УДК 004.056.5(045)

Чунарьова А.В., Пархоменко І.І., Сащук І.І.

АНАЛІЗ ПІДХОДІВ ТА ПРОГРАМНИХ РІШЕНЬ ОЦІНКИ І КОНТРОЛЮ ІНФОРМАЦІЙНИХ РИЗИКІВ В КОМП'ЮТЕРИЗОВАНИХ СИСТЕМАХ

Розглянуто підходи і програмні рішення оцінки і контролю інформаційних ризиків як фундаментального організаційного етапу при побудови системи захисту інформації комп'ютеризованих систем,

Ключові слова: *Оцінка ризиків, інформаційні ризики, загрози, уразливості, експертний метод.*

Постановка проблеми

З розвитком ІТ гостро постає проблема забезпечення інформаційної безпеки та технічного захисту інформаційних ресурсів в комп'ютеризованих системах. Одним з важливих організаційних заходів захисту інформації в комп'ютеризованих системах є визначення переліку загроз інформації, які порушують її властивості – конфіденційність, цілісність та доступність. Перелік загроз, у свою чергу, пов'язаний з уразливістю таких систем. Ці два фундаментальні поняття лежать в основі теорії оцінювання ризиків як одного з найважливіших етапів побудови підсистеми захисту інформації.

Ризик – це здатність конкретної загрози використовувати уразливості одного або декількох видів активів для завдання збитків організації. Одна загроза або група загроз можуть використовувати одну уразливість або групу уразливостей. Ризик характеризується комбінацією двох факторів: імовірністю виникнення інциденту і його руйнівним впливом. Будь-яка зміна активів, загроз, уразливостей або захисних заходів може мати значний вплив на ризик. Раннє виявлення або знання про всі ці зміни збільшує можливості щодо прийняття необхідних заходів для обробки ризику.

Мета статті

Метою даної статті є аналіз існуючих підходів і програмних рішень оцінки і контролю інформаційних ризиків на предмет зручності їх застосування при визначенні відповідних дій і пріоритетів в галузі управління ризиками для захисту інформації, а також в області реалізації засобів управління, обраних для захисту від цих ризиків в комп'ютеризованих системах.

Основні матеріали дослідження

Метою оцінювання ризику інформаційної безпеки в комп'ютеризованих системах є:

– визначення потенційно небезпечних подій, які, у разі їх здійснення, викликають можливі втрати;

– отримання відомостей, як, де і чому могла б трапитися втрата.

Якісний аналіз ризику передбачає виявлення чинників ризиків, ідентифікацію можливих ризиків, наслідків їхньої реалізації для процесу чи проекту. Кількісний аналіз ризику проводиться для визначення шляхів впливу на ризик. Кількісно ризик оцінюється за формулою:

$$R = P_{ïîä} \cdot \tilde{N}_{âò\ ðàò}$$

де $P_{ïîä} = P_ç \cdot P_ó$ – імовірність настання негативної події, що завдала шкоди інформаційній безпеці і привела до втрат;

$\tilde{N}_{âò\ ðàò}$ – величина втрат від настання негативної події, залежить від вартості того з активів, який піддавався атаці;

$P_ç$ – імовірність виникнення загрози інформаційній безпеці;

$P_ó$ – імовірність наявності уразливості.

Питання аналізу ризиків ІБ висвітлені у наукових працях, інформаційно-довідкових матеріалах та описах спеціалізованих програмних продуктів. Умовно проблематику аналізу ризиків можна поділити на дві великі групи. До першої відноситься розробка наукових методів аналізу ризиків на основі відомих теорій та вимог стандартів щодо створення СУІБ. Друга група включає спеціалізовані програмні продукти, які, як правило, базуються на методах першої групи, але мають більшу практичну спрямованість і краще враховують специфіку об'єкта захисту.

Проаналізуємо першу групу. Наукові методи аналізу ризиків використовують різні розділи вищої математики: теорію множин, теорію імовірностей, дискретну математику. Як ядро підходів вибирають принципи, засновані на теорії надійності та теорії нечітких множин. Особливістю оцінки ризиків є складність формалізації задачі та отримання кількісних оцінок. Одним із методів оцінки ризиків інформаційної безпеки, основаної на визначенні оптимальних значень є метод, заснований на обчисленні

взаємної інформації і застосуванні так званих K-means алгоритмів кластеризації [1]. Метод визначає ступінь кількісної залежності між факторами ризику і рівнем інформаційної безпеки з обчисленням взаємної інформації. На кожному рівні ризику за алгоритмом K-means визначаються оптимальні точки як початкові центри кластерів, потім алгоритм кластеризації K–means класифікує дані. Метод може динамічно регулювати центр кластера відповідно до результатів кластеризації та обчислення значення взаємної інформації. Цей метод легко застосовувати, він має менше обчислень, ніж інші методи. Метод менш чутливий до вхідних даних.

Матричний підхід аналізу ризиків інформаційної безпеки – метод аналізу ризиків інформаційної безпеки, який пов'язує активи, уразливості, загрози і засоби управління організації. Він використовує послідовність матриць, які пов'язують різні елементи в аналізі ризику. Шляхом послідовного перетворення елементів матриць будуть отримані засоби управління, які розташовані за пріоритетами ранжування та засновані на активах організації. Метод не викривлює проміжні дані в процесі аналізу, таким чином забезпечується прозорість процесу аналізу ризику і передбачається можливість модернізації даних. Перевагою методу є те, що він дозволяє організаціям починати аналіз з малої кількості даних з низькою надійністю, і поступово удосконалювати їх, використовуючи дані, отримані протягом наступного проміжку часу.

Однією з найбільш часто використовуваних теорій в методології оцінки ризиків є теорія нечітких множин, що базується на механізмі нечіткого висновку [2]. В даному випадку він перетворює вхідні дані у вигляді нечітких правил у вихідну змінну, тобто в оцінку ризику. Механізм нечіткого висновку являє собою послідовність операцій над вхідними даними відповідно до параметрів, закладених в наборі продукційних правил. Застосування механізму нечіткого висновку можливе у поєднанні з експертним методом оцінювання. Основними етапами нечіткого висновку є:

введення експертних оцінок – забезпечує механізм виведення необхідної інформації;

фазифікація – знаходження функцій належності використовуваних термів (вхідних змінних) на основі вихідних даних;

агрегування – визначення ступеня істинності умов по кожному з правил нечіткого висновку;

активізація – перевірка істинності кожного з правил нечіткого висновку;

акумуляція – знаходження функції належності для кожної з вихідних лінгвістичних змінних заданої сукупності правил нечіткого висновку;

дефазифікація – знаходження чітких значень вихідних змінних, що найбільшою мірою відповідають вхідним даними і базі продукційних правил.

Реалізація механізму нечіткого висновку полягає у використанні відомого або в розробці нового алгоритму обробки даних з метою оцінки ризиків. Такі підходи використані у [3-7].

Досить цікавий підхід до оцінки ризиків розкрито в [8]. Для побудови алгоритму оцінювання ризиків тут використовується так званий імовірнісний блок – пробіт (probability unit). Суть пробіт-аналізу полягає в спеціальному відображенні S–подібних кривих залежності втрат від характеристик реалізованих загроз в прямі лінії, які в подальшому можуть бути оброблені методами лінійного аналізу. Зворотне перетворення здійснюється шляхом перетворення значень лінійних пробіт-функцій у значення характеристик імовірності. Пробіт-функція – це математична залежність, яка пов'язує специфічні особливості негативного впливу на деякий об'єкт (у нашому випадку – інформаційний актив) з розміром можливих втрат. На основі аналогії з функціями розподілу імовірностей втрат від реалізації сценаріїв загроз безпеці інформації з S– подібними кривими варто припустити, що використання підходу на основі пробіт-аналізу може виявитися результативним. При цьому необхідно відзначити, що розв’язок задачі визначення імовірності характеристик для кожної пари (загроза, уразливість) виконується в два етапи:

– визначення значень елементів пробіт-функції;

– розрахунок пробіт-функції і визначення по відомим значенням пробіт-функції значень імовірнісних характеристик.

Друга група підходів до оцінки ризиків більшою мірою розвинена зарубіжними авторами. Статті авторів з США, Англії носять насамперед рекомендаційний характер з удосконалення вже працюючих стандартів ІБ: ISO, BS та не вимагають глибокого знання вищої математики.

Третя група підходів у багатьох випадках поєднує в собі експертні оцінки та оцінки ризиків, що базуються на визначенні їх імовірності за наявними статистичними даними. Подібні підходи можна успішно застосовувати в практичній діяльності, так як використання бази статистики дозволяє звести до мінімуму суб'єктивну точку зору експерта на вирішуване завдання і проводити роботу з оцінки ризиків ІБ фахівцям без великого досвіду та кваліфікації.

Для вирішення даної задачі був розроблений ряд програмних комплексів аналізу і контролю інформаційних ризиків, основними з яких є: британський CRAMM (компанія Insight Consulting),

американський Risk Watch (компанія Risk Watch) і російський ГРИФ (компанія Digital Security). Розглянемо далі дані методи і побудовані на їх базі програмні системи [9].

Метод CRAMM (the UK Government Risk Analysis and Management Method) був розроблений Службою Безпеки Великобританії і взятий на озброєння в якості державного стандарту.. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, поєднує кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій, як урядового, так і комерційного сектора. CRAMM передбачає поділ всієї процедури на три послідовних етапи. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення опитування, списки перевірки і набір звітних документів.

До недоліків методу CRAMM можна віднести наступне:

– використання методу CRAMM вимагає спеціальної підготовки і високої кваліфікації аудитора;

– CRAMM більшою мірою підходить для аудиту вже існуючих АС, що знаходяться на стадії експлуатації, ніж для АС, що знаходяться на стадії розробки;

– аудит за методом CRAMM – процес досить трудомісткий і може вимагати місяців безперервної роботи аудитора;

– програмний інструментарій CRAMM генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці;

– CRAMM не дозволяє створювати власні шаблони звітів або модифікувати наявні;

– можливість внесення доповнень до бази знань CRAMM недоступна користувачам, що викликає певні труднощі при адаптації цього методу до потреб конкретної організації;

– ПЗ CRAMM існує тільки англійською мовою;

– висока вартість ліцензії.

Програмне забезпечення Risk Watch є потужним засобом аналізу та управління ризиками. У сімейство Risk Watch входять програмні продукти для проведення різних видів аудиту безпеки. У методі Risk Watch в якості критеріїв для оцінки та управління ризиками використовуються “прогнозування річних втрат” і оцінка “повернення від інвестицій”. Risk Watch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту. Використовувана в програмі методика включає в себе 4 стадії:

– визначення предмета дослідження. На даному етапі описуються параметри організації – тип організації, склад досліджуваної системи, базові вимоги в галузі безпеки;

– введення даних, що описують конкретні характеристики системи. Дані можуть вводитися вручну або імпортуватися із звітів, створених інструментальними засобами дослідження уразливості автоматизованих систем. На цьому етапі докладно описуються ресурси, втрати і класи інцидентів. Класи інцидентів виходять шляхом зіставлення категорії втрат і категорії ресурсів. Задається частота виникнення кожної з виділених загроз, ступінь уразливості і цінність ресурсів. Все це використовується надалі для розрахунку ефективності впровадження засобів захисту;

– оцінка ризиків. Спочатку встановлюються зв'язки між ресурсами, втратами, загрозами і уразливостями, виділеними на попередніх етапах. Для ризиків розраховуються математичні очікування втрат за рік як добуток частоти виникнення загрози на протязі року та вартості ресурсу, який піддається загрозі.

– генерація звітів. На цій стадії формуються такі типи звітів: короткі підсумки; повні і короткі звіти про елементи, описані на стадіях 1 і 2; звіт про вартість захищуваних ресурсів та очікуваних втрат від реалізації загроз; звіт про загрози та заходи протидії; звіт про результати аудиту безпеки.

До недоліків Risk Watch можна віднести:

– такий метод підходить, якщо потрібно провести аналіз ризиків на програмно-технічному рівні захисту, без урахування організаційних і адміністративних чинників. Отримані оцінки ризиків далеко не вичерпує розуміння ризику з системних позицій – метод не враховує комплексний підхід до інформаційної безпеки;

– ПЗ Risk Watch існує тільки англійською мовою;

– висока вартість ліцензії.

Програмний комплекс ГРИФ має простий і інтуїтивно зрозумілий для користувача інтерфейс для побудови повної моделі автоматизованої системи з точки зору ІБ. Разом з тим за зовнішньою простотою ховається складний алгоритм аналізу ризиків, що враховує більше ста параметрів, який дозволяє на виході дати максимально точну оцінку існуючих ризиків, засновану на глибокому аналізі особливостей практичної реалізації комп’ютеризованої системи. Основне завдання системи ГРИФ – дати можливість ІТ менеджеру самостійно (без залучення сторонніх експертів) оцінити рівень ризиків в інформаційній системі, оцінити ефективність існуючої практики щодо забезпечення безпеки компанії. Метод включає такі етапи:

– опитування ІТ-менеджера з метою визначення повного списку інформаційних ресурсів, які мають цінність для компанії;

– опитування IT-менеджера з метою введення в систему ГРИФ всіх видів інформації, що представляє цінність для компанії. Заключна фаза етапу – визначення збитку по кожній групі цінної інформації, розташованої на відповідних ресурсах, за всіма видами загроз;

– визначення всіх видів користувальницьких груп та інформації на ресурсах, до якої має доступ кожна з груп користувачів. На закінчення визначаються види (локальний або віддалений) і права (читання, запис, видалення) доступу користувачів до всіх ресурсів, що містять цінну інформацію;

– опитування IT -менеджера для визначення засобів захисту інформації, якими захищена цінна інформація на ресурсах. В систему вводиться інформація про разові витрати на придбання всіх засобів захисту інформації та щорічні витрати на їх технічну підтримку, а також – щорічні витрати на супровід системи інформаційної безпеки компанії;

– опитування користувачів відповідно до списку питань з політики безпеки, реалізованої в системі, що дозволяє оцінити реальний рівень захищеності системи і деталізувати оцінки ризиків;

– формування звіт за систему. Звітом є докладний документ, що дає повну картину можливого збитку від інцидентів, готовий для подання керівництву компанії:

До недоліків ГРИФ можна віднести:

– відсутність прив'язки до бізнес–процесів;

– немає можливості порівняння звітів на різних етапах впровадження комплексу заходів щодо забезпечення захищеності;

– відсутня можливість додати специфічні для даної компанії вимоги політики безпеки.

Результати порівняльного аналізу програмних продуктів для оцінювання ризиків зведемо у таблицю.

Таблиця

Порівняння програмних продуктів за визначеними критеріями

Критерії порівняння	**CRAMM, Central Computer and Telecommunications Agency (UK)**	**RiskWatch, компанія RiskWatch (USA)**	**ГРИФ 2006 Digital Security Office, Компанія (Росія)**
Кількісний або якісний метод	Якісна і кількісна оцінки	Кількісна оцінка	Якісна і кількісна оцінки
Легкість в роботі кінцевого користувача	Вимагає спеціальної підготовки і високої кваліфікації аудитора.	Вимагає спеціальної підготовки і високої кваліфікації аудитора.	Не потребує спеціальних знань в області інформаційної безпеки.
Спосіб завдання шкоди	Як наслідок порушення властивостей активів	Як наслідок реалізації загроз	Як наслідок порушення властивостей активів
Вхідні дані	Ресурси; Загрози; Уразливості системи; Вибір контрзаходів. Цінність ресурсів;	Ресурси; Загрози; Уразливості; Вибір контрзаходів. Цінність ресурсів; Заходи захисту; Тип інформаційної системи; Базові вимоги в галузі безпеки; Втрати; Частота виникнення загроз	Ресурси; Загрози; Уразливості; Вибір контрзаходів. Засоби захисту; Мережеве обладнання; Види інформації; Групи користувачів;
Варіанти звітів	Звіт з аналізу ризиків; Загальний звіт з аналізу ризиків; Деталізований звіт з аналізу ризиків.	Короткі підсумки; Звіт про вартість захищаються ресурсів та очікуваних втратах від реалізації загроз; Звіт про погрози і заходи протидії; Звіт про окупність інвестицій; Звіт про результати аудиту безпеки.	Інвентаризація ресурсів; Ризики за видами інформації; Ризики по ресурсах; Співвідношення збитків та ризику інформації та ресурсу; Вибрані контрзаходи; Рекомендації експертів.
Залежність функції збитку	Для властивостей доступності залежить від	Постійна, не залежить від часу	Для властивостей доступності залежить від

	часу.Для властивостей конфіденційності, цілісності постійна		часу. Для властивостей конфіденційності, цілісності постійна
Критерії порівняння	**CRAMM, Central Computer and Telecommunications Agency (UK)**	**RiskWatch, компанія RiskWatch (USA)**	**ГРИФ 2006 Digital Security Office, Компанія (Росія)**
Облік залежностей між контрзаходами при розрахунку ризиків	Так	Ні	Ні
Облік вартості впровадження контрзаходів	Так	Так	Так
Можливість завдання власних контрзаходів	Так	Так	Є в моделі загроз і вразливостей, а в моделі інформаційних потоків немає
Визначення рівня ризиків по моделі інформаційної системи	Ні	Ні	Так
Розрахованість на організації різного розміру і область діяльності	Так	Так	Так

На підставі проведеного аналізу можна стверджувати, що часто підходи до оцінки ризиків не в повній мірі враховують концепції, вимоги різних стандартів ІБ. Це може викликати недовіру до застосовуваних підходів у експертів, що проводять аналіз ризиків ІБ, ускладнює можливу сертифікацію організації. Багато підходів, в основі яких лежить мета отримати кількісну оцінку ризиків з використанням математичних формул, моделей, заглиблюючись в математичні теорії, інколи втрачають зв'язок з практичною оцінкою ризиків, реальними бізнес-вимогами. Ряд підходів не забезпечують повного циклу управління ризиками ІБ, реалізуючи лише деякі його компоненти.

Висновки. Кожен з підходів до управління ризиками має як недоліки, так і переваги. Найбільш прийнятним є підхід, коли вимоги стандартів зі створення СУІБ та наукові методи управління ризиками поєднані з практичними напрацюваннями у вигляді спеціалізованих програмних продуктів.

Список використаних джерел

1. Козлова Е. А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации / Е. А. Козлова // Молодой учёный, 2013. – №5. – С. 154-161.

2. Герасимов Б.М., Грабовский Г.Г., Рюмшин Н.А. Нечеткие множества в задачах проектирования, управления и обработки информации. – К.: Техніка, 2002. – 324 с.

3. Ажмухамедов И.М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечёткого когнитивного моделирования. Монография. / И.М. Ажмухамедов / Астрахань: Издательство АНТУ, 2012. – 344 с.

4. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса / П.В. Плетнев, В.М. Белов // Доклады ТУСУРа, 2012. – № 1(25), часть 2. – С. 83-86.

5. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практика. – К.: ЭМК-Прес, 2006. – 302 с.

6. Бельфер Р.А., Моёров А.С. Модель оценки риска информационной безопасности сети VANET на основе теории нечётких множеств / Р.А. Бельфер, А.С. Моёров // Молодёжный научно-технический сборник. – ВПО МГТУ им. Баумана, 2012. – С. 3-12.

7. Гордій І.В. Застосування теорії нечітких множин для визначення рівня ризику витоку інформації технічними каналами. / І.В. Гордій // Автоматика, вимірювання та керування. – Львів: Видавництво Львівської політехніки,2009. № 638. - С. 215-218.

8. Мохор В.В., Цуркан В.В. Количественная оценка рисков безопасности информации на основе пробит-анализа / В.В. Мохор, В.В. Цуркан // Реєстрація, зберігання і обробка даних, 2010. Т. 12. – № 3. – С. 85-92.

9. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С.В. Симонов – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.