О.В. Чечуй, Д.С. Комін, В.Д. Ревенко

Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків

ФОРМАЛІЗОВАНА МОДЕЛЬ ОЦІНКИ ГАРАНТІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ ЗАХИЩЕНОЇ ІР-ТЕЛЕФОНІЇ

Розглянуто основні підходи, які необхідно реалізовувати при оцінюванні гарантій інформаційної безпеки систем захищеної ІР-телефонії у відповідності до державних та міжнародних стандартів. Запропоновано застосування удосконаленої формалізованої моделі процесу оцінювання вимог гарантій інформаційної безпеки систем ІР-телефонії із застосуванням процесного підходу. Така модель дозволяє здійснювати оцінювання гарантій інформаційної безпеки систем ІР-телефонії та визначати вимоги до результатів експертизи.

Ключові слова: система захищеної ІР-телефонії, процесний підхід, інформаційна безпека, протоколи безпеки ІР-телефонії, формалізована модель, експертиза, експерт.

Вступ

Постановка проблеми. Сучасна інформаційно-телекомунікаційна система (ІТС) військового призначення повинна відповідати критеріям захищеності при обробці та зберіганні даних, із забезпеченням конфіденційності, цілісності та доступності інформації. Безумовно метою захищеності ІТС має бути відповідність політиці інформаційної безпеки (ІБ), вимірюваність, врахування вимог до ІБ з оцінкою ризиків та оновлюваність. Складність у досягненні цієї мети полягає у тому, що кожна ІТС має свої особливості побудови, свою структуру та свої вимоги щодо забезпечення ІБ. Однією з таких ІТС є система захищеної ІР-телефонії, яка являє собою складну мережу, побудовану із застосуванням телекомунікаційного обладнання для передачі захищених голосових повідомлень і сигналізації та протоколів різних рівнів. Саме тому для оцінки якості та відповідності рівня захищеності систем захищеної ІР-телефонії виникає необхідність у проведенні експертиз із залученням відповідних організацій та компетентних експертів, які мають оцінити рівень гарантій ІБ. Особливістю процесу оцінювання таких систем є те, що до них висуваються окремі вимоги щодо глибини, широти та суворості, а до результатів оцінювання – вимоги залишаються типовими. Основною проблематикою процесу оцінювання, яка виникає під час оцінки гарантій ІБ, також слід вважати, що для більшості вимог гарантій ІБ застосовуються лише якісні характеристики. Отже актуальним є завдання формалізації процесу оцінювання гарантій ІБ систем захищеної ІР-телефонії.

Аналіз останніх досліджень і публікацій. В [1–4] розглянуто різні методи представлення ІТС за допомогою яких вирішується задача оцінки гарантій

ІБ у відповідності до вимог стандартів [5–12]. Огляд нормативної та наукової літератури показав, що на даний час розглянуті загальні методи забезпечення виконання вимог до процесу та результатів оцінювання. Це обумовлено: недостатньою глибиною вивчення вимог та формального їх формулювання для ІТС різних видів, які мають свої особливості та структуру.

Мета статті. В даній статті пропонується застосування формалізованого підходу для побудови моделі оцінки гарантій ІБ для систем захищеної ІР-телефонії із застосуванням процесного підходу та представлення вимог, які висуваються до результатів експертизи.

Виклад основного матеріалу

Застосування процесного підходу для оцінки гарантій ІБ для систем захищеної ІР-телефонії обумовлено тим, що при проведенні експертизи здійснюється взаємодія суб'єктів експертизи і процесів виконання дій з їх оцінки. У відповідності до [13], процес оцінки вимог гарантій ІБ – це сукупність взаємопов'язаних операцій та дій, які направлені на дослідження, перевірку, аналіз та оцінку об'єкта експертизи, шляхом перетворення вхідних матеріальних та інформаційних потоків у вихідні потоки, які необхідні для суб'єктів експертизи, з метою визначення ступеня відповідності характеристик об'єкта експертизи заданим вимогам і визначення можливості використання об'єкта, який оцінюється, у якості довіреного з точки зору безпеки інформації. Таке визначення буде вірним і для систем захищеної ІР-телефонії.

Але для розробки моделі процесу оцінки гарантій ІБ систем захищеної ІР-телефонії на відміну від моделі запропонованої в [14], де враховуються фун-

кціональний, інформаційний організаційний та каузальний аспекти необхідно враховувати ще і територіальний, який визначає рівень реалізації загроз R (зовнішніх або внутрішніх).

Це пов'язано з тим, що ІБ системи захищеної ІР-телефонії визначається наявністю уразливості джерела інформації та середою розповсюдження інформаційного сигналу і несанкціонований доступ (НСД) порушника до цієї системи може здійснюватися, як ззовні, так і з середини. Зовнішні та внутрішні загрози для реалізації НСД до системи доцільно розглядати з точки зору наявності права доступу порушника до контрольованої зони об'єкта експертизи [17–24].

Для побудови формалізованої моделі процесу оцінки вимог гарантій ІБ системи захищеної ІР-телефонії застосовуються аксіоматичні конструкції (АК), які представлені в [14] з уточненнями АК 4 та додаванням АК 7:

АК 4. Для проведення процесу оцінювання [9] гарантій матеріального потоку – об'єкту експертизи TOE для множини входів $IN_{TOE} = \{M_{TOE}^{in}\}$ і виходів $OUT = \{I^{out}, M^{out}\}$ процесу Z із заданим оператором перетворення $F: IN \rightarrow OUT$ слід надати уточнення:

$$TOE = \langle Hw, HScr, Sw, D \rangle, \quad (1)$$

де $Hw = \{Hw_i \mid i = \overline{1, I}\}$ – апаратні складові системи ІР-телефонії;

$HScr = \{HScr_j \mid j = \overline{1, J}\}$ – програмно-апаратні засоби криптографічні засоби захисту інформації (КЗІ);

$Sw = \{Sw_y \mid y = \overline{1, Y}\}$ – програмні складові системи ІР-телефонії, які реалізовані у вигляді протоколів захисту сигналізації, протоколів захисту медіа-інформації та протоколи генерації та розподілу ключів для захисту медіаінформації;

$D = \{D_z \mid z = \overline{1, Z}\}$ – комплект документації до ОЕ, до якого входять документи на систему ІР-телефонії та засоби КЗІ.

АК 7. Процес визначення рівня реалізації загроз R здійснюється за оцінкою ймовірності захищеності системи від НСД P_{pr} визначається із застосуванням математичних моделей, які містять випадкові елементи у вигляді ймовірностей успішного виконання окремих атак та формують одну загальну атаку та результуючу P_{suc} ймовірність успішної атаки (атак) порушника для реалізації НСД до системи:

$$P_{pr} = 1 - P_{suc} = 1 - \max \{P_{atk} \mid k = \overline{1, K}\}, \quad (2)$$

де P_{atk} – ймовірність успішного виконання атаки, яка залежить від варіантів їх застосування та моделей дій порушника.

У відповідності до [15–16] основними видами атак на системи ІР-телефонії можуть бути: атака на шифр, перебір пароля для доступу до обладнання мережі, атака на протоколи безпеки ІР-телефонії, зміна налаштувань терміналу користувача для часткового відключення безпеки, перехоплення даних авторизації, встановлення закладок, модифікація програмного забезпечення, тощо. І в залежності від моделей дій порушника, від його місця в мережі можуть застосовуватись різні види атак за різними алгоритмами. Саме тому значення P_{atk} може визначеним, як:

$$P_{atk} = F(l, t_{iter}, t_{act}, Sp, Tec_{equip}), \quad (3)$$

де l – довжина ключа та довжина пароля;

t_{iter} – час необхідний для здійснення перебору пароллю та ключа при здійсненні атаки;

t_{act} – час, за який данні не втрачають актуальності;

Sp – швидкість каналу зв'язку за яким здійснюється атака;

Tec_{equip} – технічні можливості порушника.

Застосування наведених конструкцій АК 1-АК 3, АК 5, АК 6 в [14] та АК 4, АК 7 дозволяє представити наступну формалізовану модель процесу оцінювання гарантій ІБ систем захищеної ІР-телефонії:

$$Z = \langle Pur(G^P, V), d(A), F(TOE, E, R), IN \rightarrow OUT, Team(B), Source \rangle,$$

де $Pur(G^P, V)$ – звіт з оцінювання гарантій безпеки який формується з дерева цілей G^P , яке описується у програмі оцінювання і множини вердиктів V , які представлені у вигляді множини висновків (вердиктів) експертів $V = \{V_i \mid i = \overline{1, I}\}$ відносно ступеня прояву окремих властивостей гарантій безпеки;

$d(A)$ – відношення d до процесу на множині дій A з оцінки вимог гарантій ІБ (домінування), яке може бути представлена у вигляді графа G^A , з описанням конкретних типів відносин на множині дій;

$F(TOE, E, R)$ – процес оцінювання гарантій, який включає три потоки:

– матеріальний – об'єкт експертизи TOE , який визначається згідно (1);

– матеріально-інформаційний – сукупність (множина) свідочств E , які отримані від замовника експертизи, документи та матеріали (програма та методика проведення експертизи), результати випробувань елементів ОЕ (протоколи випробувань);

– інформаційний – оцінка рівня реалізації зовнішніх або внутрішніх загроз R з визначенням ймовірності захищеності системи від НСД P_{pr} , як представлено в (2);

$IN \rightarrow OUT$ – множина входів відносно оцінювання властивостей гарантій (винесення вердиктів);
 $IN = \{I_R^{in}, I_E^{in}, M_E^{in}, M_{TOE}^{in}\}$ та виходів
 $OUT = \{I^{out}, M^{out}\}$ процесу Z із заданим оператором перетворення $F: IN \rightarrow OUT$.

$Team(B)$ – група експертів B із множини суб'єктів експертизи (оцінювання), які відіграють головну роль, тобто особи, які приймають рішення

$Source$ – множина фінансових, часових, трудових, економічних, матеріальних та інших ресурсів $r = \{r_n \mid n = \overline{1, N}\}$, необхідних для реалізації і виконання процесу Z .

Графічно дана модель може бути представлена наступним чином:

Рис. 1. Графічна інтерпретація моделі процесу оцінювання гарантій ІБ системи ІР-телефонії
Джерело: розроблено авторами.

Вимоги щодо об'єктивності, неупередженості, повторюваності, відтворюваності та співставленості, які висуваються до результатів проведення експертизи залишаються типовими та розглянуті в [14] із застосуванням формалізованого підходу, але умовою повторюваності слід вважати, що два об'єкта оцінювання TOE_1 та TOE_2 ідентичні, якщо виконується умова рівності множин їх складових:

$$\begin{aligned} IF(\{Hw_i \mid i = \overline{1, I}\}_{TOE_1} = \{Hw_i \mid i = \overline{1, I}\}_{TOE_2}, \\ \{HScr_j \mid j = \overline{1, J}\}_{TOE_1} = \{HScr_j \mid j = \overline{1, J}\}_{TOE_2}, \\ \{Sw_y \mid y = \overline{1, Y}\}_{TOE_1} = \{Sw_y \mid y = \overline{1, Y}\}_{TOE_2}, \\ \{D_z \mid z = \overline{1, Z}\}_{TOE_1} = \{D_z \mid z = \overline{1, Z}\}_{TOE_2}) THEN \\ TOE_1 = TOE_2. \end{aligned}$$

Якщо при порівнянні двох об'єктів оцінювання умова рівності не виконується хоча б для однієї пари множин, то об'єкти оцінювання визнаються неідентичними.

І відповідно результати оцінювання гарантій вважаються повторюваними, якщо стосовно системи захищеної ІР-телефонії було проведено дві експертизи (4) та (5)

$$\begin{aligned} Z_{(t_0, t_1)} = \langle Pur(PR_1, V_1), d(A_1), F(TOE_1, E_1, R_1), \\ IN \rightarrow OUT, Team(B_1), Source \rangle, \end{aligned} \quad (4)$$

$$\begin{aligned} Z_{(t_2, t_3)} = \langle Pur(PR_2, V_2), d(A_2), F(TOE_2, E_2, R_2), \\ IN \rightarrow OUT, Team(B_2), Source \rangle \end{aligned} \quad (5)$$

у проміжки часу (t_0, t_1) та (t_2, t_3) відповідно, виконуються умови: ідентичності об'єктів оцінювання $TOE_1 = TOE_2$, ідентичності програм оцінювання $PR_1 = PR_2$, ідентичності методик оцінювання $A_1 = A_2$, ідентичності експертів $B_1 = B_2$, ідентичності сукупності свідочств $E_1 = E_2$, ідентичності рівня зовнішніх та внутрішніх загроз $R_1 = R_2$ та при цьому забезпечується умова ідентичності результатів експертизи $V_1 = V_2$.

Висновки

В роботі запропонована удосконалена формалізована модель оцінки гарантій ІБ системи захищеної ІР-телефонії, яка може застосовуватись для подальших досліджень процесу оцінювання гарантій ІБ складних систем. В рамках представленої моделі приділено увагу питанням визначення рівня реалізації зовнішніх або внутрішніх загроз для систем захищеної ІР-телефонії внаслідок дій порушника з метою здійснення НСД до неї. Також слід зауважити, що суттєвий вплив на оцінку ІБ систем захищеної ІР-телефонії здійснює застосування КЗЗІ.

Список літератури

1. Potii O., Illiashenko O., Komin D. Advanced security assurance case based on ISO/IEC 15408. *Theory and Engineering of Complex Systems and Dependability* : proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, July 3 2015. Brunów, 2015. P. 391–401. https://doi.org/10.1007/978-3-319-19216-1_37.
2. Dotsenko S., Illiashenko O., Kamenskyi S., Kharchenko V. Integrated Model of Knowledge Management for Security of Information Technologies: Standards ISO/IEC 15408 and ISO/IEC 18045. *Information & Security: An International Journal*. 2019. Vol. 43, № 3. С. 305–317. <https://doi.org/10.11610/isij.4323>.
3. Potij A., Romin D., Rebriy I. A Method of Evaluating Assurance Requirements. *Information & Security. Information & Security: An International Journal*. 2012. Vol. 28. No. 1. P. 108–120. <https://doi.org/10.11610/isij.2809>.
4. Ілляшенко О. О. Оцінювання інформаційної безпеки систем на програмованій логіці з використанням кейсів: таксономія, нотація, концепція. *Наука і техніка Повітряних Сил Збройних Сил України*. 2018. № 2(31). С. 97–103. <https://doi.org/10.30748/nitps.2018.31.12>.
5. ДСТУ ISO/IEC 15408-1:2017. Інформаційні технології. Методи захисту. Критерії оцінки. Ч. 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT). [Чинний від 2017-10-01]. Київ, 2017.
6. ДСТУ ISO/IEC 15408-2:2017. Інформаційні технології. Методи захисту. Критерії оцінки. Ч. 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT). [Чинний від 2017-10-01]. Київ, 2017.
7. ДСТУ ISO/IEC 15408-3:2017. Інформаційні технології. Методи захисту. Критерії оцінки. Ч. 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3:2008, IDT). [Чинний від 2017-10-01]. Київ, 2017.
8. ДСТУ ISO/IEC 18045:2015. Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ (ISO/IEC 18045:2008, IDT). [Чинний від 2017-01-01]. Київ : УкрНДНЦ, 2018. 233 с.
9. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах [Чинний від 2011-03-25]. Київ : Адміністрація Державної служби спеціального зв'язку та захисту інформації України, 2011. 104 с.
10. BS EN ISO/IEC 15408-1:2020. Information technology. Security techniques. Evaluation criteria for IT security. Introduction and general model. <https://doi.org/10.3403/30167506>.
11. BS EN ISO/IEC 15408-3:2020. Information technology. Security techniques. Evaluation criteria for IT security. Security assurance components. <https://doi.org/10.3403/30162800>.
12. Prieto-Diaz R. The Common Criteria Evaluation Process. Process Explanation, Shortcomings, and Research Opportunities. Commonwealth Information Security Center Technical Report CISC-TR-2002-03, December 2002 – CISC, James Madison University, USA. 62 p.
13. Потий А. В. Формальная модель процесса защиты информации. *Радиоэлектронні і комп'ютерні системи*. 2006. № 5(17). С. 128–133.
14. Формалізована модель оцінки гарантії інформаційної безпеки комплексної системи захисту інформації / Комін Д. С. та ін. *Системи озброєння і військова техніка*. 2018. № 4(56). С. 92–99. <https://doi.org/10.30748/soivt.2018.56.13>.
15. Ковцур М. М., Никитин В. Н. Математическая модель активного нарушителя для защищенной IP-телефонии. *Актуальные проблемы инфотелекоммуникаций в науке и образовании* : сб. научных статей IV Международной научно-технической и научно-методической конф., 2–4 мар. 2015 г. Санкт-Петербург, 2015. С. 330–335.
16. Мещеряков Р. В. Шелупанов А. А. Комплексное обеспечение информационной безопасности автоматизированных систем : монография. Томск : В-Спектр, 2007. 278 с.
17. Radhika Ranjan Roy. Security Mechanisms in SIP. CRC Press, 2016. 121 p. <https://doi.org/10.1201/9781315367521-19>.
18. Exploiting IP telephony with silence suppression for hidden data transfers / S. Sabine and oth. *Computers & Security*. 2018. Vol. 79. P. 17–32. <https://doi.org/10.1016/j.cose.2018.08.006>.
19. SPIT Detection in Telephony over IP Using K-Means Algorithm / Mourade Azroua, Yousef Farhaouia, Mohammed Ouanaana, Azidine Guezaz. *Procedia Computer Science*. 2019. Vol. 148. P. 542–551. <https://doi.org/10.1016/j.procs.2019.01.027>.
20. Brent Sherman, Mike Borza, Brian Rosenberg, Charles Qi. Security Assurance Guidance for Third-Party IP. *Journal of Hardware and Systems Security*. 2017. Vol. 1. P. 38–55. <https://doi.org/10.1007/s41635-017-0002-5>.
21. Моделювання та аналіз роботи внутрішньої телефонної мережі на базі IP-станції з використанням протоколу SIP / Палагін В. В. та ін. *Вісник Черкаського державного технологічного університету*, 2020. № 2. С. 29–37. <https://doi.org/10.24025/2306-4412.2.2020.198229>.
22. Головка О. О., Новіков В. П. Комплексна система захисту інформації на основі застосування Fuzzy-технологій. *Інформаційна безпека України* : зб. наук. доп. та тез науково-технічної конф. 12-13 бер. 2015 р. Київ : КНУ ім. Тараса Шевченка, 2015. 156 с.
23. Доктрина інформаційної безпеки України : Указ Президента України від 25 лют. 2017 р. № 47/2017. URL: <https://www.president.gov.ua/documents/472017-21374> (дата звернення: 02.06.2021).
24. Salnikova O. F., Sivoha I. M., Ivashchenko A. M. Strategic Communication in the Modern Hybrid Warfare. *Journal of Scientific Papers "Social Development and Security"*. 2019. Vol. 9(5). P. 133–142. <https://doi.org/10.33445/sds.2019.9.5.9>.

Надійшла до редколегії 25.05.2021

Схвалена до друку 13.07.2021

Відомості про авторів:

Чечуй Олександр Вікторович

кандидат технічних наук доцент
доцент Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
<https://orcid.org/0000-0002-7584-4457>

Комін Дмитро Сергійович

кандидат технічних наук
старший викладач Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
<https://orcid.org/0000-0003-4439-346X>

Ревенко Владислав Дмитрович

курсант
Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
<https://orcid.org/0000-0002-6346-5775>

Information about the authors:

Oleksandr Chechui

Candidate of Technical Sciences Associate Professor
Senior Lecturer of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
<https://orcid.org/0000-0002-7584-4457>

Dmytro Komin

Candidate of Technical Sciences
Senior Instructor of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
<https://orcid.org/0000-0003-4439-346X>

Vladislav Revenko

Cadet
of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
<https://orcid.org/0000-0002-6346-5775>

**ФОРМАЛЬНАЯ МОДЕЛЬ ОЦЕНКИ ГАРАНТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ
ЗАЩИЩЕННОЙ IP-ТЕЛЕФОНИИ**

А.В. Чечуй, Д.С. Комин, В.Д. Ревенко

Рассмотрены основные подходы, которые необходимо реализовать в процессе проведения оценки гарантий информационной безопасности систем защищенной IP-телефонии в соответствии с государственными и международными стандартами. Предложено применение усовершенствованной формальной модели процесса оценки требований гарантий информационной безопасности для систем защищенной IP-телефонии с использованием процессного подхода. Такая модель позволяет осуществлять оценивание гарантий информационной безопасности IP-телефонии и определять требования к результатам экспертизы.

Ключевые слова: система защищенной IP-телефонии, процессный подход, информационная безопасность, протоколы безопасности IP-телефонии, формальная модель, экспертиза, эксперт.

**FORMALIZED MODEL OF ASSESSMENT OF INFORMATION SECURITY GUARANTEES
OF THE SECURED IP-TELEPHONY SYSTEMS**

O. Chechui, D. Komin, V. Revenko

In the article, the peculiarities of evaluating information security guarantees for the secured IP-telephony systems in accordance with state and international standards are considered. The application of the improved formalized model of the process which assessing the requirements of guarantees of information security for the secured IP-telephony systems with using a process approach is proposed. The feature of the proposed model is the use of the level of implementation of external and internal threats as an information component of the input stream for assessing the security guarantees of the secured IP-telephony system. In addition, as a component for the material input stream, it is proposed to introduce a set of software and hardware for cryptographic information security and software that provide protection for the IP-telephony system. The using of the proposed model makes it possible to carry out the process of assessing the guarantees of information security of secure IP-telephony systems and to determine the requirements for the results of the examination, regarding impartiality, objectivity, repeatability, reproducibility and comparability. Also, the article proposes the conditions for the identity of objects of assessment, assessment programs and methods, experts, levels of threat implementation, a set of evidence and assessment results, which allows to objectively confirm the fulfillment of the requirements for the examination results of secured IP-telephony systems. These conditions are clear and based on strict definitions of the equality of the corresponding sets, which allows in practice to objectively confirm the fulfillment of the requirements for the examination results.

Keywords: secured IP-telephony system, process approach, information security IP telephony security protocols, formalized model, expertise, expert.