

**Н.М.ВОЛОСНИКОВА****ДОСЛІДЖЕННЯ СТІЙКОСТІ ЗАГАЛЬНОЇ СИСТЕМИ КОРПОРАТИВНОГО УБЕЗПЕЧЕННЯ**

Метою статті є визначення механізму функціонування й підвищення стійкості загальної системи корпоративного забезпечення. При цьому створюється абстрактна та концептуальна модель системи корпоративного забезпечення, яка описується математично або функціонально та служить для оптимізації відносин між елементами і рівнями наслідків впливу інформаційної складової, як суттєвого фактора, спрямованого на підвищення економічної ефективності системи корпоративного забезпечення. Виділено структуру системи, як сукупності замкнених елементів, які об'єднані в систему певними зв'язками та є залежними один від одного. Проаналізовано систему корпоративного забезпечення з точки зору надійності. Зроблено висновок, що найбільш поширеною причиною порушення цілісності загальної системи корпоративного забезпечення є втрата стійкості. Стійкість системи розглядається, як здатність даної системи нормально функціонувати та протистояти різним неминучим впливам явищ в мікро- та макроекономічному середовищі. Під стійкістю системи корпоративної безпеки розуміється здатність динамічної системи повертатися в рівноважний стан після закінчення дії обурення, який порушив цю рівновагу. Виділено три види криз залежно від механізмів розвитку та характеру стійкості загальної системи корпоративного забезпечення, а саме критична ситуація системи корпоративного забезпечення, кризовий стан, катастрофи. Запропоновано кількісні характеристики показників надійності загальної системи корпоративного забезпечення.

**Ключові слова:** системність; промислове підприємство; діалектичні принципи; системний аналіз; система корпоративного забезпечення; системи надійності; система стійкості; імовірність відмови; імовірність відновлення

**Н.Н.ВОЛОСНИКОВА****ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ ОБЩЕЙ СИСТЕМЫ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ**

Целью статьи является определение механизма функционирования и повышения устойчивости общей системы корпоративной безопасности. При этом создается абстрактная и концептуальная модель системы корпоративной безопасности, которая описывается математически или функционально и служит для оптимизации отношений между элементами и уровнями последствий влияния информационной составляющей, как существенного фактора, направленного на повышение экономической эффективности системы корпоративной безопасности. Выделено структуру системы, как совокупности замкнутых элементов, объединенных в систему определенными связями и зависимыми друг от друга. Проанализирована система корпоративной безопасности с точки зрения надежности. Сделан вывод, что наиболее распространенной причиной нарушения целостности общей системы корпоративной безопасности является потеря устойчивости. Устойчивость системы рассматривается, как способность данной системы нормально функционировать и противостоять различным неизбежным воздействиям явлений в микро- и макроэкономической среде. Под устойчивостью системы корпоративной безопасности понимается способность динамической системы возвращаться в равновесное состояние после окончания действия возмущения, которое нарушило это равновесие. Выделены три вида кризисов в зависимости от механизмов развития и характера устойчивости общей системы корпоративной безопасности, а именно критическая ситуация системы корпоративной безопасности, кризисное состояние, катастрофы. Предложены количественные характеристики показателей надежности общей системы корпоративной безопасности.

**Ключевые слова:** системность; промышленное предприятие; диалектические принципы; системный анализ; система корпоративной безопасности; системы надежности; система устойчивости; вероятность отказа; вероятность восстановления

**N.VOLOSNIKOVA****RESEARCH OF SUSTAINABILITY OF THE GENERAL CORPORATE SECURITY SYSTEM**

The purpose of the article is to determine the mechanism of functioning and increase the stability of the general system of corporate security. This creates an abstract and conceptual model of the corporate security system, which is described mathematically or functionally and serves to optimize the relationship between the elements and levels of consequences of the information component, as a significant factor aimed at improving the economic efficiency of the corporate security system. The structure of the system is distinguished as a set of closed elements that are connected to the system by certain connections and are interdependent. The system of corporate security from the point of view of reliability is analyzed. It is concluded that the most common reason for the violation of the integrity of the overall corporate security system is the loss of stability. System resilience is seen as the ability of a system to function properly and withstand the various inevitable effects of phenomena in the micro- and macroeconomic environment. There are three types of crises depending on the mechanisms of development and the nature of the stability of the overall corporate security system, namely the critical situation of the corporate security system, the crisis, disasters. Quantitative characteristics of indicators of reliability of the general system of corporate security are offered.

**Keywords:** systematic; industrial enterprise; dialectical principles; system analysis; corporate security system; reliability systems; stability system; probability of failure; probability of recovery

**Вступ.** У концепції безпечної корпоративної організованості та системності промислових підприємств упор робиться переважно на розробку нових діалектичних принципів наукового мислення, логічного аналізу складних об'єктів з урахуванням їх взаємозв'язку і суперечливих тенденцій.

У процесі системного аналізу створюється абстрактна та концептуальна модель системи корпоративного забезпечення, яка описується математично або функціонально та служить для оптимізації відносин між елементами і рівнями. Метою побудови даної моделі є розробка адекватного уявлення реальної системи корпоративної безпеки. У зв'язку з тим, що структура системи корпоративної

безпеки досить складна, а в часовій динаміці стає ще більш складною, її відповідність реальним умовам можлива тільки при достатньому рівні формалізації. Формалізовані моделі системи корпоративної безпеки можуть бути, як кількісними, так і якісними. Важливо щоб для них були визначені умови застосування та задачі оптимізації, які вирішують складні і проблемні ситуації, що пов'язані з корпоративним забезпеченням.

**Аналіз останніх досліджень та літератури.**

Проблеми корпоративної безпеки в умовах розвинутої ринкової й трансформаційної економіки широко досліджуються науковцями, серед яких можна назвати В.Є.Духова, Я.А.Жаліло, М.П.Капустіна, А.В.Кирієнка, Г.В.Козаченко, ВА.Ліпкана,

О.М.Ляшенко, Н.О.Подлужної, В.П.Пономарьова, П.Я.Пригуновата ін.

Проте деякі теоретичні, методологічні і практичні аспекти потребують подальших досліджень, тому що результати досліджень не дають комплексної уяви особливості процесів, механізму функціонування й підвищення стійкості загальної системи корпоративного забезпечення.

**Метою** статті є визначення наслідків впливу стійкості, як суттєвого фактора, спрямованого на підвищення економічної ефективності системи корпоративного забезпечення.

Для уточнення та структурування складної системи корпоративного забезпечення, в якій доцільно виділяти впливаючі на неї елементи, підрелементи, системи, підсистеми при вирішенні задач потрібно формалізація і структуризація, що дозволяє застосовувати практичні наукові знання. Для цього необхідна формалізована модель системи. При цьому

система корпоративного забезпечення вивчається з різних точок зору на основі застосування різних формалізованих моделей, тому для всебічного наукового вивчення системи корпоративної безпеки може бути задіяні безліч моделей.

Вербальне зображення системи для більш точного опису функціонування вимагає досить чіткої деталізації процесів. Необхідно виділити структуру системи, як сукупності замкнених елементів, які об'єднані в систему певними зв'язками та є залежними один від одного. З точки зору надійності загальна система корпоративного забезпечення повинна мати (рис. 1):

- 1) конкретні вимоги та умови до функціонування загальної системи корпоративної безпеки та її окремих локальних елементів корпоративної безпеки;
- 2) певну інтегровану мету;
- 3) ієрархічну структуру.

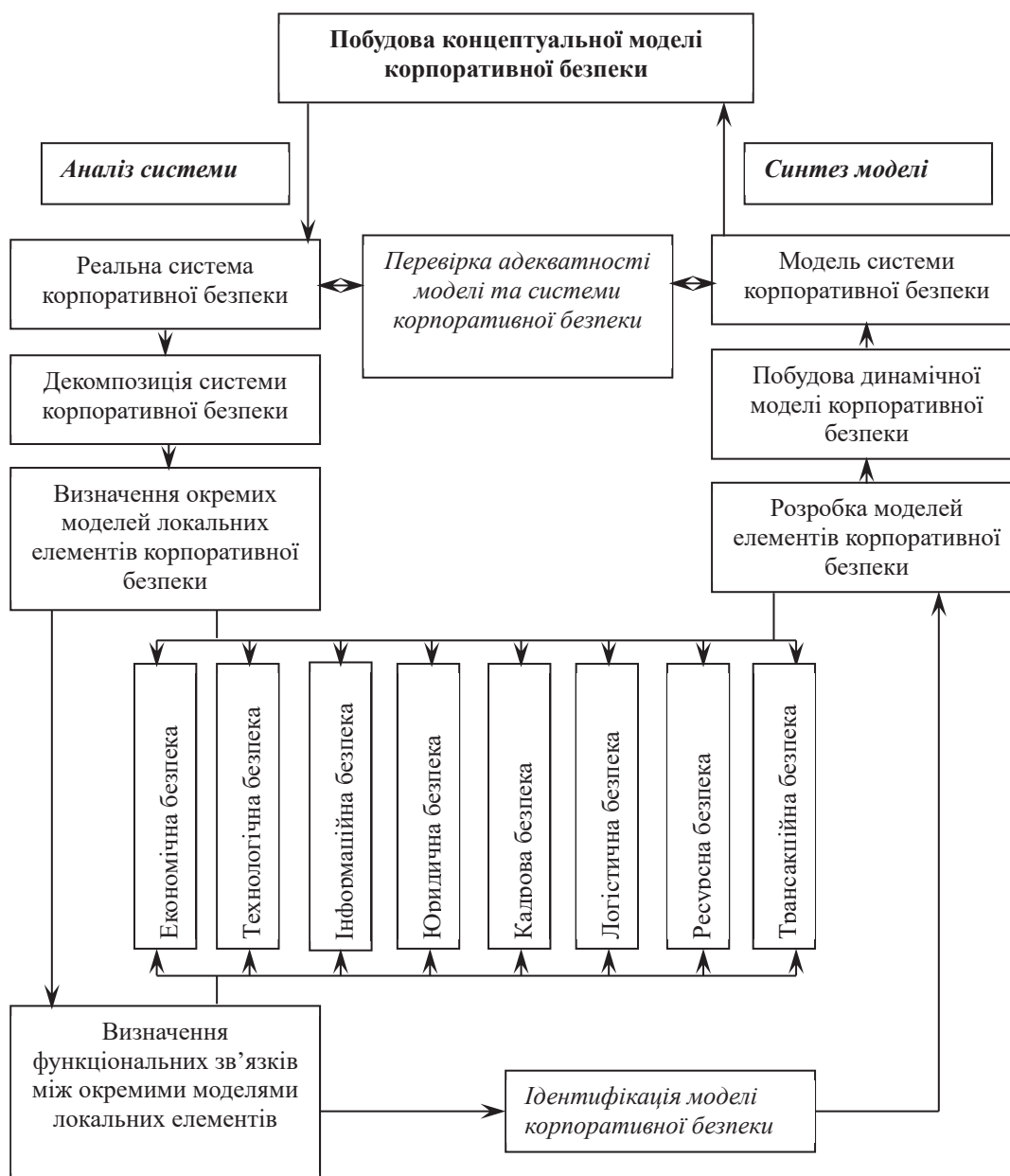


Рис. 1 – Схема формування моделі системи корпоративного забезпечення

Представимо загальну систему корпоративного забезпечення та відокремимо з цієї системи окремі локальні елементи, функціонування яких спрямоване на досягнення загальної корпоративної мети [1, 2]. Зазначену систему можна формально визначити у вигляді наступних параметрів:

$$\text{Corporate Security} \langle \text{Goal}, \text{CS}_i, \text{Pr}_i, \text{CAG}, t_i \rangle,$$

де *Corporate Security* – загальна система корпоративного забезпечення;

*Goal* – мета загальної системи корпоративного забезпечення;

$\text{CS}_i$  – окремі локальні елементи корпоративного забезпечення;

$\text{Pr}_i$  – множина процесів на різних рівнях окремих локальних елементів корпоративного забезпечення;

*CAG* – умови досягнення загальної корпоративної мети;

$t_i$  – час досягнення загальної корпоративної мети.

При нормальному функціонуванні окремих локальних елементів загальна система корпоративного забезпечення працює без збоїв. У разі дисфункціональності будь-якого окремого локального елемента порушується цілісність загальної системи. Як правило, таке порушення, не приводить до глобальної кризи, тому що автономне функціонування інших елементів корпоративної безпеки хоча і відчуває деякі впливи ззовні, але не втрачає своєї самостійності. Тільки в разі вибухового характеру порушень в окремих локальних елементах корпоративної безпеки, що призводить до вибухових порушень в інших локальних елементах корпоративної безпеки за різноспрямованим вектором може привести до глобальної кризи загальної корпоративної безпеки.

Найбільш поширеною причиною порушення цілісності загальної системи корпоративного забезпечення є втрата стійкості. Стійкість системи управління системою, так само можна розглядати, як здатність даної системи нормально функціонувати та протистояти різним неминучим впливам явищ в мікро- та макроекономічному середовищі. Стан системи корпоративного забезпечення можна вважати стійким, якщо відхилення від нього залишається як завгодно малим при будь-яких досить малих змінах вхідних

сигналів в мікро- та макроекономічному середовищі. Втрата стійкості означає появу в системі корпоративної безпеки процесів, що не піддаються управлінню і призводять до руйнування цілісності. Причиною втрати стійкості можуть бути протиріччя, як внутрішнього характеру (між загальною системою корпоративної безпеки та окремими локальними елементами корпоративної безпеки), так і зовнішнього (між загальною системою корпоративної безпеки та макроекономічним середовищем).

Вимога стійкості для системи корпоративного забезпечення відноситься до числа необхідних, але не може вважатися достатньою. Система корпоративної безпеки може бути досить стійкою до вхідних сигналів мікро- та макроекономічного середовища, але час загасання та відновлення функціональної стабільності настільки велике, що практично дана система не може бути ефективно використана. Тому система повинна бути не тільки стійкою, але мати певний допустимий перехідний процес від збурюючих впливів мікро- та макроекономічного середовища до відновлення функціональної стабільності (рис. 2).

Система корпоративного забезпечення знаходиться в стані рівноваги, якщо при відсутності впливу на систему факторів мікро- та макроекономічного середовища, помилка управління (різниця між заданим і фактичним станом системи корпоративної безпеки) прагне до нуля. Під стійкістю системи корпоративної безпеки розуміється здатність динамічної системи корпоративної безпеки повертатися в рівноважний стан після закінчення дії обурення, який порушив цю рівновагу. Нестійка система корпоративної безпеки після впливу обурення мікро- та макроекономічного середовища віддаляється від рівноважного стану або починає здійснювати навколо нього коливання з наростаючою амплітудою.

Стійкість функціонування загальної системи корпоративного забезпечення складається з великої групи факторів, які безпосередньо впливають на стійкість. Втрата стійкості може статися через зміну параметрів окремих елементів корпоративної безпеки, наявності непередбачених при формуванні системи факторів мікро- та макроекономічного середовища, або при порушенні зв'язків в системі, коли має місце структурна нестійкість.

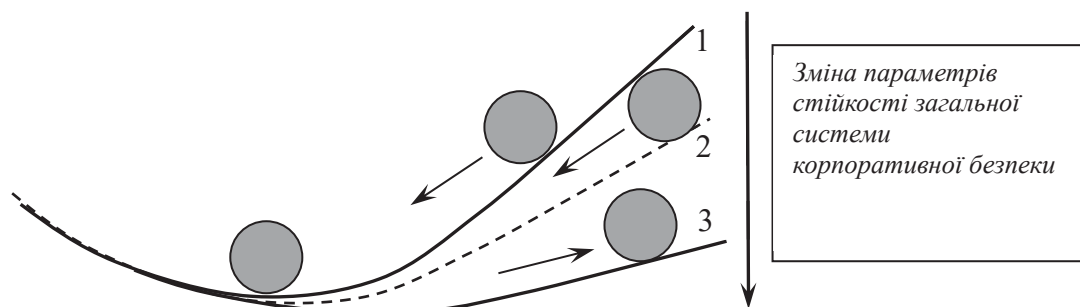


Рис. 2 – Вплив групи факторів на зміну стійкості загальної системи корпоративної безпеки

Щоб сформувати систему корпоративного забезпечення, треба крім вимог стійкості задовольняти вимогам керованості.

В.Н. Іванов розуміє керованість як «відношення між керуючою здатністю органу управління та складністю об'єкта управління» [3, с. 249], а по А.В. Тихонову керованість – це реальна можливість раціонального втручання та впливу на процес в бажаному для суспільства напрямку [4, с. 121]. Згідно В.Л. Тамбовцев, «управління як категорія характеризує керуючу систему, що включає об'єкт управління та систему управління, містить як мінімум два аспекти. По-перше, це наявність принципової можливості цілеспрямовано впливати на об'єкт управління. По-друге, це адекватність засобів, використовуваних системою управління для впливу на об'єкт управління» [5, с. 3]. Е. Демінг зазначає, що результати більшості видів управління не підлягають вимірюванню, а ефект змін від дій керівництва може проявитися через кілька місяців і навіть років [4, с. 62].

Керованість системою корпоративного забезпечення – одне з найважливіших властивостей системи управління, яке описує можливість перевести систему з одного стану в інший. Керованість системою корпоративної безпеки це характеристика системи виконувати завдання по досягненню конкретних цілей. Тут доцільно виділити два основних компоненти:

1) можливість впливати на параметри стану системи корпоративної безпеки, в яких фіксується конкретна мета;

2) достатність ресурсного забезпечення для руху по траєкторії у напрямку до конкретної мети.

Локальні випадки керованості та захисту окремими елементами корпоративної безпеки складають обов'язкові умови функціонування загальної системи корпоративного забезпечення. Ефективність таких заходів залежить від знання властивостей системи окремих локальних елементів корпоративної безпеки і здатності передбачати можливі загрози. Однак для досягнення впевненості в безпеці загальної системи корпоративної безпеки

повинні бути передбачені глобальні заходи щодо ліквідації загроз в небезпеку. В даному випадку, глобальність обмежується кордонами загальної системи корпоративного забезпечення.

Природна стійкість системи корпоративного забезпечення передбачає таку структуру системи окремих локальних елементів корпоративного забезпечення, при якій їх узгоджене функціонування здійснюється на основі внутрішньої здатності до самоорганізації. В цьому випадку збої в одній підсистемі окремих локальних елементів корпоративної безпеки можуть привести до переструктуризації окремих елементів системи, уповільнити її розвиток, але не порушуючи цілісності загальної системи корпоративної безпеки. Стійкість загальної системи корпоративної безпеки зберігається навіть при наявності деяких дезінтеграційних процесів [6, с. 248].

Стан це миттєва характеристика системи корпоративного забезпечення, що забезпечує певні властивості системи в конкретний момент часу. Стан визначається через вхідні дії та вихідні результати, також через дію факторів мікро- та макроекономічного середовища. Стан системи корпоративної безпеки може бути статичним та динамічним. Статистична системи корпоративної безпеки – це система стабільного стану. Динамічна системи корпоративної безпеки – це система з безліччю станів, що з плином часу переходить з одного стану в інший під впливом факторів мікро- та макроекономічного середовища.

З урахуванням того що стійкість різних окремих локальних елементів корпоративного забезпечення по відношенню до впливів факторів мікро- та макроекономічного середовища різна, загальна стійкість системи визначається найменш стійким зв'язком або слабкою ланкою в системі.

Залежно від механізмів розвитку та характеру стійкості загальної системи корпоративного забезпечення виділяють три види криз (рис. 3):

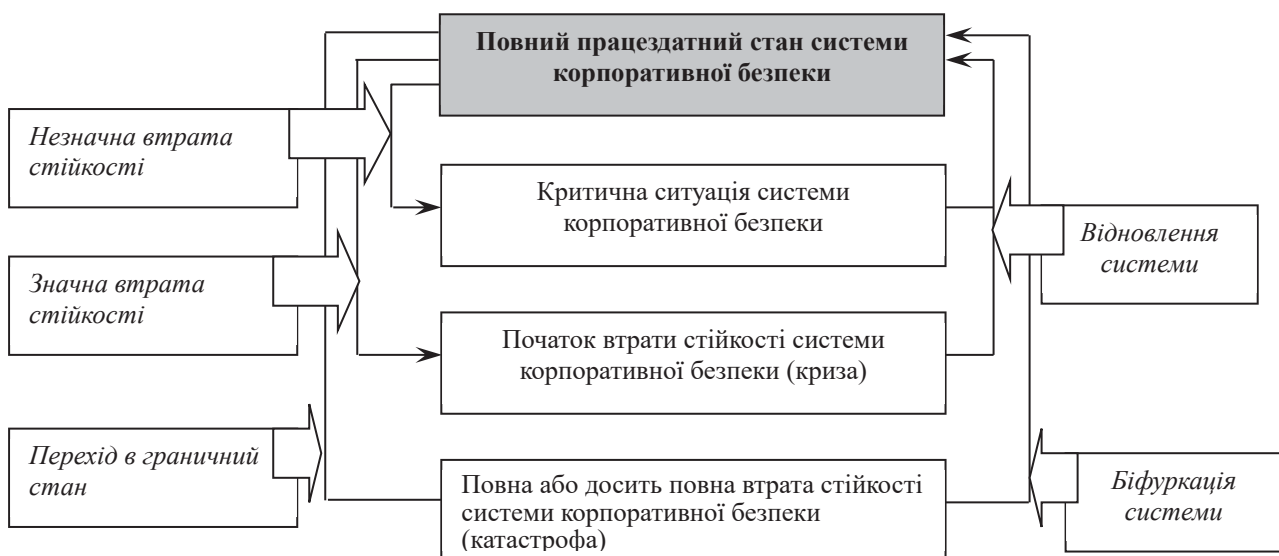


Рис. 3 – Стан загальної системи корпоративного забезпечення

1) критична ситуація системи корпоративного забезпечення – це коли порушення стійкості системи долається шляхом адаптації системи корпоративної безпеки до змін мікро- та макроекономічного середовища;

2) кризовий стан, тобто початок втрати стійкості системи корпоративного забезпечення – це має місце коли даний процес через дію факторів мікро- та макроекономічного середовища не призводить до розпаду системи корпоративної безпеки;

3) катастрофи, повна або досить повна втрата стійкості системи корпоративного забезпечення – система руйнується, можливо елементи системи частково зберігаються, але системоутворюючі ознаки системи корпоративної безпеки зникають.

Збереження стійкості різних окремих локальних елементів корпоративного забезпечення по відношенню до впливів факторів мікро- та макроекономічного середовища доцільно звести до досягнення стану гомеостазу системи корпоративної безпеки. Це такий стан системи корпоративного забезпечення, при якому дотримується деяка динамічна рівновага окремих локальних елементів корпоративної безпеки, що гарантує підтримку значень загальних параметрів в певному безпечному діапазоні, який визначає ефективне функціонування системи корпоративної безпеки. Крім того, стан гомеостазу системи корпоративної безпеки можна також розглядати як, прагнення даної системи долати опір зовнішньому середовищу [7, 8, 9].

Існують два основних етапи аналізу надійності функціонування системи корпоративного забезпечення:

1) перший етап називається апіорним аналізом надійності системи корпоративної безпеки. Цей аналіз передбачає відомі кількісні характеристики надійності різних окремих локальних елементів системи корпоративної безпеки. Для внутрішніх елементів, у яких ще немає достатніх кількісних характеристик надійності, їх враховують за аналогією з характеристиками аналогічних елементів інших підприємств. Таким чином, апіорний аналіз базується на апіорних (імовірнісних) характеристиках надійності системи корпоративної безпеки, які достатньо приблизно відображають дійсні процеси. Проте, цей апіорний аналіз дозволяє виявити слабкі з точки зору надійності місця в системі корпоративної безпеки та вжити необхідні заходи щодо їх усунення.

2) другий етап називається апостеріорним аналізом надійності системи корпоративної безпеки. Його проводять на підставі статистичної обробки економічних даних про працездатність, стійкість та відновленість різних окремих локальних елементів корпоративної безпеки. Ці оцінки отримують методами економіко-математичної статистики за результатами спостережень за системою корпоративної безпеки.

У будь-якому випадку під аналізом надійності системи корпоративної безпеки слід розуміти визначення конкретних значень показників надійності системи (апіорний аналіз), або статистичних оцінок

показників надійності (апостеріорний аналіз).

Показниками надійності називають кількісні характеристики одного або декількох властивостей системи корпоративного забезпечення, що визначають надійність різних окремих локальних елементів корпоративного забезпечення або загальної.

Розрізняють два основних види показників надійності системи корпоративного забезпечення:

1) одиничний показник надійності системи – це кількісна характеристика одного з розглянутих раніше властивостей системи.

2) комплексний показник надійності системи – це інтегрована кількісна характеристика, що визначає два або більше властивостей надійності системи корпоративної безпеки одночасно.

Вибір показників надійності системи корпоративного забезпечення багато в чому залежить від призначення різних окремих локальних елементів корпоративної безпеки та характеру їх функціонування. При виборі показників надійності слід мати на увазі, що ці показники повинні достатньо повно описувати надійнісні властивості системи, бути зручними для аналітичного розрахунку та допускати можливість переходу до показників якості та ефективності.

Кількісна оцінка надійності окремих локальних елементів корпоративного забезпечення та системи корпоративного забезпечення в цілому проводиться зазвичай за допомогою як одиничних показників, так і комплексних показників надійності системи, що визначають властивості безвідмовності і відновлюваності системи корпоративної безпеки.

Для проведення аналізу надійності загальна система корпоративного забезпечення розглядається з точки зору різних окремих локальних елементів корпоративного забезпечення, щоб отримати прийнятну точність оцінки надійності. Потім розраховуються показники надійності корпоративного забезпечення для визначення слабких місць системи та визначається спосіб підвищення ступеня надійності.

Розподіл заданої надійності загальної системи корпоративного забезпечення за різними окремими локальними елементами потребує вирішення такого нерівності:

$$f(R_1, R_2, R_3, \dots, R_n) \geq R^*,$$

де  $R^*$  – розподіл заданої надійності загальної системи корпоративної безпеки;

$f$  – функціональне співвідношення між локальними елементами корпоративної безпеки та загальною системою корпоративної безпеки.

$R_i$  – задана ймовірність безвідмовного функціонування  $i$ -го окремого локального елемента корпоративної безпеки.

Ефективність функціонування системи корпоративного забезпечення може змінюватися від нуля, що означає повне припинення роботи промислового підприємства, до деякої передбаченої задалегідь величини за фактичною надійності

системи корпоративної безпеки. На основі ретельного вибору окремих локальних елементів корпоративної безпеки та їх структурної побудови можна забезпечити високу ступінь надійності системи корпоративної безпеки.

До показників надійності загальної системи корпоративного забезпечення варто віднести такі кількісні характеристики:

1) Ймовірність безвідмовної роботи системи корпоративного забезпечення (рис. 4) – це ймовірність безвідмовної роботи на заданому інтервалі часу, тобто ймовірність того, що робота до першої кризи перевищує величину  $t$  та на зазначеному проміжку часу збій не виникне.

Якщо позначити момент початку роботи за початок відліку, то ймовірність безвідмовної роботи системи корпоративної безпеки на заданому інтервалі часу можна записати у вигляді функції надійності:

$$p(t) = P\{\xi > t\}, t \geq 0,$$

де  $p(t)$  – ймовірність безвідмовної роботи системи корпоративної безпеки;

$\xi$  – час першої кризи;

$t$  – заданий інтервал часу.

З огляду на, що в момент початку роботи системи корпоративної безпеки працездатна та  $p(0) = 1$ , функція  $p(t)$  є монотонно спадною від 1 до 0. Очевидним є факт, що  $p(\infty) = 0$  система корпоративної безпеки при  $t \rightarrow +\infty$  в певний момент часу досягне кризи, тобто відмовить. Ймовірність безвідмовної роботи системи корпоративної безпеки – це ймовірність того, що за певний час  $t$  кризового стану в системі не відбудеться.

2) Ймовірність відмови системи корпоративного забезпечення (рис. 4) – це ймовірність того, що перша криза відбудеться через деякий час, який не перевищує зазначеного проміжку часу  $t$ . Дана подія

може бути представлено у вигляді функції ненадійності:

$$q(t) = P\{\xi \leq t\} = 1 - p(t), t \geq 0,$$

де  $q(t)$  – ймовірність відмови системи корпоративної безпеки.

3) Ймовірність відновлення системи корпоративного забезпечення (рис. 5) називається ймовірність того, що після моменту настання відмови працездатність системи корпоративного забезпечення буде відновлена за час  $t$ , що не перевищує заданий час.

Ймовірність відновлення системи корпоративного забезпечення можна записати у вигляді функції такого вигляду:

$$p_e(t) = P\{\eta \leq t\}, t \geq 0,$$

де  $p_e(t)$  – ймовірність відновлення системи корпоративної безпеки.

4) Ймовірність невідновлення системи корпоративного забезпечення (рис. 5) на заданому інтервалі часу, це ймовірність того, що  $\eta > t$  та можна описати таким чином:

$$q_e(t) = P\{\eta > t\}, 1 - p_e(t),$$

де  $q_e(t)$  – ймовірність невідновлення системи корпоративного забезпечення.

У зв'язку зі специфічними особливостями загальної системи корпоративного забезпечення, її слід розглядати як сукупність суб'єктивних складових окремих локальних елементів корпоративної безпеки, таких як економічна, технологічна, інформаційна, юридична, кадрова, транзакційна, логістична та ресурсна безпека, що взаємопов'язані та взаємодіючі між собою.

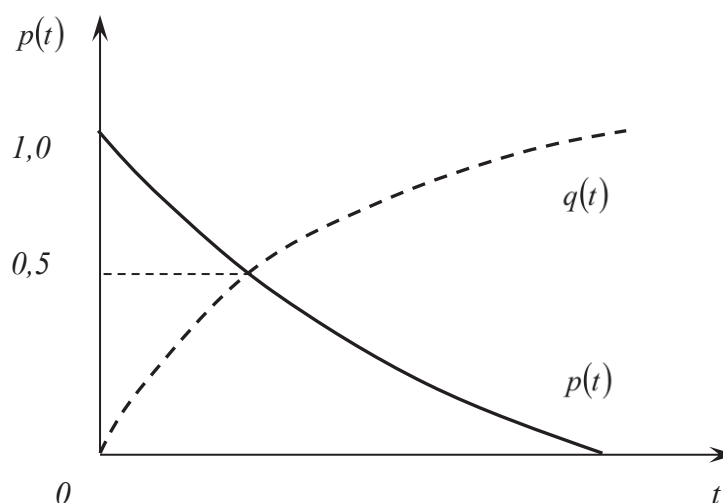


Рис. 4 – Ймовірність безвідмовної роботи та ймовірність відмови системи корпоративного забезпечення

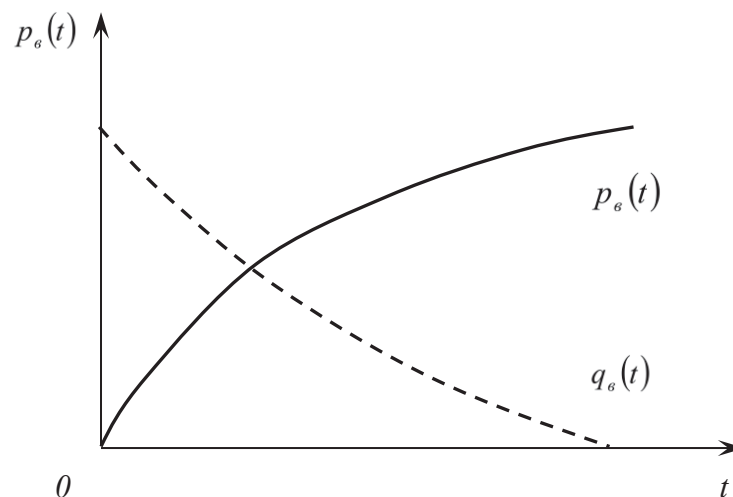


Рис. 5 – Імовірність відновлення та невідновлення системи корпоративного уозезпечення

Перевірка адекватності моделі та системи корпоративного уозезпечення повинна показувати, як вона реагує на зміни у мікро- та макроекономічному середовищі [10, с. 478-495; 11, с. 72-73; 12]. При аналізі системи корпоративної безпеки здійснюється її декомпозиція з визначення окремих моделей локальних елементів корпоративної безпеки та встановленням характеристик структурних елементів та зв'язків, а при синтезі має місце агрегування окремих моделей локальних елементів корпоративної безпеки. Слід брати до уваги, що проблема відповідності між реальною системою корпоративної безпеки та моделлю системи корпоративної безпеки досить складна, тому нами розглянута концептуальна модель, що відноситься до метиорієнтованих систем комплексної корпоративної безпеки.

#### Список літератури

1. Спицнадель В.Н. *Основы системного анализа*: Учебн. пособие. СПб.: Изд. дом «Бизнес-пресса», 2000. – 326 с.
2. Могилевский В.Д. *Методология систем: вербальный подход*. М.: ОАО «Издательство «Экономика», 1999. – 251 с.
3. *Основы современного социального управления: теория и методология*: учеб. пособие / под ред. В. Н. Иванова. – М.: Экономика, 2000. – 271 с.
4. Тихонов А. В. *Социология управления. Теоретические основы*. – СПб.: Изд-во СПбГУ, 2000. – 324 с.
5. Тамбовцев В. Л. *Государство и переходная экономика: пределы управляемости*. – М., 1997. – 125 с.
6. Аккоф Р. *Планирование будущего корпорации* / Р. Аккоф. – М.: Прогресс, 1985. – 431 с.
7. Ареф'єва О.В. *Планування економічної безпеки підприємств* / О. В. Ареф'єва, Т. Б. Кузьменко. – К. : Вид-во Європ. ун-ту, 2005. – 170 с.
8. Бандурка О. М. *Основы экономической безопасности* / О. М. Бандурка, В. С. Духов, К. Я. Петрова, І. М. Черв'яков. – Х. : Вид-во Нац. ун-ту внутр. справ, 2003. – 236 с.
9. Рапопорт А. *Общая теория систем*. – М.: «Мир», 1966. – С. 325.
10. Аккоф Р. Л., Сасиени М. *Методы исследования операций* / Пер. с англ.– М.: Мир, 1971.– 536 с.
11. Нагуманова Р.В. *Контроллинг как современный метод управления субъектами различных сфер деятельности* / Р.В. Нагуманова, А.И. Сабирова. – Казань: Изд-во Казан. ун-та,

2016. – 82 с.

12. Карминский А.М. *Контроллинг в бизнесе: методологические и практические основы построения контроллинга в организациях* /А.М. Карминский, Н.И. Оленев, А.Г. Примак, С.Г. Фалько. – М.: Финансы и статистика, 1998. – 256 с.

#### References (transliterated)

1. Spicnadel V.N. *Osnovy sistemnogo analiza* [Fundamentals of Systems Analysis]: Uchebn. posobie. SPb.: Izd. dom «Biznes-pressa», 2000. – 326 p.
2. Mogilevskij V.D. *Metodologiya sistem: verbalnyj podhod* [Systems Methodology: Verbal Approach]. Moscow: OAO «Izdatelstvo «Ekonomika», 1999. – 251 p.
3. *Osnovy sovremennogo socialnogo upravleniya: teoriya i metodologiya* [Foundations of modern social management: theory and methodology]: ucheb. posobie / pod red. V. N. Ivanova. – Moscow: Ekonomika, 2000. – 271 p.
4. Tihonov A. V. *Sociologiya upravleniya. Teoreticheskie osnovy* [Sociology of management. Theoretical basis]. – SPb.: Izd-vo SPbGU, 2000. – 324 p.
5. Tambovcev V. L. *Gosudarstvo i perehodnaya ekonomika: predely upravlyaemosti* [State and transitional economy: limits of manageability]. – Moscow, 1997. – 125 p.
6. Akkof R. *Planirovanie budushhego korporacii* [Planning the future of the corporation] – Moscow: Progress, 1985. – 431 p.
7. Aref'yeva O.V. *Planuvannya ekonomichnoyi bezpeki pidpriemstv* [Economic security planning of enterprises] / O. V. Aref'yeva, T. B. Kuzmenko. – Kiev: Vid-vo Yevrop. un-tu, 2005. – 170 p.
8. Bandurka O. M. *Osnovi ekonomichnoyi bezpeki* [Fundamentals of economic security] / O. M. Bandurka, V. Ye. Duhov, K. Ya. Petrova, I. M. Cherv'yakov. – H. : Vid-vo Nac. un-tu vnutr. sprav, 2003. – 236 p.
9. Rapoport A. *Obshaya teoriya sistem* [General systems theory]. – Moscow: «Mir», 1966. – p. 325.
10. Akof R. L., Sasieni M. *Metody issledovaniya operacij* [Operations Research Methods] / Per. s angl.– Moscow: Mir, 1971.– 536 p.
11. Nagumanova R.V. *Kontrolling kak sovremennyj metod upravleniya subektami razlichnyh sfer deyatelnosti* [Controlling as a modern method of managing subjects of various fields of activity] / R.V. Nagumanova, A.I. Sabirova. – Kazan: Izd-vo Kazan. un-ta, 2016. – 82 p.
12. Karminskij A.M. *Kontrolling v biznese: metodologicheskie i prakticheskie osnovy postroeniya kontrollinga v organizacijah* [Controlling in Business: Methodological and Practical Foundations of Building Controlling in Organizations] /A.M. Karminskij, N.I. Olenev, A.G. Primak, S.G. Falko. – Moscow: Finansy i statistika, 1998. – 256 p.

Надійшла (received) 15.02.2021

#### Відомості про авторів / Сведения об авторах / About the Authors

**Волоснікова Наталія Миколаївна (Волосникова Наталья Николаевна, Volosnikova Nataliia)** – кандидат економічних наук, доцент, доцент кафедри загальної економічної теорії, Національний технічний університет «Харківський політехнічний інститут»: (066)6546909, Nataliia.Volosnikova@khpi.edu.ua