DOI 10.15276/imms.v10.no1-2.68
УДК 004.056:351.861

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 68-74

МЕТОД ВИБОРУ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ

Ю.М. Ткач

Національний університет «Чернігівська політехніка»,
вул. Шевченка, 95, м. Чернігів, 14035, Україна; e-mail: tkach_ym@ukr.net

Запропоновано метод вибору функціонального профілю захищеності. Функціональний профіль захищеності є мінімальним набором необхідних послуг для визначеного рівня та для забезпечення обраного рівня захищеності, але вибір способів їх реалізації залишається за розробником (експертом). За рахунок реалізації обраного функціонального профілю захищеності забезпечується зменшення збитку, який може бути нанесений об'єкту захисту. У статті формалізовано завдання вибору функціонального профілю захищеності. Метод складається з таких кроків: відбір експертів для визначення та оцінки показників відповідних ймовірностей; збір інформації та її обробка; обчислення показника вірогідності появи і-ої загрози; обчислення показника вірогідності відвернення і-ої загрози, обчислення показника вірогідності використання j-ої вразливості v_{ij}; обчислення показника відверненого збитку; оцінка оптимальності функціонального профілю захищеності за умови виконання $S(F_0) = \max_{F \in \bar{F}} S(F)$ при обмеженні $C(F) \le C_r$. Таким чином, метод вибору функціонального профілю захищеності дозволяє здійснити оптимальний вибір при виконанні умови максимізації відверненого збитку та неперевищення допустимих витрат за рахунок ймовірно-вартісної оцінки показників кількості й частоти появи загрози, ймовірних збитків від реалізації визначених загроз й вартості послуги захисту. Розроблений метод може бути використаним при створенні системи захисту інформації в кіберпросторі.

Ключові слова: функціональний профіль захищеності, система захисту інформації.

Постановка проблеми

Створення будь-якої системи захисту інформації (СЗІ) в усіх сферах інформаційної діяльності в державі включає обов'язкову процедуру вибору і подальшу розробку та реалізацію системи функціонування профілю захисту [1]. У завдання розробки системи входить обстеження властивостей конкретного об'єкту захисту (ОЗ) і вибір необхідного функціонального профілю захищеності з приведеного списку ФПЗ. Дана робота присвячена саме проблемі розробці методу вибору оптимального функціонального профілю захищеності об'єкту захисту.

Аналіз останніх досліджень і публікацій

Дослідженню питання розвитку систем захисту інформації, зокрема, розробці теоретичного та методологічного підґрунтя оцінки їх ефективності присвячені роботи як вітчизняних науковців, так і закордонних (Л.М. Артюшин, Д.С.Берестов, В.Ю. Гайкович, О.Г. Корченко, Л.М. Осинский, О.О. Скопа, О.В. Потій, В.О. Хорошко, В.Л. Шевченко, Ю.В. Щеглов, Andrew Blyth, Peter Eden, Gyunyoung Heo, Hanseong Son, Pete Burnap, Rahman Khalilur, Hugh Soulsby, Kristan Stoddart та ін.). Публікації [2-7] підтверджують актуальність наявних загроз в інформаційній сфери, серед яких вже котрий рік поспіль перші позиції займають питання інформаційної безпеки держави.

Мети та завдання статті

Метою статті є підвищення рівня захищеності інформаційної системи як окремого державного органу, так і держави в цілому. Основними завданнями є аналіз процесу вибору функціонування профілю захищеності, віднаходження процедури оптимізації цього вибору.

Виклад основного матеріалу дослідження

Згідно із НД ТЗІ 2.5-005-99 [1] метою введення класифікації АС і стандартних функціональних профілів захищеності є полегшення задачі співставлення вимог до комплексу засобів захисту (КЗЗ) обчислювальної системи автоматизованої системи (АС) з характеристиками самої АС. Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС. Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Загально відомо, що інформація, з точки зору безпеки, характеризується такими властивостями: конфіденційністю, цілісністю і доступністю. При чому, кожний підклас деякого класу складається з певної кількості ієрархічних стандартних функціональних профілів. Ця кількість може бути різною від профілю до профілю. Стандартні функціональні профілі є ієрархічними, оскільки їх реалізація забезпечує наростаючу захищеність. Загрози кіберпростору за впливом на базові характеристики безпеки інформаційних ресурсів (конфіденційність, цілісність, доступність) у відповідності з джерелом [1] поділяють на: К-тип (загроза конфіденційності); Ц-тип (загроза цілісності); Д-тип (загроза доступності); КЦ-тип; КД-тип; ЦД-тип; КЦД-тип.

Природа джерела загроз та стан джерела загроз розділяють на:

- об'єктивна (загроза, виникнення якої не залежить від прямої діяльності людини і пов'язана з різними стихійними природними явищами, такими, як пожежі, блискавки, землетрусу, радіоактивне випромінювання, нападу гризунів і т.п.);
- суб'єктивна (загроза, виникнення якої залежить від діяльності людини).

Суб'єктивну загрозу за мотивом поділяють на активну, таку що пов'язана з діями людини, які направленні на отримання певної вигоди та пасивну, тобто ту, яка виключає вказану складову і пов'язана з помилками людини. Пасивні загрози - це помилки системи (пошкодження окремих компонентів обладнання, тобто апаратного забезпечення підприємства) та катастрофи. Також зазначають, що пасивна загроза - несанкціонований доступ до інформації без зміни стану самої системи, активна - несанкціонована зміна системи, яка вносить певні зміни в стан самої системи [8].

Для прикладу, представимо в таблиці 1 множину профілів та послуг, якими характеризується АС класу 1.

Примітка: 0 – ставився у випадку, якщо певна послуга в профілі взагалі відсутня, 1,2,3 – рівні захисту у відповідному СФПЗ.

З таблиці 1 видно, що до всіх профілів включені послуги НР, НИ,НК, НО, НЦ, НТ, проте відсутні НВ, НА та НП, в сукупності всі вони характеризують у СФПЗ спостереженість. Також жодного разу не зустрічались деякі характеристики і інших властивостей інформації (конфіденційність, цілісність), зокрема, КД, КК, КВ, ЦД, ЦВ.

Зауважимо, що наявність спостереженості у всіх СФПЗ обумовлюється тим, що спостереженість є властивістю системи, яка стосується її керованості, а тому має бути

притаманна всім системам, що реалізуються функції захисту інформації (ЗІ). Аналогічне явище щодо спостереженості присутнє і в СФПЗ АС класу 2 та АС класу 3.

Таблиця 1.

Стандартні функціональні профілі захищеності

Послуги		Типи загроз та рівні захисту																					
		К		Ц		Д				КЦ		КД				ЦД				КЦД			
		1	2	1	2	1	2	3	4	1	2	1	2	3	4	1	2	3	4	1	2	3	4
Конфіденційність	КА	0	1	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	1	1
	КО	0	1	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	1	1
	КК	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Цілісність	ЦА	0	0	0	2	0	0	0	0	0	2	0	0	0	0	1	1	1	1	1	1	1	1
	ЦО	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	1	1
Достовірність	ДР	0	0	0	0	1	2	2	2	0	0	1	2	2	2	1	2	2	2	1	2	2	2
	ДС	0	0	0	0	0	1	2	3	0	0	0	1	2	2	0	1	2	3	0	1	2	3
	ДЗ	0	0	0	0	0	1	2	3	0	0	0	1	2	3	0	1	2	3	0	1	2	3
	ДВ	0	0	0	0	1	2	2	3	0	0	1	2	2	3	1	2	2	3	1	2	2	3

Під час створення нових функціональних профілів необхідно дотримуватись описаних в НД ТЗІ 2.5-004-99 [2] умов для кожної із послуг, що включаються до профілю. Послуги можуть включати декілька рівнів захисту (1 – мінімальний, 2 – базовий, 3 – повний, 4 – абсолютний). Рівні розпочинаються з першого і зростають до рівня *n*, де *n* - визначене для кожного виду послуг число. Чим вище рівень послуги, тим більш складно забезпечується захист від різного типу загроз. Отже, послуга є набором функцій, що дозволяють забезпечити захист від певної сукупності загроз.

Розглянувши загальні питання формування стандартного функціонального профілю захищеності (ФПЗ), перейдемо до його вибору та оптимізації цього рішення.

У НД ТЗІ 2.5-005 -99 налічується 22 послуги, які забезпечують захист від чотирьох основних типів загроз (конфіденційності, цілісності, доступності та їх всі можливі комбінації) [1].

ФПЗ є мінімальним набором необхідних послуг для визначеного рівня та для забезпечення обраного рівня захищеності, але вибір способів їх реалізації залишається за розробником (експертом). За рахунок реалізації обраного ФПЗ забезпечується зменшення збитку, який може бути нанесений ОЗ.

Формалізуємо завдання вибору оптимального ФПЗ. Для цього побудуємо математичну модель ФПЗ.

Нехай $\overline{F}$ множина усіх можливих ФПЗ заданих рівнів, які визначаються вимогами до захищеності інформації, F – вектор розмірності 22 (нормативно

визначена кількість). Компонентами вектора F є булеві змінні $f_i \in \{0,1\}$. Розмірність вектора F введена для зручності і уніфікації опису СФПЗ, оскільки відомо, що до складу багатьох ФПЗ входять не усі послуги. У разі відсутності якої-небудь послуги відповідна компонента дорівнює нулю. $S(F)$ – загальний відвернений збиток.

Тоді, формальна постановка задачі має вигляд:

$$S(F_0) = \max_{F \in \bar{F}} S(F) \tag{1}$$

при обмеженні

$$C(F) \le C_r, \tag{2}$$

де F – деякий вектор, що описує ФПЗ, $\bar{F}$ сукупність усіх допустимих профілів, F_0 – оптимальне значення вектора F, а C_r – допустимі витрати на ФПЗ.

Таким чином, нас перш за все буде цікавити значення F_0, який визначає оптимальний при даній постановці задачі набір послуг, що будуть влючені до ФПЗ.

Відмітимо, що допустима інша постановка задачі, а саме:

$$C(F_0) = \min_{F \in \bar{F}} C(F),$$

$$S(F) \ge F_{kr}.$$

У даному випадку знаходимо F_0, при якому витрати на СФПЗ будуть мінімальними, і при цьому відвернений можливий збиток складатиме не менше F_{kr}.

Припустимо, що може бути реалізований деякий набір вразливостей, внаслідок чого може виникнути ряд загроз t_i, $i = 1,...,n$ $(n = 4)$. При цьому, кожну *i*-у загрозу характеризуватиме ймовірність її появи P_{it}, можливий збиток інформаційного середовища – S_i, тоді P_i - ймовірність відвернення *i*-ої загрози, а відвернений збиток за рахунок запобігання *i*-ої загрози через $r_i = P_i P_{it} S_i$.

Загрози нейтралізуються за рахунок реалізації функціональних послуг, тобто відповідними засобами і механізмами СЗІ. Тоді, P_i – вірогідність нейтралізації кожної *i*-ої загрози, буде основною характеристикою СЗІ. Очевидно, що ймовірність нейтралізації *i*-ої загрози: $P_i = g_i(F) = g_i(f_1, f_2, ..., f_m)$, де $m = 22$.

Позначимо p_{ij} – ймовірність відвернення *i*-ої загрози за рахунок включення до ФПЗ компоненти f_j, $I_i(f_j)$ – індикатор f_j, тобто, випадкова величина, значення якої дорівнює 1, якщо f_j входить до профілю, і дорівнює нулю у протилежному випадку. Уважаючи випадкові величини $I_i(f_j)$ незалежними, маємо:

$$P_i = \sum_{j=1}^{m} p_{ij} I_i(f)_j - \sum_{l<j} p_{ij} p_{il} I_i(f_j) I_i(f)_l + ... + (-1)^{m-1} \prod_{j=1}^{m} p_{ij} I_i(f_j). \tag{3}$$

Ймовірності p_{ij} можна визначити за допомогою експертів. Тоді загальний відвернений збиток виражається співвідношенням:

$$S(F) = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} P_i P_{it} S_i.$$

Таким чином, (3) є явним видом цільової функції $S(F)$ задачі математичного програмування (1)-(2). Однак, функція $S(F)$ нелінійна і визначена на булевій множині, тому проблема пошуку оптимального розв'язку є досить складною.

З метою спрощення задачі розглянемо дещо інший підхід до побудови цільової функції. Цілком природньо серед усіх можливих послуг f_j, які дозволяють усунути *i*-ту загрозу вибрати таку, для якої ймовірність p_{ij} є максимальною, тоді

$$S(F) = \sum_{i=1}^{n} P_{it} S_i \max_{f_i} \{p_{ij} f_j\}.$$

Вірогідність появи *i*-ої загрози P_{it} визначається таким чином. Як було вказано раніше, кожна загроза залежить від вірогідності використання деякої множини вразливостей $V_{ij} = \{v_{ij}, i = 1,...,n\}$, тобто $P_{it} = f_i(v_{ij},...,v_{in})$. Даний показник також можна визначити на основі експертного методу.

Вірогідність використання *j*-ої вразливості v_{ij} можна визначити, за допомогою обчислення відносної частоти їх появи. А саме,

$$v_{ij} = \frac{\lambda_{ij}}{\sum_{k=1}^{n} \lambda_{ik}}$$

де λ_{ij} – частота виникнення *j*-ої вразливості, а *i* - відповідний номер загрози.

Отже, запропоновано метод, який складається з наступних кроків:

- відбір експертів для визначення та оцінки показників відповідних ймовірностей;
- збір інформації та її обробка;
- обчислення показника вірогідності появи *i*-ої загрози;
- обчислення показника вірогідності відвернення *i*-ої загрози,
- обчислення показника вірогідності нейтралізації *i*-ої загрози;
- обчислення показника вірогідності використання *j*-ої вразливості v_{ij};
- обчислення показника відверненого збитку;
- оцінка оптимальності ФПЗ за умови виконання $S(F_0) = \max_{F \in \bar{F}} S(F)$ при обмеженні $C(F) \le C_r$.

Висновки

Розроблений метод може бути використаним для здійснення вибору оптимального функціонального профілю захищеності при створенні системи захисту інформації та передбачає виконання умови максимізації відверненого збитку та не перевищення допустимих витрат.

Список літератури

1. Класифікація автоматизованих систем та стандартні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. URL: http://www.dstszi.gov.ua/ dstszi/doccatalog/ document?id=41648.
2. Берестов Д.С. Гульков М.О., Козачок В.А. Побудова парето-оптимальних функціональних профілів захищеності. *Збірник наукових праць*. 39(1). К.: ЦВСД НУОУ, 2009. С. 89-94. URL: http://www.nbuv.gov.ua/ old_jrn /Soc_Gum/Znpcvsd/2009_1/12.pdf.

3. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. URL: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41649.
4. Лєншин А.В., Буслов П.В. Метод формування функціональних профілів захищеності від несанкціонованого доступу. *Радіоелектрон-ні і комп'ютерні системи : науч. тр.* Харків.: Нац. аэрокосм. ун-т ХАИ, 2010. V.48(7). С.77-81. URL: http://nbuv.gov.ua/UJRN/recs_2010_7_15.
5. Паламарчук Н.А., Хлапонін Ю.І., Овсянніков В.В. Сучасний стан нормативно-правової бази в галузі технічного захисту інформації. *Збірник наукових праць ВІТІ НТУУ "КПІ"*. К.: ВІТІ НТУУ "КПІ", 2011. №3. С.78-82. URL: http://viti.edu.ua/ files/ zbk/ 2011/11_3_2011.pdf.
6. Потій О.В., Лєншин А.В. Методи побудови та верифікації несуперечності і повноти функціональних профілів захищеності від несанкціонованого доступу. *Прикладная радиоэлектроника*. Харків, 2010. 9(3). С.479-488. URL: http://openarchive.nure.ua/handle/document/ 410.
7. Шевченко В.Л., Берестов Д.С. Метод пошуку проектних альтернатив системи захисту інформації. *Сучасний захист інформації* К.: ДУТ, 2015. №3. С.22-27. URL: http://journals.dut.edu.ua/index.php/ dataprotect/ article/viewFile/386/358

МЕТОД ВЫБОРА ФУНКЦИОНАЛЬНОГО ПРОФИЛЯ ЗАЩИЩЕННОСТИ

Ю.Н. Ткач

Национальный университет «Черниговская политехника»,
ул. Шевченко, 95, Чернигов, 14035, Украина; e-mail: tkach_ym@ukr.net

Предложен метод выбора функционального профиля защищенности. Функциональный профиль защищенности является минимальным набором необходимых услуг для определенного уровня и для обеспечения выбранного уровня защищенности, но выбор способов их реализации остается за разработчиком (экспертом). За счет реализации выбранного функционального профиля защищенности обеспечивается уменьшение ущерба, который может быть нанесен объекту защиты. В статье формализована задача выбора функционального профиля защищенности. Метод состоит из следующих шагов: отбор экспертов для определения и оценки показателей соответствующих вероятностей; сбор информации и ее обработка; вычисления показателя вероятности появления i-й угрозы; вычисления показателя достоверности предотвращения i-й угрозы, вычисления показателя достоверности использования j-й уязвимости v_{ij}; вычисления показателя отвлеченного ущерба; оценка оптимальности функционального профиля защищенности при условии выполнения $S(F_0) = \max_{F \in \bar{F}} S(F)$ при ограничении $C(F) \le C_r$. Таким образом, метод выбора функционального профиля защищенности позволяет осуществить оптимальный выбор при выполнении условия максимизации отраженного ущерба и не превышения допустимых расходов за счет вероятно-стоимостной оценки показателей количества и частоты появления угрозы, вероятных убытков от реализации найденных угроз и стоимости услуги защиты. Разработанный метод может быть использован при создании системы защиты информации в киберпространстве.

Ключевые слова: функциональный профиль защищенности, система защиты информации.

METHOD OF SELECTION OF FUNCTIONAL PROTECTION PROFILE

Y.N. Tkach

National University "Chernihiv Polytechnic",
95, Shevchenko St., Chernihiv, 14035, Ukraine; e-mail: tkach_ym@ukr.net

A method for selecting a functional security profile is proposed. The functional security profile is the minimum set of necessary services for a certain level and to ensure the selected level of security, but the choice of ways to implement them remains with the developer (expert). The implementation of the selected functional security profile reduces the damage that may be caused to the object of protection. The article formalizes the task of choosing the Functional Security Profile. The method consists of the following steps: selection of experts to determine and evaluate the indicators of the relevant probabilities; information collection and processing; calculation of the probability of the i-th threat; calculation of the probability of averting the i-th threat, calculating the probability of using the j-th vulnerability v_{ij}; calculation of the averted loss indicator; estimation of the optimality of functional security profile under the condition of $S(F_0) = \max_{F \in \bar{F}} S(F)$ under the restriction of $C(F) \le C_r$. Thus, the method of choosing the functional profile of security allows to make the optimal choice when fulfilling the condition of maximizing the averted damage and not exceeding the allowable costs for account of probabilistic cost estimation of indicators of quantity and frequency of occurrence of threat, probable losses from realization of the defined threats and cost of service of protection. The developed method can be used to create a system of information security in cyberspace.

Keywords: functional security profile, information security system.