УДК 338.43 : 004. 056
DOI: https://doi.org/10.36887/2415-8453-2019-3-21

Дмитро Володмирович ДЯЧКОВ

кандидат економічних наук, доцент,
доцент кафедри менеджменту, Полтавська державна аграрна академія
ORCID ID: 0000-0002-2637-0099
E-mail: dmiraf@ukr.net

РОЗРОБКА МЕТОДОЛОГІЧНИХ ЗАСАД ОЦІНЮВАННЯ ТА ДІАГНОСТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ АГРОПРОДОВОЛЬЧОЇ СФЕРИ

Дячков, Д. В. Розробка методологічних засад оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери [Текст] / Дмитро Володимирович Дячков // Український журнал прикладної економіки. – 2019. – Том 4. – № 3. – С. 188–197. – ISSN 2415-8453.

Анотація

Мета. *Мета статті полягає у розробці методологічних засад оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери.*

Методи дослідження. *Вирішення поставлених у статті завдань здійснено за допомогою загальнонаукових і спеціальних методів дослідження: аналізу та синтезу, систематизації та узагальнення, методу групування, діалектичного підходу.*

Результати дослідження. *Визначено та охарактеризовано способи та методи оцінки інформаційної безпеки підприємства: оцінку за еталоном, ризик-орієнтовану оцінку й оцінку за економічними показниками. Значна частина методик оцінки рівня інформаційної безпеки підприємства, аграрного підприємства зокрема, базується на визначенні інформаційних ризиків на основі американських та британських методик CRAMM, FRAP, OCTAVE, NIST, MSAT, COBRA та російської методики ГРИФ 2006.*

Висновки. *Доведено, що для розробки методологічних засад оцінки та діагностики рівня інформаційної безпеки підприємства доцільно використати переваги методів оцінки за еталоном, за ризиком інформаційної системи, використати групові та приватні показники економічної складової оцінки інформаційної безпеки.*

Практичне значення. *У статті запропоновано концепцію розробки методології економічного оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери, яка враховує переваги розглянутих методик діагностики та оцінювання рівня інформаційної безпеки аграрних підприємств, дозволяє провести кількісну та якісну оцінку її складових, визначити вплив інтегральних індексів на результативні показники діяльності та безпеки суб'єктів агарного бізнесу, і як результат, запропонувати ефективні шляхи оптимізації системи управління інформаційною безпекою підприємства агропродовольчої сфери. Основні наукові положення статті можна використовувати у практиці аграрних підприємств.*

Ключові слова: *економічні показники оцінки, еталон, концепція, методи оцінки інформаційної безпеки, методологія, підприємство агропродовольчої сфери, ризикоорієнтований підхід, управління інформаційною безпекою.*

Dmytro DIACHKOV

Candidate of Economics (PhD), associate professor of
of the Department of Management, Poltava State Agrarian Academy

DEVELOPMENT OF METHODOLOGICAL BASES FOR INFORMATION SECURITY ASSESSMENT AND DIAGNOSTICS OF AGRO-FOOD ENTERPRISES

Abstract

Introduction. *The purpose of the article was to develop methodological foundations for assessing and diagnosing the information security of agricultural enterprises.*

Methods of research. *The tasks of the article were solved by means of general and special methods of research: analysis and synthesis, systematization and generalization, method of grouping, dialectical approach.*

Results*. The ways and methods of the information security assessment of the enterprise were defined and characterized. Among them are: standard-based assessment, risk-oriented assessment and economic indicators. Much of the methodology for assessing the level of an enterprise information security, agrarian enterprise in particular, were based on the identification of information risks based on US and British methods CRAMM, FRAP, OCTAVE, NIST, MSAT, COBRA and Russian GRIF 2006 methodology.*

Originality. *It was proved that for methodological bases development of estimation and diagnostics of enterprise information security level it is expedient to use advantages of estimation methods by standard, at risk of information system and using group and private indicators of economic component of information security estimation.*

Practical importance. *The concept of the methodology development for economic assessment and information security diagnostics of agri-food enterprises was proposed, which takes into account the advantages of the considered diagnostics and assessment methods of the information security level of agricultural enterprises, offers a quantitative and qualitative assessment of its components, determines the impact of integrated indexes on the performance indicators and safety of subjects agricultural business, and, as a result, offer effective ways to optimize the management of information security companies in agri-food sector. The main scientific provisions of the article can be used in the practice of agricultural enterprises.*

Keywords: *concept, economic indicators of assessment, enterprise of agro-food sphere, management of information security, methodology, methods of assessment of information security, risk-oriented approach, standard.*

JEL classification: F52; M15

Вступ

Діяльність вітчизняних аграрних підприємств відбувається в умовах інформатизації управлінських процесів, автоматизації виробничих процесів, технологічних процесів, а також цифровізації соціально-економічних взаємовідносин суб'єктів агарного ринку. Зазначене потребує визначення не тільки рівня інформатизації та автоматизації окремих бізнес-процесів підприємства, а й визначення рівня захисту інформаційної сфери функціонування підприємств агропродовольчої сфери. Оскільки сучасна інформаційна система аграрного підприємства являє собою складну систему, що складається з великого числа компонентів різного ступеня автономності, які пов'язані між собою та між якими здійснюються процеси обміну даними. Практично кожен компонент зазначеної інформаційної системи піддається впливу атак зловмисника або впливам зовнішнього середовища. Найбільш уразливими до атак є програмні засоби, технічні засоби та засоби захисту інформації інформаційної системи. А найбільш розповсюдженими загрозами можуть бути атаки на операційну систему, на системи управління базами даних, на міжмережевий екран, на web-сервер,

на комунікаційне обладнання тощо. При здійсненні зазначених атак для агарних підприємств настають наслідки різних степенів складності. Варто відмітити, що окрім втрати інформації, розголошення комерційної таємниці, втрати іміджу підприємства, в процесі здійснення інформаційної атаки під значним ризиком перебуває економічна, зокрема фінансова складова, що виступає результатом діяльності сільськогосподарського підприємства.

Власне тому актуальності набуває розробка методологічних засад оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери.

Дослідження окремих теоретичних і практичних аспектів економічної оцінки інформаційної безпеки аграрного підприємства, зокрема розробка методології її діагностики, знайшли відображення у працях вітчизняних та зарубіжних науковців, таких як: Алексеєва В., Андріанова В., Бучика С., Гокена А., Губарєвої О., Зефірова С., Івко С., Куканової Н., Лаврута О., Оксенюка В., Пугина В., Пузиренко О., Родіна Є., Смірнової С., Стоунберна Г., Сьомкіної А., Ферінга А., Цибуліна А., Цуканової О., Шалаєва В.

Доцільно відзначити, що методологічні засади економічного оцінювання та діагностики інформаційної безпеки суб'єктів агропродовольчої сфери розроблені недостатньо. Відсутність уніфікованої та найбільш точної методики економічної оцінки рівня безпеки суб'єктів підприємницької діяльності також можна пояснити складнощами математичної формалізації більшості показників інформаційної сфери діяльності аграрного підприємства, оскільки наявні методи оцінювання рівня інформаційної безпеки підприємств агропродовольчої сфери у більшості випадків не можуть забезпечити співставність показників. Також сучасні методи характеризуються відсутністю фіксованих меж для інтегрального показника оцінки та діагностики інформаційної безпеки. Зазначене обумовило формулювання мети дослідження.

Мета дослідження

Формулювання цілей статті – розробка методологічних засад оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери.

Виклад основного матеріалу дослідження

Залежно від критерію оцінки інформаційної безпеки доцільно розділити способи оцінки інформаційної підприємства на оцінку за еталоном, ризик-орієнтовану оцінку та оцінку за економічними показниками.

Спосіб оцінки інформаційної безпеки за еталоном передбачає порівняння діяльності та заходів щодо забезпечення інформаційної безпеки з вимогами, які виконуються підприємством-еталоном. Тобто здійснюється оцінка системи управління безпекою підприємства встановленим зразковим характеристикам та визначається ступінь відхилення від них. За допомогою зазначеного методу оцінки визначається відповідність системи захисту інформації та вимірюється ефективність реалізації процесів системи забезпечення інформаційної безпеки та ідентифікуються недоліки такої реалізації.

В результаті проведення оцінки інформаційної безпеки повинна бути сформована оцінка ступеня відповідності системи інформаційної безпеки підприємства еталону, в якості якого можуть бути прийняті (в сукупності та окремо): вимоги законодавства, галузеві, вимоги нормативних, методичних та організаційно-розпорядчих документів, вимоги національних і міжнародних стандартів щодо забезпечення інформаційної безпеки.

Алгоритм оцінки інформаційної безпеки за еталоном передбачає, перш за все, вибір еталона; на його основі формування критеріїв і показників оцінки інформаційної безпеки; визначення їх нормативних значень; оцінка системи інформаційної безпеки інших об'єктів і співставлення отриманих значень з еталоном; визначення причин

відхилень; розробка заходів з метою оптимізації рівня інформаційної безпеки об'єктів дослідження [1].

Ризик-орієнтований підхід до оцінки інформаційної безпеки підприємства передбачає визначення ризиків інформаційної безпеки, що виникають в інформаційно-комунікаційній сфері аграрного підприємства, на основі яких розробляються заходи щодо недопущення ризиків, оптимізації та мінімізації їх впливів, усунення наслідків тощо. Результатом повинно стати формування системи управління ризиками інформаційної безпеки підприємства [4].

Значна частина методик оцінки рівня інформаційної безпеки підприємства, аграрного підприємства зокрема, базується на визначенні інформаційних ризиків. Відтак, за дослідженнями, проведеними Пугиним В. В., Губарєвою О. Ю., Пузиренко О. Г., Івко С. О., Лаврутом О. О., Кукановою Н., Родіним Є. С., Бучиком С. С., Шалаєвим В. О., Оксенюком В. та іншими оцінку інформаційної безпеки пропонується визначати на основі американських і британських методик CRAMM, FRAP, OCTAVE, NIST, MSAT, COBRA та російської методики ГРИФ 2006. Характеристика даних методик та їх особливості наведені в табл. 1.

На основі узагальнення основні етапи ризик-орієнтованої оцінки інформаційної безпеки можна представити у такій послідовності: формування профілю загроз інформаційній безпеці; ідентифікація ризиків інформаційної безпеки; характеристика існуючої системи управління інформаційної безпеки, зокрема інформаційними ризиками; формування критеріїв оцінки ризиків інформаційної безпеки, оцінка та вимірювання ризик-факторів інформаційної безпеки агарного підприємства; формування звіту; розробка стратегії та планів інформаційної безпеки (ризикозахищеності).

Таблиця 1. Характеристика методик оцінки та діагностики інформаційної безпеки підприємства на основі визначення інформаційних ризиків [узагальнено автором на основі 2, 5, 6, 7, 8, 9, 10]

Тип	Характеристика методики	Алгоритм проведення оцінки та діагностики
CRAMM (CCTA Risk Analysis and Managment Method)	• оцінка ризиків функціонування інформаційної системи; • проведення обстеження інформаційної системи та розробка супровідної документації на всіх етапах його проведення; • здійснення аудит згідно стандарту BS 7799: 1995 «Code of Practice for Information Security Management»; • формування політики безпеки, та її інформаційної складової, розробка заходів «безперервності» бізнесу, стратегії розвитку;	Для кожного етапу визначається набір вихідних даних, послідовність заходів, анкети для проведення інтерв'ю, списки перевірки і набір звітних документів: I етап – ідентифікація та визначення цінності ресурсів, що захищаються; II етап – ідентифікація і оцінка загрози в сфері інформаційної безпеки, пошук і оцінка вразливостей системи, яка підлягає захисту; II етап – генерування варіантів заходів протидії виявленим ризикам. Розробляються рекомендації: загального характеру; конкретні рекомендації для об'єктів захисту; приклади того, як можна організувати захист в конкретній ситуації.
FRAP (Facilitated Risk Analysis Process)	• оцінка рівня ризику для незахищеної ІС, що надалі дозволяє показати ефект від впровадження засобів захисту інформації; • кількісна методика оцінки ризику через числове значення, (наприклад розмір очікуваних річних втрат і оцінка повернення інвестицій); • оцінка вигоди від впровадження фізичних, технічних, програмних та інших засобів і механізмів захисту;	Процедура оцінки: I етап – визначення активів, в тому числі інформаційних, які потребують захисту, через опитувальні листи, інтерв'ювання, вивчення документації, використання інструментів автоматизованого аналізу (сканування) мереж; II етап – ідентифікація загроз. На цьому етапі можливе застування декількох підходів: - попередньо підготовлені переліки загроз експертами (checklists); - аналіз статистики подій в інформаційній системі (частота їх виникнення); - «мозковий штурм». II етап – визначення ймовірності виникнення загрози інформаційній безпеці; оцінка можливого збитку в наслідок виникнення загрози.

Продовження табл. 1

Тип	Характеристика методики	Алгоритм проведення оцінки та діагностики
ГРИФ 2006	• надає можливість IT менеджеру самостійно (без залучення сторонніх експертів) оцінити рівень ризиків в інформаційній системі; • оцінити ефективність існуючої практики щодо забезпечення безпеки підприємства;	Метод включає наступні етапи: I етап – опитування IT-менеджера з метою визначення повного списку інформаційних ресурсів, які мають цінність для підприємства; I етап – введення в систему ГРИФ всіх видів інформації, що представляє цінність; III етап – визначення збитку по кожній групі цінної інформації, розташованої на відповідних ресурсах, за всіма видами загроз; IV етап – визначення всіх видів користувальницьких груп та інформації на ресурсах, до якої має доступ кожна з груп користувачів; V етап – визначення видів (локальний або віддалений) і права (читання, запис, видалення) доступу користувачів до всіх ресурсів, що містять цінну інформацію; VI етап – визначення засобів захисту інформації. В систему вводиться інформація про разові витрати на придбання всіх засобів захисту інформації та щорічні витрати на їх технічну підтримку, а також – щорічні витрати на супровід системи інформаційної безпеки підприємства; VII етап – опитування користувачів відповідно до списку питань з політики безпеки, реалізованої в системі, що дозволяє оцінити реальний рівень захищеності системи і деталізувати оцінки ризиків; VIII етап – формування звіту за систему. Звітом є докладний документ, що дає повну картину можливого збитку від інцидентів.
OCTAVE	• формування профілю загроз, який передбачає інвентаризацію та оцінку цінності активів; • ідентифікація вимог законодавства та нормативної бази; • визначення системи організаційних заходів з підтримки режиму інформаційної безпеки; • при оцінці ризику дана експертна система дає тільки оцінку очікуваного збитку, без оцінки вірогідності;	Передбачає три фази аналізу ризику: I фаза – розробка профілю загроз, пов'язаних з активом; II фаза – ідентифікація інфраструктурних вразливостей; III фаза – розробка стратегії та планів безпеки.
NIST (National Institute of Standards and Technology)	• пов'язана із формуванням стратегії управління ризикам, • є базисом для розроблення власної системи управління ризиками; • процес оцінювання ризику інформаційної безпеки, представляється у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту; • значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою;	Передбачає етапи: I етап – опис характеристик системи; II етап – ідентифікація загроз; III етап – ідентифікація вразливостей; IV етап – аналіз наявних засобів/заходів захисту; V етап – визначення значення ймовірності; VI етап – аналіз впливу; VII етап – визначення значення ризику; VIII етап – вибір засобів/заходів захисту; IX етап – документування отриманих результатів.
MSAT (Microsoft Security Assessment Tool)	• дозволяє отримати якісну оцінку ризиків інформаційної безпеки за чотирма характеристиками ІКС: інфраструктура, програмне забезпечення, функціонування, персонал; для кожної характеристики визначені якісні оцінки ризиків інформаційної безпеки; • оцінка ризиків інформаційної безпеки проводиться за трьохбальною шкалою;	Процес оцінки ризиків інформаційної безпеки з використанням передбачає заповнення полів бази даних експертної системи. На цього експертна система формує звіт з переліком якісних оцінок ризиків інформаційної безпеки ІКС та пропозицій стосовно покращення організації системи захисту інформації.

Закінчення табл. 1

Тип	Характеристика методики	Алгоритм проведення оцінки та діагностики
COBRA (Consultative Objective and BiFunctional Risk Analysis)	• у комплект програмного забезпечення входять модулі COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant, а також менеджер модуля COBRA, який призначений для налаштування та зміни наявної бази знань; • дозволяє виконати в автоматизованому режимі найпростіший варіант оцінювання інформаційних ризиків будь-якого підприємства; • надає оцінку відносній важливості всіх загроз і уразливостей, • генерує відповідні рішення та рекомендації.	Передбачає три фази аналізу ризиків: I фаза – розробка профілю загроз, пов'язаних з активом; II фаза – ідентифікація інфраструктурних уразливостей; III фаза – розробка стратегії та планів безпеки. Цей метод пропонує скласти профіль загроз та дерево варіантів. Профіль загрози включає в себе вказівки на актив (asset), тип доступу до активу (access), джерело загрози (actor), тип порушення або мотив (motive), результат (outcome) і посилання на описи загрози в загальнодоступних каталогах [8].

На основі наданих характеристик розглянутих ризико-орієнтованих методик оцінки та діагностики інформаційної безпеки на ринку інформаційних технологій, їх можна розділити на дві великі групи: програми, що застосовують якісну (наприклад, «високий», «середній», «низький» чи за шкалою від 1 до 10) та кількісну оцінку ризиків (оцінюється через числове значення, наприклад, розмір очікуваних річних втрат). До першої групи належать, наприклад COBRA, FRAP, КОНДОР+, Proteus, FRAP. До другої, наприклад, – RiskWatch, OCTAVE. Проте, є комплекси, що об'єднують ці два підходи (наприклад, CRAMM, MSAT, ГРИФ, NIST, Buddy System) [6].

Розглянуті вище моделі оцінки і діагностики інформаційної безпеки базуються на процесній моделі і пропонують якісні й кількісні показники оцінювання інформаційних ризиків. В разі, якщо показник має якісне вираження, то цю якісну характеристику інтерпретують через чисельну шкалу й вимірюють через кількісний показник.

Найбільш класичною формулою оцінювання ризику (R) є його оцінка через добуток двох факторів: ймовірність реалізації загрози ($P_{реалізації}$) та розмір збитку (D):

$$R = P_{реалізації} \times D, \quad (1)$$

Деталізація ймовірності реалізації загрози можлива через вираження ймовірності виникнення загрози та ймовірність появи вразливості:

$$P_{реалізації} = P_{загрози} \times P_{вразливості}, \quad (2)$$

В основу різних методик визначення рівня ризиків інформаційної безпеки покладені модифікації наведених формул. Наприклад, ризик по всій системі – це сума ризиків по всіх активах та кожній загрозі; ефект від вжитих контрзаходів – це різниця між сумою запланованих витрат на контрзаходи та сумарною оцінкою збитків при визначеному рівні ризику по всій системі [8].

Вирізняється методика, за якої експертами визначаються ймовірності виникнення кожного виду ризику в разі порушення інформаційної безпеки, та розміри, пов'язаних з ним втрат Y (вартість збитку), а також допустимий залишковий ризик $R_{залишковий}$. Всі оцінки ризиків представляються у вигляді матриці [8, 12, 14], яка представлена в табл. 2.

Таблиця 2. Матриця ризиків інформаційної безпеки підприємства [12]

Імовірність атаки (P)	Збиток		
	Низький 0 <Y <= 10 (%)	Середній 10 <Y <= 50 (%)	Високий 50 <Y <= 100 (%)
Висока (0,5 <P <= 1)	Низька 5 <R <= 10 (%)	Середній 10 <R <= 50 (%)	Високий 50 <R <= 100 (%)
Середня (0,1 <P <= 0,5)	Низький 1 <R <= 5 (%)	Середній 5 <R <= 25 (%)	Середній 10 <R <= 50 (%)
Низька (0 <P <= 0,1)	Низький 0 < R <= 1 (%)	Низький 0 <R <= 5 (%)	Низький 0 <R <= 10 (%)

У розглянутій матриці ризиків вартісна міра збитку визначається у відсотках від цінності інформаційного ресурсу на і-му компоненті. Залишковий ризик обчислюється за формулою:

$$R_{залишковий} = P * Y, \quad (3)$$

де P – ймовірність впливу атак;

Y – вартість збитку.

Оцінка $R_{залишковий}$ буде достовірною тільки за умови врахування одночасної дії всіх атак на всі компоненти інформаційної від всіх категорій зловмисників. Нехай на i-й компонент ($i = \overline{1, I}$, де I – кількість вразливих до атак компонентів інформаційної системи) впливає j-я атака ($j = \overline{1, J}$, де J – кількість можливих атак зловмисника на об'єкт) в l-й зоні компонента з боку порушника k-ї категорії (k=$\overline{1, K}$, К – число категорій порушників).

Відповідно до цієї методики, запропонованої Сьомкиною А. А., Цибуліним А. М. вірогідність P_{ijkl} впливу j-й атаки на і-й компонент через l-ну зону уразливості. При цьому вірогідність несанкціонованого доступу до інформації на і-м компоненті інформаційної системи шляхом проведення j-ої атаки через l-ну зону буде дорівнює похідній впливають на нього атак від k-го зловмисника:

$$P_{ikj} = Y_1^{Pijkl}, \quad (4)$$

де l = $\overline{1, L_k}$, L_k – кількість захисних зон компонента для k-го зловмисника.

Імовірність впливу атак з боку k-го зловмисника буде дорівнює:

$$P_{ik} = \sum_{j=1}^{J} Pikj, \quad (5)$$

Тоді ймовірність несанкціонованого отримання інформації на і-м компоненті зі сторони всіх потенційних зловмисників:

$$P_i = \sum_{k=1}^{K} Pik, \quad (6)$$

Імовірність несанкціонованого доступу до інформації в інформаційній системі аграрного підприємства в цілому дорівнюватиме:

$$P = \sum_{i=1}^{I} Pi, \quad (7)$$

При цьому вартість збитку для всієї інформаційної системи підприємства буде дорівнює:

$$Y = \sum_{i=1}^{I} Yi, \quad (8)$$

Отримана формула загального залишкового ризику для всієї інформаційної системи аграрного підприємства:

$$R_{залишковий} = \sum_{i=1}^{I} Pi * \sum_{i=1}^{I} Yi, \quad (9)$$

А в разі невиконання умови: $R_{залишковий} \leq R_{залишковий}$ додатковий означає, що система не захищена і необхідно оновити механізми захисту [12].

Способи оцінки інформаційної безпеки на основі економічних показників є найбільш прийнятними та практично корисними для підприємців агарного ринку. Для проведення оцінки в якості критеріїв ефективності використовуються, показники сукупної вартості володіння (Total Cost of Ownership – TCO); показник очікуваних витрат (ALE), який обчислюється за такою формулою як функціональна залежність між частотою виникнення потенційної загрози та величиної можливих втрат, яка визначається на підставі ступеня тяжкості порушення; економічний ефект від впровадження системи інформаційної безпеки, який визначається різницею від збережених ресурсів за рахунок функціонування системи інформаційної безпеки аграрного підприємства та витрат на її створення (функціонування); рентабельність витрат на формування системи інформаційної безпеки тощо. Також використовуються й групові та приватні показники економічної оцінки інформаційної безпеки. Групові

показники оцінки інформаційної безпеки підприємства агропродовольчої сфери утворюють структуру напрямків оцінки, деталізуючи оцінки поточного рівня інформаційної безпеки підприємства, системи управління нею менеджменту та рівня усвідомлення інформаційної безпеки [3, 11, 13].

На основі узагальнення пропонованих методик оцінки та діагностики рівня інформаційної безпеки агарного підприємства, використання переваг кожної з розглянутих методик пропонується концепція авторської методології економічного оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери (рис. 1).

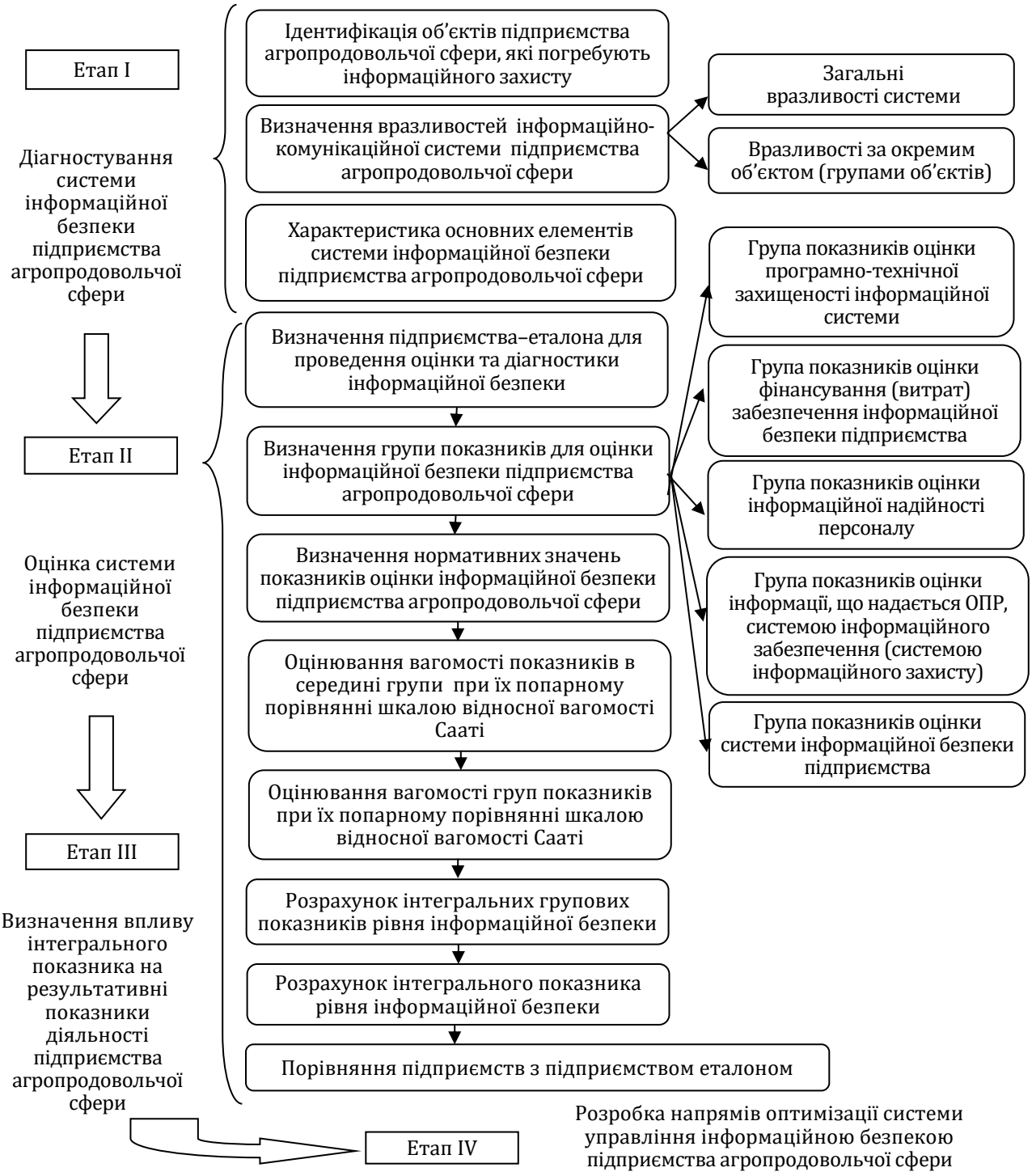

Рис. 1. Концепція розробки методології економічного оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери [розроблено автором]

Висновки та перспективи подальших розвідок

Запропонована концепція розробки методології економічного оцінювання та діагностики інформаційної безпеки підприємств агропродовольчої сфери враховує переваги розглянутих методик діагностики та оцінювання рівня інформаційної безпеки аграрних підприємств, дозволяє провести кількісну та якісну оцінку її складових, визначити виплив інтегральних показників на результативні показники діяльності та безпеки суб'єктів агарного бізнесу, і як результат, запропонувати ефективні шляхи оптимізації системи управління інформаційною безпекою підприємства агропродовольчої сфери.

Перспективами подальших досліджень є апробація пропонованої методики в практичній діяльності агарних підприємств.

Список літератури

1. Андрианов В. В. Обеспечение информационной безопасности бизнеса. URL: https://econ.wikireading.ru/25723
2. Бучик С. С., Шалаєв В. О. Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем. *Наукоємні технології*. 2017. № 3(35). С. 2015-225.
3. Дячков Д. В. Методичні підходи до оцінки інформаційної безпеки підприємства. *Вісник Сумського національного аграрного університету: Серія «Економіка і менеджмент».* 2017. № 12(74). С. 87-92.
4. Зефиров С. Л., Алексеев В. М. Способы оценки информационной безопасности организации. *Труды Международного симпозиума «Надежность и качество».* 2011. № 2. С. 407-409.
5. Куканова Н. Современные методы и средства анализа и управление рисками информационных систем компаний. URL: http://citforum.ru/products /dsec/cramm/
6. Оксенюк В. Використання програмних засобів для оцінки та управління ризиками інформаційної безпеки. URL: http://elartu.tntu.edu.ua/bitstream/lib/30437 /2/IMST_2019_Okseniuk_V-Use_of_software_for_information_75.pdf
7. Пугин В. В., Губарева О. Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия. *T-Comm.* 2012. № 6. С. 54-57.
8. Пузиренко О. Г., Івко С. О., Лаврут О. О., Климович О. К. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах. *Системи обробки інформації.* 2015. Вип. 3(128). С. 75-79.
9. Пузиренко О. Г., Івко С. О., Лаврут О.О. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем. *Системи обробки інформації*: *Інфокомунікаційні системи.* 2014. Вип. 8 (124). С. 128-134.
10. Родін Є.С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки. *Математичні машини і системи.* 2012. № 4. С. 142-148.
11. Саати Т., Кернс К. Аналитическое планирование. Организация систем: Пер. с англ. М.: Радио и связь, 1991. 224 с.
12. Семкина А. А., Цыбулин А. М. Оценка уровня информационной безопасности предприятия через остаточный риск. *Вестник ВолГУ.* 2012. Вып. 6. Серия 10. С. 156-159.
13. Цуканова О. А., Смирнов С. Б. Экономика защиты информации: учебное пособие, 2-е издание, измененное и дополненное. СПб.: НИУ ИТМО, 2014. 79 с.
14. Stoneburner G., Goquen A., Feringa A. Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology . Gaithersburg. USA, 2002. 55 p.

References

1. Andrianov, V. V. Obespecheniye informatsionnoy bezopasnosti biznes [Providing information security for business]. Available at: https://econ.wikireading. ru/25723.
2. Buchik, S. S., Shalaev, V. A. (2017). «Analysis of instrumental methods for determining information security risks of information and telecommunication systems». *Naukoyemni tekhnolohiyi*. no 3(35), pp. 2015-225.
3. Diachkov, D. V. (2017). «Methodical approaches to assessment of information security of the enterprise». *Visnyk Sums'koho natsional'noho ahrarnoho universytetu: Seriya «Ekonomika i menedzhment».* no 12 (74), pp. 87-92.
4. Zefirov, S. L., Alekseev, V. M. (2011). «Methods for assessing the information security of an organization». *Trudy Mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo».* no 2, pp. 407-409.
5. Kukanova, N. Sovremennyye metody i sredstva analiza i upravleniye riskami informatsionnykh sistem kompaniy [Modern methods and means of analysis and risk management of information systems of companies]. Available at: http://citforum.ru /products/dsec/cramm/
6. Oksenyuk, V. (2019). Vykorystannya prohramnykh zasobiv dlya otsinky ta upravlinnya ryzykamy informatsiynoyi bezpeky [Using software tools for information security risk assessment and management]. Available at: http://elartu.tntu.edu.ua/bitstream/lib/30437/2/IMST_2019_Okseniuk_V-Use_of_soft ware _for_information_75.pdf.
7. Pugin, V. V., Gubareva, O. Yu. (2012). «Overview of risk analysis techniques for information security of an enterprise information system». *T-Comm.* no 6, pp. 54-57.
8. Puzyrenko, O. H., Ivko, S. O., Lavrut, O. O., Klymovych, O. K. (2015). «Application of information security risk assessment models in information and telecommunication systems». *Systemy obrobky informatsiyi.* Vol. 3(128), pp. 75-79.
9. Puzyrenko, O. H., Ivko, S. O., Lavrut, O. O. (2014). «Analysis of the process of information security risk management in ensuring the survivability of information and telecommunication systems». *Systemy obrobky informatsiyi: Infokomunikatsiyni systemy.* Vol.8 (124), pp. 128-134.
10. Rodin, E. S. (2012). «Process approaches to modeling in the field of information security risk management». *Matematychni mashyny i systemy.* no 4, pp. 142-148.
11. Saati, T., Cairns, K. (1991). *Analiticheskoye planirovaniye. Organizatsiya system* [Analytical planning. Organization of systems]. Radio and communications. Moscow. Russia.
12. Semkina, A. A., Tsybulin. A. M. (2012). «Assessment of the level of information security of an enterprise through residual risk». *Vestnik VolGU*. Issue. 6. Series 10, pp. 156-159.
13. Tsukanova, O. A., Smirnov, S. B. (2014). *Ekonomika zashchity informatsii: uchebnoye posobiye, 2-ye izdaniye, izmenennoye i dopolnennoye*. [Economics of information security: a training manual, 2nd edition, amended and supplemented]. NRU ITMO. St. Petersburg. Russia.
14. Stoneburner, G., Goquen, A., Feringa, A. (2002). Risk management guide for information technology systems. *Recommendations of the National Institute of Standards and Technology. Gaithersburg. USA*. 55 p.

Стаття надійшла до редакції 25.07.2019 р.