РОЗДІЛ 10. МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

АНАЛІЗ МЕТОДІВ ОЦІНКИ ЕФЕКТИВНОСТІ ВНУТРІШНЬОБАНКІВСЬКОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ[1]

ANALYSIS OF METHODS OF ASSESSING THE EFFICIENCY OF INTRA-BANKING CYBERSECURITY SYSTEM

УДК 330.46
https://doi.org/10.32843/infrastruct41-52

Гриценко К.Г.
к.т.н., доцент,
доцент кафедри економічної кібернетики
Сумський державний університет

Gritsenko Konstantin
Sumy State University

Банківські установи найбільше приваблюють кіберзлочинців. У зв'язку з цим актуальним є завдання створення та оцінювання ефективності роботи внутрішньобанківської системи кібербезпеки. Перший етап його вирішення полягає в проведенні порівняльного аналізу методів, що можуть бути використані для оцінювання ефективності внутрішньобанківської системи кібербезпеки як складної системи з невизначеністю. Ці методи класифіковано за трьома групами. Якісні методи враховують невизначеність за допомогою лінгвістичних експертних оцінок і теорії нечітких множин. Кількісні методи базуються на традиційному математичному апараті. Вони враховують невизначеність за допомогою засобів статистики, теорії ймовірностей та експертних оцінок з використанням бальних шкал. Оптимальними для врахування невизначеності та оцінювання ефективності внутрішньобанківської системи кібербезпеки є комбіновані методи, що використовують сильні сторони різних підходів.

Ключові слова: *метод оцінювання, ефективність, система кібербезпеки, інформаційний актив, банківська установа.*

Банковские учреждения больше всего привлекают киберпреступников. В связи с этим актуальным является задание создания и оценивания эффективности работы внутрибанковской системы кибербезопасности. Первый этап его решения заключается в проведении сравнительного анализа методов, которые могут быть использованы для оценивания эффективности внутрибанковской системы кибербезопасности как сложной системы с неопределенностью. Эти методы классифицированы по трем группам. Качественные методы учитывают неопределенность с помощью лингвистических экспертных оценок и теории нечетких множеств. Количественные методы базируются на традиционном математическом аппарате. Они учитывают неопределенность с помощью средств статистики, теории вероятностей и экспертных оценок с использованием бальных шкал. Оптимальными для учета неопределенности и оценивания эффективности внутрибанковской системы кибербезопасности являются комбинированные методы, использующие сильные стороны различных подходов.

Ключевые слова: *метод оценивания, эффективность, система кибербезопасности, информационный актив, банковское учреждение.*

Banking institutions are most attracted to cybercriminals. It is in bank accounts that a large amount of cash is concentrated. Banks also have a significant number of customers who use a variety of electronic banking services. The efficiency of the protection of information assets directly affects the competitiveness of a banking institution. In this regard, the actual task is to create and evaluate the efficiency of the cybersecurity system. This is a difficult task, the solution of which is comprehensive and requires a systematic approach. The first stage of its solution is to conduct a comparative analysis of the methods that can be used to assess the efficiency of an intra-banking cybersecurity system as a complex system with uncertainty. These methods were classified into three groups. All methods have advantages and disadvantages. Qualitative methods address uncertainty through linguistic expert judgment (subjective categories) and methods of processing them (fuzzy set theory, fuzzy logic techniques). They make it possible to formalize in a single form input data that are not formalized by other methods. But in many cases, qualitative assessments are not enough to answer the question of how effectively the cyber security of a banking institution is. Quantitative methods are based on the traditional mathematical apparatus. They account for uncertainty by means of statistics, probability theory, and expert scores. Quantitative methods include the method of comparative multidimensional analysis, the method of comparing expected losses from potential threats with the cost of cyber security, the criterion "cost-efficiency" allowing assessing the achievement of the goals of the functioning of the cyber security system at a given cost and others. Combined methods that use the strengths of different approaches are best suited to address uncertainty and assess the efficiency of the intra-banking cyber security system. They use the risk criterion, the criterion of confidence, the multicriteria assessment and others. They make it possible to analyze a considerable amount of qualitative information received from experts and supplemented with quantitative data.

Key words: *assessment method, efficiency, cybersecurity system, information asset, banking institution.*

Постановка проблеми. Сьогодні у світі протидія кіберзлочинності визнана пріоритетною проблемою, вирішення якої потребує проведення ґрунтовних наукових досліджень. Через велику кількість грошових коштів, сконцентрованих на банківських рахунках, різноманітність електронних банківських послуг і значну кількість клієнтів, які користуються цими послугами, саме банківські установи найбільше приваблюють кіберзлочинців. У зв'язку з цим актуальною є проблема захисту інформаційних активів банківської установи (матеріальних або нематеріальних об'єктів, що є інформацією або містять інформацію, слугують для оброблення, зберігання або передачі інформації

[1] Робота виконана в рамках держбюджетної науково-дослідної роботи № 0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України».

та мають цінність для банку [1]). Ефективність захисту інформаційних активів безпосередньо впливає на конкурентоспроможність банківської установи. На державному рівні основним суб'єктом забезпечення кібербезпеки в банківському секторі є Національний банк України. Водночас на рівні бізнесу за кібербезпеку банківської установи відповідає її власник, тому одними зі шляхів протидії кіберзлочинності є впровадження внутрішньобанківської системи кібербезпеки та оцінювання ефективності її роботи.

Аналіз останніх досліджень і публікацій. Проблемі оцінювання ефективності систем захисту інформації (СЗІ) присвячено багато праць вітчизняних і зарубіжних науковців. Ця проблема є досить широкою, тому значна кількість наукових публікацій присвячена розгляду її окремих аспектів. Їм приділяють увагу С.В. Толюпа [2; 3], Н.А. Маслова [4], О.І. Гарасимчук [5], В.В. Богданов [6], Ю.М. Барташевська [7], М.В. Новожилова [8], О.М. Маковецький [9], В.В. Домарев [10], В.В. Куцаєв [11], Д.В. Тихонов [16], Ю.В. Самохвалов [17], Л.М. Михайлова [18] та багато інших вчених.

У роботі [2] наведена така класифікація моделей, що лежать в основі практично всіх відомих методик оцінювання ефективності комплексних СЗІ: за цільовою спрямованістю (оціночні); за ієрархічною структурою (однорівневі); за способом опису функціональних зв'язків (аналітичні); за способом урахування випадкових факторів (комбіновані); щодо врахування стохастичної невизначеності (ймовірнісні). В роботі [4] наведена така класифікація наявних підходів до оцінювання ефективності комплексних СЗІ: статистичний (базується на статистичній обробці загроз та їх наслідків), ймовірнісний (базується на розрахунку сумарних середніх втрат, використовує ймовірність відмови системи в результаті реалізації загроз), частотний (базується на визначенні очікуваного збитку від реалізації загрози, використовує показник частоти виникнення загрози), експертний (базується на визначенні ступеня забезпечення безпеки системи, використовує суб'єктивні оцінки експертів), інформаційно-ентропійний (базується на обчисленні інформаційної ентропії системи, використовує поняття згортки функції), нечітко-множинний (базується на поданні показників захищеності інформаційної системи у вигляді лінгвістичних змінних), мінімізації ризиків (базується на розрахунку показників, що характеризують ризики, та економічного ефекту від управління ризиками), матричний (формальні моделі захисту), багаторівневий (стан системи захисту описується сукупністю рівнів конфіденційності та набором категорій конфіденційності), оптимізаційний (комбінаторний). Наголошується на тому, що рівень захищеності об'єкта може характеризуватись ефективністю СЗІ.

Аналіз наукових праць показав недостатність вивчення цієї проблематики стосовно особливостей оцінювання ефективності роботи внутрішньобанківської системи кібербезпеки, яка протидіє кібератакам, виявляє кіберзагрози, шахрайства клієнтів і банківського персоналу, а також використовує внутрішній аудит для ефективного контролю кібербезпеки. До того ж слід враховувати, що якщо для інфраструктурної кібербезпеки більш важлива доступність до інформаційного активу, то щодо кібербезпеки банківського бізнесу більше значення мають конфіденційність і цілісність інформації. Нині відсутні аналіз та систематизація методів оцінювання ефективності роботи внутрішньобанківської системи кібербезпеки як складної системи з невизначеністю. Водночас дослідниками пропонуються підходи, які використовуються в різних сферах і можуть бути задіяні для оцінювання ефективності роботи внутрішньобанківської системи кібербезпеки. Це обумовлює необхідність подальших досліджень у цьому напрямі.

Постановка завдання. З аналізу сучасних досліджень і відкритих наукових публікацій встановлено, що нині не існує єдиного підходу до оцінювання ефективності внутрішньобанківської системи кібербезпеки. Метою статті є проведення порівняльного аналізу методів, які можуть бути використані для оцінювання ефективності внутрішньобанківської системи кібербезпеки як складної системи з невизначеністю.

Виклад основного матеріалу дослідження. В роботі [5] для оцінювання ефективності СЗІ використовується метод порівняльного багатовимірного аналізу. Він передбачає побудову матриці відстаней між показниками захищеності, що оцінюються, на основі матриці їх нормованих ознак. Матриця відстаней дає можливість впорядкувати показники захищеності за ступенем важливості, встановити залежності між ними та оцінити ступінь їх взаємного впливу. На нашу думку, цей метод може бути застосований також для оцінювання ефективності захисту інформаційних активів банку системою кібербезпеки.

У роботі [6] зазначено, що сьогодні найбільш поширеним на практиці підходом до оцінювання захищеності системи є використання критерія ризику, що вимірюється потенційними втратами від реалізації загроз. Згідно з міжнародним стандартом ISO/IEC 27005:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки» ризик інформаційної безпеки визначається як потенційна можливість використання вразливості активу або групи активів конкретною загрозою для нанесення збитку організації. У роботі [7] оцінювання рівня ефективності впровадження системи інформаційної безпеки передбачає розрахунок показника очікуваних фінансових втрат від реалізації загроз,

який визначається на підставі ступеня тяжкості потенційної загрози, а також зіставлення його з витратами на захист інформації з подальшою градацією ефективності витрат за якісними рівнями. Автор використовує суб'єктивні оцінки, але не зазначає принципи їх розрахунку, через що, на нашу думку, цей метод має обмежене застосування. Зауважимо також, що в наукових публікаціях відсутній єдиний підхід до розрахунку витрат на захист інформації (проєктування та функціонування СЗІ).

У роботі [8] для оцінювання ефективності СЗІ запропоновано використовувати економічний критерій виду «ефективність – вартість» у вигляді суми очікуваного можливого збитку від реалізації загроз і витрат на побудову СЗІ, де значення очікуваного збитку від реалізації конкретної загрози розраховується як добуток величини збитку від реалізації загрози та ймовірності її реалізації. На нашу думку, оцінювання ефективності за цим критерієм найкраще проводити в динаміці, щоби побачити, зростає значення критерія за постійних витрат на СЗІ чи залишається на досягнутому рівні за зниження витрат на СЗІ. Недоліком цього підходу є оцінювання ймовірності реалізації загрози. Статистика появи загроз та реалізованих кібератак на інформаційні активи накопичується, по-перше, в банківській установі з уже впровадженою системою кібербезпеки, по-друге, протягом певного часу, а також потребує відповідної статистичної обробки.

Відомо, що здебільшого на безпеку інформаційного активу впливає декілька загроз, які можуть бути спрямовані на різні його властивості (конфіденційність, цілісність, доступність та спостережність). У роботі [9] запропоновано метод оцінювання ефективності системи захисту інформації, перший етап якого передбачає визначення важливості кожного ресурсу системи, що захищається, як середньоарифметичного значення оцінок рівнів його властивостей. У роботі [6] важливість ресурсу системи, що захищається, запропоновано визначати як наслідки втрати інформації в разі реалізації загрози. Другий етап методу оцінювання ефективності системи захисту інформації передбачає визначення експертним шляхом бальної оцінки рівня реалізації загрози залежно від її частоти та рівня складності. Третій етап передбачає визначення остаточного рівня загрози після проходження механізму захисту. Далі визначається рівень ризику, що створюється загрозою для ресурсу системи, як добуток важливості ресурсу та остаточного рівня загрози після проходження механізму захисту. На цій основі робиться експертний висновок щодо ефективності роботи системи захисту інформації. Розглянутий метод використовує суб'єктивні оцінки експертів, а також положення теорії нечіткої логіки під час визначення рівня зниження загрози механізмом захисту [10].

У роботі [11] зазначено, що оцінка рівня кібербезпеки належить до класу багатокритеріальних завдань, а для його вирішення в умовах невизначеності найбільш раціональними є експертні методи, зокрема метод анкетування [12]. Перший етап запропонованої у джерелі [11] методики розрахунку кіберзахищеності включає визначення компонентів системи (інформаційно-телекомунікаційного вузла), які необхідно захищати (зокрема, телекомунікаційне обладнання, засоби IP-телефонії, сервери та автоматизовані робочі місця, міжмережеві екрани, мережеві сервіси, операційні системи, застосунки користувачів), та обчислення їх вагових коефіцієнтів з використанням рангових оцінок і методу парних порівнянь Сааті [13]. Чим більше ранг, тим вище важливість компонента, яка оцінюється експертами з позицій впливу компонента на працездатність, кіберзахищеність та безпечний стан системи загалом. Оцінювання кіберзахищеності кожного компонента здійснюється за критеріями кіберзахищеності згідно з вимогами нормативних документів технічного захисту інформації та індикаторів міжнародних стандартів захисту NIST SP 800-53 [14] або DOD 8530.01 [15]. Показник кожного критерія кіберзахищеності розраховується як середньоарифметичне значення оцінок експертів, отриманих за формулою нормованої суми бальних оцінок рівня кіберзахищеності згідно з критерієм, що розглядається, та вірогідності виникнення кіберзагрози. На цій основі формується матриця показників кіберзахищеності для кожного компонента системи, яку необхідно захищати, та розраховується підсумковий показник кіберзахищеності як зважена та нормована оцінка індикаторів стану кіберзахищеності компонентів. Індикатор стану кіберзахищеності кожного компонента розраховується як середньоарифметичне значення показників кіберзахищеності цього компонента. На нашу думку, розглянутий підхід є універсальним та після відповідного доопрацювання може бути застосований для оцінювання ефективності внутрішньобанківської системи кібербезпеки.

У роботі [3] в основу моделі оцінювання рівня захищеності системи покладена декомпозиція комплексної СЗІ на ієрархічні рівні, для кожного з яких обчислюється інтегральний показник рівня захищеності інформації як послідовна згортка часткових для нього показників нижнього рівня з використанням математичного апарату нечітких множин. У роботі [16] для розрахунку загального показника якості СЗІ використовувалась адитивна згортка часткових показників захищеності, отриманих як адитивна згортка характеристик часткового показника захищеності. Значення характеристик були подані у вигляді нечітких термів із трапецієподібними функціями належності,

Таблиця 1

Порівняльний аналіз методів оцінювання ефективності внутрішньобанківської системи кібербезпеки

Група методів оцінювання ефективності внутрішньобанківської системи кібербезпеки	Основні характеристики	Врахування невизначеності
Кількісні (метод порівняльного багатовимірного аналізу, метод зіставлення очікуваних втрат від потенційних загроз із витратами на захист інформації, критерій «ефективність – вартість», фінансові, ймовірнісні)	Базуються на традиційному математичному апараті.	Невизначеність враховується за допомогою засобів статистики, теорії ймовірностей та експертних оцінок із використанням бальних шкал.
Якісні (нечіткі множини)	Базуються на експертних оцінках.	Невизначеність враховується за допомогою лінгвістичних експертних оцінок та теорії нечітких множин.
Комбіновані (використовують критерій ризику, критерій впевненості, багатокритеріальне оцінювання)	Базуються на синергетичному підході (використовуються сильні сторони різних методів).	Невизначеність враховується за допомогою кількісного та якісного математичного апарату.

ваговими коефіцієнтами, значення яких були подані у вигляді нечітких термів із трикутними функціями належності. Дефазифікація отриманого нечіткого значення часткового показника здійснювалася з використанням центроїдного методу з подальшою природною нормалізацією отриманого чіткого значення часткового показника. Економічний ефект від впровадження СЗІ розраховувався як різниця між вартістю інформації та приведеною вартістю проєкту СЗІ (NPV). На нашу думку, подання часткових показників як у числовому, так і в лінгвістичному вигляді уможливлює аналіз значної кількості якісної інформації, отриманої від експертів і доповненої кількісними даними.

У роботі [17] запропоновано підхід до оцінювання інформаційної безпеки організації на основі критерія впевненості в тому, що в організації реалізується прийнята політика безпеки. Цей підхід використовує вербально-числову шкалу та функцію бажаності Харінгтона.

Ми погоджуємося з думкою автора роботи [18] про те, що багато ідей, які лежать в основі кількісних методів оцінювання ефективності впровадження проєктів інформатизації, можуть бути використані також для оцінювання економічної ефективності комплексної СЗІ, а саме фінансові (метод окупності інвестицій ROI, метод визначення економічної доданої вартості EVA, метод визначення сукупної вартості володіння TCO, метод визначення чистої приведеної вартості NPV, метод визначення сукупного економічного ефекту TEI, метод швидкого економічного обґрунтування REJ), ймовірнісні (метод справедливої оцінки опціонів ROV, метод прикладного інформаційного аналізу AIE). Вважаємо, що ці методи можуть бути використані також для оцінювання ефективності кібербезпеки банківського бізнесу але потребують суттєвого переосмислення та вдосконалення.

Підсумовуючи вищенаведене, можемо представити результати порівняльного аналізу типових методів оцінювання ефективності внутрішньобанківської системи кібербезпеки як складної системи з невизначеністю у вигляді таблиці.

Висновки з проведеного дослідження. У статті проаналізовано наявні методи, що можуть бути використані для оцінювання ефективності внутрішньобанківської системи кібербезпеки як складної системи з невизначеністю, та класифіковано їх за трьома групами. Підтверджено, що не існує єдиного підходу до оцінювання ефективності системи кібербезпеки як складної системи з невизначеністю. Якісні методи враховують невизначеність за допомогою лінгвістичних експертних оцінок та теорії нечітких множин. Кількісні методи базуються на традиційному математичному апараті. Вони враховують невизначеність за допомогою засобів статистики, теорії ймовірностей та експертних оцінок із використанням бальних шкал. Оптимальними для врахування невизначеності під час оцінювання ефективності внутрішньобанківської системи кібербезпеки є комбіновані методи, що використовують сильні сторони різних підходів. Подальші дослідження можуть розвиватися в напрямі створення моделі оцінювання кількісного та якісного рівня ефективності роботи внутрішньобанківської системи кібербезпеки, що дасть змогу підвищити загальну ефективність протидії кіберзлочинності в банківській сфері.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Криклій О.А., Павленко Л.Д. Внутрішній аудит як превентивна складова в системі кібербезпеки банку. *Облік і фінанси*. 2019. № 2 (84). С. 124–133.

2. Толюпа С.В., Іванова О.М., Демченко І.О. Підходи до проектування та оцінки ефективності системи захисту інформації в автоматизованих системах обробки та передачі даних. *Сучасний захист інформації*. 2013. № 1. С. 25–30.

3. Толюпа С.В., Борисов І.В. Методика оцінки комплексної системи захисту інформації на об'єкті інформаційної діяльності. *Сучасний захист інформації*. 2013. № 2. С. 43–48.

4. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем. *Штучний інтелект*. 2008. № 4. С. 253–264.

5. Гарасимчук О.І., Костів Ю.М. Оцінка ефективності систем захисту інформації. *Вісник КНУ імені Михайла Остроградського*. 2011. Вип. 1 (66). Ч. 1. С. 16–20.

6. Богданов В.В. Застосування критерію ризику для оцінки захищеності автоматизованої системи. *Збірник матеріалів V науково-технічної конференції ВІТІ НТУУ «КПІ»*. Київ : ВІТІ НТУУ «КПІ», 2010. С. 70–72.

7. Барташевська Ю.М. Оцінка ефективності витрат компанії на інформаційну безпеку. *Науковий вісник Міжнародного гуманітарного університету*. *Серія «Економіка і менеджмент»*. 2017. Вип. 28. С. 87–90.

8. Новожилова М.В., Овечко К.А. Оценка систем защиты информации в компьютерных информационных системах по критерию «эффективность – стоимость». *Системи обробки інформації*. 2004. Вип. 1. С. 148–151.

9. Підходи до удос коналення методики оцінки ефективності комплексної системи захисту інформації / О.М. Маковецький, І.Р. Мальцева, Н.А. Паламарчук, Ю.О. Черниш, О.В. Шемендюк. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2016. № 2 (26). С. 54–58.

10. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. Киев : ТИД ДиаСофт, 2002. 688 с.

11. Куцаєв В.В., Радченко М.М., Козубцова Л.М., Терещенко Т.П. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку. *Збірник наукових праць ВІТІ НТУУ «КПІ»*. 2018. № 2. С. 67–76.

12. Бешелев С.Д., Гурвич Ф.Г. Экспертные оценки. Москва : Наука, 1973. 263 с.

13. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетический алгоритм, нейронные сети. Винница : УНИВЕРСУМ, 1999. 320 с.

14. NIST SP 800-53 National Institute of Standards and Technology. Special Publication Security and Privacy Controls for Federal information Systems and Organizations. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft (дата звернення: 27.03.2020).

15. DoD 8530.01. Department of Defense. Indicators. Defend the nation from attack. Secure national security and military systems. URL: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf (дата звернення: 27.03.2020).

16. Тихонов Д.В. Модели оценки эффективности систем информационной безопасности : дисс. … канд. экон. наук : спец. 08.00.05. Санкт-Петербург, 2009. 126 с.

17. Самохвалов Ю.В., Браиловский Н.М. Оценка информационной безопасности организации по критерию уверенности. *Захист інформації*. 2019. № 1. С. 13–24.

18. Михайлова Л.М. Анализ существующих методов оценки эффективности мер по защите информации. *Науковий вісник Одеського національного економічного університету*. 2015. № 5. С. 90–101.

REFERENCES:

1. Kryklii O.A., Pavlenko L.D. (2019) Vnutrishnii audyt yak preventyvna skladova v systemi kiberbezpeky banku [Internal audit as a preventive component in the bank's cybersecurity system]. *Accounting and finance*, no. 2 (84), pp. 124–133.

2. Toliupa S.V., Ivanova O.M., Demchenko I.O. (2013) Pidkhody do proektuvannia ta otsinky efektyvnosti systemy zakhystu informatsii v avtomatyzovanykh systemakh obrobky ta peredachi danykh [Approaches to designing and assessing the efficiency of an information security system in automated systems of data processing and transmission]. *Modern protection of information*, no. 2, pp. 25–30.

3. Samokhvalov Yu.V., Brailovskiy N.M. (2019) Otsenka informatsionnoy bezopasnosti organizatsii po kriteriyu uverennosti [Assessment of information security of the organization by the criterion of confidence]. *Protection of information*, no. 1, pp. 13–24.

4. Maslova N.A. (2008) Metody otsenki effektivnosti sistem zashchity informatsionnykh sistem [Methods for assessing the efficiency of information systems protection systems]. *Artificial Intelligence*, no. 4, pp. 253-264.

5. Harasymchuk O.I., Kostiv Yu.M. (2011) Otsinka efektyvnosti system zakhystu informatsii [Assessing efficiency of information security systems]. *Bulletin of the Kremenchuk Mykhailo Ostrohradskyi National University*, issue 1 (66), part 1, pp. 16–20.

6. Bohdanov V.V. (2010) Zastosuvannia kryteriiu ryzyku dlia otsinky zakhyshchenosti avtomatyzovanoi systemy [Application of a risk criterion to assess the security of an automated system]. *Proceedings of the V Scientific and Technical Conference of VITI NTUU "KPI"*, Kiev : VITI NTUU "KPI", pp. 70–72.

7. Bartashevska Yu.M. (2017) Otsinka efektyvnosti vytrat kompanii na informatsiinu bezpeku [Assessing the effectiveness of a company's information security spending]. *Scientific Bulletin of the International Humanities University. «Economics and Management" Series*, issue 28, pp. 87–90.

8. Novozhilova M.V., Ovechko K.A. (2004) Otsenka sistem zashchity informatsii v komp'yuternykh informatsionnykh sistemakh po kriteriyu "effektivnost' – stoimost'" [Assesing of information security systems in computer information systems by the criterion of "efficiency – cost"]. *Information processing systems*, issue 1, pp. 148–151.

9. Makovetskyi O.M., Maltseva I.R., Palamarchuk N.A., Chernysh Yu.O., Shemendiuk O.V. (2016) Pidkhody do udoskonalennia metodyky otsinky efektyvnosti kompleksnoi systemy zakhystu informatsii [Approaches to improving the method for assessing the efficiency of a comprehensive information security system]. *Modern information technologies in the field of security and defense*, no. 2 (26), pp. 54–58.

10. Domarev V.V. (2002) *Bezopasnost' informatsionnykh tekhnologiy. Metodologiya sozdaniya sistem zashchity* [Information technology security. Methodol-

ogy for creating security systems]. Kiev : TID DiaSoft. (in Russian)

11. Kutsaiev V.V., Radchenko M.M., Kozubtsova L.M., Tereshchenko T.P. (2018) Metodyka otsinky kibernetychnoi zakhyshchenosti informatsiino-telekomunikatsiinoho vuzla zviazku [Method for assessing cyber security of a information-telecommunication connection node]. *Collection of scientific works of VITI NTUU "KPI"*, no. 2, pp. 67–76.

12. Beshelev S.D., Gurvich F.G. (1973) *Ekspertnye otsenki* [Expert estimates]. Moscow : Nauka. (in Russian)

13. Rotshteyn A.P. (1999) *Intellektual'nie tekhnologii identifikatsii: nechetkie mnozhestva, geneticheskiy algoritm, neyronnye seti* [Intelligent identification technologies: fuzzy sets, genetic algorithms, neural networks]. Vinnitsa : UNIVERSUM. (in Russian)

14. NIST SP 800-53 National Institute of Standards and Technology. Special Publication Security and Privacy Controls for Federal information Systems and Organizations. Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft (accessed 27 March 2020).

15. DoD 8530.01. Department of Defense. Indicators. Defend the nation from attack. Secure national security and military systems. Available at: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf (accessed 27 March 2020).

16. Tikhonov D.V. (2009) Modeli otsenki effektivnosti sistem informatsionnoy bezopasnosti [Models for assessing the efficiency of information security systems] (PhD Thesis), St. Petersburg: St. Petersburg State University of Engineering and Economics.

17. Toliupa S.V., Borysov I.V. (2013) Metodyka otsinky kompleksnoi systemy zakhystu informatsii na obiekti informatsiinoi diialnosti [Method for assessing a comprehensive information security system at an information activity object]. *Modern protection of information*, no. 2, pp. 43–48.

18. Mikhaylova L.M. (2015) Analiz sushchestvuyushchikh metodov otsenki effektivnosti mer po zashchite informatsii [Analysis of existing methods for assessing the efficiency of information protection measures]. *Science bulletin of the Odessa National Economic University*, no. 5. pp. 90–101.