УДК 004.056.5 DOI: 10.31673/2412-4338.2021.042027

Асєєва Л.А. *Державний університет телекомунікацій, Київ*
Шушура О.М. *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ*

НЕЧІТКЕ МОДЕЛЮВАННЯ РИЗИКІВ ПОРУШЕННЯ ЦІЛІСНОСТІ ДОКУМЕНТІВ ПРОЕКТУ

***Анотація**: Моделювання та управління ризиками відповідно до світових стандартів є основою для побудови політики інформаційної безпеки підприємства. Огляд існуючого стану розробок в цій галузі, сучасна актуалізація задач кібербезпеки та відповідне зростання витрат свідчать про необхідність розробки нових підходів до вимірювання ризиків інформаційної безпеки. Одним з можливих напрямків досліджень є моделювання ризиків безпеки проектів, оскільки проектна діяльність властива підприємствам багатьох галузей, в тому числі IT-підприємствам, будівельним підприємствам та іншим. У статті питання інформаційної безпеки проекту розглядається на основі його формального представлення у вигляді множини документів та операцій над ними. Під час обробки кожного документу, яка в загальному випадку включає створення документу, його збереження, редагування та передачу, виникають ризики щодо порушення його конфіденційності, цілісності чи доступності. Розмитість та неповнота інформації відносно характеристик ризиків інформаційної безпеки документів обумовлює необхідність використання нечіткої логіки для їх формалізації. В даній роботі запропонована модель для оцінки можливості порушення цілісності документів проекту та шкоди від такого порушення на основі математичного апарату нечіткої логіки. Розроблена модель має узагальнену структуру, оскільки базується на формалізації множини документів проекту та операцій над ними з використанням певних інформаційних систем і персоналу. Для оцінки шкоди від реалізації загрози порушення цілісності документу запропоновано застосувати метод аналізу ієрархій на основі наведеного в роботі дерева критеріїв. Розроблена модель може бути використана при створенні спеціалізованих інформаційних систем оцінки ризиків проектів та застосована для управління інформаційною безпекою на підприємствах, діяльність яких має проектний характер.*

***Ключові слова:** ризик інформаційної безпеки, оцінка ризиків проекту, нечітка логіка, ризик порушення цілісності*

Asieieva L.A. *State University of Telecommunications, Kyiv*
Shushura O.M. *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv*

FUZZY SIMULATION OF INTEGRITY BREAK RISKS OF PROJECT DOCUMENTS

***Abstract**: Simulation and risk management in accordance with international standards is the basis for building an information security policy of the enterprise. An overview of the current state of development in this area, the current update of cybersecurity tasks and the corresponding increase in costs indicate the need to develop new approaches to measuring information security risks. One of the possible areas of research is the simulation of project security risks, as project activities are inherent in enterprises of many industries, including IT companies, construction companies and others. In the article the issue of information security of the project is considered on the basis of its formal presentation in the form of a set of documents and operations on them. During the processing of each document, which generally includes the creation, storage, editing and transmission of the document, there are risks of breach of its confidentiality, integrity or accessibility. Blurring and incomplete information regarding the characteristics of information security risks of documents necessitates using of fuzzy logic to formalize them. In this paper, a model is proposed to assess the possibility of violation of the integrity of project documents and the damage from such a violation on the basis of the mathematical apparatus of fuzzy logic. The developed model has a generalized structure, as it is based on the formalization of set of project documents and operations on them using certain information systems and personnel. To assess the damage from the implementation of the threat of violation of the*

document integrity, it is proposed to use the method of hierarchies analysis on the basis of the tree of criteria. The developed model can be used in the creation of specialized information systems for risk assessment of projects and used to manage information security in enterprises whose activities are of a project nature.

***Keywords**: information security risk, project risk assessment, fuzzy logic, risk of integrity breach*

Асеева Л.А. *Государственный университет телекоммуникаций, Киев*
Шушура А.Н. *Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», Киев*

НЕЧЕТКОЕ МОДЕЛИРОВАНИЕ РИСКОВ НАРУШЕНИЯ ЦЕЛОСНОСТИ ДОКУМЕНТОВ ПРОЕКТА

***Аннотация:** Моделирование и управление рисками в соответствии с мировыми стандартами является основой для построения политики информационной безопасности предприятия. Обзор существующего состояния разработок в этой области, современная актуализация задач кибербезопасности и соответствующий рост затрат свидетельствуют о необходимости разработки новых подходов к измерению рисков информационной безопасности. Одним из возможных направлений исследований является моделирование рисков безопасности проектов, поскольку проектная деятельность свойственна предприятиям многих отраслей, в том числе ИТ-предприятиям, строительным предприятиям и другим. В статье вопрос информационной безопасности проекта рассматривается на основе его формального представления в виде множества документов и операций над ними. При обработке каждого документа, который в общем случае включает создание документа, его сохранение, редактирование и передачу, возникают риски нарушения его конфиденциальности, целостности или доступности. Размытость и неполнота информации о характеристиках рисков информационной безопасности документов обуславливает необходимость использования нечеткой логики для их формализации. В данной работе предложена модель для оценки возможности нарушения целостности документов проекта и вреда от такого нарушения на основе математического аппарата нечеткой логики. Разработанная модель имеет обобщенную структуру, поскольку базируется на формализации множества документов проекта и операций над ними с использованием определенных информационных систем и персонала. Для оценки вреда от угрозы нарушения целостности документа предложено применить метод анализа иерархий на основе приведенного в работе дерева критериев. Разработанная модель может быть использована при создании специализированных информационных систем оценки рисков проектов и применена для управления информационной безопасностью на предприятиях, деятельность которых носит проектный характер.*

Ключевые слова: *риск информационной безопасности, оценка рисков проекта, нечеткая логика, риск нарушения целостности*

1. Вступ

Управління інформаційною безпекою є необхідною складовою комплексної системи менеджменту будь-якого солідного підприємства, що особливо актуально для вітчизняних підприємств в умовах гібридної агресії РФ та загального зростання рівня кіберзлочинності. Сучасні підприємства приділяють багато уваги розробці систем управління інформаційною безпекою, що призначені для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

2. Аналіз досліджень і публікацій

Відповідно до ISMS Framework, який розроблено міжнародною європейською агенцією з кібербезпеки, в основі побудови системи управління інформаційною безпекою є визначення підходів до виявлення, аналізу, прогнозування та обробки ризиків [1]. Беручи до уваги, що діяльність підприємств часто характеризується неповнотою та розмитістю інформації, в моделях оцінки ризиків інформаційної безпеки отримала широке застосування нечітка логіка, вперше запропонована Л. Заде [2]. Традиційно проблеми інформаційної

безпеки на основі нечіткої логіки активно розглядалися дослідниками в першу чергу для банківської сфери, корпоративних інформаційних мереж [3] та ERP систем [4], однак з часом настало усвідомлення їх актуальності для підприємств інших галузей, серед яких можна виділити підприємства критичної інфраструктури [5] та будівельні підприємства, що з ними пов'язані [6]. Багатьом підприємствам в цих галузях властива проектна діяльність, що потребує удосконалення існуючих та розробки нових підходів до побудови їх систем управління інформаційної безпеки, а розробка способів вимірювання ризиків та ефективності кіберзахисту є актуальним напрямом для досліджень [7].

3. Мета та задачі роботи

Метою даної роботи є створення підходів для нечіткого моделювання ризиків інформаційної безпеки порушення цілісності документів проекту. Для досягнення поставленої мети необхідно виконати задачі формального опису проекту як множини певних документів, розробити моделі для оцінки можливості порушення цілісності документів проекту та шкоди від такого порушення на основі математичного апарату нечіткої логіки.

4. Результати дослідження

4.1 Формалізація проекту як множини документів

Одним з найбільш розповсюдженим підходом до визначення проекту є його представлення як сукупності операцій для досягнення поставлених цілей при наявності обмежень щодо часу та ресурсів. Поточний стан цих операцій та їх результати можуть бути в загальному випадку описані в документах проекту, що характерно, наприклад, для будівельної галузі. Такі документи є основним інформаційним активом проекту і щодо них потрібно розглянути модель оцінки ризиків порушення цілісності. З метою узагальнення підходів до моделювання ризиків проведено формалізацію структури документів проекту, що наведена нижче [8].

Позначимо D множину документів проекту, елементами якої є документ $d_{lk}^{i} \in D$, де i - номер документа; l - форма документу, $l \in \{0,1,2,3\}$: 0-електронний екземпляр, 1-підписаний паперовий оригінал, 2-паперова копія, 3-електронний з ЕЦП; k - номер екземпляра документа.

З метою узагальнення всі екземпляри l- форми документа $d_{lk}^{i} \in D$ позначимо як d_{l}^{i}, що визначається за формулою:

$$d_{l}^{i} = \bigcup_{k} d_{lk}^{i} . \quad (1)$$

Ще більшим рівнем узагальнення документа по всім формам представлення буде узагальнений документ d^{i}, який може бути визначений формулою:

$$d^{i} = \bigcup_{l} d_{l}^{i} . \quad (2)$$

Крім того, множину документів D можна розбити на підмножини за видами документів, що використовуються у проекті:

$$D = \bigcup_{j=1}^{n} D_{j}, D_{j} \bigcap D_{m} = \varnothing, j \neq m . \quad (3)$$

Життєвий цикл документа в загальному випадку передбачає виконання над ним певних операцій, до яких можна віднести його створення, редагування, погодження, використання, архівування, знищення та інші. Відповідно до цього введемо множину P_i операцій над документом d^{i}. Будь-яка операція $p_{ij} \in P_i$ може передбачати застосування

певного обладнання, програмного забезпечення, задіяння персоналу із певним рівнем доступу, який може складатися як зі співробітників основного підприємства, так із працівників сторонніх підприємств та організацій. Для подальшого врахування питань кіберзахисту інформаційних систем, що задіюються під час виконання операції $p_{ij} \in P_i$, введемо ISP_{ij} як множину цих інформаційних систем.

4.2 Розробка моделі оцінки можливості порушення цілісності документу проекту

Під загрозою цілісності документа в загальному випадку розуміють пошкодження і знищення інформації, перекручення інформації – як не навмисне в разі помилок і збоїв, так і зловмисне.

Рівень ризику порушення цілісності RIn^i документу d^i визначимо як :

$$RIn^i = PIn^i \cdot UIn^i, \tag{4}$$

де PIn^i – оцінка можливості загрози порушення цілісності документа d^i, яка приймає значення з відрізку [0,1]; UIn^i – оцінка шкоди від загрози порушення цілісності документа d^i.

Формула для розрахунку оцінки можливості порушення цілісності PIn^i документа d^i має вид:

$$PIn^i = \prod_{p_j \in P_i} PIn^i_j, \tag{5}$$

де PIn^i_j – оцінка можливості порушення цілісності документа d^i під час виконання операції $p_{ij} \in P_i$.

Враховуючи, що інформація щодо ризиків інформаційної безпеки документів при виконанні проектів в багатьох галузях є нечіткою, для оцінки можливості загрози порушення цілісності документу та шкоди від цього порушення в роботі запропоновано застосувати лінгвістичний підхід на основі нечіткої логіки.

З метою розрахунку оцінки PIn^i_j можливості порушення цілісності документа d^i при виконанні операції $p_{ij} \in P_i$ розроблена нечітка модель, вхідні та вихідні змінні якої наведені на рисунку 1.

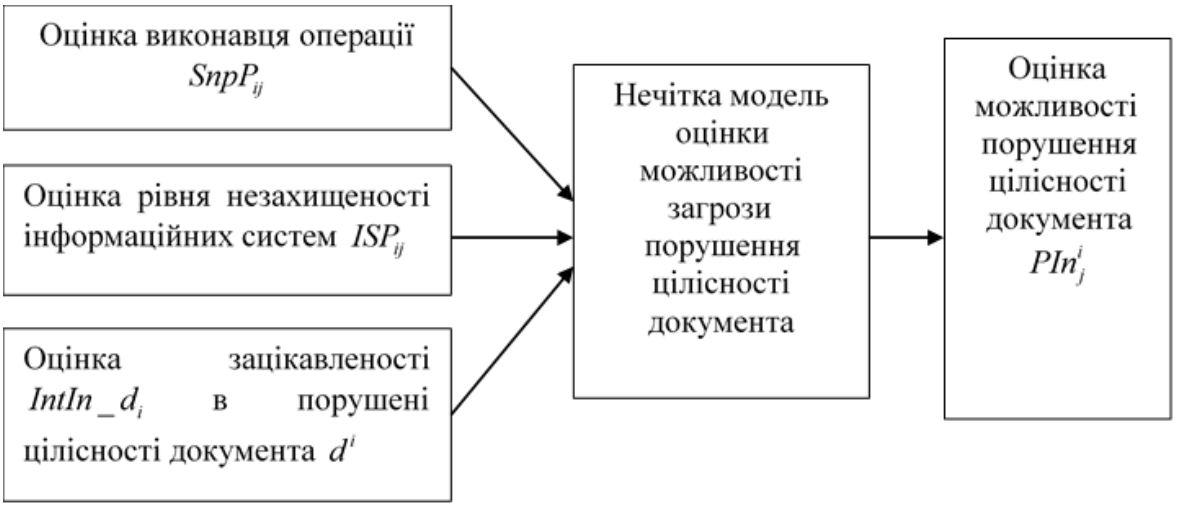

Рис. 1. Вхідні та вихідні змінні нечіткої моделі оцінки можливості загрози порушення

цілісності документа

З рисунку 1 видно, що в даної нечіткої моделі вхідні лінгвістичні змінні:

- оцінка виконавця операції $SnpP_{ij}$;
- оцінка рівня незахищеності інформаційних систем ISP_{ij};
- оцінка зацікавленості $IntIn\_d_i$ зовнішніх акторів в порушені цілісності документа d^i.

З метою спрощення приймемо припущення, що у кожної операції $p_{ij} \in P_i$ завжди один виконавець, чого легко можна досягнути при формуванні множини операцій для документа. Оцінка виконавця операції $SnpP_{ij}$ характеризує можливість пошкодження ним документа зумисно або через недостатній рівень кваліфікації. Для розрахунку даної оцінки розроблена відповідна нечітка підмодель.

Розрахунок рівня незахищеності інформаційних систем ISP_{ij}, що використовуються при виконанні операції, слід виконувати на основі стандарту CVSS [9]. Результати розрахунку показника вразливості інформаційних систем є значенням базової вхідної змінної, для якої сформована відповідна лінгвістична змінна.

Оцінка $IntIn\_d_i$ зацікавленості зовнішніх акторів в порушенні цілісності документа формалізована у вигляді лінгвістичної змінної, яка відповідно до методу інфологічного моделювання предметних областей задач нечіткого управління [10] представлена у вигляді фрейму на рисунку 2.

Рівень зацікавленості в порушені цілісності документу	
Тип	Input
Блок змінних	
Рівень зацікавленості	Множина допустимих значень [0…9]
Блок термів	
низький	Лінійна z-образна функція належності $\mu(x,2,3)$
середній	Трикутна функція належності $\mu(x,3,5,3)$
високий	Лінійна s-образна функція належності $\mu(x,7,8)$
Опис процедури формування нових термів - відсутня	
Опис процедури формування функцій належності термів - відсутня	

Рис. 2. Опис лінгвістичної змінної рівня зацікавленості в порушенні цілісності документа

Для лінгвістичної змінної оцінки рівня зацікавленості в порушенні цілісності документу, що представлена на рисунку 2, значення базової змінної з множини допустимих значень формується на основі методу аналізу ієрархій Сааті з використанням експертних оцінок зацікавленості в порушенні цілісності для дерева рішень, в якому на передостанньому та останньому рівнях знаходяться множини зовнішніх акторів та множин видів документів. Таким чином, оцінка зацікавленості в порушенні цілісності конкретного документу d^i

приймається рівною зацікавленості для всього виду документів. Однак при наявності виключень з цього правила можливо доповнення дерева ієрархії рівнем документів чи безпосереднє встановлення значення експертом.

Використовуючи запропоновані лінгвістичні змінні та їх терми для розрахунку оцінки можливості загрози порушення цілісності документа d^i сформована база правил нечіткого логічного виведення у вигляді нечітких продукцій. В загальному випадку множину правил цієї нечіткої бази знань можна представити у вигляді:

$$\text{Правило } R\text{: <Якщо> } \bigcap_{i=1}^{N} A_i \text{ <ТО> } \bigcap_{j=1}^{M} C_j \,, \qquad (6)$$

де N – кількість підумов, що входять до антецеденту правила; M – кількість підвисновків, що входять в консеквент правила; A_i – підумова, що входить до антецеденту правила та є нечітким висловлюванням, що позначає прийняття певною лінгвістичною змінною значення з множини свої термів; C_j – підвисновок, що входить до консеквента правила та є нечітким висловлюванням, що позначає прийняття певною лінгвістичною змінною значення з множини свої термів.

На основі бази правил нечітких продукцій (6) з використанням методу Мамдані розраховується оцінка PIn_j^i можливості загрози порушення цілісності документа d^i, при виконанні операції $p_{ij} \in P_i^{lk}$. Потім по формулі (5) розраховується загальна оцінка PIn^i можливості загрози порушення цілісності документа d^i.

4.3 Розробка моделі оцінки шкоді від порушення цілісності документу проекту

Для обчислення оцінки UIn^i шкоди від виконання загрози порушення цілісності документа d^i сформована множина Y частинних показників, з яких складається величина збитків або шкоди [8]. Ці показники характеризують зовнішній збиток або шкоду для підприємства, внутрішній збиток або шкоду підприємства та його фінансові збитки. Розрахунок значення UIn^i пропонується здійснювати за допомогою методу аналізу ієрархій Сааті на основі дерева критеріїв, представленого на рисунку 3.

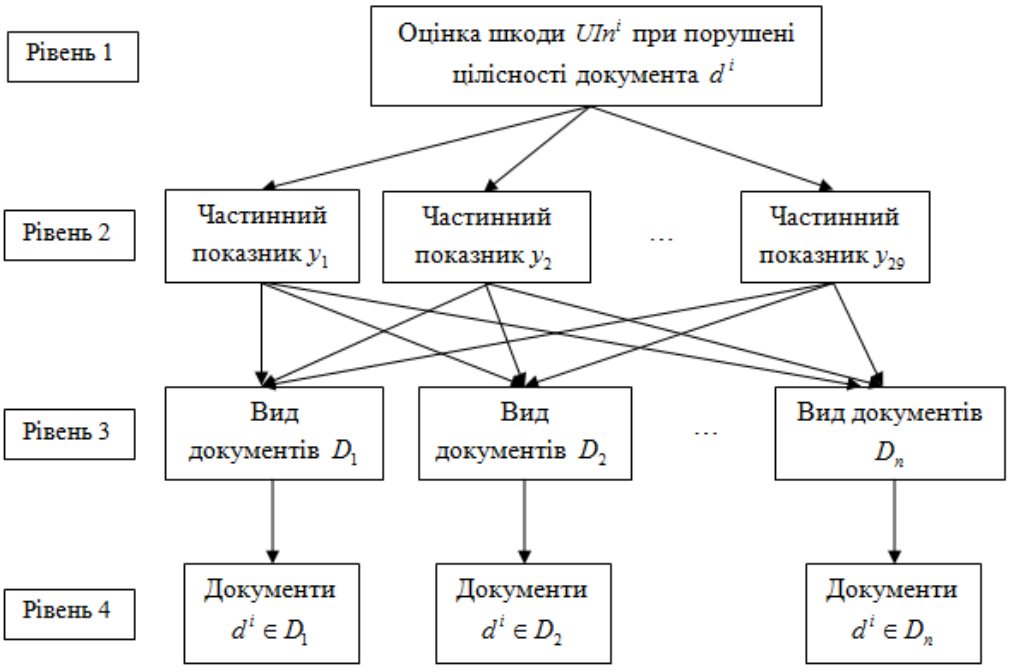

Рис. 3. Дерево ієрархії критеріїв оцінки шкоди при порушенні цілісності документу

Як видно на рисунку 3, дерево критеріїв для оцінки шкоди від порушення цілісності документів має чотири рівні. Крім частинних показників шкоди з множини *Y*, використовуються множини видів документів, що формуються для кожної галузі індивідуально. Приклад сформованих множин видів документів для будівельного підприємства наведено в таблиці 1.

Таблиця 1

Види документів проектів будівельного підприємства

Вид документу	Опис
D_1	комерційні пропозиції;
D_2	обов'язкові для подання та забезпечення проектування об'єкта вихідні дані (містобудівні умови та обмеження, технічні умови, завдання на проектування);
D_3	договори та специфікації до них;
D_4	проектна документація на різних її стадіях після схвалення та/або після затвердження, як підставою для розроблення наступних стадій проектування (техніко-економічне обґрунтування, техніко-економічний розрахунок або «Ескізний проект»), що розробляється на об'єкт будівництва в цілому чи з відображенням окремих черг чи пускових комплексів;
D_5	в визначених регуляторами випадках документи щодо експертизи проектів;
D_6	дозвільні документи та ліцензії;
D_7	креслення;
D_8	витяги;
D_9	документи, що містять фінансові оцінки стадій та черг чи пускових комплексів по роботах, що передбачаються, кошториси;
D_{10}	документи, що містять фінансові оцінки стадій та черг чи пускових комплексів по виконаним роботам, акти виконаних робіт;
D_{11}	тендерні документі;
D_{12}	інші юридично значимі документи.

Шкода оцінюється в балах чи в грошову еквіваленті.

5. Висновки. В роботі представлено модель оцінки ризику порушення цілісності документів проекту на основі нечіткої логіки. Розроблена модель має узагальнену структуру, оскільки базується на формалізації множини документів проекту та операцій над ними з використанням певних інформаційних систем і персоналу. Завдяки використанню нечіткої логіки модель дозволяє врахувати розмитість та неповноту інформації щодо ризиків проекту. Розроблена модель може бути використана при створенні спеціалізованих інформаційних систем оцінки ризиків проектів та застосована для управління інформаційною безпекою на підприємствах, діяльність яких має проектний характер.

Список використаних джерел

1. ISMS Framework. [Електронний ресурс] – Режим доступу: https://www.enisa.europa.eu /topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework.

2. Zadeh L.A. Fuzzy sets // Information and Control. – 1965. – Vol. 8. – PP. 338–353.

3. Аникин, И.В. Анализ подходов к оценке рисков информационной безопасности в корпоративных информационных сетях / И.В. Аникин, Л.Ю. Емалетдинова // Вестник Казанского государственного энергетического университета. - 2015. -NQ (25). - С. 55-67.

4. Міщенко А.В., Курило О.В., Золотухіна О.А. Нечітка модель оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем. Телекомунікаційні та інформаційні технології. 2020. №1(66). DOI: 10.31673/2412-4338.2020.011451 с.142-151.

5. Bharadwaj R. K. Manthaa, Borja Garcia de Sotob. Cyber security challenges and vulnerability assessment in the construction industry. Conference Creative Construction 2019. 29 June - 2 July 2019. Budapest, Hungary. DOI:10.3311/CCC2019-005. PP 30-37.

6. Construction Industry Institute. CII. *CyberSecurity for Construction*. July 21, 2021. [Електронний ресурс] – Режим доступу: https://www.construction-institute.org/events/education/free-webinar-cybersecurity-for-construction.

7. NIST. Measurements for Information Security. Created September 15, 2020, Updated December 3, 2020. [Електронний ресурс] – Режим доступу: https://www.nist.gov/cybersecurity/measurements-information-security.

8. Асєєва Л.А. Шушура О.М. Оцінка ризиків конфіденційності інформаційної безпеки проектів на основі нечіткої логіки. *Телекомунікаційні та інформаційні технології*. 2021. № 1 (70). Київ 2021. ISSN 2412-4338. DOI:10.31673/2412-4338.2021.0108895 . С. 88-95.

9. Common Vulnerability Scoring System v3.1. [Електронний ресурс] – Режим доступу:https://www.first.org/cvss/v3.1/user-guide.

10. Shushura O. M. Infological modeling of information systems subject industries in solving of fuzzy control tasks. *Зв'язок*. 2018. № 2. С. 53–56.

References

1. ISMS Framework. [Electronic resource] URL: https://www.enisa.europa.eu /topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework.

2. Zadeh L.A. Fuzzy sets // Information and Control. – 1965. – Vol. 8. – PP. 338–353.

3. Anikin, I. V., Emaletdinova L.Yu. “Analysis of approaches to assessing information security risks in corporate information networks”. *Bulletin of Kazan State Power Engineering University*. - 2015. NQ (25). PP. 55-67.

4. Mishchenko A.V., Kurilo O.V., Zolotukhina O.A. “A vague model for assessing the security of information security and the level of security of ERP systems”. *Telecommunications and Information Technologies*. 2020. №1(66). DOI: 10.31673/2412-4338.2020.011451 с.142-151.

5. Bharadwaj R. K. Manthaa, Borja Garcia de Sotob. “Cyber security challenges and vulnerability assessment in the construction industry”. *Conference Creative Construction* 2019. 29 June - 2 July 201. Budapest, Hungary. DOI:10.3311/CCC2019-005. PP 30-37.

6. Construction Industry Institute. CII. *CyberSecurity for Construction*. July 21, 2021. [Electronic resource] URL: https://www.construction-institute.org/events/education/free-webinar-cybersecurity-for-construction.

7. NIST. Measurements for Information Security. Created September 15, 2020, Updated December 3, 2020. [Electronic resource] URL: https://www.nist.gov/cybersecurity/measurements - information-security.

8. Asieieva L.A. Shushura O. M. Assessment of confidentiality risks of information security of projects based on fuzzy logic. Telecommunications and information technologies. 2021. № 1 (70). Kyiv 2021. ISSN 2412-4338. DOI:10.31673/2412-4338.2021.0108895 . С. 88-95.

9. Common Vulnerability Scoring System v3.1. [Electronic resource] URL:https://www.first.org/cvss/v3.1/user-guide.

10. Shushura O. M. “Infological modeling of information systems subject industries in solving of fuzzy control tasks”. *Link*. 2018. № 2. PP. 53–56.