**УДК 004:657**

# МОДЕЛЮВАННЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**А. С. Паламарчук**
здобувач вищої освіти першого (бакалаврського) рівня, 1 курс
спеціальність «Інформаційні системи та технології»,
навчально-науковий інститут кібернетики, інформаційних технологій та інженерії
Науковий керівник – к.ф.-м.н., доцент І. М. Карпович

*Національний університет водного господарства та природокористування, м. Рівне, Україна*

**В роботі проаналізовано прийоми і методи аналізу ризиків, моделі загроз та засоби захисту інформації. Відмічено, що криптографічний захист інформації передбачає створення програмно-апаратного комплексу, який здатний забезпечити необхідні класи захисту усіх інформаційних компонентів. Запропоновано математичну модель оцінки інформаційних ризиків та оптимізації витрат на їх уникнення чи мінімізацію.**
**Ключові слова:** інформаційна безпека; аналіз ризиків; засоби захисту інформації; математична модель.

**The paper analyzes the techniques and methods of risk analysis, threat models and information protection tools. It is noted that cryptographic information protection involves the creation of a software and hardware complex that is capable of providing the necessary protection classes for all information components. A mathematical model for assessing information risks and optimizing the costs of avoiding or minimizing them is proposed.**
**Keywords:** information security; risk analysis; information protection tools; mathematical model.

**У зв'язку із** загальною інформатизацією суспільства та комп'ютеризацією практично усіх видів людської діяльності значно зросла актуальність інформаційної безпеки (ІБ). Зазвичай, всі загрози впливають на три властивості інформаційних активів: конфіденційність, цілісність та доступність. Загрози, що впливають на інформаційні активи і призводять до реалізації інформаційного ризику, умовно можна поділити на загрози, зумовлені внутрішніми причинами, та загрози, зумовлені зовнішніми чинниками.

**Мета роботи:** на основі аналізу загроз, характеристик порушника та ідентифікації вразливостей запропонувати математичну модель оцінки ризиків ІБ та оптимізації витрат на їх уникнення чи мінімізацію.

**Об'єкт дослідження:** математичні моделі оцінки ризиків ІБ, які дозволяють оптимізувати ефективність системи захисту інформації в умовах відведеного фінансування.

**Детально процес** аналізу ризиків ІБ описується в стандарті [1]. Під час аналізу ризиків розглядається реальний стан інформаційної системи, оцінюється розмір очікуваних втрат від інцидентів, пов'язаних з інформаційною безпекою за певний період. Після цього робиться оцінка того, як запропоновані засоби та заходи безпеки впливають на зниження ризиків і яка їх вартість.

Предмет захисту інформації в загальному вигляді можна подати у вигляді схеми «загрози – вразливості – активи», де взаємодія складових відбувається під впливом заходів із захисту інформації з метою забезпечення неперервності технологічних процесів компанії.

Процес аналізу ризиків – це інструмент, за допомогою якого можна визначити цілі управління ІБ, оцінити основні критичні фактори, що негативно впливають на основні бізнес-процеси організації, і виробити ефективні та обґрунтовані рішення для усунення або мінімізації ризиків. Концептуальні засади аналізу ризиків, системи показників для їх оцінювання, основних підходів до моделювання, управління та методів зниження величини ризику детально проаналізовані в монографії [2]. Мета управління ІБ полягає у збереженні конфіденційності, цілісності та доступності інформації. Для цього необхідно провести інвентаризацію та оцінку активів організації і їх оточення, тобто всього, що забезпечує функціонування виробничої діяльності. З точки зору аналізу ризиків ІБ до основних активів належать безпосередньо інформація, інфраструктура, персонал, імідж та репутація компанії. Важливим завданням управління ризиками є визначення найцінніших активів. Цінність активу визначається величиною втрат, які зазнає компанія у випадку порушення безпеки активу.

**У процесі аналізу ризиків** необхідно оцінити мотивованість порушників щодо реалізації загроз. Потенційним порушником насамперед може бути сторона, зацікавлена в отриманні вигоди шляхом порушення безпеки активу. Відомості, необхідні для розробки моделі порушника, можна отримати із спеціалізованих досліджень щодо порушень у галузі комп'ютерної безпеки у тій сфері бізнесу, для якої проводиться аналіз ризиків. Всебічна характеристика можливого порушника доповнює цілі забезпечення ІБ, підвищує якість розроблених моделей оцінки інформаційних ризиків.

Інвентаризація інформаційних активів компанії тісно пов'язана з ідентифікацією вразливостей та розробкою моделі загроз. Розробка моделі загроз виконується фахівцями у галузі ІБ, що добре розуміють, яким чином порушник може отримати несанкціонований доступ до інформації, порушуючи засоби захисту або діючи методами соціальної інженерії. Розробка моделі загроз передбачає розгляд сценаріїв у вигляді послідовних кроків, відповідно до яких можуть бути реалізовані загрози. Крім того, загрози необхідно ранжувати за рівнем ймовірності їх реалізації. Для цього для кожної загрози необхідно вказати найбільш значущі фактори, які сприяють її реалізації. Після розробки моделі загроз необхідно ідентифікувати та оцінити вразливості в оточенні активів.

Результати аналізу моделі загроз, моделі порушника та ідентифікації вразливостей визначають причини, що впливають на досягнення певного рівня інформаційної безпеки організації. Разом з тим, вони служать основою для розробки якісних математичних моделей, які дозволяють оцінити ефективність системи ІБ.

Отримані результати аналізу ризиків необхідно оцінити, а схожі ризики агрегувати, класифікувати та систематизувати. Класифікація ризиків, в загальному випадку, може бути багатогранною. З одного боку, можна розглядати ризики інформаційної безпеки, з іншого – ризики збитків для репутації чи втрати клієнта. Класифіковані ризики необхідно ранжувати за ймовірністю їх виникнення та за значущістю для організації. Оскільки збитки визначаються на етапі ідентифікації та оцінки активів, необхідно оцінити ймовірність події ризику. Як і у випадку з оцінкою активів, оцінку ймовірності можна отримати на підставі статистики за інцидентами, причини яких збігаються з погрозами ІБ, що розглядаються, або методом прогнозування – на підставі зважених факторів, що відповідають розробленій моделі загроз. Прогнозування ймовірності загроз проводиться на підставі властивостей вразливості та груп порушників, від яких надходять загрози. В процесі ідентифікації та оцінки вразливостей важливими є експертний досвід фахівців з ІБ, які виконують оцінку ризиків, та статистичні матеріали і звіти щодо вразливостей та загроз у сфері ІБ. Рівень ризику слід визначити для всіх ідентифікованих відповідних наборів «актив – загроза».

Захист інформації, в загальному, – це прийняття правових, організаційних та технічних заходів, спрямованих на забезпечення захисту інформації від неправомірного доступу,

знищення, модифікування, блокування, копіювання, надання, розповсюдження, а також інших неправомірних дій щодо такої інформації; дотримання конфіденційності інформації обмеженого доступу; реалізація права на доступ до інформації.

Засоби захисту інформації поділяють на нормативні (неформальні) та технічні (формальні). Неформальними засобами захисту інформації є нормативні, адміністративні і морально-етичні засоби, до яких належать документи, правила, заходи. До формальних засобів захисту відносять спеціальні технічні засоби та програмне забезпечення, які можна поділити на фізичні, апаратні, програмні та криптографічні. Фізичні засоби захисту (механічні, електричні та електронні механізми) функціонують незалежно від інформаційних систем та створюють перешкоди для доступу до них.

Апаратні засоби захисту інформації (електричні, електронні, оптичні, лазерні та інші пристрої) вбудовуються в інформаційні та телекомунікаційні системи. Серед них спеціальні комп'ютери, мережеві фільтри, системи контролю працівників, захист серверів та корпоративних мереж тощо. Вони перешкоджають доступу до інформації, зокрема, з допомогою її маскування. Програмні засоби захисту інформації – прості і комплексні програми, призначені для виконання завдань інформаційної безпеки. Прикладами комплексних програм є системи DLP (Data Leak Prevention) та SIEM (Security Information and Event Management).

Криптографічний та стенографічний методи захисту даних використовують для безпечної передачі їх по корпоративній чи глобальній мережі. Криптографія вважається найнадійнішим способом захисту даних, адже вона охороняє саме інформацію, а не доступ до неї. Криптографічно перетворена інформація має підвищений ступінь захисту. В роботі [3] описано математичні основи криптології, розглянуто сучасні методи та алгоритми криптографії, криптоаналізу, стеганографії, висвітлено питання ідентифікації, автентифікації та санкціонованого доступу.

Впровадження засобів криптографічного захисту інформації вимагає створення програмно-апаратного комплексу, архітектура та склад якого визначається із врахуванням потреб конкретного замовника, вимог законодавства, поставлених завдань та необхідних методів і алгоритмів шифрування. Засоби шифрування можуть підтримувати алгоритми шифрування, передбачені державним стандартом, та забезпечувати необхідні класи криптозахисту залежно від нормативної бази та вимог сумісності з іншими системами. В цьому випадку забезпечується захист усіх інформаційних компонентів, зокрема, файлів, каталогів з файлами, фізичних та віртуальних носіїв інформації, серверів та систем зберігання даних.

**Наше завдання** – побудувати математичну модель оцінки ризиків ІБ, яка дозволяє зробити чисельну оцінку ефективності засобів захисту інформації із врахуванням заданих вимог до системи захисту та забезпечити засоби захисту інформації відповідно до цих критеріїв.

Нехай в технічній чи соціально-економічній системі відомі залежності ризиків *Ri* відмови працездатності системи від витрат *Xi* на їх уникнення (мінімізацію) в *i*-му напрямку забезпечення ІБ (відмова апаратного чи програмного забезпечення, відмова працездатності системи через недостатню кваліфікацію співробітників, управлінців тощо): $Ri = F(X_i)$, i = 1..*n*, де *n* – кількість визначених напрямів забезпечення ІБ. Тоді сумарний ризик відмови працездатності системи розраховується як сума ризиків за кожним напрямом:

$$R = \sum_{i=1}^{n} R_i \,. \qquad (1)$$

Для мінімізації ризиків ІБ будемо використовувати такий показник, як рівень витрат на відновлення працездатності системи у разі її відмови в одному чи кількох напрямках. Кожній загрозі поставимо у відповідність параметри: $\omega_i$ – частота виникнення *i*-ї загрози; $p_i$ – ймовірність реалізації загрози, наприклад, внаслідок успішного використання деякої

вразливості. За допомогою формули розрахунку вартості ризику можна обчислити ймовірні втрати від реалізації окремих загроз [4]:

$$R_i = \sum_{k=1}^{k1} \omega_i p_i d_i c(a_k) , \quad (2)$$

де $k1$ – кількість активів, на які спрямована $i$-та загроза, $i$=1..$n$; $c(a_k)$ – вартість активу $a_k \in A_i$ – набір активів або ресурсів, на які спрямована $i$-та загроза. Коефіцієнт пошкодження (руйнування) $d_i \in [0;1]$, що виражає міру руйнівної дії загрози на актив чи активи, може служити критерієм відбору (селектором) тих активів, на які поширюється руйнівна дія $i$-ї загрози.

Визначимо такі величини: $S$ – максимальна сума витрат на уникнення (мінімізацію) виділених ризиків; $S_{1i}$ – мінімальна, $S_{2i}$ – максимальна сума витрат на реалізацію $i$-го напряму відповідно.

Сформулюємо задачу оптимізації, в якій кожен із ризиків необхідно звести до мінімуму, при цьому загальна сума витрат на їх уникнення (мінімізацію) не повинна перевищувати максимальної суми витрат на мінімізацію (уникнення) виділених ризиків, де витрати на уникнення загроз у кожному з напрямків повинні бути в межах передбаченого фінансування [$S_{1i}$; $S_{2i}$]:

$$\begin{gathered} R_i \to min \\ \sum_{i=1}^{n} X_i \leq S \\ S_1 \leq X_i \leq S_2 \end{gathered} \quad (3)$$

Побудована модель системи мінімізації ризиків ІБ буде економічно виправданою в тому випадку, якщо сума всіх витрат на уникнення (мінімізацію) визначених ризиків не перевищує загальної суми фінансування, виділеної на мінімізацію (уникнення) сумарних ризиків. На основі оцінки експертів ймовірності реалізації загрози інформаційній безпеці розраховується значимість кожної загрози, а також оцінюється рівень витрат на відновлення працездатності системи. Модель може бути використана для кількісних оцінок уразливості об’єкта, побудови алгоритму захисту, оцінки ризиків з метою підвищення ефективності вжитих заходів. Крім того, вона сприятиме раціональному розподілу фінансового ресурсу за виділеними напрямами діяльності компанії, що мінімізує ризики відмови працездатності системи за критерієм інформаційної безпеки.

**Загалом** необхідно передбачити заходи для забезпечення життєвого циклу розробленої системи інформаційної безпеки чи її частини, який в тому чи іншому вигляді передбачає планування і розробку, впровадження, моніторинг, коригування чи удосконалення системи. Це дозволить створити і підтримувати певний рівень ІБ, необхідний для інформаційної системи компанії.

Залежно від мети сформульованого завдання, можуть бути розроблені та використані інші математичні моделі, які є частиною системи інформаційної безпеки і допоможуть ще на стадії проєктування системи інформаційної безпеки оцінити її ефективність. Основна мета заходів з управління ризиками інформаційної безпеки та захисту інформації, зокрема, математичного моделювання полягає в тому, щоб забезпечити цілісність, доступність та конфіденційність інформації, що обробляється, зберігається та передається в інформаційних системах у всіх її видах та формах.

**1.** Information technology. Security techniques. Information security risk management: BS ISO/IEC 27005:2008. 64 с. **2.** Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві : монографія. К. : КНЕУ, 2004. 480 с. **3.** Інформаційна безпека: навч. посіб. / Бобало Ю. Я. та ін. ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с. **4.** Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. *Technical sciences and technologies: scientific journal.* Chernihiv : Chernihiv Polytechnic National University, 2021. № 1(23). P. 62–68.