Грищук В. В., д-р техн. наук, проф.,
начальник кафедри захисту інформації та кібербезпеки,
Савчук В. С., науковий співробітник,
Бондарчук А. А., науковий співробітник
Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКА ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕЦІ

Загроза кібербезпеці є ймовірною можливістю перешкоди цілям та завданням суб'єкту господарювання критичних інфраструктур та її складовим. Ризик загрози вимірює та оцінює цю загрозу, дає уявлення щодо математичного виразу ймовірності настання таких перешкод, тобто оцінка ризику є ступенем загрози.

На даний час розроблено безліч нормативно-правових документів та стандартів, що визначають перелік основних загроз в сфері інформаційної та кібер-нетичної безпеки та правила їх визначення для організацій, основними з яких є "Керівництво з управління ризиками в інформаційних технологіях" NIST 800-30 [1]; стандарти ISO/IEC 27002 та ISO/IEC 31000 [2]; Тому методологія оцінки ризиків може бути покладена в основу підходу до визначення тих факторів, що впливають на виникнення гібридних загроз з урахуванням особливостей організації для якої визначуються типові гібридні загрози. Основною особливістю теперішнього часу є поєднання технологічної та соціальної компоненти, що призводить до виникнення гібридних кіберзагроз.

Проблема з багатьма з цих методологій полягає в тому, що вони концентруються в основному на загальних принципах і керівних принципах для профільних задач, залишаючи користувачів без адекватних деталей для реалізації оцінки ризиків [3]. Навіть промислові стандарти, такі як COBIT (контрольні цілі для інформації і суміжних технологій) [4] і ISO/IEC 27002 [2], не забезпечують чіткими алгоритмами оцінки ризиків і залишають не врахованим спектр факторів що впливають на інформаційну безпеку з боку соціально-технічної компоненти [5]. Виділяють два основні внутрішні фактори, що впливають на появу загрози: наявність активів чи процесів які цікавлять зловмисника та можуть стати об'єктом загроз; уразливості інформаційної системи для яких характерна соціо-технічна складова. Окрім цього важливо враховувати і зовнішні фактори, що в більшості впливають на соціальну компоненту ризику загрози.

Запропоновано наступний комплексний метод формалізації ризиків кібер-безпеці, що в загальному вигляді включає наступні кроки:

1. Інтегроване представлення набору активів, схильних до ризиків. Таке представлення засноване на використанні фундаментальної моделі архітектури організації. Вона може бути представлена онтологією підприємства, зокрема моделлю Захмана (ZF) [6], яка може бути подана у вигляді матриці:

$$ZF = A \times P \tag{1}$$

де A – це категорія активів; P – це точка зору на перспективу опису різних аспектів діяльності організації та її існування (актив, процес, бізнес-процес).

2. Визначення уразливостей інформаційних систем з урахуванням особливостей діяльності організації. Відповідно до ISO/IEC 27005 [2] уразливості пов'язані з властивостями активу і можуть бути класифіковані відповідно до типу активів.

3. Оцінювання активу, послуги чи бізнес-процесу та уразливостей – відок-ремлення критичних і некритичних ресурсів, розглядають функціональні за-лежності між рівнями, щоб з'ясувати, який ресурс відіграє критичну роль в організації. Оцінка ризику за категоріями активів R_A може визначатись за виразом:

$$R_A = K_A * V_A \tag{2}$$

де K_A - кількість активів в категорії A, V_A - вартість активів категорії A.

Кількісний показник ризику за уразливостями $R_{ур}$ визначається за виразом:

$$R_{ур} = K_{ур} * K_A + V + T \tag{3}$$

де $K_{ур.}$ – кількість уразливостей за типом активів, V – вартість обладнання чи програмного забезпечення, що виведена зі строю за рахунок реалізації заг-рози, T – час простою інформаційної системи.

4. Виділення меж поширення ризику, тобто визначення чи поширеться загроза на інші ресурси та оцінювання їх за кроком 2 [7].

5. Визначення зовнішніх факторів відповідно до особливостей діяльності та структури організації та інформаційних систем, що в них циркулюють.

Список використаних джерел

1. NIST, "NIST SP - 800-30rev1," 2012. [Online]. Available: http://www.nist.gov/customcf/get pdf.cfm?pub id=912091. [Accessed March 2014].

2. International Organization for Standardization, ISO/IEC 27005:2011. Information security risk management.

3. A. Shameli-Sendi, M. Jabbarifar, M. Shajari, and M. Dagenais, "FEMRA: Fuzzy Expert Model for Risk Assessment," in the Fifth International Conference on Internet Monitoring and Protection (ICIMP), pp. 48-53, 2010.

4. ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012.

5. A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security Ontologies: Improving Quantitative Risk Analysis," in The 40th Hawaii International Conference on System Sciences, Hawaii, 2007.

6. X. Su, D. Bolzoni, P. van Eck, and R. Wieringa, "A Business Goal Driven Approach for Understanding and Specifying Information Security Requirements," arXiv preprint cs/0603129, 2006

7. B. Mahmoud, N. Larrieu, and A. Pirovano, "A Risk Propagation Based Quantitative Assessment Methodology for Network Security-Aeronautical Network Case Study," In IEEE Conference on Network and Information Systems Security (SAR-SSI), pp. 1-9, 2011.