УДК 004:657
DOI: https://doi.org/10.32840/2522-4263/2020-2-15

Гаркуша В.О.
аспірант кафедри економічного аналізу та обліку
Національного технічного університету
«Харківський політехнічний інститут»
ORCid: http://orcid.org/0000-0003-2605-2653

Garkusha Victoria
postgraduate of the Department of Economic Analysis and Accounting,
National Technical University "Kharkiv Polytechnic Institute"
ORCid: http://orcid.org/0000-0003-2605-2653

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

METHODICAL APPROACH TO THE RISK ASSESSMENT OF AN ENTERPRISE INFORMATION SECURITY

АНОТАЦІЯ

У статті проаналізовано економічні аспекти інформаційної безпеки і запропоновано методичний підхід до оцінювання ризиків для забезпечення захисту активів підприємства від певних загроз інформаційної безпеки в цілому, прийняття обґрунтованих рішень. Досліджено підходи до оцінки ризиків за міжнародними стандартів ISO для своєчасного зменшення рівня ризику інформаційної безпеки. Наведено моделювання процесів управління ризиками інформаційної безпеки підприємства шляхом побудови моделей ідентифікації, оцінка кількісного та якісного підходу. Виділені основні переваги і недоліки підходів, визначені основні етапи припустимого та існуючого ризику здійснення загрози, запропонована класифікація оцінки ризиків для їх мінімізації, досліджено використання статистичного та нестатистичного методу, експертної оцінки та визначено ряд заходів для встановлення порогів механізму ефективного управління ризиками.

Ключові слова: інформаційна безпека, міжнародні стандарти, ризики, оцінка ризиків, управління ризиками, управлінські рішення, експертна оцінка.

АННОТАЦИЯ

В статье проанализированы экономические аспекты информационной безопасности и предложен подход к оценке рисков для обеспечения защиты активов предприятия от определенных угроз информационной безопасности в целом, принятие обоснованных решений. Исследуются подходы к оценке рисков по международным стандартам ISO для своевременного уменьшения уровня риска информационной безопасности. Приведены моделирования процессов управления рисками информационной безопасности предприятия путем построения моделей идентификации, оценка количественного и качественного подхода. Выделены основные преимущества и недостатки подходов, определены основные этапы допустимого и существующего риска осуществления угрозы, предложена классификация оценки рисков для их минимизации, исследованы использования статистического и нестатистические метода, экспертной оценки и определен ряд мероприятий для установления порогов эффективного управления рисками.

Ключевые слова: информационная безопасность, международные стандарты, риск, оценка рисков, управление рисками, управленческие решения, экспертная оценка.

ANNOTATION

The article analyzes the economic aspects of information security and proposes a methodical approach to assess the risks of ensuring the protection of the assets of the enterprise from certain threats to information security in general, and making grounded decisions. This approach to risk assessment becomes not only an instrument of choosing means of protection, but also a tool of making efficient management decisions at the enterprise. The consistency of steps from collecting input data, their processing and interpreting, calculations of information security risk levels, priority, enterprise risk ranking allows to combine maximum of economic efficiency with the acceptation of risk level and provide not only the construction of a risk processing system that must be successfully implemented, but also an optimal option for choosing the methodology of the management process of the risk information security. Approaches to the risk assessment according to the international ISO standards have been investigated for timely reduction of the level of information security risk. The modeling of processes of information security risk management of the enterprise is presented by means of identification models construction, estimation of quantitative and qualitative approach. The main advantages and disadvantages of the approaches are picked out, the main stages of acceptable and existing risks are identified, the classification to minimize risk assessment is offered, the use of statistical and non-statistical method, expert evaluation is scientifically resrarched and a number of measures for setting the thresholds of the effective risk management mechanism are defined. The proposed methodological approach to the information security risk assessment of the enterprise will allow obtaining scientifically grounded and organizationally-technical solutions aimed at reducing the potential consequences from the realization of threats and lowering the chance of their occurrence in the future. Investigation of the existing methods of information security risk management of the enterprise makes it possible to offer new approaches to the organization of the process of information security risk management, to assess the threats, the general state of information security, as to prevent possible losses in the implementation of existing threats.

Key words: information security, international standards, risks, risk assessment, risk management, management decisions.

Постановка проблеми. Діяльність підприємства пов'язана із значною частиною невизначеності та ризиками. Нині не існує механізмів, що дозволяють повністю захистити підприємство від загроз та ризиків, але ризики інформаційної безпеки можливо істотно знизити шляхом визначення методики оцінки та обробки ризиків. Тому даний підхід до оцінки ризику стає не лише інструментом виборів засобів захисту, а й інструментом прийняття оперативних управлінських рішень на підприємстві.

Методика оцінки ризиків інформаційної безпеки один із основних аспектів для впровадження стійкої, надійної та ефективної системи забезпечення інформаційної безпеки підприємства. Що дозволяє підприємствам здійснювати економічний ефективний контроль ризику з метою мінімізації матеріальних витрат в результаті несанкціонованого втручання.

Аналіз останніх досліджень і публікацій. Окремі аспекти аналізу та оцінки управління ризиками в системі економічної безпеки підприємства досліджуються у роботах М.І. Небава, Ю.В. Міронова [9], О.А. Сороківської [8], Н.Ю. Єршової [6], І.Л. Сазонець [15]. Питанням формування системи інформаційної безпеки підприємства присвячені праці В.І Андрєєва, [10], І.В. Рішняк [12], О.К. Юдіна, О.Г. Корченко, Г.Ф. Конахович [11], Л.Дж. Хоффмана [13], В. Богуш [14].

Мета статті. Метою статті є дослідження та аналіз інформативності оцінки ризиків інформаційної безпеки, вибір варіанту обробки ризиків шляхом побудови моделей процесу управління ризиками інформаційної безпеки.

Виклад основного матеріалу дослідження. Ризики інформаційної безпеки є складовою частиною операційних ризиків підприємства. Одним із шляхів вирішення проблеми оцінки ризиків та вибору оптимального варіанта їх обробки є визначення методики з отриманням необхідної інформації для проведення оцінки з метою прийняття обґрунтованих рішень стосовно того, яким чином краще забезпечувати захист активів підприємства від певних загроз інформаційної безпеки. Оцінка ризиків інформаційної безпеки може здійснюватися у розрізі підприємства або інформаційних систем. Послідовність кроків зі збору вхідних даних, їх обробка та інтерпретація, розрахунки рівнів ризиків інформаційної безпеки, пріоритетність, ранжування ризиків підприємства дозволяє поєднати максимальну економічну ефективність із прийнятим рівнем ризику й надати не тільки побудова системи обробки ризиків, яка повинна бути успішно виконана, а також оптимальний варіант для вибору методики процесу управління ризиками інформаційної безпеки.

Не існує універсального рішення та єдиної моделі процесу управління ризиками, тому процес управління ризиками залежить від особливостей підприємства, визначення підходів до проведення оцінки ризиків, оцінки ризику, обробки ризику, а також удосконалення процесу.

У кожному випадку ідентифікація, оцінка ризиків інформаційної безпеки та контрольні заходи по обробці ризиків мають бути спрямовані на зменшення ризиків порушення безпеки, розуміння причин, які роблять інформаційні системи вразливими. Тому, оцінка ризиків підприємства є одним із основних факторів формування вимог до інформаційної безпеки.

Запропоновані моделі процесів управління ризиками інформаційної безпеки дають зручно та точно розв'язати рішення відносно ризиків інформаційної безпеки підприємства, такі як: CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), ГРИФ, CORAS і ряд інших. Найчастіше використовуваними на практиці є методи наведені у міжнародних стандартах ISO/IEC 27001:2015 [2], NIST SP800-30 [3], OCTAVE [4] та EBIOS [5] які лягли в основу принців загального менеджменту.

Визначення обставин, аналізування, оцінювання та оброблення ризику розглядається в ISO / IEC 27001: 2005 як процес ідентифікації інформаційних ресурсів системи і загроз цих ресурсів для своєчасного зменшення рівня ризику та впровадження моніторингу, аудиту та контролю стану інформаційної безпеки для ефективності процесу управління та є послідовними взаємопов'язаними процедурами процесу управління ризиками інформаційної безпеки [2]. Суть процесу ідентифікації інформаційних ресурсів полягає в оцінки кількісного (більш детального) або якісного (більш простого) підходу, які дозволяють керівництву встановити пріоритети ризиків інформаційної безпеки до їх очікуваної серйозності або іншим встановленим категоріям на кожному кроці оцінювання.

– Якісна оцінка ризиків інформаційної безпеки:

Одним із способів якісної оцінки є відносні показники, процес оцінки включає в себе зв'язок ділової інформації в залежності від її важливості (стратегічна, тактична, оперативна і особиста інформація) та класифікує інформацію за віком(стара, середня або нова інформація). Також відносні показники подаються у формі інтуїтивного зрозуміння, відчутних одиницях(категоріях), таких як ризик – високий, вплив – низький, цінність – значна. Якісні дискретні категорії дозволяють виділити лише найбільш пріоритетні ризики інформаційної безпеки та визначити заходи захисту, які можуть знизити дані ризики. В результаті отримана якісна школа може бути зведена до простого загального рейтингу ризику, наприклад: низький ризик: 0-2, середній ризик: 3–5, високий ризик: 6–8.

– Кількісна оцінка ризиків інформаційної безпеки:

Кількісна оцінка ризиків інформаційної безпеки в більшості випадків оцінюється за трьома факторами: цінність активу(ступінь тяжкості наслідків), ймовірність реалізації загрози інформаційної безпеки, потенційний(повний) вплив загрози використання уразливості. Результатом такої оцінки є фінансова цінність, яка визначає межі інвестицій в інформаційну безпеку. При використанні кількісного підходу всі оцінки представляються в числовій оцінці в деякому діапазоні величин оцінюваних параметрів. Чим менша ймовірність настання, тим важче виміряти ризик.

Під час використання будь-якого з підходів можливо оцінити ризик інформаційної безпеки за формулою:

$$R = A \times I \times P$$

Таблиця 1

Порівняльна характеристика кількісної і якісної оцінки ризиків інформаційної безпеки

	Підхід до оцінки ризиків інформаційної безпеки	
	Кількісний	**Якісний**
Переваги	– Висока точність оцінки ризику ІБ; – Прямий зв'язок між рівнем ризику і величиною потенційних витрат; – Вимірювання ризику у вартісному виражені; – Результати оцінки можуть бути використані для оцінки ефективності заходів захисту	– Висока наочність проміжних і остаточних результатів; – Простота реалізації, невелика кількість розрахунків – Легше зібрати та інтерпретувати вхідні дані;
Недоліки	– Низька наочність проміжних остаточних результатів; – Складність реалізації, дуже велика кількість розрахунків; – Висока складність отримання вхідних даних, виражених у вартісних одиницях; – Складність оцінки ймовірності реалізації загрози інформаційної безпеки; – Існує висока небезпека суб'єктивного оцінювання кількісної цінності інформаційних ресурсів і як результат втрати всіх переваг даного підходу.	– Низька точність оцінки ризику інформаційної безпеки; – З результатів оцінки ризику не можна зробити висновок про потенційні втрати від його реалізації; – Рівень ризику виражається в відносних суб'єктивних категоріях.

де R – рівень ризику інформаційної безпеки;

A – цінність (критичність) інформаційного ресурсу;

I – потенційний (повний) вплив загрози інформаційної безпеки на інформаційний ресурс;

P – ймовірність реалізації загрози інформаційної безпеки;

$A \times I$ – дорівнює потенційним витратам, які виникають підчас реалізації ризику.

Пропонуємо такі основні переваги і недоліки підходів до оцінки ризиків інформаційної безпеки (табл. 1).

Таким чином, можливо зробити висновки, що кількісний підхід є більш точним у порівняні з якісним підходом, оскільки цей підхід уможливлює оцінку імовірності виникнення кожної загрози безпеці для діяльності підприємства. Але, основною проблемою використання кількісного підходу до оцінки ризиків на підприємстві є висока складність точного визначення чисельних значень інформаційних ресурсів.

Оцінка ризиків інформаційної безпеки складається з етапів припустимого та існуючого ризику здійснення загрози, значення ймовірності кожного із загроз допомагає співвіднести оцінку можливих збитків із витратами на захист (рис. 1).

Збитки активів підприємства складаються з витрат на відновлення інформаційних ресурсів (службова інформація, фінансово-аналітична, керуюча), фізичних об'єктів (заміну чи ремонт устаткування), програмних ресурсів (комунікації та програмне забезпечення), на впровадження нових структурних елементів підприємства, на навчання і перепідготовку персоналу, на відновлення позицій на ринку та іміджу підприємства тощо.

Сучасний підхід при виборі оцінки ризиків зводиться до максимально можливого використання статистичних або нестатистичних методів які вимагають людських, матеріальних та часових ресурсів, тому варто взаємодіяти з підрозділами підприємства для отримання реальних результатів.

Статистичний метод оцінки ризиків використовується при наявності накопичувальної статистичної бази з операційних ризиків, що ведеться на підприємстві. Оцінки ризиків інформаційної безпеки нестатистичним методом застосовується на основі теоретичної гіпотези або методів сценарію експертної оцінки, що припускає виділення подій, які відбуваються нечасто, та не потрапляють до накопичувальних баз даних.

Показники здобуті методом експертного опитування для прийняття рішень ґрунтуються на експертних знаннях, щодо розрахунків можливих витрат в інформаційної сфері для відображення об'єктивної ймовірності його реалізації і можливих витрат в рамках ідентифікації інформаційних ризиків, а саме:

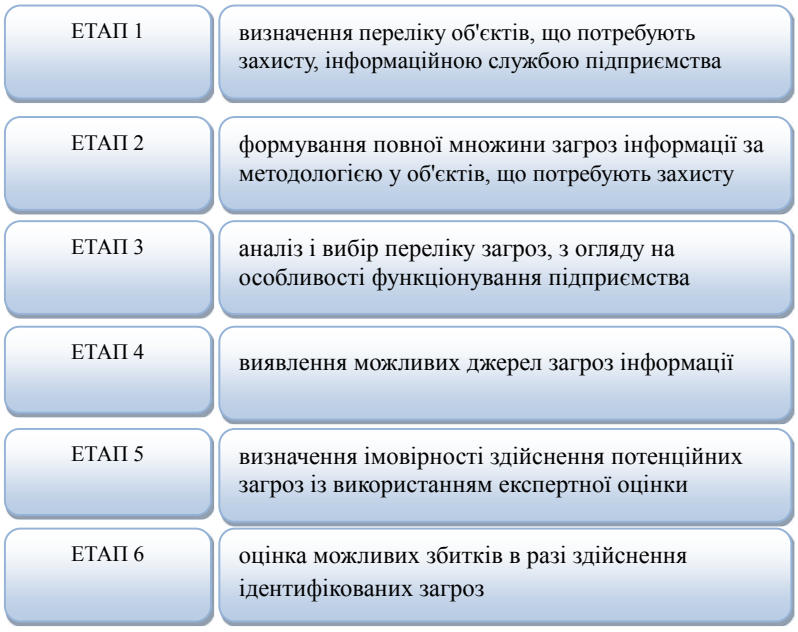

Рис. 1. Етапи оцінки ризиків інформаційної безпеки

– вплив загроз інформаційної безпеки на інформаційні ресурси;

– ймовірність виникнення загроз інформаційної безпеки;

– коефіцієнт ефективності заходів безпеки.

Структура Анкети передбачає документ MS Excel (табл. 2).

При оцінки та обробці ризиків інформаційної безпеки, суб'єктивна шкала ризиків представлено експертами базується на емпіричному досвіді фахівців, суттєво може різниться та прийняття рішень може полягати на пошук компромісів, то для оцінки ризиків можливо використовувати статистичні показники, вивірені бухгалтерські стандарти і процедури, результати, отримані в рамках незалежного аудиту, як це застосовується в країнах з розвиненою інформаційною інфраструктурою.

З метою спрощення процесу обробки ризиків оцінюються ризики за відповідністю до пріоритетності процесу обробки ризику. Відповідно до даної Методики по завершеною етапу оцінки ризиків можливо застосувати класифікацію ризиків (табл. 3).

Відповідно до кожного визначеного ризику власник ризику інформаційної безпеки або власник інформаційного ресурсу.

Процес обробки ризику здійснюється на основі вибору одного з варіантів обробки ризиків. Для кожного ризику, що потребує заходів повинно бути розроблено основний та декілька альтернативних методів мінімізації ризиків (табл. 4).

За умови використання варіанту обробки ризику «Зниження» методи мінімізації ризику мають задовольняти такі умови:

– очікувана оцінка ризику в результаті впровадження відповідних заходів повинна мати рівень не вище «Помірний»(бажано «Низький»)

– вартість заходів не повинна перевищувати можливі сумарні збитки підприємства

Після проведення обробки ризиків наступними задачами є:

– регулярна оцінка інформаційних ризиків (не рідше разу на рік або в разі істотних змін);

– у разі виявлення ризиків неприйнятного рівня – розробка плану щодо мінімізації ризиків;

– впровадження плану заходів щодо мінімізації ризиків.

Для кожного виду ризику потрібні заходи, які сприяють його мінімізації, для чого необхідно виконувати такі дії:

– встановлення причини ризику;

– оцінка ризику;

– виявлення методів мінімізації ризику;

– визначення переліку необхідних ресурсів;

– визначення додаткових переваг.

Визначення рівня ефективності заходів безпеки виконується шляхом аналізу факторів зниження ймовірності реалізації загрози та

Таблиця 2

Оціночний лист ідентифікації інформаційних ризиків

Категорія оцінок	Група експертів
Оцінка впливу загроз інформаційної безпеки на інформаційні ресурси	Представники підрозділів підприємства та служби захисту інформації
Оцінка ймовірності виникнення загроз інформаційної безпеки	Представники служби захисту інформації, операційних ризиків, служби інформатизації
Оцінка коефіцієнту ефективності заходів безпеки	Представники служби захисту інформації

Таблиця 3

Класифікація ризиків оцінки інформаційної безпеки

Рівень ризику	Опис ризику
Критичний	Ризик вважається надзвичайно критичним для інформаційних активів підприємства і потребує обробки в найкоротший термін. Причиною даного ризику є відсутність або неефективність, застосованих контролів для основних інформаційних ресурсів підприємства
Значний	Ризик вважається досить значним для активів підприємства і потребує розробки планових заходів по мінімізації ризиків
Помірний	Ризик призводить до невисоких втрат підприємства і наслідки реалізації даного ризику можливо усунути в прийнятий підприємством термін
Низький	Ризик вважається прийнятим оскільки його реалізація практично не призводить до втрати підприємства

Таблиця 4

Заходи обробки ризиків інформаційної безпеки

Варіант обробки	Заходи
Прийняття	Підтвердження можливості реалізації загрози та свідоме прийняття наслідків її реалізації за рахунок коштів підприємства
Передача	Перенесення відповідальності за ризик на треті сторони (використання відповідних умов контракту, страхування ризику)
Ухилення	Повне усунення відповідної загрози або джерела загрози через виключення потенціальної можливості її виникнення
Зниження	Зменшення ймовірності виникнення ризику або розміру можливих збитків від реалізації загроз. Джерело загрози не ліквідується

ефективності їх реалізації, Показник рівня ефективності реалізації заходів безпеки можливо визначити як відношення заходів безпеки до конкретної загрози.

З кожним роком проблема ризиків інформаційної безпеки і пошук шляхів зниження ризиків постають все актуальніше. Однак, самостійно забезпечити надійний захист інформації та гарантоване покриття можливих витрат від ризиків можуть не всі власники ризику інформаційної безпеки або власник інформаційного ресурсу.

Даний етап передбачає можливі рішення з управління ризиками:

– забезпечення належного контролю для зниження ризиків інформаційної безпеки;

– виважене рішення щодо ризиків, які задовольняють систему підприємства та критерії оцінки ризиків;

– заходи уникнення дій, що можуть спричинити виникнення ризиків;

– страхування ризиків.

Графічні та розрахункові докладні документи повинні бути на рівні середньої ланки для опрацювання, надання результатів аналізу ризиків інформаційної безпеки повинні обов'язково надаватися вищому керівництву для визначення порогів ризиків інформаційної безпеки. Процедура для реалізації і управління системою менеджменту інформаційної безпеки можуть бути організовані як дерево процесів при виборі підходу щодо ризиків інформаційної безпеки з врахуванням рекомендацій методів міжнародного стандарту ISO, які ґрунтуються на методології підхідного процесу до методів оцінки та обробки ризиків інформаційної безпеки. Оскільки безпека – важлива функція підприємства, що відіграє важливу роль у переході на більш високий рівень зрілості процесів забезпечення інформаційної безпеки.

Процес управління всіма ризиками повинен бути зав'язані на ризик – менеджменту, оскільки підприємство зацікавлено в тому, щоб ризики, які виникають при порушені інформаційної безпеки, зменшувалися.

Висновки. У сучасних умовах господарювання, коли інформаційні технології набувають глобального характеру, інформаційна безпека є невід'ємною частиною системи економічної безпеки підприємства. Одним із найважніших видів діяльності із забезпечення інформаційної безпеки підприємства є виявлення, оцінка та обробка ризиків інформаційної безпеки. В статті представлений огляд існуючого методу оцінки міжнародного стандарту ISO / IEC 27001, що дозволяє отримувати цілісну картину ситуації відносно оцінки та удосконалення методик для мінімізації недоліків ризиків.

Механізм ефективного управління ризиками має забезпечити прийняття та реалізацію ефективний управлінських рішень на підприємстві. Як і будь-яка інша система, система управління ризиками має забезпечувати надійний захист через:

– постійний моніторинг;

– постійний контроль;

– прогнозування.

Запропонований методичний підхід до оцінки ризиків інформаційної безпеки підприємства дозволить отримати науково-обґрунтовані та організаційно-технічні рішення, спрямовані на зменшення потенційних наслідків від реалізації загроз та зниженню ймовірності їх виникнення у майбутньому. Таким чином, дослідження існуючих методів управління ризиками інформаційної безпеки підприємства дає можливість запропонувати нові підходи до організації процесу управління ризиками інформаційної безпеки, оцінити загрози, загальний стан інформаційної безпеки, тим самим попереджуючи виникнення можливих збитків при реалізації існуючих загроз.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Керівництво з управління ризиками для систем інформаційних технологій. Рекомендації Національного інституту Стандартів і технологій (Guide for Conducting Risk Assessments. National Institute of Standards and Technology). Gaithersburg: National Institute of Standards and Technology, 200.332, 95 с.
2. ISO I. IEC 27001Information technology, securityte chniques, information security management systems requirements. ISO, Geneva, 2005.
3. NIST Special Publication 800-30. Guide for Conducting Risk Assessments. Gaithersburg, 2012. 95 с.
4. Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Hanscom AFB, 2007. 154 с.
5. EBIOS Méthode de gestion des risques. Париж, 2010. 95 с.
6. Н.Ю. Єршова, М.О. Ткаченко, В.О. Гаркуша, О.Ю. Мірошник, Л.М. Новак-Каляєва. Економічна безпека підприємства: науково-практичні аспекти обліково-аналітичного забезпечення». *Фінансово-кредитна діяльність: проблеми теорії та практики.* 2019. Т. 2. № 29. С. 130–141. URL: http://fkd.org.ua/article/view/172365/173387 (дата звернення: 24.03.2020). DOI: https://doi.org/10.18371/fcaptp.v2i29.172365
7. Єршова Н.Ю., Ткаченко М.О., Гаркуша В.О. Моніторинг та оцінка господарської діяльності для забезпечення економічної безпеки підприємств ресторанного бізнесу. *Modern Economics* Електронне наукове видання (фахове). 2018. № 11. С. 66–71. URL: https://modecon.mnau.edu.ua/monitoring-and-evaluation-of-economic-activity-to/ (дата звернення: 21.03.2020).
8. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету. Серія : Економічні науки*. Хмельницьк, 2010. № 2. Т. 2. С. 32–35.
9. Небава М.І., Міронова Ю.В. Економічна безпека підприємства : навчальний посібник. Вінниця : ВНТУ, 2017. 73 с.
10. Основи інформаційної безпеки / В.І. Андрєєв, В.О. та інш. ; за ред. В.О. Хорошка. Київ, 2009. 292 с.
11. Юдін О.К. Захист інформації в мережах передачі даних : підручник / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. Київ, 2009. 714 с.

12. Рішняк І.В. Системний аналіз категорій ризику та невизначеності. *Вісник Національного університету «Львівська політехніка»*. 2003. № 489.
13. Хоффман Л.Дж. Современные методы защиты информации / пер. с англ. Москва : Советское радио, 1980. 57 с.
14. Інформаційна безпека держави / В. Богуш, О. Юдін; за заг. ред. Ю.О. Шпак. Київ : «МК-Прес», 2005. 432 с.
15. Сазонець І.Л. Міжнародні стандарти безпеки підприємств : навчальний посібник. Рівне : Волин. обереги, 2015. 118 с.

REFERENCE:

1. Kerivnytstvo z upravlinnia ryzykamy dlia system informatsiinykh tekhnolohii. Rekomendatsii Natsionalnoho instytutu Standartiv i tekhnolohii [Guide for Conducting Risk Assessments. National Institute of Standards and Technology]. Gaithersburg: *National Institute of Standards and Technology*, 200. 332 p.
2. ISO I. IEC 27001 (2005) Information technology, securityte chniques, information security management systems requirements. ISO, Geneva.
3. NIST Special Publication 800-30 (2012) Guide for Conducting Risk Assessments. Gaithersburg.
4. Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson (2007) Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Hanscom AFB.
5. EBIOS (2010) Méthode de gestion des risques. Paris.
6. Iershova N.Yu., Tkachenko M.O., Garkusha V.O., Miroshnyk O.Yu., Novak-Kaliaieva L.M. (2019) Ekonomichna bezpeka pidpryiemstva: naukovo-praktychni aspekty oblikovo-analitychnoho zabezpechennia [Economic security of the enterprise: scientific and practical aspects of accounting and analytical support]. *Finansovo-kredytna diialnist: problemy teorii ta praktyky,* vol. 2, no 29, pp. 130–141. Available at: http://fkd.org.ua/article/view/172365/173387 (accessed 24 March 2020). DOI: https://doi.org/10.18371/fcaptp.v2i29.172365
7. Iershova N.Yu., Tkachenko M.O., Garkusha V.O. (2018) Monitorynh ta otsinka hospodarskoi diialnosti dlia zabezpechennia ekonomichnoi bezpeky pidpryiemstv restorannoho biznesu [Monitoring and evaluation of economic activity toensure economic safety of enterprises of the restaurant business]. *Modern Economics* (electronic journal), no 11, pp. 66–71. Available at: https://modecon.mnau.edu.ua/monitoring-and-evaluation-of-economic-activity-to/ (accessed 21 March 2020).
8. Sorokivska O.A., Hevko O.A. (2010) Informatsiina bezpeka pidpryiemstva [Information security of the enterprise]. *Visnyk Khmelnytskoho natsionalnoho universytetu: Ekonomichni nauky,* vol. 2, no 2, pp. 32–35.
9. Nebava M.I., Mironova Yu.V. (2017) *Ekonomichna bezpeka pidpryiemstva : navchalnyi posibnyk* [Economic security of the enterprise]. Vinnytsia: VNTU. (in Ukrainian)
10. Andrieiev V.I., Khoroshko V.O., Cherednychenko B.C., Shelest M.Ye. (2009) *Osnovy informatsiinoi bezpeky* [Fundamentals of Information Security]. Kiev: DUIKT. (in Ukrainian)
11. Yudin O.K. (2009) *Zakhyst informatsii v merezhakh peredachi danykh* [Protection of information in data networks]. Kiev: NVP “INTERSERVIS”. (in Ukrainian)
12. Rishniak I.V. (2003) Systemnyi analiz katehorii ryzyku ta nevyznachenosti [Systematic analysis of risk and uncertainty categories]. *Visnyk Natsionalnoho universitetu “Lvivska politekhnika”,* no 489.
13. Khoffman L.Dzh.(1980) Sovremennye metody zashchity informatsii [Modern methods of information protection]. Moscow: Sovetskoe radio. (in Russian)
14. Bohush V., Yudin O. (2005) *Informatsiina bezpeka derzhavy* [Information security of the state]. Kiev: «MK-Pres». (in Ukrainian)
15. Sazonets I.L. (2015) *Mizhnarodni standarty bezpeky pidpryiemstv* [International enterprise security standards]. Rivne: Volyn. oberehy. (in Ukrainian)