УДК 004.056:338
DOI https://doi.org/10.32838/2663-5941/2020.5/12

***Карпович І.М.***
Національний університет водного господарства та природокористування

***Гладка О.М.***
Національний університет водного господарства та природокористування

***Наконечна Ю.А.***
Національний університет водного господарства та природокористування

# АНАЛІЗ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІТ-ПІДПРИЄМСТВА

*Статтю присвячено дослідженню кібербезпеки інформаційних ресурсів підприємства в ІТ-галузі. Функціонування ІТ-підприємства пов'язане з інноваційними процесами, розробкою та виробництвом нової продукції, робіт, послуг. Інноваційна діяльність, прагнення до конкурентної переваги змушує компанію впроваджувати новітні досягнення науки, нову продукцію і технологію, нову систему управління працею та виробництвом з метою утримання передових ринкових позицій, що поєднується з численними ризиками, вплив яких на результати господарювання компанії може бути доволі значний. Розвиток інформаційної інфраструктури підприємства тягне за собою неконтрольоване збільшення кількості вразливостей інформаційних ресурсів та інформаційних загроз, основними типами джерел яких є природні, техногенні і людські.*

*Розглядаються методи, що дозволяють провести аналіз рівня ризиків інформаційної безпеки і оцінити оптимальні витрати підприємства на захист інформації. Аналіз ризиків передбачає процедуру виявлення чинників ризиків, оцінку їх значимості і методи зниження ризиків або зменшення пов'язаних із цим несприятливих наслідків. Актуальні задачі аналізу і оцінки ризиків інформаційної безпеки дозволяють визначити необхідний рівень захисту інформації, а також розробити рекомендації щодо вдосконалення системи захисту і мінімізації ризиків. Розв'язання проблеми забезпечення кібербезпеки інформаційних ресурсів вимагає підготовки та прийняття організаційних і технічних заходів, розробка яких базується на запропонованих підходах.*

*В основі методики лежить використання експертної та статистичної інформації про загрози і вразливості. Для оцінки ризиків в інформаційній системі підприємства визначається захищеність кожного цінного ресурсу за допомогою оцінки ймовірностей реалізації загроз, що діють на конкретний ресурс, а також вразливостей, через які ці загрози можуть бути реалізовані. Зазначена оцінка ймовірностей дозволяє ранжувати загрози і вразливості за ступенем ризиків. Результатом розв'язання задачі вважається розподіл фінансового ресурсу за виділеними напрямками діяльності підприємства, що мінімізує ризики відмови працездатності системи за критерієм інформаційної безпеки.*

***Ключові слова:*** *ризик, інформаційна безпека, загрози, мінімізація ризиків, кібербезпека.*

**Постановка проблеми.** В умовах прискореної динаміки розвитку інформатизації суспільства спостерігається щорічна тенденція зростання кіберзагроз інформаційним ресурсам, тому їх захист є однією з важливих проблем. Розв'язання такої задачі вимагає підготовки і прийняття організаційних і технічних заходів щодо забезпечення кібербезпеки інформаційних ресурсів підприємств. У цій роботі розглядаються деякі з методів, які дозволяють провести аналіз ризиків і оцінити оптимальні витрати на захист інформації.

Поняття ризику, як відомо, є наслідком тісної взаємодії таких понять, як актив, вразливість, загроза і збиток. Активи – це ключові компоненти інфраструктури і важлива інформація, яка опрацьовується в інформаційній системі. Виходячи із стандарту ISO/IEC 27000 [1], який детально описує процедури системи управління інформаційною безпекою, цінні активи організації умовно можна розділити на основні і допоміжні.

До основних активів відносять бізнес-процеси – сукупність видів діяльності, в результаті якої створюється продукт або послуга, що становить інтерес для споживача. Основним активом виступає також інформація – відомості, які є предметом власності, що підлягають захисту від порушення конфіденційності, цілісності та доступності відповідно до вимог правових

документів і вимог власника інформації, незалежно від форми подання, зокрема, інформаційні ресурси (бази і файли даних, системна документація, науково-дослідна інформація та документація, контракти і угоди тощо). До допоміжних активів належить, насамперед, апаратно-програмний комплекс –сукупність технічних і програмних засобів, призначених для виконання взаємозалежних експлуатаційних функцій з обробки інформації обмеженого поширення, що включає в себе активну апаратуру обробки даних, стаціонарну апаратуру, периферійні пристрої, операційні системи та прикладне програмне забезпечення. До цієї ж категорії входять носії даних; сукупність телекомунікаційних пристроїв, що використовуються для з'єднання декількох фізично віддалених сегментів інформаційної системи; співробітники компанії, їх кваліфікація і досвід, а також нематеріальні ресурси (репутація і імідж компанії).

Вразливість – слабке місце в засобах захисту, спричинене помилками чи недосконалістю процедур, проектів, реалізації, яке загроза може подолати. Іншими словами, вразливості – це будь-які чинники, що роблять можливою успішну реалізацію загроз. Практика свідчить, що вразливості є основною причиною виникнення атак. Загрозою вважають потенційну можливість причинити збиток якимось наперед відомим способом. Загрози інформаційній безпеці можуть бути здійснені шляхом використання вразливостей системи. Слабкості захисту можуть використовуватися однією або декількома загрозами, що є причиною небажаних інцидентів, які можуть призвести до нестабільного функціонування компонентів інформаційної системи. Наявність слабких місць в захисті інформаційної системи може бути обумовлена різними чинниками, починаючи з простої недбалості співробітників і закінчуючи навмисними діями зловмисників. Збиток складають витрати на відновлення системи після можливого порушення інформаційної безпеки.

Наявність ризику – це ймовірність того, що відбудуться певні небажані події, які можуть негативно вплинути на досягнення цілей конкретного бізнес-процесу. Зокрема, функціонування підприємства в ІТ-галузі пов'язане з інноваційними процесами, розробкою та виробництвом нової продукції, робіт, послуг. Інноваційна діяльність, прагнення до конкурентної переваги змушує компанію впроваджувати новітні досягнення науки, нову продукцію і технологію, нову систему управління працею та виробництвом з метою утримання передових ринкових позицій, що поєднується з численними ризиками, вплив яких на результати господарювання компанії доволі значний. У зв'язку із цим своєчасна, оперативна і коректна оцінка ризиків зниження або повної втрати інформаційної безпеки сьогодні є актуальною проблемою в діяльності будь-якої організації.

Інформаційна безпека, визначаючи рівень захищеності бізнес-середовища, стає важливим аспектом загальної економічної безпеки в діяльності сучасної компанії. Захист інформації – особливий вид діяльності щодо запобігання витоку інформації, несанкціонованих змін її потоків та інших чинників, які негативно впливають на стабільну роботу підприємства і пов'язаних з ним економічних партнерів (клієнтів, постачальників обладнання, інвесторів та ін.).

**Аналіз останніх досліджень і публікацій.** Розвиток інформаційної інфраструктури підприємства тягне за собою неконтрольоване збільшення кількості інформаційних загроз і вразливостей інформаційних ресурсів. Сучасні дослідження відзначають такі типи джерел загроз, що впливають на інформаційну безпеку: природні; техногенні; людські навмисні і людські ненавмисні. Для підприємств інноваційного типу, до яких належать компанії ІТ-галузі, характерні наступні види ризиків діяльності: організаційні (низька кваліфікація розробників проекту, затримка виконання етапів його реалізації); науково-технічні (зношеність технологічного обладнання, відсутність резервів потужностей або типових проектних рішень); фінансово-економічні (маркетинговий, ризик фінансування проекту, інфляційний, процентний, податковий і операційний ризики).

У сучасних умовах перед кожним підприємством, яке дбає про безпеку своїх інформаційних ресурсів, постає питання про організацію системи захисту інформації, що дозволила б гарантувати безпеку функціонування телекомунікаційного обладнання і циркулюючої інформації в інформаційній системі підприємства. Ефективність захисту інформації залежить від підходу до її організації та правильного вибору методів розрахунку ризиків інформаційної безпеки. Існує чимало методик оцінки та опрацювання ризиків, які можуть застосовуватися до будь-якої інформаційної системи, незалежно від рівня конфіденційності наявної інформації. Однак, зазвичай, для якісної побудови системи захисту інформації з використанням таких методик потрібен значний обсяг інформації про потенційні атаки, а також про спроби їх реалізації, який підлягає програмному аналізу з метою виявлення найбільш актуальних загроз інформаційній безпеці.

Аналіз ризиків передбачає процедуру виявлення чинників ризиків, оцінку їх значимості і методи зниження ризиків або зменшення пов'язаних із цим несприятливих наслідків. Актуальні задачі аналізу і оцінки ризиків інформаційної безпеки дозволяють визначити необхідний рівень захисту інформації, а також розробити рекомендації щодо удосконалення системи захисту і мінімізації ризиків.

Аналіз ризиків поділяють на два види: якісний і кількісний. Якісний аналіз дозволяє визначити (ідентифікувати) чинники, області та види ризиків. Кількісний аналіз ризиків дає можливість чисельно визначити розміри окремих ризиків і загальний розмір ризику в цілому. Підсумкові результати якісного аналізу ризиків, у свою чергу, можуть стати вхідною інформацією для проведення кількісного аналізу. Однак для здійснення кількісного аналізу ризиків потрібна надійна вхідна інформація (збір статистичної інформації ускладнений жорсткою конкуренцією в бізнесовому середовищі) і чітко визначена шкала оцінки параметрів. Концептуальні засади якісного та кількісного аналізу ризику, системи показників його оцінювання, основних підходів до моделювання, управління та методів зниження ступеня ризику детально проаналізовані в монографії [2].

**Формулювання цілей статті.** Процес розрахунку ризиків інформаційної безпеки актуальний на всіх етапах роботи системи захисту інформації та є цікавим для власника інформації, насамперед, з точки зору втрат в економічній сфері. Вибір методу оцінки ризиків інформаційної безпеки в більшості випадків ґрунтується на таких чинниках: часові, фінансові, інформаційні ресурси; ступінь невизначеності оцінки ризиків інформаційної безпеки; наявність або відсутність можливості отримання кількісних оцінок вхідних даних, де вхідними даними можуть бути висновки, рішення, переліки, а також рекомендації, залежно від методу та етапу оцінки ризиків інформаційної безпеки. Разом із тим у процесі оцінки ризиків повинні бути встановлені критерії прийнятності ризику та критерії для оцінки ризиків інформаційної безпеки, а також повинні бути дані гарантії того, що аналіз ризиків дасть надійні і несуперечливі масиви актуальних для даної системи ризиків. Необхідно провести ідентифікацію ризиків інформаційної безпеки, спрямованих на такі властивості інформаційних ресурсів, як конфіденційність, цілісність і доступність. Потрібно виконати ідентифікацію власника ризику, де під власником розуміється фізична, юридична особа або підрозділ, що відповідає за управління ризиком і має необхідні для цього повноваження, в даному випадку, мова може йти про керівників, фахівців з інформаційної захисту, відділів з інформаційної безпеки тощо.

Аналіз і оцінка ризиків в задачі управління інформаційною безпекою на сьогодні – одне із складних і актуальних завдань. Складність полягає в тому, що відсутні загальноприйняті підходи і методики для оцінки ризиків. Чинники ризику (загроза, вразливість, збиток) аналізуються за допомогою евристичних методів, які містять суб'єктивну складову частину.

У процесі аналізу ризиків інформаційної безпеки здійснюється оцінка потенційних втрат у випадку реалізації ризику, оцінюється ймовірність реалізації ризиків і визначається величина ризиків. У ході оцінки ризиків інформаційної безпеки має бути виконано порівняння ризиків із встановленими критеріями, а також визначено вектор пріоритетних напрямків з їх опрацювання.

**Виклад основного матеріалу.** У рамках кількісного аналізу ризик $R$ розглядається як комплексна величина, що залежить від таких чинників, як загрози, вразливості і збитки [3]:

$$R = \lambda P_T P_V(z) \qquad (1)$$

де $\lambda$ – розмір збитків, викликаних порушенням безпеки інформаційного активу; $P_T$ – ймовірність виникнення загрози; $P_V(z)$ – функція, яка описує ймовірність реалізації загрози для інформаційного активу в залежності від витрат $z$ на забезпечення захисних заходів.

Таким чином, розмір збитків залежить як від інформації, що підлягає захисту, так і від заданої ймовірності виникнення загрози. Значення ймовірності реалізації загрози може бути суттєво знижено за рахунок здійснення інвестицій в інформаційну безпеку активу.

Завдання управління ризиками компанії полягає у зменшенні впливу небажаних чинників на життєдіяльність підприємства для отримання результатів роботи максимально наближених до бажаних, які відповідають поставленим цілям. Управління ризиками – сукупність методів аналізу і нейтралізації чинників ризику, об'єднаних у систему планування, моніторингу та коригуючих впливів [4; 5]. Цей комплекс заходів містить ідентифікацію, аналіз ризиків та прийняття рішень, спрямованих на зниження ймовірності і ступеня їх впливу на результати діяльності підприємства.

Як показали дослідження з інформаційної безпеки, всі ризики інформаційної безпеки повинні узгоджуватися з ризиками підприємства в цілому. Так виникла задача інтеграції системи управління

інформаційними ризиками із системою управління всією компанією. Кількісні методи розрахунку дають можливість фінансово обґрунтувати інвестиції в інформаційну безпеку, а також виявити економічну ефективність цих витрат. Однак залишається недослідженим питання оптимальності обсягів інвестицій в інформаційну безпеку та визначення тих ділянок системи, підвищення витрат на захист яких найбільш суттєво знизить загрозу ризику для системи в цілому.

Аналіз наявних підходів до проблеми управління ризиками складних систем показує, що ця проблемна область ще недостатньо формалізована і вивчена. Для зменшення ступеня невизначеності у виборі можливих варіантів розв'язку задач управління ризиками використовується різний математичний апарат: методи суб'єктивної ймовірності, нечіткі множини, нейронні мережі тощо.

З огляду на істотну різнотипність загроз, розробка методик і алгоритмів оцінки ризику зниження або повної втрати інформаційної безпеки – досить трудомістке і важливе завдання для будь-якої інформаційної системи. Перш за все, необхідна побудова гнучких комплексних моделей інформаційної системи із врахуванням програмних, апаратних ресурсів, внутрішніх та зовнішніх загроз і вразливостей, здатних налаштовуватися відповідно до особливостей конкретного підприємства. Крім того, з урахуванням значної кількості факторів ризику математична модель оцінки інформаційної безпеки повинна допускати розробку ефективних числових алгоритмів обробки інформації.

Для оцінки ризиків інформаційної безпеки важливо виділити і проаналізувати основні чинники, через які реалізуються загрози, що діють на інформаційну систему в сенсі відмов або зниження її працездатності. Серед значної кількості методів оцінки ризиків інформаційної безпеки можна виділити метод оцінки ризиків, який ґрунтується на побудові моделі загроз і вразливостей.

В основі цієї методики лежить використання експертної та статистичної інформації про загрози і вразливості. Для оцінки ризиків в інформаційній системі підприємства визначається захищеність кожного цінного ресурсу за допомогою оцінки ймовірностей реалізації загроз, що діють на конкретний ресурс організації (наприклад, ймовірність збоїв у роботі системи інформаційної безпеки в зв'язку з низькою кваліфікацією співробітників, відсутністю або старінням програмного чи апаратного забезпечення тощо), а також вразливостей, через які дані загрози можуть бути реалізовані. Зазначена оцінка ймовірностей дозволяє ранжувати загрози і вразливості за ступенем ризиків.

Оскільки ризики інформаційної безпеки тісно пов'язані із застосуванням сучасних інформаційних технологій, що визначають ефективність діяльності ІТ-підприємства в його інноваційному аспекті, то їх можна віднести до різновиду інноваційних ризиків. Визначаючи інноваційний ризик як ймовірність втрат внаслідок помилково поставленої або не досягнутої стратегічної мети [6], в характеристиці ризиків відмови працездатності системи доцільно використовувати такий показник, як рівень витрат (в матеріальному або вартісному вираженні) на відновлення працездатності системи.

Виходячи з експертних даних про ризики, вразливості і витрати за кожним з ресурсів, можна побудувати модель, актуальних для інформаційної системи підприємства, і провести аналіз функціонування інформаційної системи з точки зору мінімізації ризиків відмови або зниження працездатності системи і, отже, максимізації її ефективності за критерієм інформаційної безпеки.

На першому етапі розв'язування такої задачі виділяються найбільш важливі для підприємства напрямки діяльності, які визначають (з точки зору його керівництва) рівень інформаційної безпеки. На другому етапі для виділених напрямків діяльності на основі експертної оцінки ймовірності реалізації загроз інформаційної безпеки розраховується значимість кожної загрози, а також оцінюється рівень витрат у вартісному вираженні на відновлення працездатності системи. Далі розраховується сумарний ризик відмови працездатності системи як сума ризиків за кожним з напрямків.

Результатом розв'язання описаної задачі будемо вважати розподіл фінансового ресурсу за виділеними напрямками діяльності підприємства, що мінімізує ризики відмови працездатності системи за критерієм інформаційної безпеки.

За значної кількості загроз інформаційній безпеці для числової (кількісної) оцінки ризиків можуть бути використані методи оптимізації. Розглянемо математичну модель мінімізації ризиків інформаційної безпеки.

Нехай у технічній або соціально-економічній системі відомі залежності $r_i = f(x_i)$ ризиків $r_i$ відмови працездатності системи від витрат $x_i$ на їх уникнення (виключення, зменшення) в $i$-му ($i = 1, \ldots, n$) напрямку забезпечення інформаційної безпеки (відмова апаратного, програмного забезпечення, відмова працездатності системи через недостатню кваліфікацію програмістів, менеджерів тощо). Для

мінімізації ризиків інформаційної безпеки будемо використовувати такий показник, як рівень витрат (в матеріальному або вартісному вираженні) на відновлення працездатності системи у разі її відмови за одним або декількома напрямками.

Визначимо такі величини: $R = \sum_{i=1}^{n} r_i$ – сумарний ризик відмови системи; $Z$ – максимальна сума витрат на зменшення (усунення) виділених ризиків. Нехай функції витрат є лінійними функціями від $x_i$, тобто $f(x_i) = a_i - b_i x_i$ ($i = 1, \ldots, n$). Коефіцієнти $a_i$ можна трактувати як витрати, які може понести система за відсутності витрат на попередження ризиків або, інакше, як максимальні витрати на організацію безкризової роботи системи на $i$-му напрямку гарантування безпеки, а коефіцієнти $b_i$ – як вагові коефіцієнти, що відображають відносну значимість $i$-го напряму гарантування безпеки [7].

Розглядаючи $R \to \min$ як функцію мети, можна сформулювати наступну задачу математичного програмування:

$$\begin{cases} \sum_{i=1}^{n} b_i x_i \to \max; \\ \sum_{i=1}^{n} x_i \le Z; \\ x_i \ge 0 \quad . \end{cases} \qquad (2)$$

Модель (2) являє собою багатопараметричну задачу лінійного програмування. З огляду на обмеженість всіх змінних задачі і нестрогість обмежень можна стверджувати, що допустима множина є непорожньою і дана задача може бути розв'язана за допомогою симплекс-методу (див., напр., [8]) чи за більш оптимальним сучасним алгоритмом [9], які дозволяють з використанням сучасної комп'ютерної техніки розглядати практично необмежену кількість $n$ загроз інформаційної безпеки.

Практичне застосування моделі (2) можна розділити на два етапи. Перший – оцінка тиску кожної із суттєвих груп негативного впливу на позиції підприємства; другий – вибір відповідної стратегії захисних дій.

У реальних умовах кількість груп ризиків, що створюють реальну загрозу інформаційній безпеці компанії, порівняно невелика. Зокрема, за висновками теоретичних досліджень [10], ризик загроз інформаційній безпеці підприємства зумовлений дією п'яти основних конкурентних сил: ризик появи товарів-субститутів, внутрішньогалузеві загрози конкуренції, виникнення нових конкурентів, загроза (ризик) втрати клієнтів, загроза (ризик) нестабільності постачальника. Основними показниками, що визначають дію цих факторів, є: умови попиту, виробничі умови, характер стратегії компанії, наявність супутніх або пов'язаних галузей. Ця теорія дає можливість оцінити конкурентний стан на ринку і на цій основі розробити такий варіант довгострокової стратегії підприємства, який в найбільшій мірі забезпечить його захист і одночасно сприятиме створенню додаткових конкурентних переваг. Проведений у роботі [11] аналіз дозволив виділити групи ризиків, що мають досить високу ймовірність виникнення, та оцінити рівень основних ризиків компанії.

**Висновки.** Підприємства малого і середнього бізнесу сьогодні є частиною тієї сфери економіки, яка найбільш сприйнятлива до технологічних, інформаційних, бізнес-інновацій. Тим часом багато підприємств малого і середнього бізнесу, перебуваючи в інформаційному середовищі, ігнорують різного роду загрози для їх інформаційної системи, тим самим піддаючи себе ризику фінансових втрат. Зменшення (мінімізація) ризиків, що притаманні діяльності компанії, сприяє посиленню її конкурентної здатності і життєздатності загалом [12].

**Список літератури:**

1. ISO/IEC 27000:2009. Information technology – Security techniques – Information security management systems – Overview and vocabulary (Інформаційні технології. Методи безпеки. Системи управління інформаційною безпекою. Огляд і словник).

2. Вітлінський ВВ., Великоіваненко Г.І. Ризикологія в економіці та підприємництві : монографія. Київ : КНЕУ, 2004. 480 с.

3. Королев В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории риска. Москва : ФИЗМАТЛИТ, 2011. 620 с.

4. Листер Т., Демарко Т. Вальсируя с медведями. Управление рисками в проектах по разработке программного обеспечения. Москва : Компания p.m. Office, 2005. 196 с.

5. A Guide to the Project Management Body of Knowledge. (PMBOK Guide) – Fifth edition. Project Management Institute, 2013. URL : http://dinus.ac.id/repository/docs/ajar/PMBOKGuide_5th_Ed.pdf.

6. Ильенкова Н.Д. Проблемы анализа инновационного риска. *Инвестиции и инновации*. 2011. № 5. С. 90–92.

7. Медведев А.В. Математическая модель оценки инвестиционной привлекательности региона. *Современные наукоемкие технологии*. 2013. № 8-2. С. 357–361.

8. Наконечний С.І., Савіна С.С. Математичне програмування : навч. посіб. Київ : КНЕУ, 2003. 452 с.

9. Tkachuk V.M., Kozlenko M.I., Kuz M.V., Lazarovych I.M., Dutchak M.C. Function Optimization Based on Higher-Order Quantum Genetic Algorithm. 2019. T. 41, № 3. С. 43–57. URL : http://nbuv.gov.ua/UJRN/elmo_2019_41_3_6.

10. Портер М. Конкурентное преимущество. Как достичь высокого результата и обеспечить его устойчивость. Москва : Альпина Паблишер, 2008. 720 с.

11. Нечаєва І.А., Дьордій Є.А. Управління ризиками підприємства в секторі ІТ-послуг як інструмент підвищення його конкурентоспроможності. *Ефективна економіка*. 2018. № 12. URL : http://www.economy.nayka.com.ua/?op=1&z=6797.

12. Білоус АЯ., Репін М. В. Мінімізація ризиків на підприємстві шляхом впровадження системи екологічного менеджменту. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки.* Том 31(70). № 1. 2020. С. 51–55.

**Karpovych I.M., Hladka O.M., Nakonechna Yu.A. ANALYSIS OF SECURITY RISKS OF THE INFORMATION SYSTEM AT AN IT-ENTERPRISE**

*The paper is devoted to the study of cybersecurity of information resources at an enterprise in the IT industry. The functioning of the IT enterprise is related to innovative processes, development and production of new products, works, services. Innovative activity, the pursuit of competitive advantage, compels the company to introduce the latest achievements of science, new products and technology, a new system of labor and production management in order to maintain leading market positions, which is combined with numerous risks that have a significant impact on the company's business results. The development of enterprise information infrastructure entails an uncontrolled increase in the number of information threats and vulnerabilities of information resources. Current research has identified the following types of sources of threats that affect information security: natural, technogenic and human.*

*We consider some of the methods that allow you to analyze information security risks and evaluate the optimal costs for an enterprise to protect information. Risk analysis involves a procedure for identifying risk factors, assessing their significance and methods for reducing of risk or reducing the associated adverse effects. The current tasks of analysis and assessment of information security risks make it possible to determine the required level of information security, as well as to develop recommendations for improving the system of protection and minimization of risks. Addressing the cybersecurity problem of information resources requires the preparation and adoption of organizational and technical measures, the development of which is based on the approaches proposed.*

*This methodology is based on the use of expert and statistical information on threats and vulnerabilities. To evaluate risks in an organization's information system, security of each valuable resource is determined by assessing the probability of implementation of threats affecting a specific resource of the enterprise, and the vulnerabilities through which these threats can be addressed. This probability assessment allows you to rank threats and vulnerabilities by degree of risk. The result of the solution of the described problem will be the allocation of financial resources in the selected areas of activity of the organization, which minimizes the risks of failure of the system by the criterion of information security.*

***Key words:*** *risk, informational security, threats, minimizing risks, cybersecurity.*