УДК 004.896

МОДЕЛЬ ЗНАНЬ ДЛЯ УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Т.О. Коваленко, О.Є. Коваленко
Інститут проблем математичних машин і систем НАН України
e-mail: taraspatriot1991@gmail.com

Управління безпекою є важливою складовою у різних сферах діяльності. Підтримка прийняття рішень у сфері управління безпекою – це специфічна діяльність, пов'язана із багатофакторним аналізом загроз, ризиків і уразливостей в процесі функціонування організації. Такий аналіз проводиться на основі визначення стану безпеки організації та співставлення його з існуючою системою знань в галузі безпеки. Таким чином, управління безпекою потребує підтримки депозитарію знань, зокрема, у вигляді бази знань.

Один із способів використання бази знань в галузі управління безпекою є «підхід заснований на онтології безпеки», який встановлює концептуальні відношення між суб'єктами, які представляють інформацію і мають системний погляд на проблему з метою ідентифікації, аналізу та визначення заходів протидії загрозам безпеки. Багато міжнародних та інших стандартів безпеки і захисту визначають правила для оцінки ризиків і підготовки профілів захисту та цілей безпеки.

Не існує єдиних рекомендацій щодо створення систем безпеки і захисту для підприємств. Кожен випадок унікальний і специфічний. Таким чином, процес створення систем безпеки та захисту для підприємств буде більш ефективним з використанням бази знань. Питання щодо структури бази знань є основним і пов'язане з урахуванням множини різних факторів. Одна з найбільш цитованих праць з онтології безпеки [1], а також робота [2] визначають підхід до управління безпекою орієнтований на діяльність. Системна точка зору на інформаційну безпеку вимагає комплексного обліку різних активів організації та їх атрибутів безпеки. Такий системний підхід може бути реалізований з використанням різних моделей.

Кожен тип організації потребує адекватних способів забезпечення безпеки і захисту. Система ситуаційного управління безпекою або система управління інформаційною безпекою (СУІБ) являє собою особливий тип організації, яка включає в себе систему(и) підтримки прийняття рішень, в якості її складової частини. Існує багато міжнародних стандартів, пов'язаних з розробкою, створенням і впровадження систем управління безпекою. Але всі вони надають лише загальні рекомендації з різних аспектів організації системи безпеки та захисту. Створення робочої системи управління безпекою потребує використання адаптованих до середовища засобів, і, зокрема, бази знань з проблем безпеки.

Загальний підхід до управління безпекою, визначений у стандартах це ризик-орієнтований підхід. Таким чином, основною метою управління безпекою є мінімізація ризиків. Існує багато визначень поняття «ризик». Зокрема, ISO/IEC 27005 визначає ризик як «вплив ненадійності щодо цілей», а примітка 6 до цього визначення говорить «ризик інформаційної безпеки пов'язаний з можливістю того, що загрози будуть використовувати уразливості інформаційного активу або групи інформаційних активів, завдаючи тим самим шкоди організації» [3]. Крім того, в ISO/IEC 27005 констатується, що «уразливості можуть бути пов'язані з властивостями активу, які можуть бути використані в спосіб, або для цілей, відмінних від тих, які були визначені під час придбання або виготовлення активу» [3], або, кажучи простіше, уразливістю є слабкість активу або групи активів, які можуть бути використані одним або декількома загрозами, проте загроза, яка не має відповідної уразливості може не призвести до ризику. І врешті-решт, «оцінка ризику визначає цінність інформаційних активів, ідентифікує відповідні загрози і уразливості, які

існують (або можуть існувати), ідентифікує існуючі елементи управління та їх вплив на ризик ідентифікації, визначає потенційні наслідки і, нарешті, визначає пріоритети отриманих ризиків і класифікує їх відповідно до критеріїв оцінки ризику, встановлених у створенні контексту» [3].

Оцінка ризику є основою для управління безпекою та використанням належного набору моделей безпеки [4]. Інформаційні активи є складовою архітектури інформаційнох системи (ІС). Так, говорячи про інформаційні активи, ми розглядаємо їх як деталізацію архітектури ІС. Фактори ризику, пов'язані з загрозами, уразливостями та архітектурою ІС описують за допомогою моделей. У статистичному сенсі ризик є очікуване значення реалізації загроз, спрямованих на інформаційний актив з використанням уразливості. Математично ризик для ІС описується як очікуване значення функції втрат, пов’язаної з втратою інформації активу. Таким чином, для визначення функції втрат ми повинні визначити вплив реалізації загрози через уразливість, пов'язану з інформацією активу.

Існуючі методи аналізу ризиків ґрунтуються на *кількісних, якісних* і *гібридних* (напівкількісних) парадигмах [5] та використовують підхід, заснований на моделі використання. Існує багато моделей для кожного компонента залежностей ризику і організації безпеки. Система управління інформаційною безпекою (СУІБ) базується на збалансованому обліку ризиків та використанні належних заходів контролю для досягнення цілей діяльності. Отже, аналіз і прийняття рішень в питаннях побудови СУІБ є складною, орієнтованою на знання, проблемою та потребує використання бази знань про різні компоненти інформаційної безпеки. Знання про кожний компонент СУІБ засновані на їх систематиці. Розглянемо ці компоненти і систематику.

Активи і уразливості. Відповідно до ISO/IEC 27005 [3] уразливості пов'язані з властивостями активу і можуть бути класифіковані відповідно до *типу активів*, пов'язаних з:

- організацією;
- процесами і процедурами;
- процедурами управління;
- персоналом;
- фізичним середовищем;
- конфігурацією інформаційної системи;
- обладнанням, програмним забезпеченням або обладнанням зв'язку;
- залежністю від зовнішніх сторін.

Загрози. Одна з найбільш повних систематик загроз наведена в таксономії загроз ENISA [6]. Зазначена таксономія ґрунтується на типах загроз, таких як:

- юридична;
- шкідлива діяльність/зловживання;
- підслуховування/перехоплення/викрадення;
- відключення (збої живлення);
- фізичні атаки;
- ненавмисні (випадкові) ушкодження;
- стихійні лиха;
- пошкодження/втрата ІТ активів;
- технічні збої/несправності.

Ризик. Оцінка ризиків інформаційної безпеки (ISRA) є важливою складовою системи управління інформаційною безпекою (СУІБ). Таксономія оцінки ризиків може бути заснована на різних підходах. Зокрема, одна з останніх таксономій [5] заснована на чотирьох підходах:

- визначенні вартості;
- перспективі;

- оцінці ресурсів;
- вимірюванні ризику.

Сучасна редакція стандарту управління безпекою ISO 27001: 2013 (на відміну від попередньої його редакції ISO 27001:2005, що орієнтувалась на цикл Plan-Do-Check-Act, PDCA) орієнтована на організаційний контекст інформаційної безпеки з відповідним підходом до оцінки ризиків.

Інтегроване представлення набору організаційних активів, схильних до ризиків, засноване на використанні фундаментальної моделі *архітектури організації*, яка забезпечує формальний і структурований спосіб розгляду і опису організації. Ця фундаментальна структура представлена онтологією підприємства. Однією з найбільш повних онтологій підприємства є модель Захмана (ZF) [7], яка може бути представлена у вигляді матриці:

$$Z_F=A\times P,$$

де A – це категорія активів з питальною характеристикою; P – це точка зору на перспективу опису різних аспектів діяльності організації та її існування. Оскільки ZF є онтологією підприємства, то для прийняття цієї моделі для конкретного використання, ми повинні визначити конкретну семантику абстрактних компонентів онтологій:

$$O=\langle C, T, I, R, F, D, S, A, E\rangle,$$

де C – класи, тобто набори, колекції, поняття, типи об'єктів, або види речей;

T – атрибути, тобто аспекти, властивості, особливості, характеристики або параметри, які об'єкти (і класи) можуть мати;

I – екземпляри або об'єкти (основні або «рівня землі» об'єктів);

R – відношення, тобто способи, в які класи і окремі екземпляри можуть бути пов'язані між собою;

F – функціональні терміни, тобто складні структури, утворені з певних взаємозв’язків, і які можуть бути використані замість окремого терміну у формулі (твердженні);

E – обмеження, тобто формально сформульований опис того, що повинно бути істинним, для того, щоб певне твердження було прийняте в якості вхідних даних;

S – правила, тобто казуальні (причинно-наслідкові) твердження у формі речення/пропозиції/фрази, які описують логічні висновки, які можна зробити з твердження в тій чи іншій формі;

A – аксіоми, тобто твердження (включаючи правила) в логічній формі, які в сукупності складають загальну теорію, яку онтологія описує в своїй галузі застосування;

E – події, тобто поточна зміна атрибутів або взаємозв’язків.

Онтологія домену для управління безпекою організації включає в себе основні категорії активів, які визначені у архітектурі підприємства та ризиків, пов'язаних з ними. Загалом активи – це "ресурс з економічною цінністю, яким фізична особа, корпорація або країна володіє або контролює із очікуванням того, що він принесе економічну вигоди в майбутньому» [8].

Отже, організаційно-орієнтований підхід до управління безпекою ґрунтується на моделі організації. Різні типи організацій мають різні конкретні класи атрибутів, які описують свої специфічні особливості. Наприклад, у роботі [9] була запропонована формальна організаційна модель для одного типу організацій, відомої як система ситуаційного управління (ССУ). Згідно [9] формальна модель діяльності ССУ заснована на визначенні категорій моделі ССУ M_K, параметрів організаційної моделі M_O, архітектурної моделі M_A, моделі обробки (функціональної моделі) M_F, логічної моделі (в тому числі моделі умов) M_L:

$$W=\langle M_K; M_O; M_A; M_F; M_L\rangle. \quad (1)$$

Відповідно до (1) загальна (інтегрована) модель ризиків такої організації буде мати наступний вигляд:

$$R_W=\langle R_K; R_O; R_A; R_F; R_L\rangle.$$

де R_K – ризики для конкретної категорії ССУ; R_O – ризики для організаційних компонентів ССУ; R_A – ризики для архітектурних компонентів ССУ; R_F – ризики функціонування ССУ; R_L - ризики правильності (достовірності) логічних тверджень для висновків/підсумків в ССУ.

Подальші дослідження щодо створення моделі знань для систем управління інформаційною безпекою можна розвивати у напрямку конкретизації функцій інтерпретації функціональних компонентів безпеки та уточненню і розширенню означень окремих понять (концепцій) моделі знань. Також можливе створення адаптованої онтології для управління безпекою систем ситуаційного управління.

Висновки

Запропонована модель для управління безпекою інформаційної системи включає в себе набір понять, які відображають об'єднання складових частин управління безпекою: інтегровану модель ризиків; інтегровану модель процесу забезпечення безпеки; інтегровані функціональні компоненти безпеки. Взаємозв’язок між поняттями і категоріями бази знань визначають зміст (семантику) управління безпекою та функцій, які визначають правила інтерпретації суперпозиції різних складових моделей.

Розробка моделей знань для управління безпекою інформаційних систем пов'язана з підтримкою діяльності цих систем у відповідності до їх призначення. Ці моделі в сукупності описують аспекти діяльності щодо управління безпекою. Зокрема, були розглянуті ключові компоненти моделі ризиків системи ситуаційного управління.

Література

1. Fenz, S., Ekelhart, A. (2009, March). Formalizing information security knowledge. In Proceedings of the 4th international Symposium on information, Computer, and Communications Security, pp. 183-194. ACM.

2. Fenz, S., Fenz, S., Plieschnegger, S., Plieschnegger, S., Hobel, H., & Hobel, H. (2016). Mapping information security standard ISO 27002 to an ontological structure. Information & Computer Security, 24(5), 452-473.

3. ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management. URL:https://www.iso.org/standard/56742.html

4. Taubenberger, S., & Jürjens, J. (2008, September). IT Security Risk Analysis Based on Business Process Models Enhanced with Security Requirements. In: Modeling Security Workshop, Toulouse, France.

5. Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14-30.

6. ENISA Threat Taxonomy Initial Version 1.0 January 2016. URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

7. The Concise Definition of The Zachman Framework by: John A. Zachman. URL: https://www.zachman.com/about-the-zachman-framework.

8. Asset (definition). URL: http://www.investopedia.com/terms/a/asset.asp

9. Kovalenko Oleksii E. (2015) The Formalization of Organizational Support Creation for Systems of Situational Management // Proceedings of 5th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE–2015),), November 13-14th, 2015. – University of National and World Economy (UNWE), Sofia, Bulgaria. – Issued for Publication: August 15th 2016 – P.292-301.