УДК 4.056

А.І. Андрухів, Д.О. Тарасов
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин,
кафедра інформаційних систем та мереж

ПОРІВНЯННЯ МЕТОДІВ ОЦІНКИ ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Розглянуто завдання та методи аудиту захищеності корпоративних інформаційних систем (ІС). Оцінювання захищеності (аудиту) корпоративної ІС дає змогу знайти потенційні вразливості системи, визначити можливі втрати. Результати аудиту є вхідними даними для оцінювання затрат на заходи щодо захисту інформації у системі. Проаналізовано сучасні алгоритми оцінювання захищеності корпоративних інформаційних систем, зокрема RiskWatch, CRAMM, ГРИФ.

The tasks and methods of audit of the corporative information system are considered . Audit of the corporate information system can show potential threat, calculate possible losses. The audit results can serve as input data to calculate losses estimation to measure to protect information. The actual algorithms of making analysis of the corporative information systems are considered and analysed especially RiskWatch, CRAMM, GRIF.

Вступ

Сьогодні не існує стандартизованих методик аналізу захищеності ІС, тому в конкретних ситуаціях алгоритми дій аудиторів можуть істотно відрізнятися. Проте можливо побудувати загальну модель проведення аудиту, яка має містити такі кроки [7]:

- Ініціювання процедури аудиту. Аудит проводять не за ініціативою аудитора, а за ініціативою керівництва компанії, яке і є основною зацікавленою стороною.
- Збирання інформації для аудиту, зокрема про організаційну структуру користувачів та обслуговувальних підрозділів, про власника та розробника підрозділів, склад та структура систем захисту інформації тощо.
- Аналіз даних, зокрема оцінювання ризиків, пов'язаних із реалізацією загроз безпеки, аналіз механізмів безпеки організаційного рівня, політики безпеки організації, документації із забезпечення режиму інформаційної безпеки тощо.
- Генерація рекомендацій. На цьому кроці після проведення аналізу генерують перелік рекомендацій із вдосконалення (заміни) аспектів, що впливають на загальний рівень безпеки системи.
- Підготовка аудиторського звіту. Цей звіт є основним результатом проведення аудиту. Він повинен містити опис цілей проведення аудиту, характеристику досліджуваної ІС, вказання границь проведення аудиту та використовуваних методів, результати аналізу даних аудиту, висновки, які грунтуються на цих результатах і містять оцінку рівня захищеності ІС чи відповідність вимогам стандартів і рекомендації аудитора щодо ліквідації існуючих недоліків та вдосконалення системи захисту.

Результати аудиту дають змогу:

- визначити істотні недоліки СЗІ;
- визначити відповідність/невідповідність стандартам захищеності ІС з метою подальшої сертифікації системи;
- оцінити витрати власника ІС у випадку реалізації загрози тощо.

Постановка задачі

Сьогодні розроблено декілька методів та стандартів для оцінювання захищеності інформації. Кожен із розроблених підходів має свої особливості, які грунтуються на властивостях та характеристиках об’єктів корпоративної інформаційної системи. Основна ідея аналізу – застосування системи аналізу ризиків, за якою оцінюють існуючі в системі ризики та вибирають найефективніший варіант захисту (за співвідношенням існуючих в системі ризиків до затрат на інформаційну безпеку). Основним завданням дослідження є оцінювання найпоширеніших методів аудиту безпеки корпоративної ІС.

Загальна модель проведення аудиту

Загальну модель проведення аудиту захищеності можна подати за допомогою такої схеми.

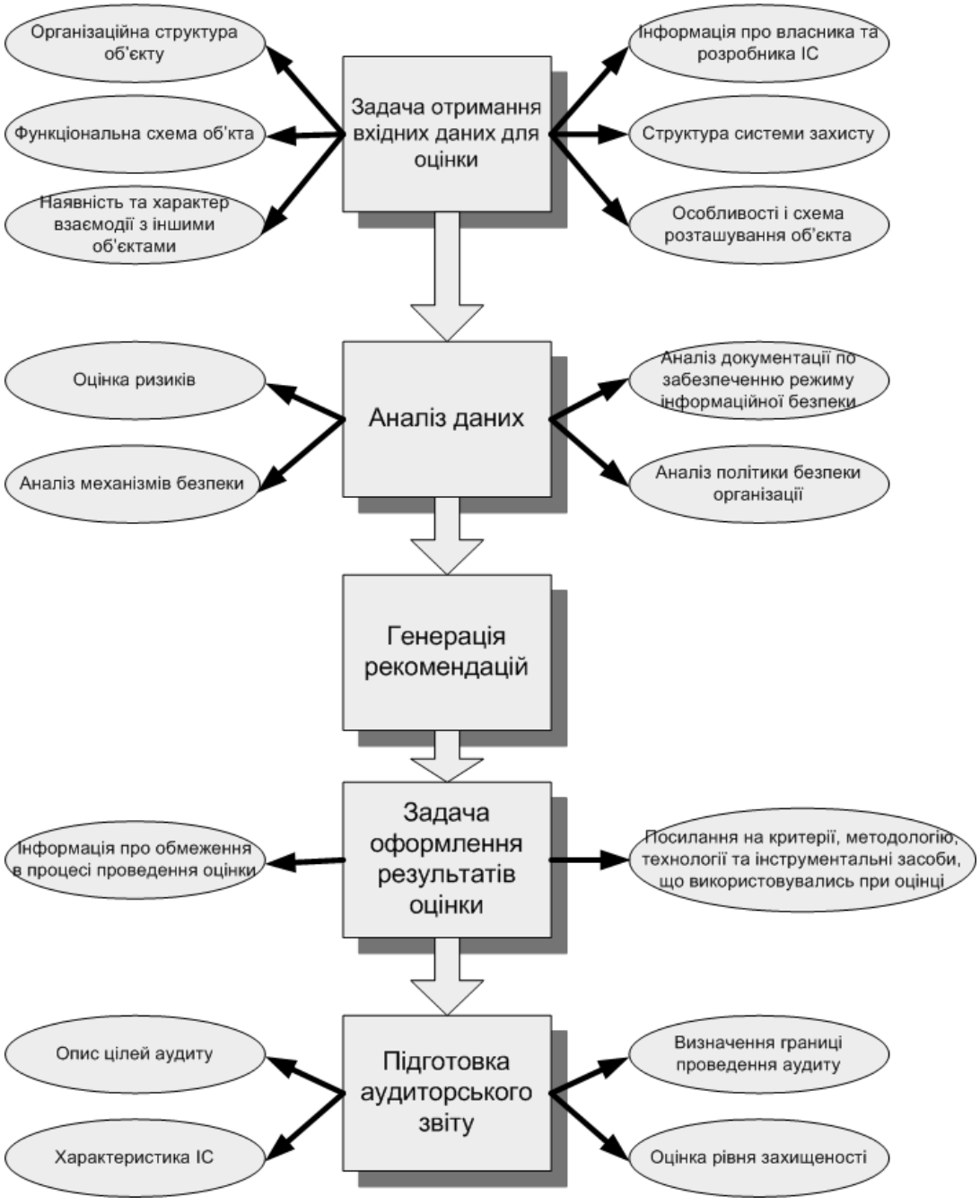

Рис. 1. Основні етапи проведення оцінки захищеності

Формула для розрахунку ризику складається з трьох компонент :

- вартість ресурсу (Asset Value, Av). Ця величина характеризує цінність ресурсу.
- міра вразливості ресурсу до загрози (Exposure Factor, EF) .Цей параметр вказує, якою мірою ресурс є вразливим відносно цієї загрози.
- оцінка ймовірності реалізації загрози (Annual Rate of Occurrence, ARO) свдчить, наскільки є ймовірною реалізація певної загрози на визначений період часу (зазвичай, протягом року).

На основі отриманих даних виводиться оцінка очікуваних втрат (рівень ризику) [6]:

- оцінку очікуваних можливих втрат від одиничної реалізації певної загрози (Single Loss Exposure, SLE) розраховують за формулою

$$SLE= AV*EF;$$

- сумарні можливі втрати від конкретної загрози за рік (Annual Loss Exposure, ALE) характеризують величину ризику та визначають за формулою

$$ALE= SLE*ARO$$

Кінцева формула розрахунку ризику набуває вигляду:

$$ALE= ((AV*EF=SLE)*ARO). \quad (1)$$

Оцінювати ризик можна, враховуючи як якісні, так і кількісні мірки.

Для прикладу проведемо якісний розрахунок інформаційних ризиків.

Розглянемо сервер торгової компанії, що займається продажем комп'ютерної техніки через власний Internet-магазин. Припустимо, що річний торговий оборот становить 50 тис. доларів США на рік. Сервер використовує ПО Microsoft IIS і СУБД Microsoft SQL Server. Для спрощення розрахунку приймемо дві моделі порушників : зовнішній легальний користувач і зовнішній хакер.

Першого позначимо як A1, а другого – як A2.

Відносно сервера можуть бути ідентифіковані такі загрози:

- порушення цілісності інформації, що зберігається в СУБД Internet-магазину;
- порушення доступності сервера;
- порушення конфіденційності інформації, що зберігається в СУБД Internet-магазину.

Результати ідентифікації загроз і побудови моделі порушника зображено в табл. 1.

Таблиця 1

Ідентифікація загроз та модель порушника

Ресурс	Цінність ресурсу	Загроза	Модель порушника	EF	ARO	SLE, тис. дол.	ALE, тис. дол.
Web-сервер	3	Порушення цілісності	A1	3	2	9	18
		Порушення конфіденційності	A1	3	2	9	18
		Порушення доступності	A1, A2	2	3	6	18

У цій таблиці:

- *Цінність ресурсу* визначається: 1 – мінімальна вартість; 2 – середня вартість; 3 – максимальна вартість;
- EF (*міра вразливості ресурсу до загрози*) визначається: 1 – мінімальна міра вразливості (слабкий вплив); 2 – середня (ресурс потрібно відновлювати); 3 – максимальна (заміна ресурсу після реалізації загрози);
- ARO *(оцінка ймовірності реалізації загрози*): 1 – низька; 2 – середня; 3 – висока.

Ресурс сервера є критичним для функціонування компанії, тому йому присвоюють значення AV=3. Загрозі порушення цілісності (EF) присвоєне максимальне значення (3), тому що порушення цілісності збережених у СУБД даних сприяє зриву постачань. Ймовірність реалізації загрози порушення цілісності оцінено як середню. Параметри EF і ARO відносно загроз порушення

конфіденційності і доступності розраховувалися аналогічно. Більшість параметрів, крім AV, ґрунтувалися на експертній думці аудитора. Всі ідентифіковані ризики є високими , оскільки реалізація цих загроз завдасть істотної шкоди компанії.

Компанія повинна вжити заходів щодо зниження значення ризику. В цьому випадку такими заходами можуть бути налаштування програмного забезпечення сервера, встановлення міжмережевого екрана.

Розрахуємо витрати на впровадження цих заходів. Наприклад, налаштування програмного забезпечення сервера міститиме трудозатрати в 20 людино-годин, а фінансові вкладення становитимуть 1000 доларів США. Встановлення міжмережевого екрана: трудозатрати в 50 людино-годин і 5 тис. доларів. Отже, загальні витрати на впровадження запропонованих заходів – 70 людино-годин і 6 тис. доларів. Порівняно з річним оборотом Internet-магазина ці витрати хоч і високі, але цілком виправдані. Найважливіше, щоб ризики були правильно ідентифіковано та проранжовано відповідно до ступеня їх критичності для організації.

Зараз на світовому ринку існує 3 базові алгоритми для розрахунків ризику: ГРИФ, CRAMM, RiskWatch.

Алгоритм RiskWatch

За методом RiskWatch критеріями вважають “можливі річні втрати” (Annual Loss Expectancy) та оцінку “поверенення від інвестицій” (Return Investment). Алгоритм RiskWatch у загальному випадку можна звести до таких кроків:

1. Визначення предмета дослідження. Тут визначено тип організації, базові вимоги у галузі безпеки, склад організації.

2. Введення даних, що описують конкретні характеристики. На цьому етапі детально описують ресурси, втрати, класи інцидентів. Задають частоту виникнення кожної з можливих загроз, ступінь вразливості та цінність ресурсів.

3. Визначення ризику. Спочатку встановлюють зв’язок між ресурсами, втратами, загрозами, вразливостями. Математичне сподівання для ризику за рік розраховують за формулою:

$$R = p*D, \quad (2)$$

де R – ризик; p – частота виникнення загрози за рік; D – вартість ресурсу.

4. Генерація звіту. Це може бути звіт втрат від реалізації загроз; звіт про заходи щодо протидій; звіт про результат аудиту безпеки тощо.

Програмне забезпечення, реалізоване на основі методу, має такі недоліки:

- аналіз відбувається на програмно-технічному рівні захисту, коли не враховуються адміністративно-організаційні фактори;
- відсутність комплексного підходу до інформаційної безпеки;
- висока вартість ліцензії.

Алгоритм CRAMM

Метод CRAMM – потужніший та універсальніший інструмент, який грунтується на методі, який поєднує кількісні та якісні методи аналізу з комплексним підходом до оцінки ризиків.

Метод CRAMM передбачає наявність таких етапів аналізу:

- на першому етапі визначають наявний рівень безпеки ресурсів. Якщо цей рівень є низьким, то до системи висувають мінімальний набір вимог безпеки і переходять на 3-й етап.
- на другому етапі ідентифікують ризики та визначають їхню величину. Вихідні дані аудитор отримує від представників організації.
- керування ризиками, вибір контрзаходів. Найважливішим критерієм у цьому випадку є обгрунтування вибраних контрзаходів.

Можна зобразити концептуальну схему CRAMM.

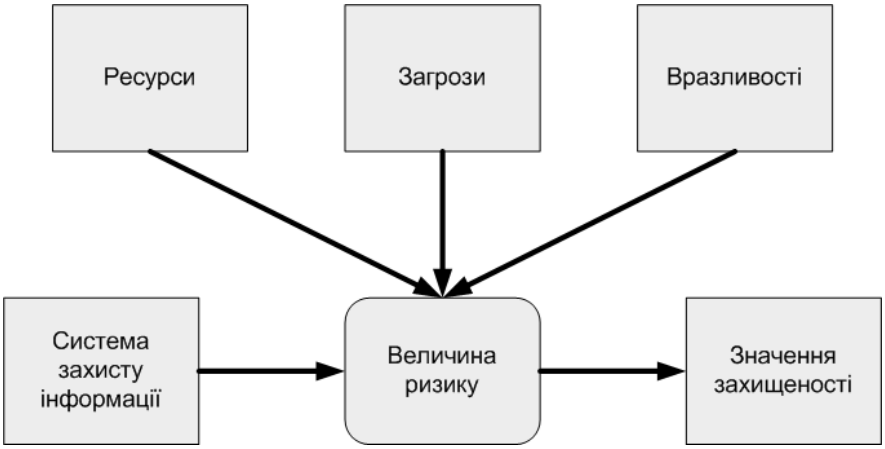

Рис. 2. Концептуальна схема методу CRAMM

До переваг методу належать:

- метод є добре структуризованим та випробуваним;
- в основі програмного продукту є хороша база знань з контрзаходів у галузі інформаційної безпеки;
- гнучкість й універсальність методу дає змогу використовувати його для аудиту ІС довільного рівня складності та призначення;
- можна використати як засіб документування існуючих механізмів безпеки ІС.

До недоліків методу належать такі особливості:

- вимагає спеціальної підготовки та високої кваліфікації аудитора;
- аудит за цим методом дуже трудомісткий і потребує багато часу;
- немає можливості змінювати шаблон звітів;
- висока вартість ліцензії.

Вищенаведені алгоритми використовують підхід, коли користувач вказує повний перелік загроз безпеки, специфічних для цієї системи, разом із оцінкою збитків за кожним видом загроз. Проте не враховано факт, що на один вид інформації може бути скеровано відразу декілька загроз, що, своєю чергою, призведе до того, що сумарні збитки, підраховані за загрозами, будуть нереалістичними. Враховуючи цей факт, що об'єктом захисту є інформація, алгоритм аналізу ризику повинен відштовхуватись не від загроз і збитків за ними, а від інформації і від збитків щодо інформації, але при цьому враховувати і самі загрози.

Алгоритм ГРИФ

Порівняно з іншими алгоритмами, ГРИФ має істотні переваги: можливість абстрагуватися на етапі моделювання системи від загроз безпеки, розбити ІС на визначену множину ситуацій , кожну з яких проаналізувати окремо. Враховуючи практичність та легкість використання, пропонується детальніше розглянути цей алгоритм.

Вхідними даними є: ресурси, критичність ресурсів, вразливості, ймовірність реалізації загрози через певну вразливість, критичність реалізації загрози [5].

Алгоритм предбачає два режими роботи – коли існує одна базова загроза (сумарна) та коли є три базові загрози. У цьому огляді розглянемо одну базову загрозу. Для роботи з алгоритмом використано шкалу від 0 до 100 %, яку можна розбити на 100 частин. Кожна частина займає певний інтервал. Розбиття можна провести рівномірно та логарифмічно. Так, наприклад, для 5 рівнів рівномірне розбиття набуде вигляду: 1-й рівень – 20 %, 2-й рівень – 40 %, 3-й рівень – 60 %, 4-й рівень – 80 %, 5-й рівень – 100 %; логарифмічне – 1-й рівень – 7 %, 2-й рівень – 18 %, 3-й рівень – 35 %, 4-й рівень – 62 %, 5-й рівень – 100 %.

На **першому** етапі роботи алгоритму розраховують рівень загрози за вразливістю Th на основі критичності та ймовірності реалізації загрози через цю вразливість. Рівень загрози передбачає, наскільки критичним є вплив цієї загрози на ресурс з врахуванням ймовірності її реалізації.

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}, \tag{3}$$

де ER – критичність реалізації загрози (у %), P(V) – ймовірність реалізації загрози через цю вразливість (у %), Th – рівень загрози за вразливістю.

Другий етап передбачає розрахунок рівня загроз за всіма вразливостями CTh , через які можлива реаліація цієї загрози на ресурсі. Підсумуємо отримані рівні загроз через конкрентні вразливості за такою схемою:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i) \ , \tag{4}$$

де CTh – рівень загрози за всіма вразливостями, Th – рівень загрози за вразливістю.

Значення рівня загрози за всіма вразливостями має знаходитись у межах від 0 до1.

На **третьму** етапі аналогічно розраховуємо загальний рівень загроз за ресурсом CThR (враховуючи всі загрози, що впливають на ресурс)

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i), \tag{5}$$

де CThR – загальний рівень загроз за ресурсом, CTh – рівень загрози за всіма вразливостями.

Значення загального рівня загрози має знаходитися в інтервалі від 0 до 1.

На **четвертому** етапі ризик за ресурсом R розраховують так:

$$R = CTh \times D, \tag{6}$$

де R – ризик за ресурсом, CThR – загальний рівень загроз за ресурсом, D – критичність ресурсу.

Критичність ресурсу визначають за такою формулою:

$$D = D_t \times T \ , \tag{7}$$

де D_t – критичність ресурсу за загрозою доступності на годину, T – максимально критичний час простою ресурсу.

На **п'ятому** етапі ризик за ІС CR розраховують за формулою:

Для режиму роботи в грошах :

$$CR = \sum_{i=1}^{n} R_i \ , \tag{8}$$

де CR – ризик за ІС, R – ризик за ресурсом.

Для режиму роботи в рівнях:

$$CR = (1 - \prod_{i=1}^{n} (1 - \frac{R_i}{100})) \times 100 \, , \tag{9}$$

де CR – ризик за ІС, R – ризик за ресурсом.

Порівняльний аналіз методів можна звести до табл. 2 [4].

Таблиця 2

Порівняльний аналіз методів оцінки захищеності

	CRAMM	RiskWatch	ГРИФ
Підтримка	наявна	наявна	наявна
Вид оцінки	якісна	кількісна	якісна + кількісна
Простота в користуванні	спеціальна підготовка	спеціальна підготовка	не потребує спеціальної підготовки
Ціна за програмне забезпечення	2 000–5 000 дол. США	понад 10 000 дол. США	понад 1 000 дол. США

Аналіз інформаційних ризиків є важкою практичною задачею. Підходи до його реалізації можуть бути найрізноманітніші – від досить простих, але зручних і потужних (RiskWatch) до дуже складних у роботі систем (CRAMM). RiskWatch та CRAMM оперують конкретними видами загроз і вибудовують складну модель ІС. Метод ГРИФ грунтується на комплексі параметрів, що визначаються захищеністю досліджуваного об'єкта. Аналізуються як технологічні аспекти захищеності, так і питання комплексної безпеки.

Висновки

Розглянуто завдання та методи аудиту захищеності корпоративних інформаційних систем. Оцінювання захищеності корпоративної ІС допомагає знайти потенційні вразливості системи, визначити можливі втрати. Результати аудиту слугують вхідними даними для оцінки затрат на заходи щодо захисту інформації у системі. Проаналізовано сучасні алгоритми оцінювання захищеності корпоративних інформаційних систем, зокрема RiskWatch, CRAMM, ГРИФ

Але оцінювання ризиків не дає змоги аргументувати рівень інвестицій, оскільки неможливо визначити точні цифри (а у разі проведення якісного аналізу вони абстрагуються) для визначення затрат на зменшення ризиків.

Використання наведених методів має територіальні обмеження, а саме – RiskWatch використовують на території США, CRAMM – у Великобританії, ГРИФ – більш адаптований для країн СНД. Серед наведених методів ГРИФ має найкращі характеристики: порівняно низька вартість ліцензії, можливість якісного та кількісного оцінювання, побудови детального звіту; використання ПЗ на основі цього методу не потребує спеціальних знань.

Надалі продовжуватимуть роботи щодо адаптації методів аудиту оцінки захищеності для роботи з інформаційними системами у вищих навчальних закладах.

1. Guide for Production of Protection Profiles and Security Targets. ISO/JTC1/SC27/N2449. DRAFT v0.9, January 2000. 2. Information technology – Security techniques – Protection Profile registration procedures. ISO/IEC 15292: 2000 http://www.iso.ch/iso/en/commcentre/pdf/Itsecurity0006.pdf. 3. Куканова Н., Методика оценки риска ГРИФ 2006 из состава Digital Security Office http://www.dsec.ru/about/articles/grif_ar_methods/. 4. Куканова Н. Современные методы и средства анализа и управления рисками информационных систем компаний http://www.dsec.ru/about/articles/ar_compare/. 5. Липаев В.В. Анализ и сокращение рисков проектов программных средств http://jetinfo.isib.ru/2005/1/2005.1.pdf. 6. Сидак А., Марк К. Методология оценки безопасности информационных технологий по общим критериям, http://jetinfo.isib.ru/2004/6/2004.6.pdf. 7. Симонов С. Технологии и инструментарий для управления рисками http://jetinfo.isib.ru/2003/2/2003.2.pdf. 8. Тарасов Д.О. Аудит баз даних // Защита информации: Сб. науч. тр. – К.: КМУГА, 2000. – С. 137–143.