УДК 004.855

Л.В. Загоруйко, Т.А. Мартьянова, А.В.Скирда

МОДЕЛІ АНАЛІЗУ РИЗИКУ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Донецький національний університет ім.Василя Стуса, м. Вінниця, Україна

Анотація. На основі аналізу стандартів з інформаційної безпеки визначено основні елементи ризиків, що описують інформаційну структуру та визначають вплив на функціонування інформаційних систем, розглянуто методологічну основу моделювання аналізу ризиків інформаційних технологій, запропонований найбільш ефективний метод для практичного застосування моделі аналізу ризику в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих чинників та спеціалізований програмний засіб для його реалізації.
Ключові слова: ризики безпеки, модель аналізу ризиків, інформаційні технології.

Аннотация. На основе анализа стандартов информационной безопасности определены основные элементы рисков, описывающие информационную структуру и определяющие воздействие на функционирование информационных систем, рассмотрено методологическую основу моделирования анализа рисков информационных технологий, предложен наиболее эффективный метод для практического использования модели в условиях неопределенности, конфликтности и нечеткой оценки влияния отдельных факторов и специализированное программное обеспечение для его реализации.
Ключевые слова: риски безопасности, модель анализа рисков, информационные технологии.

Abstract: Based on the analysis of information security standards, the subject area is determined, which consists of the main elements of risks that describe the information structure and determine the impact on the functioning of information systems, the methodological basis for modeling the analysis of information technology risks is considered, the most effective method for the practical use of the model in conditions of uncertainty is proposed, conflict and fuzzy assessment of the influence of individual factors and specialized software for its implementation.
Keywords: security risks, risk analysis model, information technology.
DOI: 10.31649/1681-7893-2020-40-2-16-20

Вступ

У сучасних реаліях будь-яке підприємство або організація не може існувати окремо від інформаційних технологій (ІТ). Широко використовують ІТ для пересилання електронних повідомлень, пошуку нових клієнтів і партнерів в мережі Інтернет, використовують месенджери та соціальні мережі для спілкування і, що найважливіше, активно використовують клієнт-банкінг для проведення фінансових операцій та програм бухгалтерського обліку і звітності. Вочевидь, що таке стрімке інтегрування ІТ в бізнес передбачає підвищення рівня існуючих інформаційних загроз та виникнення нових (щодня з'являється близько 200 тисяч нових зразків шкідливого коду, які можуть використовуватись проти будь-якої інформаційної системи).

Сучасні методи та моделі аналізу ризиків мають ряд недоліків, серед яких виділяють: по-перше, значна кількість методів передбачає залучення великої кількості експертів у різноманітних галузях; по-друге, значна кількість методів не передбачає структурування об’єктів та процесів порушення безпеки, або цей процес слабо формалізований; по-третє, більшість методів потребує знань про всі процеси, які відбуваються в системі, та точні кількісні характеристики цих процесів.

У відповідності до зазначених проблем, актуальним завданням стала розробка таких моделей та методів аналізу ризиків, перевагою яких є:

а) мінімізація кількості експертів за рахунок автоматизації етапів аналізу ризиків;

б) використання моделей, які дозволяють здійснювати етапи оцінки рівня ризиків в умовах невизначеності.

Аналіз стандартів з інформаційної безпеки [2-5] дозволяє виявити основні елементи ризиків, які описуються інформаційною структурою та визначають вплив на діяльність інформаційних систем.

Під ризиком, в загальному розумінні цього слова, розуміють можливість або ймовірність настання подій з негативними або позитивними наслідками в результаті певних рішень або дій [6].

Оцінка ризику розглядається як процес ідентифікації інформаційних ресурсів системи і загроз цих ресурсів, а також можливих втрат, заснований на оцінці частоти виникнення подій і розмір збитку.

Кількісна оцінка ризику інформаційної безпеки відкриває можливість більш оптимально розподіляти існуючи обмежені ресурси запобігання виникненню ризикових ситуацій та планувати подальші заходи їх запобігання. Процес оцінки повинен бути адаптований до індивідуальних особливостей організації, але в той же час узгоджений з кращими стандартами та провідними практиками.

Після проведення оцінки ризику, необхідно прийняти рішення: прийняти ризик, знизити ризик або перенести ризик.

В загальному випадку, предметна область оцінки ризиків безпеки інформаційних систем може бути представлена діаграмою класів в нотації *Unified Modeling Language* (*UML*), як показано на рис. 1:

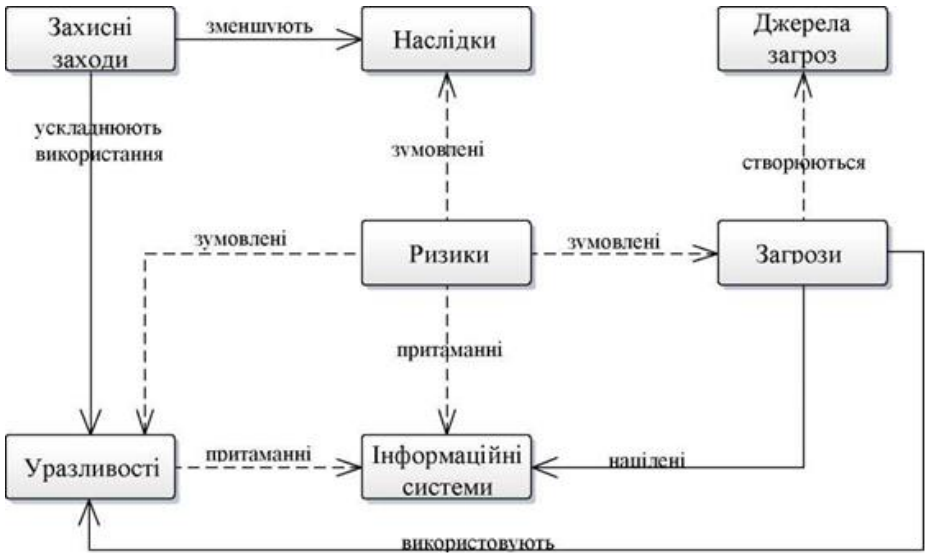

Рисунок 1. - Предметна область оцінки ризиків безпеки.

Під ризиком розуміється ризик інформаційної безпеки, що представляє собою комбінацію ймовірності виникнення ризикової події (наприклад, реалізації загрози) і завдання при цьому шкоди.

Ризики, як правило, пов'язують з активами, під якими розуміється «що небудь, що має цінність для організації і, отже, потребує захисту». В ISO/IEC 27005:2011 активи поділяються на первинні та вторинні. До первинних активів відносять інформацію і бізнес-процеси, а до вторинних - технічні засоби, програмне забезпечення, мережа, персонал, місця функціонування і організаційну структуру.

Методологічна основа моделювання аналізу ризиків

Суворої класифікації для методів аналізу ризиків не існує, однак існують відмінності в підходах до аналізу ризиків, способах подання елементів ризику, функціональних можливостях та ін. На основі таких відмінностей можна виділити три основні групи - графічні, математичні та лінгвістичні методи.

Графічні методи - методи, які передбачають візуалізацію об'єктів аналізу і процесів взаємодії між ними. При цьому будуються графи, дерева або діаграми, що дозволяють різним способом відображати інформацію про досліджувані об'єкти. У більшості випадків ці методи дозволяють здійснити лише ідентифікацію елементів ризику і способи взаємодії між ними.

Математичні методи - методи, які передбачають визначення властивостей об'єктів і їх взаємодії за допомогою деяких формальних мов опису, що визначають закони функціонування, зміни властивостей і ін. Дані методи дозволяють не тільки ідентифікувати елементи, але і аналізувати їх поведінку, зміну їх властивостей і вплив на інші елементи.

Лінгвістичні методи є найбільш популярними і простими у використанні, проте не завжди здатні привести до адекватної оцінки ситуації. Дані методи не передбачають будь-яких інструментальних засобів і програм, і вимагають лише наявності команди осіб, відповідальних за аналіз ризику. При цьому всі етапи оцінки ризику, на скільки це можливо, припускають тільки усне спілкування між групою осіб, в ході якого ідентифікуються елементи ризику, будуються припущення про їх поведінку і здійснюється приблизна оцінка можливостей і збитків.

Методи експертних оцінок є комплексом логічних і математико- статистичних методів і процедур по обробці результатів опитування групи експертів, причому результати опиту є єдиним джерелом інформації. В цьому випадку виникає можливість використання інтуїції, життєвого і професійного досвіду учасників опитування [21].

Методи експертної оцінки ризику історично виникли першими. Вони мають ту істотну перевагу над іншими методами, що експертна оцінка може використовуватися в умовах дефіциту і навіть браку інформації. Головна умова досконалої експертної оцінки - виключення взаємного впливу експертів один на одного (так звана дельфійська процедура). Легкість експертної оцінки і недостатність інформації про оцінювані процеси сприяли появі в Україні величезної кількості фахівців і спеціалізованих видань, які пропонують розроблені ними прогнози. Далеко не завжди це робиться на достатньо професійному рівні. Проблема, яка виникає при цьому, полягає в тому, що в результаті прийняття рішення ймовірність правильної оцінки знижується. Парадоксальність цього явища випливає з самого процесу обговорення. У переважній більшості випадків погляд експертів-аналітиків відрізняється від погляду практиків. Ця розбіжність може бути формалізована через так званий коефіцієнт розбіжності. Задавши цьому коефіцієнту декілька практичних значень, можна одержати ряд можливих ймовірностей розробки точної оцінки.

На сьогодні існують різні підходи і методи оцінки ризиків, запропоновані різними виробниками. Так методика «*Facilitated Risk Analysis Process* (*FRAP*)» [7], запропонована компанією *Peltier and Associates*, дозволяє компаніям віднайти баланс між витратами на засоби захисту й отримуваним ефектом. Оцінка визначається за правилами, що задаються матрицею ризиків, яка виділяє чотири рівні ризиків: рівень А - дії, пов'язані з ризиком, повинні бути виконані обов'язково й негайно, рівень В - пов'язані з ризиком дії повинні бути виконані, рівень С - попередження, що потрібен моніторинг ситуації, рівень D, який визначає, що ніяких дій на цей час здійснювати не потрібно.

Компанія *RiskWatch* [8] розробила однойменну методику аналізу ризиків для проведення різних видів аудиту безпеки, в якому як критерії для оцінки і управління ризиками використовуються очікувані річні втрати і оцінка повернення інвестицій. *RiskWatch* орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки і витрат на створення системи захисту. На виході отримується деяке значення оцінки очікуваних втрат для одного конкретного активу від реалізації однієї загрози Коли всі активи і дії ідентифіковані і зібрані разом, то з'являється можливість оцінити загальний ризик інформаційної системи як суму всіх окремих значень.

В основу методу *CRAMM* [9] покладено комплексний підхід до оцінки ризиків, що поєднує кількісні і якісні методи аналізу і проводиться у три стадії. Для кожного інформаційного процесу будується дерево зв'язків використовуваних ресурсів. Побудована модель дозволяє виділити критичні елементи. Цінність фізичних ресурсів в CRAMM визначається вартістю їх відновлення в разі руйнування, дається оцінка збитків за шкалою зі значеннями від 1 до 10.

Методологія *OCTAVE* (*Operationally Critical Threat, Asset and Vulnerability Evaluation*) [10] була розроблена в Інституті програмної інженерії при Університеті Карнегі-Меллона (*Carnegie Mellon University*) і передбачає активне залучення власників інформації в процес визначення критичних інформаційних активів і асоційованих з ними ризиків.

Методологія *CORAS* [11] розроблена в рамках програми *Information Society Technologies*. Її суть полягає в адаптації, уточненні і комбінуванні таких методів проведення аналізу ризиків, як *Event-Tree-Analysis*, ланцюги Маркова, *HazOp* і *FMECA*. *CORAS* використовує технологію *UML* і базується на *AS/NZS* 4360:1999 та *ISO/IEC* 17799-1:2000 .

Модель оцінки ризиків інформаційної безпеки на основі нечітких множин будується з використанням нечітких когнітивних карт (НКК) [12]. Нечіткі когнітивні карти представляють собою простий граф з вузлів і зважених дуг, де вузли - концепти предметної області (наприклад: безліч порушників, безліч способів подолання системи захисту), а дуги причинно-наслідкові зв'язки між ними (наприклад: ймовірність наявності певного виду порушників, ймовірність реалізації атаки і ін.).

Вибір ефективного методу для побудови моделі

В основу оцінки ризику вигідно застосувати метод факторного аналізу, який є найбільш адекватним в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих чинників, та дозволяє поєднати якісну і кількісну складові аналізу.

Для забезпечення правдоподібності побудованої моделі та її використанні на практиці, модель повинна відповідати ряду вимог. Так, модель аналізу (оцінювання) ризиків інформаційних технологій має відповідати таким вимогам:

-модель має бути узгодженою відносно досліджуваного процесу та давати результати, наближені до реальних;

-давати характеристику сучасного стану безпеки застосування інформаційних технологій підприємством;

-повинна надавати кількісну і якісну оцінку ризиків;

-має дозволяти виділити найбільш небезпечні фактори ризику і їх ймовірність настання;

-давати можливість використання даної моделі для прийняття управлінських рішень в галузі інформаційної безпеки.

Вибір програмного забезпечення

Для виконання моделювання інформаційних ризиків використовують спеціалізоване програмне забезпечення спрямоване на створення моделі системи та визначення вразливих місць. На практиці найбільш прийнятним є використання пакету аналізу даних *STATISTICA*. Програма *STATISTICA* містить вичерпний набір аналітичних процедур в галузі вивчення бізнесу, здобуття даних, науки і промислового виробництва. Вона дозволяє будувати різні графіки, ефективно керувати даними і розробляти власне програмне забезпечення. *STATISTICA* не тільки включає в себе універсальні статистичні, графічні процедури та засоби керування даними, але також реалізує спеціалізовані методи аналізу даних. Всі аналітичні інструменти *STATISTICA* доступні як окремі компоненти єдиного інтегрованого пакета. Розробником пакету є фірма *StatSoft, Inc* (США). *STATISTICA* дозволяє проводити різні процедури (модулі) обробки статистичних даних (в термінології програми – аналізи): розрахунок описових статистик, аналіз динамічних рядів й прогнозування, аналіз множинної регресії, дискримінантний аналіз, аналіз відповідності, кластерний аналіз, факторний аналіз.

Висновок

Для розробки ефективної та практичної математичної моделі аналізу ризиків інформаційних технологій необхідно здійснення наступних складових:

- огляд та аналіз існуючих підходів до моделювання оцінювання ризиків та вибір оптимального;
- формування вимог до моделі та визначення ознакового простору моделі;
- використання в процесі розробки математичної моделі сучасного програмного забезпечення.

В більшості випадків для оцінки ризику безпеки інформаційних технологій доцільно використання методу факторного аналізу, який є найбільш узгодженим в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих чинників, та дозволяє поєднати якісну і кількісну складові аналізу. Запропонований факторний підхід є універсальним і може бути використаний для оцінювання ризику на різних стадіях розвитку підприємства та етапах вибору й обґрунтування напрямів мінімізації ризиків інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стрічка новин урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, яка функціонує в рамках Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Офіційний сайт.

URL: https://cert.gov.ua

2. Національний стандарт України ДСТУ ISO/IEC 27001:2015 «Методи захисту системи управління інформаційною безпекою» / Офіційне видання. Київ. ДП «УкрНДНЦ». 2016 – с. 22.

3. Національний стандарт України ДСТУ ISO/IEC 27002:2005 «Звід правил для управління інформаційною безпекою» / Офіційне видання. Київ. НБУ. 2010 – с. 149.

4. Міжнародний стандарт ISO/IEC 27005:2011 «Менеджмент ризиків інформаційної безпеки» / Технический перевод v.1 от 11.02.2012.- с. 94.

5. Національний стандарт України ДСТУ IEC/ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» / Офіційне видання. Київ. Мінекономрозвитку України. 2015 – с. 73.

6. Кучер, В.А. Использование методов теории вероятностей и математической статистики для оценки вероятностей обнаружения уязвимостей в информационных автоматизированных системах [Текст] / В.А. Кучер, В.С. Агранович // Информационное противодействие угрозам терроризма. – 2015. – №5. – С. 187-191.

7. К.Коротнев. Методики управления рисками информационной безопасности и их оценки (часть 2) [Електронний ресурс]

URL: https://safe-surf.ru/specialists/article/5194/587935/

8. Современные методы и средства анализа и управление рисками информационных систем компаний [Електронний ресурс]

URL: http://citforum.ru/products/dsec/cramm/cramm1.shtml#:~:text=RiskWatch%

9. Управление рисками. Метод CRAMM / ITEMS – IT Expert Management School [Електронний ресурс]

URL: https://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf

10. П.Пастоев. Методологии управления ИТ-рисками [Електроний ресурс]

URL: https://www.osp.ru/os/2006/08/3584582

11. Dahl Heidi E. I. Structured semantics forthe CORAS security risk modelling language. /Heidi E. I. Dahl, Ida Hogganvik, Ketil Stolen //Technical Report A970, SINTEF ICT, 2007.

12. Корниенко М.А. Модель оценки рисков информационной безопасности на основе теории нечетких множеств / М.А. Корниенко, Е.А. Островерхова // Материалы XVIII международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». Т. 4 – Харків: ХНУРЭ, 2014. – 279 с.

13. Фетісов В.С. Пакет статистичного аналізу даних STATISTICA: навч. посіб. – Ніжин : НДУ ім. М. Гоголя, 2018. – 114 с.

Загоруйко Любов Василівна – к.т.н., доцент кафедри радіофізики та кібербезпеки Донецького національного університету імені Василя Стуса, м. Вінниця, Україна

Мартьянова Тетяна Андріївна - кандидат технічних наук, старший викладач кафедри інформаційних технологій, Донецького національного університету імені Василя Стуса, м. Вінниця, Україна

Скирда А.В.