DOI: https://doi.org/10.32782/2524-0072/2021-31-12

УДК 65.011.3:658

УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНИХ СИСТЕМ: ЕТАПИ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ

RISK MANAGEMENT OF INFORMATION SYSTEMS: STAGES OF THE RISK MANAGEMENT PROCESS

Терещенко Лариса Олександрівна
кандидат економічних наук, професор,
Український гуманітарний інститут
ORCID: https://orcid.org/0000-0003-0680-5259

Tereshchenko Larisa
Ukrainian Institute of Arts and Sciences

Використання інформаційних систем (ІС) пов'язано з певною сукупністю ризиків. Під ризиком, як правило, розуміється можливість того, що будь-які цілі під час реалізації проєкту автоматизації діяльності підприємства не будуть досягнуті. Аналізу факторів ризику передують: планування заходів для зниження впливу факторів ризику на результат проєкту і прийняття рішень на різних етапах процесу створення інформаційної системи. Усі суб'єкти, які беруть участь і приймають рішення у процесі автоматизації підприємства (замовник – підприємство і системний інтегратор – постачальник), здійснюють аналіз ризиків кожний зі своєї позиції. Тому необхідно вжити економічно виправдані заходи захисту, коли можливий збиток неприйнятно великий, З точки зору інформаційної безпеки, періодичне переоцінювання ризиків є необхідним для контролю ефективності діяльності в галузі інформаційної безпеки,

Ключові слова: ризики інформаційних систем. ризики інформаційної безпеки, фактори ризику, оцінка ризиків. управління ризиками, заходи захисту.

Использование информационных систем (ІС) связано с определенной совокупностью рисков. Под риском, как правило, понимается возможность того, что любые цели во время реализации проекта автоматизации деятельности предприятия не будут достигнуты. Анализу факторов риска предшествуют: планирование мер для снижения влияния факторов риска на результат проекта и принятие решений на разных этапах процесса создания информационной системы. Все субъекты, которые принимают участие и принимают решение в процессе автоматизации предприятия (заказчик – предприятие и системный интегратор – поставщик), осуществляют анализ рисков каждый со своей позиции. Поэтому необходимо употребить экономически оправданные меры защиты, когда возможный убыток неприемлемо большой, С точки зрения информационной безопасности, периодическое переоценивание рисков есть необходимым для контроля эффективности деятельности в области информационной безопасности.

Ключевые слова: риски информационных систем. риски информационной безопасности, факторы риска. оценка рисков. управление рисками. меры защиты.

The use of information systems (IS) is associated with a certain set of risks. Any assessment of information security risks begins with an inspection of the information system, identification of information resources and a description of information processing technologies. Risk, as a rule, means the possibility that a certain goal will not be achieved during the implementation of the project of automation of the enterprise. The analysis of risk factors is preceded by: planning measures to reduce the impact of risk factors on the outcome of the project and decision-making at various stages of the process of creating an information system. Risk analysis is a procedure for identifying information security (IS) risk factors and assessing their severity. IS risk analysis includes risk assessment and methods to reduce risks or reduce the associated adverse effects. The analysis first identifies the relevant factors and assesses their severity; the completeness of the identified factors increases the quality and accuracy of the predicted risks [1]. All entities that participate and make decisions in the process of enterprise automation (customer – enterprise and system integrator – supplier), carry out risk analysis, each one from his own position. Therefore, it is necessary to take economically justified protection measures when the possible damage is unacceptably large. To monitor the effectiveness of information security, periodic reassessment of risks is necessary, from the point of view of information security. Resources on the likelihood of such a breach and as part of business risks and handled in a similar manner.

Thus, the overall risk assessment allows to implement the necessary measures at the level of departments, projects, specific risks or at the level of the organization as a whole. Upon completion of the overall risk assessment, risk processing is performed, which involves the adoption of one or more appropriate options that reduce the likelihood of risks and their impact on the information system.

Keywords: risks of information systems. information security risks, risk factors, risk assessment. risk management.

Постановка проблеми. Використання інформаційних систем (ІС) пов'язане з певною сукупністю ризиків. В разі, якщо можливий збиток надто великий, необхідно вживати економічно виправдані заходи щодо захисту. Періодична оцінка ризиків необхідна для контролю ефективності діяльності в сфері безпеки. Ризик інформаційної безпеки розглядають як порушення конфіденційності, цілісності, автентичності, доступності до інформаційних ресурсів і як частину бізнес-ризиків. Суть заходів щодо управління ризиками полягає в оцінені їх розміру, виробленні ефективних економічних заходів щодо зниження ризиків.

Формулювання цілей статті. Метою статті є розгляд концепції формування системи управління ризиками інформаційних систем, етапи процесу управління ризиками

Аналіз досліджень і публікацій. Питання управління ризиками в сучасних умовах є одним з найбільш істотних управлінських процесів. Це стосується і управління ризиками інформаційних систем, що є предметом дослідження. Теоретико-методологічні та практичні аспекти управління ризиками інформаційних систем та етапи процесу управління ризиками досліджуються у працях Ібадулаева В.А., Космачева В.П., Терещенко Л.О., Гужко С.В., Шайкан А.В., Андрианова В., Зефирова С.Л., Голованова В.Б. та ін. науковців. Проте, розгляд даного питання та його актуальність не втрачається і потребує детальнішого розгляду й аналізу.

Виклад основних матеріалів дослідження. Управління ризиками в сучасних умовах є одним з найбільш істотних управлінських процесів. Це стосується і управління ризиками інформаційних систем. З кількісного погляду рівень ризику є функцією ймовірності реалізації певної загрози, а також величини можливого збитку.

Управління ризиками включає два види діяльності, а саме, які працюють циклічно, це оцінка ризиків та вибір ефективних і економічних заходів.

Процес управління ризиками можна поділити на такі етапи:

I. Вибір аналізованих об'єктів і рівня деталізації їх розгляду.

II. Вибір методології оцінки ризиків.

III. Ідентифікація активів.

IV. Аналіз загроз і їх наслідків, виявлення вразливих місць у захисті.

V. Оцінка ризиків.

VI. Вибір захисних заходів.

VII. Реалізація і перевірка вибраних заходів.

VIII. Оцінка залишкового ризику.

Шостий та сьомий етапи відносяться до вибору захисних засобів (нейтралізації ризиків), інші – до оцінки ризиків.

Управління ризиками, наведений у переліку етапів – процес циклічний.

Ризики слід постійно контролювати, періодично проводячи їх переоцінку. Управління ризиками необхідно інтегрувати в життєвий цикл інформаційної системи, як діяльність в галузі інформаційної безпеки і ефект виявиться найбільшим з мінімальними витратами.

Відповідно до етапів життєвого циклу, слід зазначити, що може дати управління ризиками на кожному з них, а саме:

на 1-му етапі – етапі ініціації, під час розробки вимог до системи взагалі і до засобів безпеки зокрема слід врахувати відомі ризики;

на 2-му етапі – розробки або закупівлі, саме знання ризиків допоможе вибрати відповідні архітектурні рішення, які відіграють ключову роль в гарантуванні безпеки;

на 3-му етапі – етапі встановлення, виявлені ризики слід враховувати під час конфігурації, тестування і перевірки вимог, які були сформульовані раніше, а цикл управління ризиками має відбуватися раніше за впровадження системи в експлуатацію;

на 4-му етапі – етапі експлуатації, управління ризиками повинно супроводжувати всі зміни в системі.

У разі виведення системи з експлуатації управління ризиками допомагає переконатись у тому, що міграція даних відбувається безпечно [3].

Вибір аналізованих об'єктів і рівень деталізації їх розгляду – це перший крок в оцінці ризиків. Для невеликої компанії допустимо розглядати всю інформаційну інфраструктуру, проте, якщо компанія велика, то під час оцінки можуть відбуватися непередбачувані витрати часу і сили. У такому разі слід зосередитись на найбільш важливих сервісах.

Для управління ризиками важливі функціональні можливості інформаційної системи,

оскільки вони предметно показують, які сервіси вибрані для аналізу, а якими довелося знехтувати.

Метою щодо оцінки ризиків є отримання відповіді на питання: чи прийнятні наявні ризики, а якщо ні, то які захисні засоби слід використовувати? Оцінка повинна бути кількісною, щоб припускати зіставлення з вибраними наперед межами нових регуляторів безпеки, а саме допустимості і витратами на реалізацію, адже управління ризиками інформаційних систем – типове оптимізаційне завдання. Існує багато програмних продуктів (ПП), які зможуть допомогти в його рішенні.

Але треба відмітити – управління ризиками процес непростий. Практично всі його етапи пов'язані між собою. Початковий аналіз особливо важкий, в разі якщо численні повернення до початку неминучі.

Етапи, які мають місце перед аналізом загроз, можна вважати підготовчими, оскільки вони безпосередньо з ризиками не пов'язані. Ризик існує там, де є загроза.

Перший крок в аналізі загроз – ідентифікація загроз. Види загроз обираються після проведення максимально змістовного аналізу.

Доцільно виявляти не тільки самі загрози, але і джерела їх виникнення – це допоможе у виборі додаткових засобів захисту. Наприклад, нелегальний вхід в систему може стати відтворення початкового діалогу, підбору пароля або підключення до мережі неавторизованого устаткування. Очевидно, для протидії кожному з перерахованих способів нелегального входу потрібні свої механізми безпеки [2].

Після ідентифікації загрози необхідно оцінити її здійснення, використовуючи, наприклад, трибальну шкалу.

Оцінюючи розмір збитку, необхідно мати на увазі не тільки безпосередні витрати на заміну устаткування або відновлення інформації, але і більш віддалені, такі як підрив репутації, ослаблення позицій на ринку. Оцінюючи ймовірність здійснення загроз, доцільно виходити не тільки із середньостатистичних даних, але зважати також на специфіку конкретних інформаційних систем. Після того, як накопичено первісні дані й оцінено ступінь невизначеності, можна переходити до обробки інформації, тобто власне до оцінки ризиків. Цілком допустимо застосувати такий простий метод, як множення ймовірності здійснення загрози на передбачуваний збиток. Якщо для ймовірності і збитку використовувати трибальну шкалу, то можливих результатів буде шість. Перші два результати можна віднести до низького ризику, третій і четвертий – до середнього, два останніх – до високого, після чого з'являється можливість знову привести їх до трибальної шкали. За цією шкалою і слід оцінювати прийнятність ризиків [4]. Можуть траплятися граничні випадки, коли обчислена величина збігається з прийнятною, та доцільним є розглядати їх ретельніше через наближеність характеру результату.

Процес управління ризиком припускає оцінку та аналіз потенційних небезпек, а також пошук заходів, що дозволяють знизити ризики до прийнятного. Управління ризиком може бути реалізовано тільки за умови виконання таких вимог:

– наявності докладної інформації щодо просторового розміщення об'єктів і взаємозв'язків між ними;

– наявності докладної інформації щодо технічних характеристик усього устаткування;

– наявності відомостей про потенційно небезпечні чинники, їх вплив на устаткування і персонал, можливі наслідки їх вияву;

– наявності комплексу моделей, що дозволяють оцінювати вплив небезпечних чинників на устаткування і персонал, оцінювати масштаби можливого збитку;

– наявності моделей розвитку небезпечних ситуацій і критеріїв прийняття рішень щодо управління ризиком [3].

Розв’язання завдань аналізу ризику можливо тільки за умови використання спеціалізованих інформаційних систем, що реалізовують в собі функції зберігання й обробки масивів даних, моделювання і виконання розрахункових завдань, подання результатів у доступній формі, розроблення порад і рекомендацій особам, котрі приймають рішення щодо управління ризиками. Отже, для розв’язання завдань управління ризиком інформаційних систем необхідна орієнтація на підтримку процесів прийняття стратегічних рішень.

Система управління ризиком інформаційних систем включає такі функціональні блоки (рис. 1):

– блок підготовки інформації, що забезпечує формування банків даних, графічне зображення схем інформаційних потоків;

– блок розробки моделей, що забезпечує надійність системи;

– блок сценаріїв, що дозволяє описувати сценарії позаштатних ситуацій і визначати критерії моделювання;

– блок моделювання наслідків відхилень в роботі інформаційної системи;

– блок оцінки результатів моделювання, що проводить аналіз наслідків, і розрахунок інтегральних показників надійності, безпеки і ризику;

– розрахунковий блок, призначений для вирішення завдань моделювання надійності і безпеки устаткування;

– інтерфейсний блок, призначений для підготовки даних, необхідних для роботи розрахункового блока;

– інтеграційний блок, призначений для відображення інтеграції економічної і технологічної інформаційної складової;

– блок даних, призначений для зберігання інформації необхідної для роботи системи. Основою блока даних є автоматизований банк даних, що містить відомості про об'єкти і устаткування небезпечного виробництва.

Інтерфейсний блок забезпечує підготовку і передачу в розрахунковий блок усіх необхідних відомостей, що дозволяє виконувати моделювання для розробленого сценарію. Моделювання в розрахунковому блоці виконується на основі аналізу схем функціональної цілісності, розроблених на основі опису процесу обробки економічної інформації.

На виході розрахункового блока формуються такі результати:

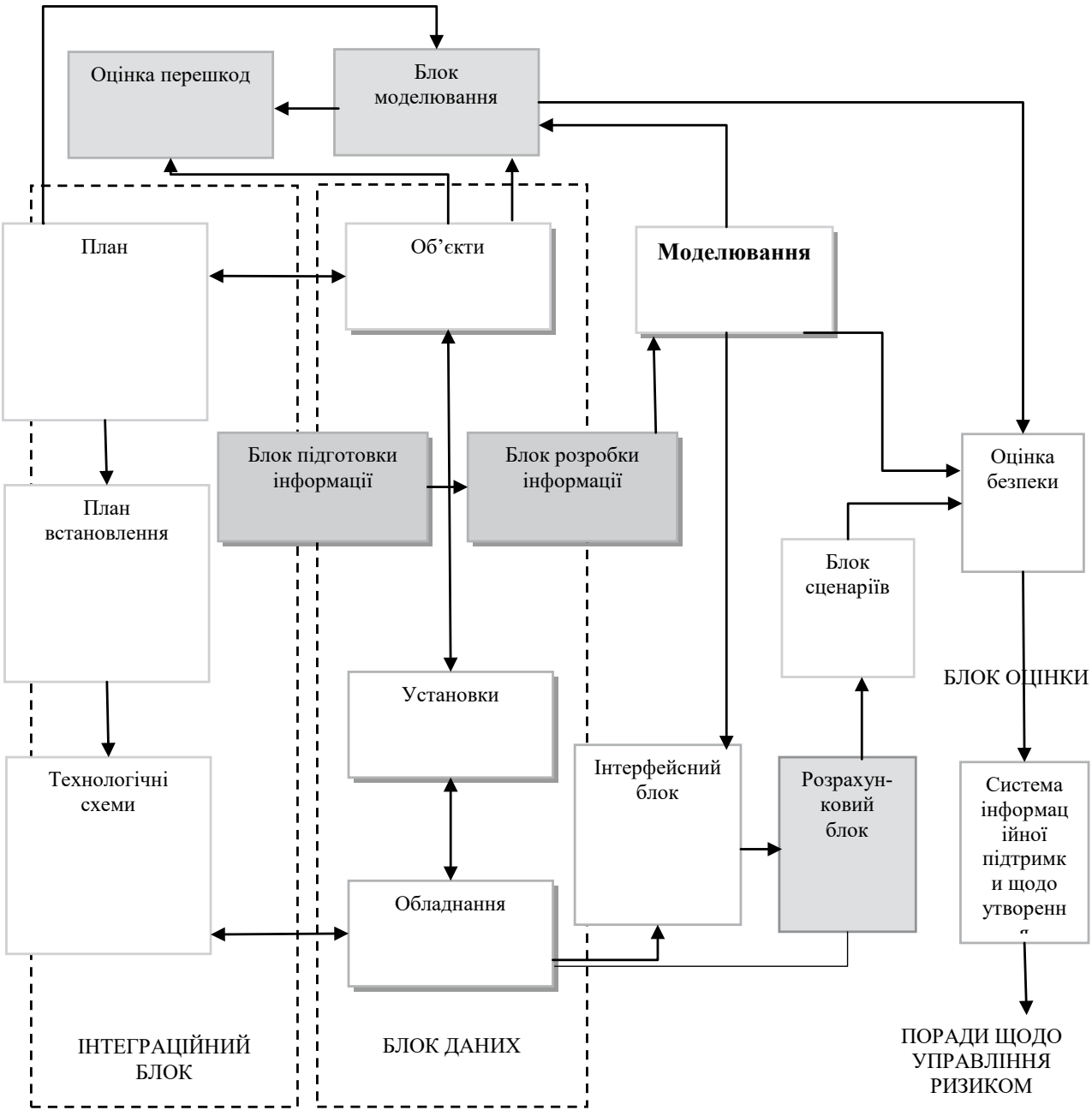

Рис. 1. Структура системи управління ризиком (СУР) інформаційних систем

– імовірність виконання або невиконання заданого сценарію з урахуванням вибраних критеріїв оцінки;

– значущість або ролеві функції різних вузлів під час реалізації заданого сценарію.

Блок моделювання, за заданим сценарієм, забезпечує розрахунок можливих масштабів і оцінки втрат з урахуванням заданих критеріїв.

Блок оцінки виконує аналіз результатів, одержаних під час роботи блока моделювання і розрахункового блока, розрахунок інтегральних показників надійності, безпеки і ризику з урахуванням заданих сценаріїв і критеріїв оцінки.

В основі ризику управління інформаційними системами лежить концепція єдиного інформаційного простору і відкритих систем. Концепція єдиного інформаційного простору припускає використання загальних для всіх блоків структур даних, способів подання та інтерпретації моделей і критеріїв. Концепція відкритих систем припускає можливість нарощування інформаційних систем для вирішення конкретних завдань користувача за рахунок використання протоколів обміну.

Інформаційне забезпечення СУР є сукупністю єдиної системи класифікації і кодування інформації, а також уніфікованих систем документації. Інформаційне забезпечення визначає процедури збирання, обробки і передання інформації; процедури підготовки і рішень у сфері управління ризиком [3].

Основою інформаційного забезпечення СУР є комплекс моделей, які повинні задовольняти вимоги:

– єдність формального апарату, що використовується;

– забезпечення побудови стратифікованого комплексу моделей, в якому кожна вершина моделі описується власною моделлю;

– забезпечення можливості розв'язання завдань аналізу і синтезу з різною кількістю рівнів стратифікації, яке визначається необхідною глибиною аналізу;

– забезпечення можливості моделей за схемою вихід-вхід у разі, якщо результат, одержаний на виході однієї моделі, є вхідним значенням для іншої;

– забезпечення можливості виконання розрахунків від входу до виходу і від виходу до входу з обчисленням параметрів на основі комплексних критеріїв (адитивні, мультиплікативні тощо).

Висновки. Підсумовуючи викладене, можна стверджувати що перевірку і реалізацію нових регуляторів безпеки слід заздалегідь планувати. як і іншу будь-яку діяльність, Терміни навчання персоналу і наявність коштів необхідно врахувати у плані. А сам план тестування. і автономного і комплексного. потрібно скласти, якщо йдеться про програмно-технічний механізм захисту, У разі, якщо накреслені заходи прийняті, необхідно перевірити їх дієвість, тобто переконатися, що залишкові ризики стали прийнятними і якщо це так, то можна спокійно планувати дату найближчої переоцінки, інакше доведеться проаналізувати припущені помилки і виконати негайно повторний сеанс управління ризиками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Андрианов В.В., Зефиров С.Л., Голованов В.Б. Обеспечение информационной безопасности бизнеса. Москва : ЦИПСиР, 2016. 373 с.

2. Ибадулаев В.А., Космачев В.П. Концепция построения информационного обеспечения системы управления риском. URL: http://www.alf-center.com (дата звернення: 14.09.2021).

3. Основы информационной безопасности. *Интернет-Университет Информационных Технологий*. URL: http://www.intuit.ru (дата звернення: 15.09.2021).

4. Терещенко Л.О., Гужко С., Шайкан А.В. Управлінські інформаційні системи : підручник. Київ : КНЕУ, 2008. 485 с.

REFERENCES:

1. Andrianov V.V., Zefirov S.L., Golovanov V.B. (2016) *Obespechenie informacionnoj bezopasnosti biznesa* [Ensuring business information security]. Moscow: CIPSiR. (in Russian)

2. Ibadulaev V.A., Kosmachev V.P. (n. d.). *Koncepciya postroeniya informacionnogo obespecheniya sistemy upravleniya riskom* [The concept of building information support for the risk management system]. Retrieved from: http://www.alf-center.com (in Russian)

3. Osnovy informacionnoj bezopasnosti [Fundamentals of Information Security] (n. d.). *Internet-Universitet Informacionnyh Tekhnologij*. Retrieved from: http://www.intuit.ru (in Russian)

4. Tereshchenko L.O., Huzhko C., Shaykan A.V. (2008) *Upravlins'ki informatsiyni systemy* [Management information systems]. Kyiv: KNEU. (in Ukrainian)