УДК 681.51:519.876

ОЦІНКА ІНФОРМАЦІЙНИХ РИЗИКІВ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Степанова О.М., Волков А.А.

ASSESSMENT OF THE INFORMATION RISKS IN THE CONDITIONS OF THE ENTERPRISE INFORMATION SYSTEM DEVELOPTMENT

Stepanova E.M., Volkov A.A.

У статті визначені етапи процесу оцінювання ризиків, обґрунтовано використання ймовірносного підходу щодо оцінки інформаційних ризиків. Запропонована методика оцінки сукупного впливу загроз на рівень інформаційного ризику на основі їх ієрархічної класифікації за допомогою ймовірнісних показників, виокремлені етапи управління інформаційними ризиками.

Ключові слова: *інформаційна система, інформаційний ризик, оцінка, ієрархічна класифікація, ймовірність*

Вступ. Інформаційні системи в сучасних умовах перетворюються на інструмент підвищення ефективності управління і створення нових конкурентних переваг і тому займають не останнє місце у всіх галузях бізнесу. Невід'ємною частиною будь-якого підприємства стають інформаційні системи, які забезпечують управління виробництвом, фінансами, персоналом, документами та ін. Як наслідок, все більше критично важливої для підприємства інформації зберігається і оброблюється в таких системах. Окрім того, підприємства неухильно розвивають свої інформаційні системи. Разом з цим поступово підвищується їх складність і, відповідно, збільшується кількість уразливостей і загроз інформації (як випадкових, так і умисних), збитків (фінансових та інших) від реалізації цих загроз. Все це призводить до зростання інформаційних ризиків.

Таким чином однією з найбільш серйозних проблем, що ускладнюють розвиток інформаційної системи підприємства є забезпечення інформаційної безпеки. При формуванні ефективної системи захисту необхідно передбачити виконання робіт щодо управління ризиками, суть яких полягає в тому, щоб оцінити розмір ризиків, виробити ефективні і економічні заходи зі зменшення їх розміру і потім переконатися, що ризики знаходяться в прийнятних рамках.

Аналіз останніх досягнень і публікацій. В науковій літературі велика увага приділяється проблемам оцінки ризиків, що пов’язані з впровадженням нових інформаційних технологій в діяльність підприємства. Так питання оцінювання ризику в автоматизованій інформаційній системі досліджується Астаховим А.М. [2], який використовує системний підхід до управління інформаційними ризиками, що ґрунтується на міжнародних стандартах BS 7799-3 та ISO/IEC 27005. При розробці сучасних перспективних систем захисту інформації наразі широко використовується теоретичний апарат експертних систем, нейронних мереж [1,5,7,8]. При врахуванні ризиків різних типів існує спроба використання нечіткої логіки, яка є одним з засобів моделювання в умовах невизначеності [1,7]. Застосування ймовірнісного підходу висвітлено в роботі Гончара С.Ф. [4], Черней Г.А. [11] поєднує експертний та ймовірнісний підходи щодо аналізу інформаційних ризиків, Бєлов В.М. [9] використовує експертний підхід з урахуванням міжнародних стандартів тощо. Але слід зазначити, що для більшості запропонованих методик характерна складність використаного апарату і висока коштовність, що знижує їх переваги при практичному використанні. Відкритим поки є питання оцінки сукупної дії загроз на систему або ресурс, поза межами залишається можливість оцінки ризиків при різноманітних сценаріях реалізації множини загроз.

Постановка проблеми. На основі результатів кількісної оцінки ризиків здійснюється оптимізація витрат на створення системи захисту інформації в умовах розвитку інформаційної системи підприємства. **Метою дослідження** є розробка методики оцінки сукупного впливу загроз на рівень інформаційного ризику на основі їх ієрархічної класифікації за допомогою ймовірнісних показників.

Виклад основного матеріалу дослідження. Використання інформаційних систем пов'язане з певною сукупністю ризиків. Ризик характеризує небе-

зпеку, якій може піддаватися система і організація, що використовує її [8]. Ризик залежить від:

показників цінності ресурсів;

вірогідності нанесення збитку ресурсам (які виражені через вірогідність реалізації загроз для ресурсів);

ступені легкості, з якою уразливості можуть бути використані при виникненні загроз (уразливості системи захисту);

дійсних або планованих засобів забезпечення інформаційної безпеки.

Коли ризик неприйнятно великий, необхідно застосувати економічно виправдані захисні заходи. Періодична переоцінка ризиків необхідна для контролю ефективності діяльності в області безпеки і для обліку змін у інформаційних системах.

Процес оцінювання ризиків містить наступні етапи [8]:

опис об'єкту і засобів захисту;

ідентифікація ресурсу і оцінювання його кількісних показників (визначення потенційної негативної дії на бізнес);

аналіз загроз інформаційної безпеки;

оцінювання уразливостей;

оцінювання дійсних і передбачуваних засобів забезпечення інформаційної безпеки;

оцінювання ризиків.

З кількісної точки зору розмір ризику є функцією вірогідності реалізації певної загрози, а також величини можливого збитку. Для оцінки інформаційних ризиків підприємства пропонуємо захищеність кожного цінного ресурсу визначати за допомогою аналізу загроз, що можуть діяти на конкретний ресурс. Оцінюючи вірогідність реалізації актуальних для цінного ресурсу загроз і ступінь впливу реалізації загрози на ресурси, аналізуються інформаційні ризики підприємства. Важливим для даної процедури є вибір такої класифікації загроз, яка надає можливість зручного практичного використання і забезпечує можливість зв’язку цієї класифікації з подіями безпеки [3]. Слід зазначити, що закріпленого законодавчим чином виду класифікації загроз інформаційної безпеки не існує, а питання їх класифікації до цих пір активно досліджуються. Формалізація завдання опису повної множини загроз значно ускладнена у зв’язку з тим, що інформація, яка зберігається і оброблюється в сучасних інформаційних системах, схильна до впливу надзвичайно великого числа чинників. Так в даний час існує обширний перелік загроз інформаційної безпеки, який містить сотні позицій. Тому для системи, що захищається, доцільно визначати не повний перелік загроз, а перелік класів загроз.

Дослідження довели доцільність розробки і використання ієрархічної системи класифікації. Ієрархічна структура дозволить спростити процес оцінки ризиків, зробити його більш прозорим, а також чітко визначити критичні фактори.

Розглянемо одну з класифікацій, за якою виокремлені крупні класи загроз інформаційної безпеки:

несанкціонований доступ і копіювання інформації;

інформаційна фальсифікація (нав'язування помилкової інформації);

порушення початкової функціональності (програм і апаратно-програмних засобів).

Клас несанкціонованого доступу і копіювання інформації містить ряд підкласів, що описують засоби процесу здійснення доступу:

доступ до аутентифікаційної інформації (для подальшого доступу в ІС у якості легітимного користувача);

несанкціонований доступ і копіювання службової інформації (про роботу системи);

несанкціоноване копіювання призначеної для користувача інформації;

доступ до механізмів управління обробкою і зберіганням інформації;

доступ до каналу передачі даних.

Клас інформаційної фальсифікації містить наступні підкласи:

в процесі аутентифікації;

модифікація інформації, що зберігається;

в процесі штатної взаємодії з системою (наприклад, XSS-атака).

Клас загроз порушення початкової функціональності містить підкласи:

повне руйнування функцій управління;

знищення інформації, що зберігається і оброблюється;

блокування можливості управління (знищення/модифікація ключів, паролів і так далі);

цілеспрямована зміна початкової функціональності (наприклад, внесення інженерного пароля або проведення SQL ін'єкції, включення стороннього PHP-коду).

Розглянемо засіб оцінювання інформаційних ризиків, спираючись на наведену вище ієрархічну класифікацію загроз.

Доцільність застосування методів теорії ймовірностей для прогнозування суттєвості впливу загроз на рівень ризиків випливає із самого поняття ризиків. Для оцінки і урахування комплексного впливу загроз на рівень ризику застосуємо поняття умовної ймовірності та формули повної ймовірності [6], які реалізуються через такі умови:

Нехай A, B - дві події. Умовною ймовірністю появи події A за умови впливу події B назвемо вираз $P(A/B)$.

Послідовність подій $\{H_i\}_{i=1}^{n}$, $H_i \subseteq U$ утворює повну групу подій, якщо: $H_i \cap H_j = \varnothing$, $(i \neq j)$; $\bigcup_{i-1}^{n} H_j = \Omega$, $(n \leq \infty)$, де $\varnothing$ - неможлива подія, Ω – вірогідна подія.

Будемо вважати, що $\{H_i\}$ - повна група подій, кожна з яких має ненульову ймовірність $P(H_i) \neq 0$, $P\left(A/H_i\right)$ - умовна ймовірність (подія А відбувається

при появі події H_i). Ймовірність появи події А при $A \subseteq U$, визначимо формулою повної ймовірності:

$$P(A) = \sum_{i-1}^{n} P(H_i) \cdot P\left(A / H_i\right) \quad (1)$$

Приймаючи до уваги класифікацію загроз, алгоритм їхнього оцінювання представимо у вигляді трирівневої ієрархічної класифікації та перезначимо загрози (рис.).

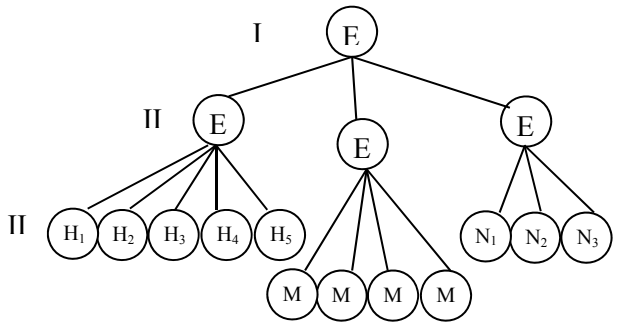

Рис. Позначення елементами загроз у ієрархічній класифікації

де E - рівень сукупного ризику;

E_1 , E_2 , E_3 - оцінка суттєвості впливу загроз на рівень інформаційного ризику;

H_1, H_2, H_3, H_4, H_5 - оцінка суттєвості впливу загроз класу несанкціонованого доступу і копіювання інформації;

M_1, M_2, M_3, M_4 - оцінка суттєвості впливу загроз порушення початкової функціональності;

N_1, N_2, N_3 - оцінка суттєвості впливу загроз інформаційної фальсифікації.

Визначаємо повні групи подій на кожному рівні ієрархії впливу загроз на рівень ризиків:

для E повною групою подій є E_1, E_2, E_3 ;

для E_1 повною групою подій є H_1, H_2, H_3, H_4, H_5 ;

для E_2 повною групою подій є M_1, M_2, M_3, M_4 ;

для E_3 аналогічно - N_1, N_2, N_3 .

Використовуючи методи теорії ймовірностей [6], записуємо формулу повної ймовірності для визначених в нашому випадку повних груп подій на кожному рівні ієрархії впливу загроз на рівень інформаційного ризику.

На I рівні ієрархічної класифікації формула повної ймовірності для визначення впливу загроз на рівень ризику набуватиме вигляду:

$$P(E) = \sum_{i-1}^{3} P(E_i) \cdot P\left(E / E_i\right) = P(E_1) * \\ * P\left(E / E_1\right) + P(E_2) \cdot P\left(E / E_2\right) + P(E_3) \cdot P\left(E / E_3\right), \quad (2)$$

де $P(E)$ - ймовірнісна оцінка рівня ризику виражена за допомогою формули повної ймовірності – I рівень ієрархії у моделі;

$\sum_{i=1}^{n} P(E_i) \cdot P\left(E / E_i\right)$, при $n = 3$ - умовні ймовірності сукупного впливу чинників II рівня ієрархії на I рівень ієрархії у класифікації на рівень ризику.

На II рівні ієрархічної класифікації вплив чинників на вищий рівень ієрархії визначається за допомогою формули повної ймовірності у такому вигляді:

$$P(E_1) = \sum_{j=1}^{s} P\left(E_i / H_j\right) \cdot P(H_j), \quad (3)$$

де $P(E_1)$ - значення суттєвості впливу загроз класу несанкціонованого доступу виражене через вплив чинників нижчого рівня ієрархії;

H_j - чинники, що впливають на чинник E_1 на II рівні ієрархії;

$P(H_j)$ - ймовірнісна оцінка впливу чинника H_j на рівень ризику;

j – порядковий номер чинників II рівня ієрархії;

s - кількість чинників впливу на чинник E_1 на II рівня ієрархії ($s = 5$).

Аналогічно можна записати формули повної ймовірності для визначення впливу чинників II рівня ієрархії на інші чинники I рівня ієрархії класифікації, відповідно $P(E_2)$ через вплив чинників групи M_j $(j = 4)$ та $P(E_3)$ через вплив чинників групи N_j $(j = 3)$.

Для визначення ймовірнісного показника сукупного впливу загроз на рівень ризику через оцінки впливу загроз I та II рівня ієрархічної класифікації з урахуванням умовних позначень запишемо формулу повної ймовірності таким чином:

$$P(E) = \sum_{j=1}^{5} P(H_j) \cdot P\left(E_1 / H_j\right) \cdot P\left(E / E_1\right) + \sum_{j-1}^{4} P(M_j) \cdot P\left(E_2 / M_j\right) \cdot \\ \cdot P\left(E / E_2\right) + \sum_{j=1}^{3} P(N_j) \cdot P\left(E_3 / N_j\right) \cdot P\left(E / E_3\right), \quad (4)$$

де повні ймовірності впливу груп загроз є складовими формули 4:

$\sum_{j=1}^{n} P(H_j) \cdot P\left(E_1 / H_j\right)$, $n = 5$, - повні ймовірності впливу групи загроз несанкціонованого доступу і копіювання інформації нижчого рівня ієрархії на чинники вищого рівня ієрархії;

$\sum_{j=1}^{n} P(M_j) \cdot P\left(E_2 / M_j\right)$, $n = 4$, - повні ймовірності впливу групи загроз порушення початкової функціональності нижчого рівня ієрархії на чинники вищого рівня ієрархії;

$\sum_{j=1}^{n} P(N_j) \cdot P\left(E_3 / N_j\right)$, $n = 3$ - повні ймовірності впливу групи загроз інформаційної фальсифікації нижчого рівня ієрархії на чинники вищого рівня ієрархії; $P(E_1)$, $P(E_2)$, $P(E_3)$ - ймовірнісні оцінки впливу загроз II рівня ієрархії на показник інформаційного ризику;

$P\left(E / E_k\right)$, $k = 3$ - умовна ймовірність впливу загроз II рівня ієрархії на рівень інформаційного ризику.

В процесі управління ризиками можна виокремити наступні етапи: вибір аналізованих об'єктів і рівня деталізації їх розгляду, вибір методики оцінки ризиків, ідентифікація активів, аналіз загроз і їх наслідків, визначення уразливостей в захисті, оцінка ризиків, вибір захисних засобів, реалізація і перевірка вибраних засобів, оцінка залишкових ризиків. Шостий і сьомий етапи відносяться до процедури вибору захисних засобів (нейтралізація ризиків), останні — до оцінки ризиків. Аналіз складових процесу управління ризиками також доводить, що управління ризиками — процес циклічний. За суттю, останній етап — це оператор кінця циклу, який дає наказ повернутися до початку. Ризики потрібно контролювати постійно, періодично проводячи їх переоцінку, тому запропонований засіб має незаперечні переваги завдяки простоті та відносно низької коштовності реалізації моделі на відміну від запропонованих раніше.

Висновки. Інформаційна безпека є місткою, складною і актуальною проблемою. В умовах постійних змін та розвитку інформаційної системи підприємства побудова комплексу інформаційної безпеки повинна ґрунтуватись на застосуванні оцінки інформаційних ризиків. Розроблені методичні рекомендації реалізують ієрархічну класифікацію ранжування загроз і дають змогу оцінити їх сукупний вплив на рівень інформаційного ризику за допомогою ймовірнісних показників. Такі рекомендації є основою для побудови системи захисту інформації та вибору адекватних методів регулювання інформаційної безпеки. Розробка методики формування комплексу інформаційної безпеки за визначеними підходами є напрямком наступних досліджень.

Література

1. Архипов А.Е., Кущ С.М., Шутовский В.О. Сравнение количественных оценок рисков при использовании теории нечетких множеств // «Технології безпеки інформації» Збірка тез доповідей учасників. – К.: 2007. – с. 30.
2. Астахов А.М. Искусство управления информационными рисками / А.М. Астахов. –М.: ДМК Пресс, 2010. – 312 с.
3. Бармен С. Разработка правил информационной безопасности.: Пер. с англ. - М.: Издательский дом «Вильямс», 2002. - 208 с.
4. Гончар С.Ф. Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом / С. Ф. Гончар // Захист інформації. – 2014. – № 1 (16). – С. 40–46.
5. Домарев В.В. Безопасность информационных технологий. Системный подход: - К.: ООО «ТИД «Диасофт»», 2004. – 992с.
6. Королюк В.С., Портенко Н.И., Скороход А.В., Турбин А.Ф. Справочник по теории вероятностей и математической статистике. - М.: Наука, 1985. – 262 с.
7. Корченко А.Г. Построение систем защиты информации на нечетких множествах. – К.:«МК-Пресс», 2006. – 316 с.
8. Петренко С.А., Симонов С.В. - Управление информационными рисками. Экономически оправданная безопасность – М.: ДМКпрес, 2004. – 392 с.
9. Плетнев П.В. Методика оценки рисков информационной безопасности : докл. ТУСУРа [Электронный ресурс] / П.В. Плетнев, В.М. Белов. – Режим доступа: www.tusur.ru/filearchive/reports-magazine/2012-25-2/083.p
10. Черныш В.И. Методы оценивания информационных рисков компании [Текст] / В.И.Черныш // Материалы XV Международного юбилейного м о- лодёжного форума «Радиоэлек т роника и молодежь в XXI веке»: с б. тезисов, 18 – 20 апреля 2011 р., Т.5. - Харьков: ХНУРЭ , 2011. – С . 195.
11. Черней Г.А. Оценка угроз безопасности автоматизированным информационным системам [Электронный ресурс] / Г.А. Черней. – Режим доступа http://security.ase.md/publ/ru/pubru01.html

References

1. Arkhipov A.E., Kushch S.M., Shutovsky V.O. Comparison of quantitative risk assessments using the theory of fuzzy sets // “Information Security Technologies” Collection of abstracts from participants' reports. – K.: 2007. – p.30.
2. Astakhov A.M. The art of information risk management / AM Astakhov. -M.: DMK Press, 2010. – p.312.
3. Barman S. Writing Information Security Policies.: -IN.: New Riders, 2002, - p.208.
4. Gonchar SF Probability analysis of threats realization in information protection of technological processes’ automated control systems / S.F.Gonchar // Information protection. - 2014 - No. 1 (16). - P. 40-46.
5. Domarev V.V. Security of information technologies. The system approach: - K .: LLC «TID «Diasoft», 2004. – p.992.
6. Korolyuk V.S., Portenko N.I., Skorokhod A.V., Turbin A.F. A handbook on probability theory and mathematical statistics. – M.: Nauka, 1985. – p.262.
7. Korchenko A.G. Construction of information security systems using fuzzy sets. - K.: "MK-Press", 2006. – p.316.
8. Petrenko S.A., Simonov S.V. Information Risks Management. Economically justified safety - M.: DMK Press, 2004. – p.392.
9. Pletnev P.V. Method of assessing risks to the information security: Dokl. TUSUR [Electronic resource] / P.V. Pletnev, V.M. Belov. - Access mode: www.tusur.ru/filearchive/reports-magazine/2012-25-2/083.p
10. Chernysh V.I. Methods of assessing the company's information risks [Text] / Chernysh V.I. // Proceedings of the XV International Anniversary Youth Forum "Radioelectronics and Youth in the 21st Century": with b. theses, April 18 - 20, 2011, T.5. - Kharkov: KHNURE, 2011. - p.195.
11. Cherney G.A. Estimation of Security Threats to Automated Information Systems [Electronic resource] / G.A. Cherney. - Access mode http://security.ase.md/publ/en/pubru01.html.

Степанова Е.М., Волков А.А. Оценка информационных рисков в условиях развития информационной системы предприятия

В статье определены этапы процесса оценки рисков, обосновано использование вероятностно подхода к оценке информационных рисков, предложена методика оценки совокупного воздействия угроз на уровень информационного риска на основе их иерархической классификации с помощью вероятностных показателей, выделены этапы управления информационными рисками.

***Ключевые слова**: информационная система, информационный риск, оценка, иерархическая классификация, вероятность.*

Stepanova E.M., Volkov A.A. Assessment of the information risks in the conditions of the enterprise information system developtment

In this article, we define stages of the risks assessment, substantiate the use of a probabilistic approach to the assessment of information risks, suggest a methodology for assessing the combined impact of threats on the level of information risk based on their hierarchical classification using probabilistic indicators and identify stages of the information risk management.

***Key words**: information system, information risk, evaluation, hierarchical classification, probability.*

Степанова О.М. – к.е.н., доцент, доцент кафедри менеджменту та маркетингу Східноукраїнського національного університету ім.В.Даля, e-mail: stepelen@gmail.com

Волков А.А. – магістр, менеджер (управитель) з адміністративної діяльності, PR-менеджер, ТОВ «PublBox», e-mail: andrii.volkov.1990@gmail.com

Рецензент: д.т.н, д.е.н, проф. ***Рамазанов С.К.***

Стаття подана 15.12.2017.