Список використаної літератури

1. Кавя’рня як різновид спеціалізованих закладів ресторанного господарства [Електроний ресурс]. – 2018. Режим доступу до ресурсу: http://ujae.org.ua/kav-yarnya-yak-riznovyd-spetsializovanyh-zakladiv-restorannogo-gospodarstva/
2. Хмарна система jSolution [Електроний ресурс] – Режим доступу до ресурсу: https://jsolutions.ua/ua/sistema-upravleniya-restoranom%203
3. Програма для обліку в пекарні [Електроний ресурс] – Режим доступу до ресурсу: https://skyservice.pro/uk/automation/bakery/
4. Автоматизація кав’ярні Poster [Електроний ресурс] – 2017. Режим доступу до ресурсу: https://joinposter.com/business/coffeeshop

УДК 004.056.5:004.7

Скирда А.В., *студент 4 курсу спеціальності 125 «Кіберзахист»*
Загоруйко Л.В., *к.т.н., доцент кафедри радіофізики та кібербезпеки,*
Мартьянова Т.А., *старший викладач кафедри комп`ютерних наук та інформаційних технологій*

МОДЕЛІ АНАЛІЗУ РИЗИКУ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Донецький національний університет імені Василя Стуса, м. Вінниця

Актуальність 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. Підтвердженням такого ствердження є статистика, що щодня з'являється близько 200 тисяч нових зразків шкідливого коду [1], які можуть використовуватись проти будь-якої інформаційної системи або технології.

Аналіз наукових робіт та досліджень. Сучасним методам та методикам оцінки ризиків інформаційної безпеки та їх моделюванню присвячені окремі роботи вітчизняних та зарубіжних науковців, серед яких: Архипов А.Е., Война О.А., Домарев В.В. Кучер В.А., Коротнев К.К., Корниенко М.А., Авраменко В.С. та інші. Не зважаючи на велику кількість фундаментальних та прикладних робіт можна побачити, що більшість сучасних методів та моделей аналізу ризиків мають ряд суттєвих 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, **метою роботи** є вибір такої моделі та методу аналізу ризиків, перевагою яких буде: мінімізація кількості експертів за рахунок автоматизації етапів аналізу ризиків; можливість оцінки та аналізу в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих чинників (в інтерпретації термінології теорії прийняття рішень); наявність програмного забезпечення, спрямованого на створення моделі та визначення вразливих місць.

Онтологічна модель аналізу ризиків безпеки

Аналіз національних стандартів ДСТУ ISO/IEC 27001:2015, ДСТУ ISO/IEC 27002:2005, ДСТУ ISO/IEC 27005:2015, ДСТУ ISO/IEC 31010:2013 дозволяє виявити основні елементи ризиків, які описуються інформаційною структурою та визначають вплив на діяльність інформаційних систем та технологій. Під ризиком, в загальному розумінні цього слова, розуміють можливість або ймовірність настання подій з негативними або позитивними наслідками в результаті певних рішень або дій [2]. Також під ризиком розуміється ризик інформаційної безпеки, що представляє собою комбінацію ймовірності виникнення події та її наслідку. При цьому «подія» - це реалізація загрози, а «наслідок» - завдана при цьому шкода. Ризики, як правило, пов'язують з активами, під якими (згідно ДСТУ ISO/IEC 13335-1) розуміється «що небудь, що має цінність для організації і, отже, потребує захисту». Стандартами з інформаційної безпеки аналіз, оцінка та оцінювання ризику розглядається як процеси ідентифікації інформаційних ресурсів системи (або технології), уразливості цих ресурсів, загроз та їх джерел, а також можливих наслідків (втрат), заснований на оцінці частоти виникнення подій і розмірів збитку.

Модель аналізу ризиків безпеки інформаційних технологій зручно сприймати у вигляді спрощеного варіанту онтологічної моделі, що містилась в першій версії стандарту BS 7799-3 (рис. 1):

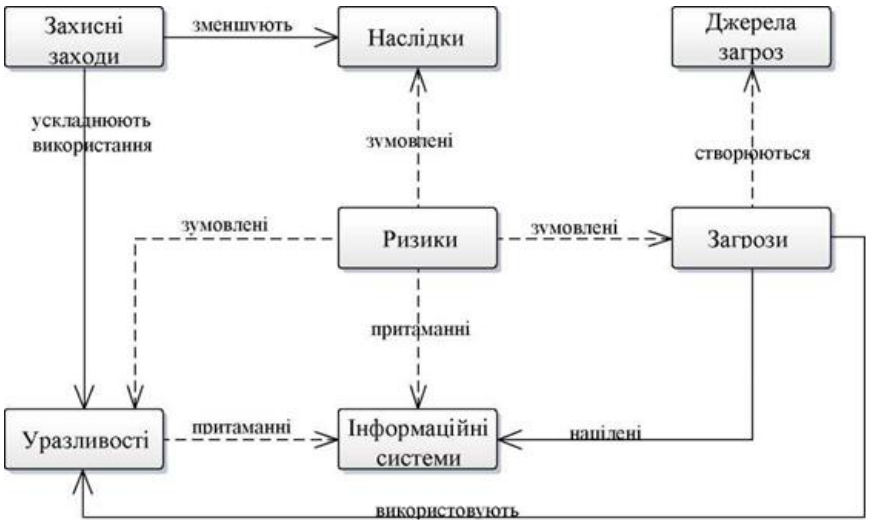

Рисунок 1 - Онтологічна модель аналізу ризиків безпеки

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. Широко застосовують [2, 4] графічні, математичні та лінгвістичні методи. Для практичного застосування доступні: методики *FRAP (Facilitated Risk Analysis Process*), *OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)*, *CORAS*, *RiskWatch* [3]. Відомий метод *CRAMM*, в якому для кожного інформаційного процесу будується дерево зв'язків використовуваних ресурсів, а побудована за цим методом модель дозволяє виділити критичні елементи. Модель оцінки ризиків інформаційної безпеки на основі нечітких множин [4] використовує побудову простих графів 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

Для забезпечення правдоподібності побудованої моделі та її використанні на практиці, модель повинна відповідати ряду вимог: 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. В ході дослідження з'ясовано, що для 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.

Вибір програмного забезпечення

Для виконання моделювання та оцінки інформаційних ризиків використовують різноманітне спеціалізоване програмне забезпечення. На практиці найбільш зручним для використання виявився програмний продукт *STATISTICA*. Програма *STATISTICA* [5] дозволяє проводити різні процедури та методи 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 (як статистичний метод аналізу впливу окремих факторів (чинників) на результативний показник) та інші.

Висновок

Для моделювання аналізу ризиків безпеки інформаційних технологій вигідне використання спрощеної онтологічної моделі, що представлена в роботі. Така модель відображає взаємозв'язок основних концептів, які використовуються в ризик-менеджменті, та є досить універсальною, оскільки поняття та терміни, на яких вона побудована, інваріантні щодо різних визначень ризику, а смислове значення концептів може бути легко адаптоване до конкретної інформаційної системи або технології. Серед різноманіття методик оцінки ризику безпеки рекомендується використання методу факторного аналізу, який є найбільш доцільним в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих чинників, та дозволяє поєднати якісну і кількісну складові аналізу та може бути використаний для оцінювання ризику на різних стадіях впровадження інформаційних систем або технологій. Зручним інструментом для автоматизації процесів моделювання та оцінки є програмний продукт *STATISTICA*, який містить великий набір аналітичних процедур та дозволяє застосування відомих методів аналізу даних.

Список використаної літератури

1. Стрічка новин урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA, яка функціонує в рамках Державного центру кіберзахисту ДССЗЗІ України. Офіційний сайт. URL: https://cert.gov.ua

2. 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.

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

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

4. 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.

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