперервно змінюються. Здобуття і використання знань повинні здійснюватися безпосередньо в процесі функціонування системи шляхом поступового накопичення необхідної інформації, аналізу і використання її для ефективного виконання системою заданої цільової функції та управління компонентами під впливом внутрішнього і зовнішнього середовища, які постійно змінюються.

Аналіз останніх досліджень і публікацій. Проведений аналіз останніх досліджень і публікацій [1-17] показав, що вирішення завдання аналізу і синтезу СЗІ насьогодні ускладнюється рядом особливостей, основними з яких є: складний опосередкований взаємозв'язок показників якості СЗІ з показниками якості інформаційної системи; необхідність обліку великого числа показників (вимог) щодо СЗІ при оцінці і виборі раціонального варіанту; переважно якісний характер показників (вимог), що враховуються при аналізі і синтезі СЗІ; істотний взаємозв'язок і взаємозалежність цих показників (вимог), що мають суперечливий характер; важкість здобуття вихідних даних, необхідних для СЗІ, особливо на ранніх етапах їх проектування, майже відсутність автоматизованого управління складовими вже створених СЗІ для здійснення швидкого управління ними відповідно до зміни сучасних загроз, або визначення моменту проведення управління з метою реконфігурування або модернізації.

В зв’язку з цим постановка задачі забезпечення захисту інформації, як правило, виявляється обмеженою, оскільки часто формулюється в умовах непередбачуваності поведінки системи в нестандартних і, особливо, екстремальних ситуаціях. Вплив невизначеності особливо сильно проявляється у системах, які повинні трансформуватися, в залежності від загроз, у зв’язку з невчасністю, неповнотою та низькою достовірністю інформації.

Вказані особливості істотно обмежують застосування традиційних математичних методів, у тому числі методів математичної статистики і теорії ймовірності, а також класичних методів оптимізації для вирішення прикладних завдань аналізу і синтезу СЗІ на яких ґрунтуються роботи [11-17].

Аналіз показав, що відомі методи та моделі, які використовуються для опису структури, поведінки і управління СЗІ, у таких умовах дають тільки частковий і тимчасовий ефект, та мають обмежене застосування [11-17]. Теоретичні основи побудови систем захисту виключно складні і, не дивлячись на інтенсивність досліджень в цій предметній області, ще далекі від досконалості. Крім того відсутність досить загальної теорії, що формує методологічні підстави вивчення явищ з невизначеними чинниками, істотно обмежує можливості застосування байесовських методів класичної теорії статистичних рішень для синтезу раціональних систем захисту.

Формулювання цілей статті. У зв’язку з цим постає актуальним вирішення завдання, щодо наукового обґрунтування вимог для аналізу і синтезу СЗІ для здійснення управління її компонентами на етапі її експлуатації, як складною технічною системою, що і є **метою й основним змістом статті**.

Виклад основного матеріалу досліджень. У процесі аналізу і синтезу раціональної СЗІ неминуче виникає завдання щодо реконфігурування та управління компонентами СЗІ відповідно до вимог сучасності. Складність цього рішення полягає у тому, що на цей процес впливає низка невизначеностей, які викликані: швидкими темпами розвитку та удосконалення систем нападу, способи дії яких дослідник може тільки припускати; недостатньою вивченістю деяких явищ, що супроводжують процес функціонування систем захисту; нечітким представленням мети операції, складністю процесу пошуку і аналізу альтернативних рішень, щодо побудови СЗІ, що призводить до неоднозначного трактування відповідності реального результату необхідному.

У зв’язку з цим пропонується науково-обгрунтовати вимоги для аналізу і синтезу СЗІ.

У самому загальному вигляді запропонований формалізований опис процесу функціонування СЗІ можливо представити у вигляді (рис. 1).

В якості показників ефективності для оцінки альтернативних рішень при аналізі і синтезі СЗІ пропонується використовувати: ймовірність усунення кожної i-тої загрози $P_{i_{заг}}^{ус}$ та загальну успішно попереджену шкоду ІС.

Використання показника ефективності, дозволить в подальшому зіставляти стратегії, альтернативні рішення, які характеризуються різною мірою досягнення мети, та здійснювати вибір раціональної стратегії із множини припустимих.

Припустимо, що джерело загроз (ДЗ) генерує сукупність загроз, при цьому кількість загроз буде вважати кінцевою і такою, що рахується.

Кожна загроза характеризується ймовірністю появи та шкодою, яка наноситься інформаційній системі.

Для визначення виду шкоди, показників шкоди, побудови структурної функціональної схеми механізму виникнення шкоди від загроз безпеки інформації можуть бути використані роботи [2, 3].

Система захисту інформації, з одного боку, є складовою частиною інформаційної системи, з іншого боку сама по собі представляє складну технічну систему.

Система захисту інформації (СЗІ) виконує функцію повної або часткової компенсації загроз для інформаційної системи.

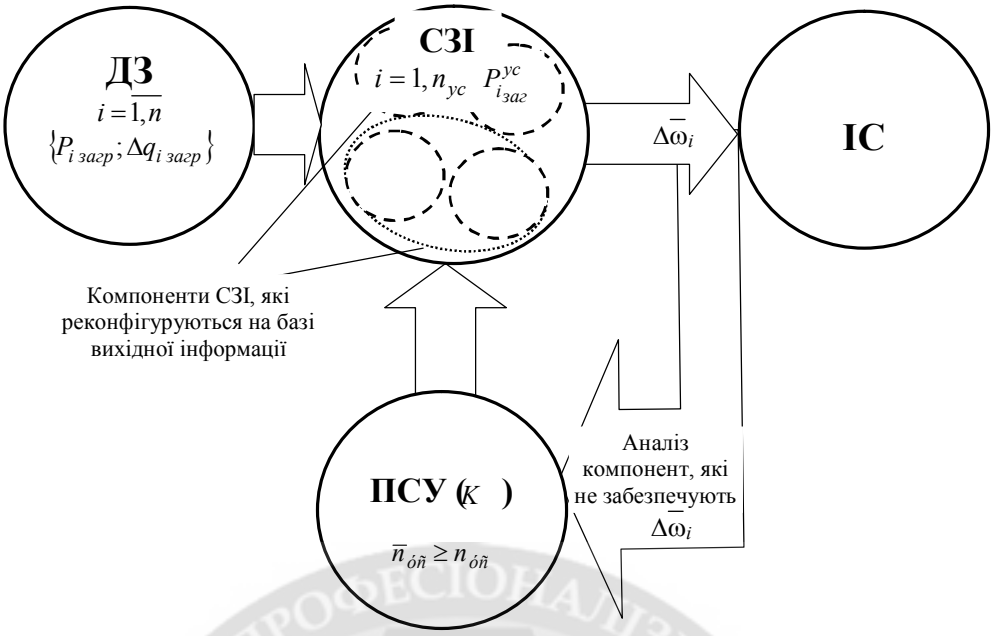

Рис. 1. Запропонований формалізований опис процесу функціонування СЗІ

Виходячи з того, що ймовірність усунення кожної i-тої загрози $P_{i_{заг}}^{ус}$ та ймовірність не усунення СЗІ i-тої загрози $P_{i_{заг}}^{не\ ус}$ утворюють повну групу подій буде справедливим вираз: $P_{i_{заг}}^{не\ ус} = 1 - P_{i_{заг}}^{ус}$.

За рахунок функціонування СЗІ забезпечується зменшення шкоди W, яка наноситься ІС впливом загроз. Позначимо загальну успішно попереджену шкоду ІС, через $\overline{W}$, а попереджену шкоду за рахунок ліквідації впливу i - тої загрози через $\bar{\omega}_i$.

Для здійснення аналізу вихідної інформації, щодо функціонування СЗІ за кількісним і якісним показником попередження впливу i - тої загрози $\bar{\omega}_i$ для управління компонентами з метою зменшення впливу кожної i-тої загрози на СЗІ пропонується ввести підсистему управління ПСУ, яка здійснюватиме управління з загальним впливом $K_i = 0 \div 1$.

Отже загальний вплив системи підсистеми управляння на СЗІ, щодо зменшення впливу i -тої загрози значення ймовірності не усунення i -тої загрози на наступному етапі функціонування СЗІ визначатиметься виразом:

$$\bar{P}_{i_{заг}}^{не\ ус} = K_i P_{i_{заг}}^{не\ ус} = K_i (1 - P_{i_{заг}}^{ус}),\ \bar{n}_{ус} > n_{ус}.$$

Після введення позначень сформулюємо у загальному випадку задачу синтезу системи захисту інформації у ІС, яка полягає у тому, що необхідно обрати такий варіант реалізації СЗІ, який забезпечує максимум попередження шкоди від впливу загроз при припустимих витратах на СЗІ.

Математична постановка задачі має вигляд:

$$\text{Знайти} \quad \begin{aligned} T_{опт} &= \arg\max \overline{W}(T) \\ T_{опт} &\in T_{прип} \\ C(T_{опт}) &\leq C_{прип} \end{aligned} \qquad (1)$$

де T - деякий вектор, що характеризує варіант технічної реалізації СЗІ, $T_{опт}, T_{прип}$ – оптимальне і припустиме значення вектора T, $C_{прип}$ – припустимі витрати на СЗІ.

Показник якості функціонування СЗІ загальна успішно попереджена шкода ІС

$$\overline{W}(T) = F(P_{i\ загр}; \Delta q_{i\ загр}; P_{i\ заг}^{ус}); i = \overline{1,n} \tag{2}$$

Тоді попереджену шкоду за рахунок ліквідації впливу i - тої загрози

$$\overline{\omega}_i = P_{i\ загр} \times \Delta q_{i\ загр} \times P_{i\ заг}^{ус}; i = \overline{1,n} \tag{3}$$

При умові незалежності загроз та вважаючи, що наслідки загроз мають адитивний характер отримаємо:

$$\overline{W}(T) = \sum_{i=1}^{n} P_{i\ загр} \times \Delta q_{i\ загр} \times P_{i\ заг}^{ус} \tag{4}$$

Визначимо множники формули (4). Ймовірність появи i-тої загрози:

$$P_{i\ загр} = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} = \overline{\lambda}_i, \tag{5}$$

де λ_i - частота появи i-тої загрози.

Шкода, яка викликана i-тою загрозою Δq_i, може визначатися в абсолютних одиницях: економічних втратах, часових втратах, об'ємі інформації, яка знищена або модифікована.

На практиці можливо використовувати відносну шкоду, яка являє собою ступінь небезпеки i-тої загрози для інформаційної системи. Ступінь небезпеки може бути визначена експертним шляхом, враховуючи, що усі загрози для інформаційної системи складають повну групу подій:

$$0 \le \Delta q_i \le 1; \sum_{i=1}^{n} \Delta q_i = 1. \tag{6}$$

Ймовірність усунення i - тої загрози $P_{i\ заг}^{ус}$ визначається наскільки повно враховані якісні і кількісні вимоги до СЗІ, та визначається наступним виразом:

$$P_{i\ заг}^{ус} = f_i(x_{i1},...,x_{ij},...,x_{im}), \tag{7}$$

де x_{ij} - ступінь виконання j - тої вимоги до СЗІ для усунення i - тої загрози, $i = \overline{1,n}$, $j = \overline{1,m}$,

Для недопущення шкоди від кожної i-тої загрози у ПСУ проводиться аналіз ступінь виконання j - тої якісної вимоги визначається функцією приналежності до найкращого значення $\mu(x_{ij})$.

Хай перші k - вимог будемо вважати кількісними ($j = \overline{1,k}$), а інші $m-k$ - якісними ($j = \overline{k+1,m}$).

Ступінь виконання j- тої кількісної вимоги визначається його близькістю до необхідного (оптимального) значення $\overline{x}_{ij}$ ($j = \overline{1,k}$), $0 \le x_{ij} < 1$.

Як показано у [7,10], для нормування зручно використовувати функцію вигляду:

$$\overline{x}_{ij} = \frac{x_{ij} - x_{ij_{нг}}}{x_{ij_{нк}} - x_{ij_{нг}}},$$

де x_{ij} - поточне значення j -ї вимоги; $x_{ij_{нк}}; x_{ij_{нг}}$ - найкраще і найгірше значення.

З врахуванням формули отримаємо наступні розрахункові співвідношення:

При $x_{ij_{нк}} = x_{ij\max}; x_{ij_{нг}} = x_{ij\min}$

$$\bar{x}_{ij} = \frac{x_{ij} - x_{ij\min}}{x_{ij\max} - x_{ij\min}}$$

При $x_{ij_{нк}} = x_{ij\min}; x_{ij_{нг}} = x_{ij\max}$

$$\bar{x}_{ij} = \frac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\min}}$$

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

Розклавши функцію (7) у ряд Макларена, та взявши тільки перші члени ряду отримаємо:

$$P_{i\,заг}^{ус} = P_{i\,заг}^{ус}(0) + \sum_{\gamma=1}^{m} \frac{\partial P_{i\,заг}^{ус}}{\partial x_{ij}} \times x_{ij} \qquad (8)$$

де $P_{i\,заг}^{ус}(0) = 0$ - ймовірність усунення i - тої загрози при невиконанні вимог до СЗІ;

$\dfrac{\partial P_{i\,заг}^{ус}}{\partial x_{ij}} = \alpha_{ij}$ - величина, яка характеризує ступінь впливу вимог на ймовірність усунення i -тої загрози (важливість виконання j -тої якісної вимоги для усунення i -тої загрози).

$$0 \le \alpha_{ij} \le 1; \sum_{j=1}^{m} \alpha_{ij} = 1 \text{ для } i = \overline{1,n}.$$

Після підстановки у (8) відповідних значень отримаємо:

$$P_{i\,заг}^{ус} = \sum_{j=1}^{k} \alpha_{ij} \overline{x_{ij}} + \sum_{j=k+1}^{m} \alpha_{ij} \mu(x_{ij}).$$

Виходячи з загального впливу на СЗІ підсистеми управління, щодо зменшення впливу i -тої загрози значення ймовірності не усунення i -тої загрози на наступному етапі функціонування СЗІ визначатиметься виразом:

$$\overline{P}_{i_{заг}}^{не\,ус} = K_i P_{i_{заг}}^{не\,ус} = K_i \{1 - [\sum_{j=1}^{k} \alpha_{ij} \overline{x_{ij}} + \sum_{j=k+1}^{m} \alpha_{ij} \mu(x_{ij})]\} \qquad (14).$$

Кінцевий вираз (4) для оцінки величини $\overline{W}(T)$ попереджувальної загрози приймає вигляд:

$$\overline{W}(T) = \sum_{i=1}^{n} \sum_{j=1}^{k} \bar{\lambda}_i \Delta q_{i\,загр} \alpha_{ij} \bar{x}_{ij} + \sum_{j=1}^{n} \sum_{j=k+1}^{m} \bar{\lambda}_i \Delta q_{i\,загр} \alpha_{ij} \mu(x_{ij}) \qquad (15)$$

Таким чином задача синтезу СЗІ у вигляді (1), (2) зводиться до оптимального обґрунтування кількісних і якісних вимог до СЗІ при припустимих витратах $C(T_{опт}) \le C_{прип}$.

У відповідності з формулюванням задачі (15) основними елементами її розв'язання повинні бути: здійснення моніторингу та обробки інформації про характеристики загроз; здійснення моніторингу і обробки інформації в т. ч. може використовуватися експертна, для визначення важливості виконання кожної вимоги для усунення кожної загрози; проведення техніко-економічного аналізу конкретного варіанту СЗІ та її реалізації, яка залежить від ступеня виконання вимог; розробка відповідних математичних моделей і методики вибору варіанту побудови СЗІ (раціонального завдання вимог), чому і будуть присвячені подальші дослідження.

Висновки. Таким чином в статті проведено обґрунтування вимог для аналізу і синтезу системи захисту інформації (СЗІ) інформаційної системи. СЗІ при цьому представлено у вигляді складної технічної системи. В результаті отримано у явному вигляді аналітичні залежності для обраних показників ефективності: ймовірності усунення загрози СЗІ та загальну успішної попередженої шкоди ІС. Отримані результати дозволяють науково-обгрунтовано формулювати вимоги до архітектури СЗІ, здійснювати кількісну оцінку якості її функціонування та оцінку практичної чутливості розроблених моделей до відхилень від апріорних даних про СЗІ на етапі розробки, а також дозволяють здійснювати управління її компонентами на етапі її експлуатації.

Також визначено, що для здобуття інформації про поведінку СЗІ для здійснення управління з метою реконфігурування або модернізації компонентами необхідно виділити групи параметрів і визначити терміни перевірки їх значень. При цьому повинні розглядатися особливо значимі і важливі з точки зору реалізації мети функціонування СЗІ параметри. Перевірка і аналіз значень вказаних параметрів, необхідні для підвищення знань про систему, та повинні здійснюватися таким чином, щоб забезпечити можливість ухвалення своєчасних і достовірних рішень і управління СЗІ через ПСУ в процесі функціонування. Таким чином, в СЗІ обов'язково має бути передбачене виконання процедур контролю її працездатності та діагностування станів, цим питанням також будуть присвячені подальші дослідження.

ЛИТЕРАТУРА:

1. Хорошко В.О. Информационная безопасность Украины. Основные проблемы и перспективы / В. О. Хорошко // Захист інформації. – 2008. – № 40 (спец. вип.). – С. 6–9.

2. Ленков С.В. Методы и средства защиты информации: монография [в 2-х т.] Т. 2. Информационная безопасность / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К.: Арий, 2008. – 344 с.

3. Гайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Гайворонський, О.М. Новиков. За заг. ред. академіка НАН України М.З. Згуровського. – К. : Видавнича група BHV, 2009. – 608 с.

4. Голубенко О.Л. Політика інформаційної безпеки / О. Л. Голубенко, В. О. Хорошко, О. С. Петров та ін. – Луганськ : СНУ ім. В.Даля, 2009 – 376 с.

5. Голубев В.А. Информационная безопасность: проблемы борьбы с киберпреступлениями : монография / В.А. Голубев. – Запорожье : ЗИГМУ, 2003. – 336 с.

6. Корченко О.Г. Системи захисту інформації : монографія / О. Г. Корченко. – К. : НАУ, 2004. – 264 с.

7. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения : монография / А. Г. Корченко. – К. : "МК-Пресс", 2006. – 320 с.

8. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. – М. : Горячая линия – Телеком, 2004. – 280 с.

9. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : "МК-Прес", 2005. – 432 с.

10. Домарев В.В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К. : ООО "ТИД "ДС", 2004. – 992 с.

11. Грищук Р.В. Нетейлорівська модель процесу нападу на інформацію / Р. В. Грищук // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2009. – № 6 (136). – С. 60–64.

12. Грищук Р.В. Метод гібридного P-L-моделювання процесів нападу на інформацію / Р. В. Грищук // Зб. наук. пр. Військового інституту Київського національного університету імені Тараса Шевченка. – К. : ВІКНУ, 2009. – № 19. – С. 90–94.

13. Романов О.І. Математична модель захисту інформації в автоматизованих мережах спеціального призначення / О.І. Романов, С.П. Лівенцев, І.М. Павлов // Збірник наукових праць ВІТІ НТУУ „КПІ". – Київ: – 2004. – № 5. – С. 23 – 31.

14. Андон П.І. Атаки на відмову в мережі Інтернет: опис проблеми та підходів до її вирішення / П.І. Андон, О.П. Ігнатенко. – К. : Ін-т ПС, 2008. – 52 с. – (Препринт / НАН України, Ін-т програмних систем).

15. Schneier. B. Attack Trees / Schneier. B. // Dr Dobb's Journal. –2007. – № 24. – P. 12–18. 3. Sheyner O. Tools for Generating and Analyzing Attack Graphs // Oleg Sheyner, Jeannette Wing // Springer. – 2003. – LNSC 3188. – P. 344–371.

16. Todd Hughes. Attack scenario graphs for computer network threat analysis and prediction. / Todd Hughes, Oleg Sheyner // Complexity. – 2003. – №9 (2). – P. 15–18.

17. Новіков О.М. Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем / О.М. Новіков, А.М. Родіонов // Інформаційні технології та комп'ютерна інженерія (ВНТУ). 2008. – №1 (11). – С. 170–175.

Рецензент: д.т.н., проф. Жердєв М.К., провідний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.т.н., с.н.с. Буяло А.В.

ОБОСНОВАНИЕ ТРЕБОВАНИЙ ДЛЯ АНАЛИЗА И СИНТЕЗА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, КАК СЛОЖНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ

В статье проведено обоснование требований для анализа и синтеза системы защиты информации (СЗИ) информационной системы. СЗИ при этом представлена в виде сложной технической системы. В результате получена в явном виде аналитических зависимостей для выбраных показателей эффективности: вероятности устранения угрозы СЗИ и общую успешно предупрежденного вреда ИС. Полученные результаты позволяют научно-обоснованно формулировать требования к архитектуре СЗИ на этапе разработки, а также позволяют осуществлять управление ее компонентами на этапе эксплуатации.

Ключевые слова: информационная система, угрозы, система защиты информации, сложная техническая система.

Ph.D. Byjalo A.V.

THE JUSTIFICATION OF THE REQUIREMENTS FOR THE ANALYSIS AND SYNTHESIS OF THE INFORMATION SECURITY SYSTEM, AS A COMPLEX TECHNICAL SYSTEM

The article deals with the substantiation requirements for analysis and synthesis of the information security system (ISS) information system. ISS thus presented as a complex technical system. The result is obtained in an explicit form of the analytical dependence for the selected performance indicator: the probability of eliminating the threat of ISS and overall successful pomeridiano harm information system. The results obtained allow scientifically grounded to formulate requirements to the architecture of ISS, to make a quantitative assessment of quality of functioning of the ISS at the design stage, and also allow the management of its components at the stage of its operation.

Keywords: information system, threats, information security system, a complex technical system.