DOI 10.31891/2307-5732-2024-341-5-75
УДК 004.023

ТІТОВА ВІРА
Хмельницький національний університет
https://orcid.org/0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ ЮРІЙ
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
КАЛЬЧУН БОГДАН
Хмельницький національний університет
e-mail: bkalchun27@gmail.com
КУВІЛА АННА
Хмельницький національний університет
e-mail: anyuakuvila@gmail.com
РАК ІРИНА
Хмельницький національний університет
e-mail: irarak928@gmail.com

МЕТОДИКА ІДЕНТИФІКАЦІЇ ТА ОЦІНЮВАННЯ ВАЖЛИВОСТІ ІНФОРМАЦІЙНИХ АКТИВІВ

У даній статті було проведено аналіз стандартів та практик у галузі ідентифікації та оцінювання важливості інформаційних активів організації. Було розглянуто підходи та способи ідентифікації та оцінювання важливості інформаційних активів організації при оцінці ризиків інформаційної безпеки. На підставі отриманих знань було розроблено методику ідентифікації та оцінювання важливості інформаційних активів, яка визначає важливість інформаційного активу на діяльність організації.

Ключові слова: модель загроз, інформаційна безпека, управління ризиками, інформаційні активи, оцінювання важливості.

TITOVA VIRA, KLOTS YURII, KALCHUN BOHDAN, KUVILA ANNA, RAK IRYNA
Khmelnitskyi National University

METHOD OF IDENTIFICATION AND INFORMATION ASSETS IMPORTANCE ASSESSMENT

The work of determining the value of information assets across the entire organization is both the most significant and the most difficult. It is the assessment of information assets that will allow the head of the IS department to choose the main areas of activity to ensure information security. First of all, when carrying out this procedure, it is necessary to obtain information about the organization's assets, which are used in its daily activities. The value of the asset is expressed by the amount of losses that the organization suffers in the event of a security breach of the asset.

A threat has the potential to harm assets such as information, processes and systems, and therefore the organization itself. Threats can be of various origins: natural, man-made or anthropogenic; can be intentional or accidental. All sources of threats to assets must be taken into account during identification. The purpose of the process of identification and assessment of the importance of information assets is to obtain importance values for the selected assets of the organization. The result of this process is important both for risk assessment and for understanding the need for IS measures.

In this article, an analysis of international and domestic standards and practices in the field of identification and assessment of the importance of the organization's information assets was carried out, as well as approaches and methods of identification and assessment of the importance of the organization's information assets in the assessment of information security risks were considered. Based on the results of the performed analysis, a method of identification and assessment of the importance of the organization's information assets was developed.

As a result of the work, the implementation of a more advanced approach to risk management and, accordingly, information security was achieved.

Keywords: threat model, information security, risk management, information assets, importance assessment.

Постановка проблеми

На даний час управління інформаційними ризиками є одним з найбільш актуальних напрямів стратегічного та оперативного менеджменту в галузі захисту інформації. Його основне завдання – об'єктивно ідентифікувати та оцінити найбільш значущі для бізнесу інформаційні ризики організації, а також адекватність засобів контролю ризиків, що використовуються для збільшення ефективності та рентабельності економічної діяльності організації. Оцінювання важливості інформаційних активів є початковим кроком у процесі управління інформаційними ризиками.

Робота з визначення цінності інформаційних активів у розрізі всієї організації одночасно найбільш значуща і складна. Саме оцінювання інформаційних активів дозволить начальнику відділу інформаційної безпеки (ІБ) обрати основні напрямки діяльності із забезпечення захисту інформації. Насамперед при проведенні даної процедури необхідно отримати відомості про активи організації, що використовуються у її повсякденній діяльності. Цінність активу виражається величиною втрат, які зазнає організація у разі порушення безпеки активу.

Метою процесу ідентифікації та оцінювання важливості інформаційних активів є отримання значень важливості для обраних активів організації. Результат цього процесу важливий як для проведення оцінювання ризиків, так і для розуміння необхідності заходів у сфері ІБ.

Формулювання цілей статті

В результаті ідентифікації активів повинні бути розглянуті всі активи в рамках визначених на етапі встановлення контексту оцінювання кордонів та області оцінювання ризиків ІБ. Для виконання цього завдання доцільно використовувати опис об'єкта оцінювання, отриманий при встановленні кордонів та області оцінювання ризиків ІБ, а також опис основних та допоміжних активів організації.

Основною метою ідентифікації активів є визначення найважливіших з точки зору цілей діяльності організації інформаційних активів, а також допоміжних активів, що забезпечують належні збирання, обробку та зберігання таких активів, які, у свою чергу, крім власної вартості як майна організації, мають цінність як засіб обробки більш цінного інформаційного активу.

Оцінювання важливості ідентифікованих активів має проводитись у рамках процесу оцінювання ризиків, проте часто розглядається та реалізується як самостійний процес, результати якого несуть цінну інформацію для керівництва та служби безпеки організації.

До кожного інформаційного активу має бути визначено його тип, бізнес-процес, у якому він бере участь, використовуваний технічний засіб, підрозділ, у якому даний актив обробляється. За допомогою визначення впливу різних факторів на інформаційних активів обчислюються відповідні значення оцінювання важливості.

Результатом організації цього процесу має стати сформований перелік активів, оцінених з погляду їх важливості для організації та класифікованих за їх можливими типами.

Огляд існуючих рішень

Перед тим, як отримати вихідні дані для ідентифікації та оцінювання активів, необхідно визначити межі розгляду. Місце процесу ідентифікації та оцінювання важливості інформаційних активів у моделі управління ризиками інформаційної безпеки можна побачити на рисунку 1.

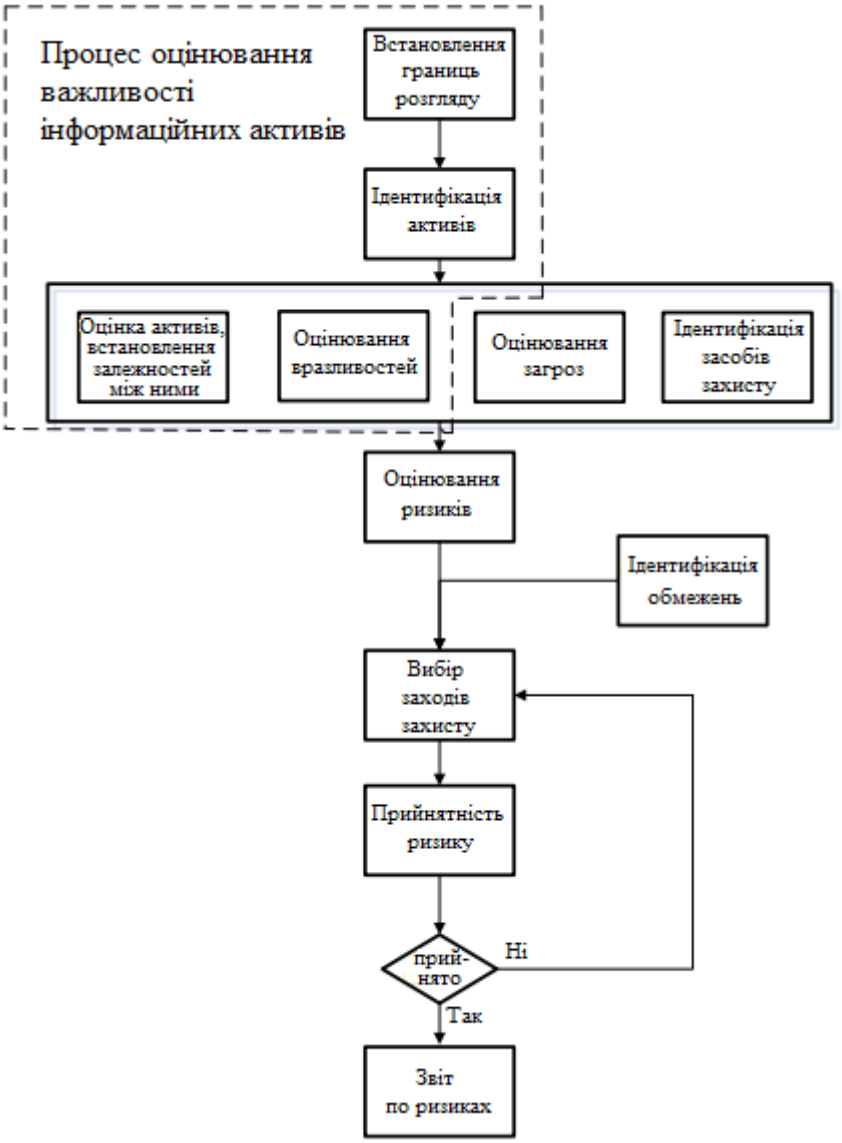

Рис. 1. Місце оцінювання важливості інформаційних активів в моделі менеджменту ІБ

Ретельне визначення меж на цій стадії аналізу ризику дозволяє уникнути непотрібних операцій та підвищити якість аналізу ризику. Встановлення меж розгляду має чітко визначити, які з наведених нижче ресурсів мають бути враховані під час розгляду результатів аналізу ризику Для конкретної системи інформаційних технологій враховують:

- активи інформаційних технологій (наприклад, апаратні засоби, інформаційне забезпечення, інформація);
- службовців (наприклад, персонал організації, субпідрядники, персонал сторонніх організацій);
- умови провадження виробничої діяльності (наприклад, будівлі, обладнання);
- ділову діяльність (операції) [1].

Оцінювання активів організації є важливим етапом у загальному процесі ідентифікації та оцінювання ризику ІБ та взагалі у системі менеджменту ризику організації. Для того, щоб виконати оцінювання активів організації, в першу чергу потрібно визначити область оцінювання важливості інформаційних активів та ідентифікувати всі активи організації, а потім розпочати оцінювання важливості.

Існує чотири різні підходи до оцінювання ризиків (ОР) ІБ:

- базова ОР;
- неформальна ОР;
- детальна ОР;
- комбінована ОР, що складається з комбінації базової, неформальної або детальної ОР.

При базовій ОР використовується єдиний підхід до всіх систем та компонентів інформаційних систем. Ця ОР використовується у тому випадку, якщо організація не може або не вважає за потрібне витрачати час та засоби до вибору захисних заходів без попереднього оцінювання. Можливі два способи застосування базової ОР:

- вибір захисних заходів відповідно до типу та характеристик аналізованої системи;
- вибір захисних заходів відповідно до цілей, політиків та загроз ІБ.

Базові захисні заходи можна визначити в різних каталогах захисних заходів. Каталоги можуть визначати самі захисні заходи або вони можуть визначати безліч вимог ІБ, які повинні бути виконані за допомогою будь-яких захисних заходів, що підходять для даної системи. Переваги: потрібні мінімальні ресурси для вибору та реалізації захисних заходів. Недоліки: якщо базовий рівень встановлений надто високим, то для деяких систем рівень може бути надмірним і навпаки. Таким чином, якщо всі активи мають приблизно однакові вимоги щодо значущості та практичності впливу загроз, то базовий підхід найбільш ефективний.

Неформальна ОР ґрунтується на використанні знання та досвіду окремих осіб. Переваги: мінімальна витрата ресурсів та часу. Недоліки: висока ймовірність того, що не будуть враховані деякі аспекти забезпечення ІБ, можливість виникнення проблем із забезпечення ІБ, якщо особа, яка проводила ОР, йде з організації на ОР ІБ сильно впливає суб'єктивність підходу розробника та його переваги. Неформальна ОР не є ефективним підходом для багатьох організацій та систем.

Детальна ОР. Переваги: адекватність захисних заходів активам, що захищаються. Недоліки: значний час та ресурси, що витрачаються на реалізацію. Процеси детальної ОР: визначення сфери застосування та меж ОР ІБ; визначення цінності активів; аналіз та оцінювання загроз ІБ; аналіз та оцінювання вразливостей ІБ; аналіз та оцінювання існуючих захисних заходів; якісне чи кількісне ОР ІБ.

Для визначення меж оцінювання необхідно враховувати такі елементи: особливості організації (визначені. через цілі особливості бізнесу та структуру організації); корпоративну політику; обмеження, що впливають на організацію (стратегічні, територіальні економічні, структурні, функціональні, бюджетні); правові, регулюючі та договірні вимоги; архітектура інформаційної системи.

Для визначення цінності активів необхідно визначити критерії та шкалу. Критерії такі:

- критерії оцінювання активів з погляду наслідків та витрат, пов'язані із втратою конфіденційності, цілісності, доступності, невідмовності;
- критерії на основі оцінювання вихідної вартості активів, вартості заміни активів, оцінювання абстрактної цінності (репутація).

Результатом цього етапу детальної ОР має бути перелік вразливостей та оцінювання можливості їх виконання.

Виклад основного матеріалу

Загроза має потенціал заподіяння шкоди активам, таким, як інформація, процеси та системи, а, отже, і самої організації. Загрози може бути різного походження: природного, техногенного чи антропогенного; можуть мати навмисний або випадковий характер. При ідентифікації мають бути враховані всі джерела загроз активам.

Для кількісного оцінювання ймовірності загроз необхідно мати формальну модель порушника, яка передбачає різні можливості порушника щодо доступу до інформаційних ресурсів та технічних можливостей реалізації загроз. Джерелом загроз у формальній моделі є зовнішній або внутрішній суб'єкт, який отримав деякі можливості доступу до мережі зі штатними засобами автоматизованої системи та засобів обчислювальної техніки, що має певний рівень знань у галузі експлуатації та захисту.

Нижче представлена формальна модель порушника передбачає п'ять рівнів цих можливостей.

Перший рівень – відсутність повноважень доступу до ресурсів корпоративної мережі. Порушник першого рівня не має в своєму розпорядженні імен зареєстрованих користувачів мережі.

Другий рівень – порушник має повноваження на запуск низки завдань (програм) з фіксованого набору, що реалізує заздалегідь передбачені функції з обробки інформації. Як правило, це користувачі мережі, права яких визначаються у прийнятій безпековій політиці.

Третій рівень – визначається можливістю порушника створення та запуску власних програм із новими функціями з обробки інформації. Користувачами третього рівня повноважень найчастіше є зовнішні інформаційні посередники. Він може мати у своєму розпорядженні будь-які фрагменти інформації про топологію та технічні засоби обробки інформації мережі, будь-які фрагменти конфіденційних даних, до яких даний користувач має доступ.

Четвертий рівень визначається можливістю функціонуванням управління інформаційної системи, тобто впливом на базове програмне забезпечення системи, склад і конфігурацію устаткування мережі. Користувачами четвертого рівня найчастіше є внутрішні інформаційні посередники. Вони мають повноваження системного адміністратора стосовно частини технічних засобів обробки інформації, мають повну інформацію про мережу, доступ до всіх технічних засобів обробки даних, крім шифрування даних та засобів протоколювання дій операторів.

П'ятий рівень визначається можливістю доступу до засобів захисту інформації та протоколювання дій операторів, частини криптографічних ключів. Користувачами п'ятого рівня є найчастіше співробітники служби ІБ [2].

На підставі даних для зазначених параметрів виставляються оцінки.

Так, наприклад, якщо джерело антропогенного характеру, то залежно від його рівня, йому присвоюється оцінка від 0 до 2, таким чином: 0 – низький – джерело антропогенного характеру першого рівня; 1 – середній – джерело антропогенного характеру другого та третього рівня; 2 – високий – джерело антропогенного характеру четвертого та п'ятого рівня.

Залежно від складності виявлення реалізації загрози виставляються такі оцінки: 0 – низька складність виявлення; 1 – середня складність виявлення; 2 – висока складність виявлення.

Для захисних заходів також вказуються такі оцінки: 0 – захисні заходи запобігають можливості реалізації загрози; 1 – захисні заходи ускладнюють можливість реалізації загрози; 2 – захисні заходи спрямовані лише на зменшення шкоди у внаслідок реалізації загрози і у разі, якщо вони не впливають на реалізації загрози. За сукупністю цих оцінок визначається можливість реалізації загрози даним джерелом для активу.

Для оцінювання можливості використання вразливості для реалізації загрози враховуються такі параметри як: наявність уразливості та наявність захисних заходів. Якщо для аналізованої загрози для даного активу немає вразливості, яка могла б бути використана, можливість використання вразливості дорівнює 0.

Якщо вразливість все ж таки є, то розглядаються захисні заходи та виставляються оцінки: 0 – захисні заходи запобігають можливості використання вразливості; 1 – захисні заходи ускладнюють можливість використання вразливості; 2 – захисні заходи не впливають на можливість використання вразливості чи захисних заходів немає.

Для важливості активу визначаються: 0 – персональна інформація; 1 – оперативна інформація; 2 – тактична інформація; 3 – стратегічна інформація.

Вихідними даними для ОР ІБ є: перелік активів та відповідні їм оцінювання важливості; оцінювання можливості реалізації загрози; оцінювання можливості використання вразливості [3, 4].

Оцінювання ризиків ІБ проводиться за допомогою таблиці 1.

Якщо в процесі аналізу загроз для цієї загрози було зафіксовано захисний захід, то обчислюється початковий та залишковий ризик. Початковий ризик передбачає оцінювання ризику без урахування захисних заходів. Залишковий ризик – ризик, що залишився після застосування захисних заходів. Такий підхід до оцінювання ризику дозволяє визначити ефективність вжитих захисних заходів [5].

При необхідності визначення того, який ризик є допустимим, а який ні, вводиться межа допустимості ризику і всі значення вище зазначеного вважаються неприпустимими. При цьому слід враховувати, що рівний 7-ми ризик є максимальним, а 0 – мінімальним.

Таблиця 1

Матриця ризиків

Можливість реалізації загрози		**Низька**			**Середня**			**Висока**		
Можливість використання вразливості		**0**	**1**	**2**	**0**	**1**	**2**	**0**	**1**	**2**
Значення цінності активів	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7

Висновки

В дані статті було проведено аналіз міжнародних та вітчизняних стандартів та практик у галузі ідентифікації та оцінювання важливості інформаційних активів організації, а також було розглянуто підходи та способи ідентифікації та оцінювання важливості інформаційних активів організації при ОР ІБ. За результатами виконаного аналізу було розроблено методику ідентифікації та оцінювання важливості інформаційних активів організації. В результаті роботи було досягнуто реалізацію більш досконалого підходу до управління ризиками та, відповідно, ІБ.

Література

,

1. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE/ Ю.М. Якименко, Т.М. Мужанова, С.В. Легомінова// Кібербезпека: освіта, наука, техніка. №4 (12). 2021. С. 36-50.

2. Класифікація моделей систем захисту інформації/ Клочкова Д.Ю., Пшеничних С.В.// ІКТК-2023. Харків. С. 196-197.

3. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT)

4. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства/ Карпович І.М., Гладка О.М., Наконечна Ю.А// Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. Т. 31 (70). № 5. 2020. С.69-74.

5. Інформаційна безпека: курс лекцій./ Нестеренко Г. Київ: НАУ, 2022. 102 с.

References

1. . Systemnyi analiz tekhnichnykh system zabezpechennia informatsiinoi bezpeky pidpryiemstv vid kompanii FIREEYE/ Yu.M. Yakymenko, T.M. Muzhanova, S.V. Lehominova// Kiberbezpeka: osvita, nauka, tekhnika. №4 (12). 2021. S. 36-50.

2. Klasyfikatsiia modelei system zakhystu informatsii/ Klochkova D.Iu., Pshenychnykh S.V.// IKTK-2023. Kharkiv. S. 196-197.

3. DSTU ISO/IEC 27005:2015 Informatsiini tekhnolohii. Metody zakhystu. Upravlinnia ryzykamy informatsiinoi bezpeky (ISO/IEC 27005:2011, IDT)

4. Analiz ryzykiv bezpeky informatsiinoi systemy IT-pidpryiemstva/ Karpovych I.M., Hladka O.M., Nakonechna Yu.A// Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: tekhnichni nauky. T. 31 (70). № 5. 2020. S.69-74.

5. Informatsiina bezpeka: kurs lektsii./ Nesterenko H. Kyiv: NAU, 2022. 102 s.