УДК 004.056

Михайло Анатолійович СТРЕЛЬБІЦЬКИЙ,
кандидат технічних наук, доцент,
докторант Національної академії Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький

ОКРЕМІ ПИТАННЯ СИНТЕЗУ СИСТЕМНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІНТЕГРОВАНІЙ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ ПРИКОРДОННОГО ВІДОМСТВА НА СТАДІЇ МОДЕРНІЗАЦІЇ

У статті наведені необхідні вихідні дані та сформульовані аналітичні залежності синтезу системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України на стадії модернізації. Прийнята гіпотеза найбільш несприятливого порушника для системи та визначені необхідні та достатні умови щодо запобігання витоку інформації з відомчої системи в цих умовах. Визначені необхідні рівні захищеності доданих на стадії модернізації можливих каналів витоку інформації. Розглянуто розподіл засобів захисту інформації за можливими каналами витоку інформації. Наведено ітераційний спосіб досягнення заданого рівня захищеності системи різними групами засобів захисту інформації.

Ключові слова: *синтез, захист інформації, інформаційна система.*

Вступ. Побудова системи охорони та захисту державного кордону з урахуванням викликів гібридної війни [1] вимагає розгортання в зоні проведення антитерористичної операції прикордонних підрозділів

нового типу із специфічними завданнями, які притаманні функціонуванню прикордонного відомства в особливий період. Зазначені підрозділи створені в рамках реформування Державної прикордонної служби України з метою посилення рівня захищеності державного кордону з урахуванням викликів національній безпеці України, а також базових підходів щодо реформування системи державного управління, сектору безпеки та оборони України, її інтеграції в європейське та світове демократичне співтовариство [2, 5]. Відповідно до основних напрямів діяльності та подальшого розвитку Державної прикордонної служби України [2] передбачається також розгортання та функціонування прикордонних сервісних центрів і підключення пунктів пропуску, контрольних постів в'їзду (виїзду) до єдиної міжнародної системи розшуку злочинців – баз даних Інтерполу [3, 4].

Вищезазначене приводить до необхідності постійної модернізації телекомунікаційних мереж та інформаційно-телекомунікаційних систем прикордонного відомства, запровадження обладнання і технологій, що відповідають сучасним міжнародним стандартам та рекомендаціям. Одним із найважливіших завдань, яке виникає при модернізації корпоративної мережі Державної прикордонної служби України, залишається системний захист інформації.

Питанням системного захисту інформації присвячено низку наукових праць [6–8], в яких надано ґрунтовну інформацію щодо питань визначення рівня системного захисту інформації об'єктів в цілому. Однак в інтегрованій інформаційно-телекомунікаційній системі "Гарт" як гетерогенній системі, яка постійно розвивається, адаптуючись до викликів сучасності, потребує модернізації і система захисту інформації. Причому захищеність системи в цілому при спільному функціонуванні як існуючих, так і модернізованих (нових) складових не повинна знижуватись. Отже, постає проблема у визначенні характеристик доданих (модернізованих) складових при забезпеченні заданого рівня захищеності системи в цілому, тобто в синтезі системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі (ІІТС) Державної прикордонної служби України на стадії модернізації.

Метою статті є вирішення зворотної задачі системного захисту інформації, а саме синтез системного захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України на стадії модернізації.

Результати дослідження. При розробці технічного завдання на модернізацію ІІТС "Гарт" (упровадження нових інформаційно-телекомунікаційних систем або їх модернізація) Державна прикордонна служба України визначає вимоги до захищеності відомчої системи в цілому (Х) та вказує на вже реалізовані щодо окремих можливих каналів витоку інформації (МКВІ). Розробник у результаті обстеження, аналізу або моделювання отримав значення ваг МКВІ і визначає проектні рішення щодо вибору засобів захисту інформації для незахищених МКВІ з метою забезпечення норми захищеності системи.

Отже, зворотну задачу чи задачу синтезу системного захисту сформулюємо так.

Дано величини:

X – захищеність об'єкта (ІІТС);

C_i – вага i-го МКВІ;

x_i – захищеність і-го МКВІ;

М – кількість МКВІ в ІІТС до модернізації;

N – кількість МКВІ в ІІТС після модернізації;

де $i = \overline{1, M}$, $M < N$.

Необхідно знайти величини $x_i, i = \overline{M+1, N}$

Рішення такої задачі в загальному вигляді є невизначеним і має нескінченно багато рішень, якщо не вводити додаткові умови, значна кількість яких пов'язана з моделлю порушника. Разом із тим щодо інтегрованої інформаційно-телекомунікаційної системи "Гарт" в цілому така модель відсутня. Це істотно ускладнює подальші дослідження та знижує їх ефективність. У цьому випадку захист інформації будується від гіпотетичного порушника.

Щоб знайти одне з рішень оберненої задачі, приймемо найбільш несприятливу для нас гіпотезу про порушника, яка полягає в тому, що

він має в своєму розпорядженні достатньо ресурсів, щоб добувати інформацію з будь-якого МКВІ в будь-який момент часу.

При такій гіпотезі про порушника системний захист інформації повинен бути рівноміцним, тобто допустимий витік через всі МКВІ повинен бути однаковим, що математично означає

$$C_i(1-x_i) = C_j(1-x_j) = const, i, j = \overline{M+1, N}\ , \tag{1}$$

або

$$C_i(1-x_i) = C, C = const\ . \tag{2}$$

З виразу (2) та обмежень [9] маємо

$$x_i = 1 - \frac{C}{C_i}, 0 \le C \le C_i\ . \tag{3}$$

Іншими словами, якщо відома вага C_i і допустима величина C, то необхідна захищеність МКВІ знаходиться за виразом (3).

Виразимо C через вихідні дані задачі. Для цього уточнимо постановку задачі. Нехай замовником задані значення X та $x_i, i = \overline{M+1, N}$ а розробником визначено значення $C_i, i = \overline{1, N}$. Необхідно знайти значення x_i, за яких забезпечується рівноміцність системного захисту.

Зауважимо, що випадок M=N не представляє інтересу, оскільки величини $x_i, i = \overline{1, N}$ та X повинні задовольняти співвідношення [9]:

$$X = \sum_{i=1}^{N} C_i x_i\ . \tag{4}$$

Подамо це співвідношення у вигляді:

$$X = \sum_{i=1}^{M} C_i x_i + \sum_{i=M+1}^{N} C_i x_i\ . \tag{5}$$

Перенесемо задані величини в праву частину, а шукані величини в ліву частину рівняння (3).

Визначимо сумарний допустимий витік через ті МКВІ, відносно яких замовник не обумовив вимоги щодо захищеності $x_i, i = \overline{M+1, N}$.

Для цього просумуємо співвідношення (2) за кожним доданим МКВІ, тобто (M-N) раз:

$$\sum_{i=M+1}^{N} C_i(1-x_i) = C(N-M). \qquad (7)$$

З цього виразу випливає, що

$$C = \frac{1}{N-M}\left(\sum_{i=M+1}^{N} C_i - \sum_{i=M+1}^{N} C_i x_i\right).$$

Зазначимо, що, оскільки [9]:

$$\sum_{i=1}^{N} C_i = 1,$$

то

$$\sum_{i=M+1}^{N} C_i = 1 - \sum_{i=1}^{M} C_i. \qquad (9)$$

Об'єднаймо вирази (3), (6), (8), отримаємо остаточно

$$\left.\begin{aligned} x_i &= 1 - \frac{C}{C_i}, i = \overline{M+1, N} \\ C &= \frac{1}{N-M}\left[(1-X) - \sum_{i=1}^{M}(1-x_i)C_i\right] \end{aligned}\right\}. \qquad (10)$$

Якщо замовником задані вимоги із захищеності об'єкта (X) і із захищеності перших M МКВІ ($x_i, i = \overline{1, M}$), а розробником визначені ваги $C_i, i = \overline{1, N}$ усіх МКВІ, то необхідні для рівноміцного системного захисту інформації значення захищеності $x_i, i = \overline{M+1, N}$ решти МКВІ можна знайти за отриманими вище виразами (10). Іншими словами, отримано рішення оберненої задачі для випадку рівноміцного системного захисту. Інші варіанти системного захисту, які відповідають різним моделям порушника, вимагають окремого розгляду.

Зазначимо, що рішення (10) задачі синтезу рівноміцного системного захисту нескладно реалізувати на ЕОМ, зокрема на

ПЕОМ, у діалоговому режимі, а також представити у вигляді таблиць і графіків, зручних для математично непідготовленого користувача. Розробка цих питань також вимагає окремого розгляду.

Розглянемо здійснення розподілу засобів захисту інформації (ЗЗІ) за МКВІ. Якщо в результаті синтезу системного захисту знайдено необхідне значення захищеності МКВІ, то ця задача зводиться до дослідження одиночного МКВІ, для якого справедливе рівняння [9]

$$x_i = 1 - \prod_{j=1}^{S} (1 - q_{ij}), \qquad (11)$$

де q_{ij} – коефіцієнт захисту інформації; S – кількість типів ЗЗІ.

Це рівняння має рішення щодо невідомих тільки при використанні одного типу ЗЗІ, тобто $S=1$, тоді:

$$x_i = q_{ij}, j = 1.$$

У цьому випадку визначається необхідний коефіцієнт q_{ij} захисту ЗЗІ і далі серед S типів ЗЗІ підбирається такий, що задовольняє (11).

Якщо $S > 1$, то рішення рівняння (11) є невизначеним і потребує введення додаткових умов. У цьому випадку, зважючи на те, що для захисту МКВІ, як правило, не застосовують більше 3–5 ЗЗІ, рівняння (11) можна вирішити шляхом перебору комбінацій ЗЗІ, за необхідності використовуючи ЕОМ. При цьому, щоб зменшити число комбінацій ЗЗІ, їх доцільно ранжувати в групи за критеріями, наприклад: обов'язковості, сучасності і т. п. Позначимо коефіцієнтами захисту кожну з груп (розглянемо як приклад три групи ЗЗІ, кількість яких за потреби можна збільшити) $q_{ij}^1, q_{ij}^2, q_{ij}^3$, проранжувавши ЗЗІ всередині кожної з цих груп.

У цьому випадку спочатку аналіз комбінацій ЗЗІ проводиться за нерівності

$$x_i \le 1 - \prod_{j=1}^{S_1} (1 - q_{ij}^1). \qquad (12)$$

Якщо ця нерівність задовольняється, то вибирається така комбінація ЗЗІ, за якої досягається мінімальне значення захищеності МКВІ і йому присвоюється номер $m+1$.

$$(x_i)_{\min} = x_{m+1}, \qquad (13)$$

де m – кількість МКВІ, для яких раніше були знайдені комбінації ЗЗІ, що задовольняють необхідні значення захищеності цих каналів. Далі для решти незахищених МКВІ проводиться перерахунок необхідних значень їх захищеності за виразами (10) при $M = m + 1$ і проводиться перехід до підбору ЗЗІ чергового незахищеного МКВІ.

Якщо ж нерівність (12) не задовольняється, то склад комбінацій ЗЗІ розширюється за рахунок іншої групи ЗЗІ і потім аналіз комбінацій проводиться за нерівності

$$x_i - 2 + \prod_{j=1}^{S_1}(1-q_{ij}^1) \le -\prod_{j=S_1+1}^{S_2}(1-q_{ij}^2). \qquad (14)$$

Якщо ця нерівність задовольняється, то вибирається така комбінація ЗЗІ, за якої досягається мінімальне значення захищеності, МКВІ вважається захищеним, і процедура перерахунку, викладена вище, повторюється.

Якщо ж нерівність (14) не задовольняється, то склад комбінацій ЗЗІ розширюється за рахунок третьої групи ЗЗІ і потім аналіз комбінацій проводиться за нерівності:

$$x_i - 3 + \prod_{j=1}^{S_1}(1-q_{ij}^1) + \prod_{j=S_1+1}^{S_2}(1-q_{ij}^2) \le -\prod_{j=S_2+1}^{S_3}(1-q_{ij}^3), \qquad (15)$$

де $S_1 < S_2 < S_3$.

При цьому передбачається, що набір ЗЗІ такий, що, якщо не задовольняється нерівність (12), то мають задовольнятися нерівність (14) або нерівність (15). В іншому випадку треба розширювати склад ЗЗІ за рахунок розроблення і створення нових типів та продовження розрахунку з більшою кількістю груп аналогічно. Більш детально питання раціонального розподілу ЗЗІ за МКВІ вимагають окремого розгляду.

Висновок. Наведені функціональні залежності дозволять на етапі формування технічного завдання на модернізацію ІІТС сформувати вимоги до рівня захищеності модифікованих (нових) складових відомчої корпоративної системи з метою забезпечення заданого

загального рівня захищеності системи в цілому, тобто синтезувати системний захист інформації в інтегрованій інформаційно-телекомунікаційній системі "Гарт" на стадії модернізації.

У подальшому передбачається дослідження системного захисту інформації відомчої системи з урахуванням моделі порушника, а також питання раціонального розподілу засобів захисту інформації за можливими каналами її витоку.

Список використаної літератури

1. Магда Є. В. Виклики гібридної війни: інформаційний вимір / Є. В. Магда // Наукові записки Інституту законодавства Верховної Ради України. – 2014. – № 5. – С. 138–142.

2. Основні напрями діяльності та подальшого розвитку Державної прикордонної служби України у 2015 році [Електронний ресурс]. – Режим доступу: http://dpsu.gov.ua/ua/about/mission.htm

3. Прикордонники презентували Прем'єр-міністру України Стратегію розвитку відомства [Електронний ресурс]. – Режим доступу: http://dpsu.gov.ua/ua/about/news/news_8319.htm

4. Представники іноземної делегації ознайомилися з інноваціями прикордонного контролю [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/publish/article?art_id=248441509

5. Про основи національної безпеки України: Закон України // Відомості Верховної Ради України (ВВР). – 2003.

6. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-телекомунікаційних системах / О. Я. Матов, В. С. Василенко, М. М. Будько // Реєстрація, зберігання і оброб. даних. – 2004. – Т. 6, № 2. – С. 62-74.

7. Рибальський О. В. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України / О. В. Рибальський, В. Г. Хахановський, В. А. Кудінов. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

8. Горбенко И. Д. Критерии и методология оценки безопасности информационных технологий / И. Д. Горбенко, А. В. Потий, П. И. Терещенко. // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2000. – Вып. 114. – С. 25–38.

9. Стрельбіцький М. А. Обґрунтування та вибір цільової функції системного захисту інформації в інтегрованій інформаційно-

телекомунікаційній системі Державної прикордонної служби України / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер. : Військові та технічні науки. – 2011. – № 56. – С. 63–64.

Рецензент – доктор військових наук, професор, Кириленко В. А.

Стаття надійшла до редакції 16.11.2015.

Стрельбицкий М. А. **Отдельные вопросы синтеза системной защиты информации в интегрированной информационно-телекоммуникационной системе пограничного ведомства на стадии модернизации**

В статье приведены необходимые исходные данные и сформулированы аналитические зависимости синтеза системной защиты информации в интегрированной информационно-телекоммуникационной системе Государственной пограничной службы Украины на стадии модернизации. Принята гипотеза наиболее неблагоприятного нарушителя для системы и определены необходимые и достаточные условия для предотвращения утечки информации из ведомственной системы в этих условиях. Определены необходимые уровни защищенности добавленных на стадии модернизации возможных каналов утечки информации. Рассмотрено распределение средств защиты информации по возможным каналам утечки информации. Приведен итерационный способ достижения заданного уровня защищенности системы различными группами средств защиты информации.

Ключевые слова: *синтез, защита информации, информационная система.*

Strelbitskyi M. A. **Some questions of system information protection synthesis in information and telecommunication systems of border agencies at the stage of modernization**

*B*uilding a system of security and protection of the state border on the basis of the hybrid war challenges requires deployment of a new type

of border departments with specific functions that are inherent in the functioning of the border agency in a particular period in the zone of the antiterrorist operation.

These units are created under the reforms of the State Border Guard Service of Ukraine to strengthen the security of the state border taking into account the new security sphere, as well as basic approaches to the reforms of public administration, the defense and security sector of Ukraine, its integration into the European and the global democratic community.

In accordance with the main activities and further development of the State Border Guard Service the following functions are expected: deployment and operation of cross-border service centers and connection of checkpoints, entry (exit) control posts to a single international system of wanted criminals – the Interpol databases.

All of the above-mentioned leads to the need for continuous upgrading of telecommunication networks as well as information and telecommunication systems of the border agency, the introduction of equipment and technologies that meet modern international standards and recommendations. One of the major problems that arises when upgrading the corporate network of the State Border Guard Service of Ukraine is system protection.

Thus, the question of system information security synthesis in heterogeneous information and telecommunication systems at the stage of modernization requires additional research, namely solving the inverse problem of the system of information security. In practice this means that the development of the technical project for the modernization of "Hart", the integrated information and telecommunication system, (introduction of new information and telecommunication systems or their upgrading) State Border Guard Service of Ukraine defines the requirements for the security of departmental systems as a whole and indicates what is already implemented concerning individual possible information leakage channels. The developer as a result of surveys, analysis and simulation received the value weights of possible information leakage and determined project decisions on the choice of means of protection for the vulnerable MKVI to ensure security standards of the system.

The solution of this problem in general is uncertain, and has infinitely many solutions if additional conditions are not impose, many of which are related to the model violator.

However, in terms of "Hart", the integrated information and telecommunication system, in general, such a model is missing.

This greatly complicates further research and reduces its effectiveness.

In fact in this case the protection of information is based on a hypothetical offender. To find one of the solutions to this inverse problem, we shall accept the most unfavorable for us hypothesis of the violator, which is that he has sufficient resources to obtain information from any possible information leakage channel at any time.

With this hypothesis of the violator systematic data protection should be equable, that means permissible leakage through all possible channels of information leakage has to be the same. This research allowed us to form functional relations that will allow to form requirements for the security of modified (new) corporate departmental components at the stage of technical project formation for the modernization of integrated information and telecommunication systems to provide a given level of total security of the system as a whole.

Further research is expected on the departmental information security system Ii accordance with the model of the violator, as well as the rational distribution of information security for the possible channels of information leakage.

Keywords: *synthesis, information security, information system.*