УДК 004.056.5 DOI:10.31673/2412-4338.2021.0108895

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

# ОЦІНКА РИЗИКІВ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОЕКТІВ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

***Анотація:*** *Однією з головних складових управління інформаційною безпекою підприємства є оцінка її ризиків. Особливо це стосується підприємств критичної інфраструктури та їх бізнес-партнерів, в тому числі будівельних підприємств. Однак вимірювання кібербезпеки навіть при поточному стрімкому зростанні витрат на кібербезпеку залишається недостатньо розвиненою темою, тому розробка та узгодження надійних способів вимірювання її ризиків та ефективності є актуальними для досліджень. В багатьох галузях діяльність підприємств має проектний характер і управління інформаційною безпекою також необхідно реалізовувати в межах проекту, що вимагає подальших досліджень в цій області. Враховуючи неповноту та розмитість інформації щодо складових інформаційної безпеки, в моделях оцінки ризиків активно використовується нечітка логіка. У статті наведено підхід для оцінки ризиків порушення конфіденційності документів при вирішенні задач інформаційної безпеки проектів. Формалізовано набір документів проекту в вигляді узагальненої ієрархічної структури та визначено зв'язок документів з операціями та інформаційними системами, які використовуються під час операцій над документами. На основі формалізованої структури документів розроблено модель для оцінки ризику від порушення конфіденційності документа на засадах нечіткої логіки, яка дозволяє врахувати неповноту та розмитість даних. Результати роботи можуть бути використані при прийнятті рішень щодо заходів інформаційної безпеки проектів на підприємствах, які мають проектні види діяльності, в тому числі на підприємствах критичної інфраструктури, IT- підприємствах, в будівельних компаніях та інших. Запропоновані підходи можуть слугувати основою для розробки інформаційних технологій автоматизації оцінки ризиків інформаційної безпеки проектів.*

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

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

# ASSESSMENT OF CONFIDENTIALITY RISKS OF INFORMATION SECURITY OF PROJECTS BASED ON FUZZY LOGIC

***Abstract:*** *One of the main components of enterprise information security management is its risk assessment. This is especially true for critical infrastructure enterprises and their business partners, including construction companies. However, measuring cybersecurity, even with the current skyrocketing costs of cybersecurity, remains an underdeveloped topic, so developing and agreeing on reliable ways to measure its risks and effectiveness is relevant for research. In many industries, the activities of enterprises are of a design nature and information security management must also be implemented within the framework of the project, which requires further research in this area. Given the incompleteness and vagueness of information about the components of information security, fuzzy logic is actively used in risk assessment models. The article proposes an approach for assessing the risks of violating the confidentiality of documents when solving information security problems of projects. The set of project documents is formalized in the form of a generalized hierarchical structure and the relationship of documents with operations and information systems that are used during operations with documents is determined. Based on the formalized structure of documents, a model has been developed for assessing the risk of violating the confidentiality of a document based on fuzzy logic, which allows one to take into account the incompleteness and blurring of data. The results of the work can be used when making decisions on information security measures for projects at enterprises with project activities, including at critical infrastructure enterprises, IT*

*enterprises, construction companies and others. The proposed approaches can serve as a basis for the development of information technologies to automate the assessment of information security risks of projects.*

***Keywords**: information security risk, project risk assessment, fuzzy logic, confidentiality risk*

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

## ОЦЕНКА РИСКОВ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЕКТОВ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ

***Аннотация:** Одной из главных составляющих управления информационной безопасностью предприятия является оценка ее рисков. Особенно это касается предприятий критической инфраструктуры и их бизнес-партнеров, в том числе строительных предприятий. Однако измерение кибербезопасности даже при текущем стремительном росте расходов на кибербезопасность остается недостаточно развитой темой, поэтому разработка и согласование надежных способов измерения ее рисков и эффективности актуальны для исследований. Во многих отраслях деятельность предприятий имеет проектный характер и управление информационной безопасностью также необходимо реализовывать в рамках проекта, что требует дальнейших исследований в этой области. Учитывая неполноту и размытость информации о составляющих информационной безопасности, в моделях оценки рисков активно используется нечеткая логика. В статье приведен подход для оценки рисков нарушения конфиденциальности документов при решении задач информационной безопасности проектов. Формализован набор документов проекта в виде обобщенной иерархической структуры и определена связь документов с операциями и информационными системами, которые используются во время операций над документами. На основе формализованной структуры документов разработана модель для оценки риска нарушения конфиденциальности документа на основе нечеткой логики, которая позволяет учесть неполноту и размытость данных. Результаты работы могут быть использованы при принятии решений о мерах информационной безопасности проектов на предприятиях, имеющих проектные виды деятельности, в том числе на предприятиях критической инфраструктуры, ИТ предприятиях, в строительных компаниях и других. Предложенные подходы могут служить основой для разработки информационных технологий автоматизации оценки рисков информационной безопасности проектов.*

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

### Вступ

Загальне зростання рівня кіберзлочинності, розширення форм та видів використання вразливостей інформаційних технологій при проведенні гібридних атак певними державами та організаціями вимагають системного застосування методів кібербезпеки як на рівні держави, так і на рівні окремих підприємств. Особливо це стосується підприємств критичної інфраструктури та їх бізнес-партнерів, в тому числі будівельних підприємств [1-3].

Однією з головних складових управління інформаційною безпекою підприємства є оцінка її ризиків. Керівництво організацій вимагає від служб безпеки більш точних та кількісних методів та способів, що відображають та оцінюють фактори ризиків кібербезпеки. Надання надійних відповідей на ці питання вимагає від організацій системного підходу. Але навіть у міру зростання ризиків та витрат на основі кібербезпеки, вимірювання кібербезпеки залишається недостатньо розвиненою темою, у якій немає стандартної систематики для таких термінів, як “вимірювання” та “показники”, тому розробка та узгодження надійних способів вимірювання ризиків та ефективності є актуальним для досліджень [4].

Враховуючи неповноту та розмитість інформації щодо складових інформаційної безпеки в моделях оцінки ризиків активно використовується нечітка логіка, запропонована Л. Заде [5]. Зокрема, нечітка логіка задіяна для оцінки ризиків інформаційної безпеки

корпоративних мереж та ERP систем [2,6]. Однак в багатьох галузях діяльність підприємств має проектний характер і управління інформаційною безпекою також необхідно реалізовувати в межах проекту, що вимагає подальших досліджень в цій області.

**Основна частина**

Метою даної роботи є розробка підходів для оцінки ризиків інформаційної безпеки проекту на основі нечіткої логіки. Для досягнення поставленої мети проведена формалізація інформаційної структури проекту як сукупності певних документів. Під час життєвого циклу кожного документу, що включає створення, передачу, збереження і перетворення виникають загрози щодо його конфіденційності, цілісності, доступності та достовірності. В даній роботі розроблено модель оцінки ризиків порушення конфіденційності документів проекту на основі використання нечіткої логіки.

У загальному випадку проект розглядається як сукупність операцій із досягнення цілей при обмежені часу та ресурсів. Прояв змін та поточний стан результатів проекту в певні моменту часу описують документи, що його супроводжують. Наприклад, для будівельного підприємства документ, що супроводжує проект, є основним інформаційним активом проекту.

Позначимо документ в загальному випадку як $d_{lk}^{i} \in D$, де D - множина документів проекту; $i$ - 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.

Всі екземпляри і-го документа форми $l$ позначимо як $d_{l}^{i}$, що визначається за формулою:

$$d_{l}^{i} = \bigcup_{k} d_{lk}^{i} . \tag{1}$$

Всі екземпляри документа і-го документа всіх форм позначимо як $d^{i}$ (узагальнений документ), що визначається за формулою:

$$d^{i} = \bigcup_{l} d_{l}^{i} . \tag{2}$$

Стан документа представимо як функцію:

$$F_{S} : D \times T \to S , \tag{3}$$

де $D$ – множина документів; $T$ – вісь часу; $S$ – множина станів документа $S$ ={project, actual, inoperative}.

Множину документів $D$ розіб’ємо по їх видам:

$$D = \bigcup_{j=1}^{n} D_{j}, D_{j} \bigcap D_{m} = \varnothing, j \neq m . \tag{4}$$

Протягом життєвого циклу документа з ним може виконуватися безліч різних операцій, серед яких створення, редагування, погодження, затвердження, використання, утилізація, архівування тощо. Позначимо множину операцій над документом $d^{i}$ як $P_{i}$. Кожна операція $p_{ij} \in P_{i}$ передбачає використання певного програмного та технічного

забезпечення, обладнання, роботу певного персоналу із різним рівнем доступу тощо. Позначимо $ISP_{ij}$ множину інформаційних систем, що використовуються під час виконання операції $p_{ij} \in P_i$ над документом.

Для виконання операції $p_{ij} \in P_i$ може залучатися як співробітник підприємства, так і співробітник підрядника чи замовника (власника). Сукупність операцій $P_i$ по документу $d^i$ може бути представлена у вигляді мережевого графу, що відображає технологічну схему обробки документа. При цьому можуть створюватися різні екземпляри документів в різних формах $d^i_{lk} \in D$, тобто кожній операції $p_{ij} \in P_i$ у загальному випадку співставлений деякий набір документів.

Під порушенням конфіденційності документа розуміють фактор стороннього ознайомлення з інформацією документа, він стає відомим тому, хто не володіє повноваженнями доступу до нього. Воно має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається тому числі в комп'ютерній системі або передається від однієї системи до іншої.

Рівень ризику порушення конфіденційності $RConf^i$ документу $d^i$ визначимо як :

$$RConf^i = PConf^i \cdot UConf^i, \tag{5}$$

де $PConf^i$ – оцінка можливості загрози порушення конфіденційності документа $d^i$; $UConf^i$ – оцінка шкоди від загрози порушення конфіденційності документа $d^i$.

Розрахунок оцінки можливості порушення конфіденційності $PConf^i$ документа $d^i$ здійснюється так:

$$PConf^i = \max_{p_{ij} \in P_i} PConf^i_j, \tag{6}$$

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

До опису факторів ризику інформаційної безпеки проекту застосуємо лінгвістичний підхід. Це забезпечить створення кількісних оцінок для елементів моделі в умовах нечіткої інформації про значення рівня ризику, шкоди від загрози, можливостей виникнення певних загроз, рівнів незахищеності з вразливостями [6].

Для розрахунку оцінки $PConf^i_j$ можливості порушення конфіденційності документа $d^i$ під час операції $p_{ij} \in P_i$ пропонується нечітка модель, узагальнена структура якої наведена на рисунку 1.

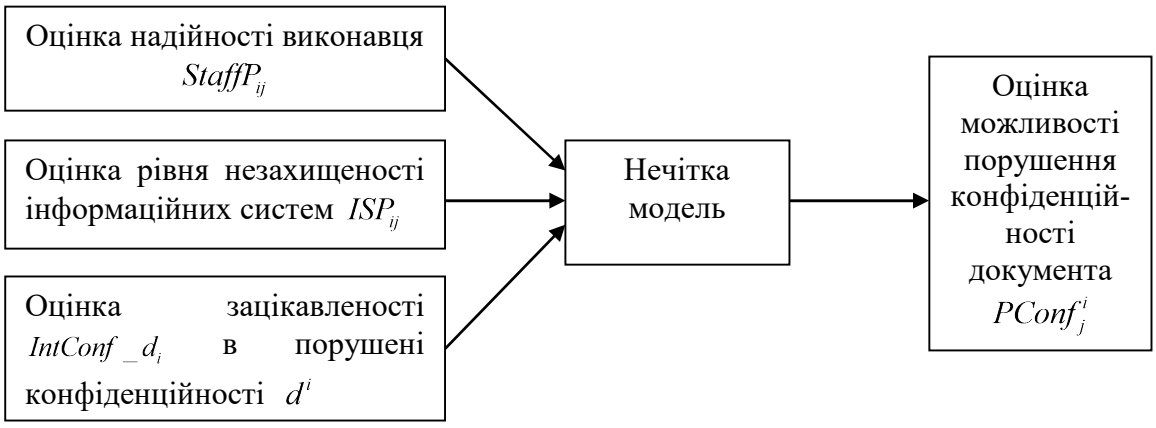


Рис. 1. Нечітка модель оцінки можливості загрози порушення конфіденційності документа

Як видно на рисунку 1, в нечіткій моделі вхідними є лінгвістичні змінні:

- рівень надійності виконавця операції $StaffP_{ij}$;
- оцінка рівня незахищеності інформаційних систем $ISP_{ij}$;
- оцінка зацікавленості $IntConf\_d_i$ сторонніх акторів в порушені конфіденційності документа $d^i$.

Для спрощення будемо вважати, що у операції $p_{ij} \in P_i$ лише один виконавець. Цього можна легко досягнути, врахувавши дане припущення при формуванні множини операцій над документом. Для оцінки рівня надійності виконавця може бути використана відповідна модель, побудована на засадах нечіткої логіки. В такому випадку для проведення розрахунків слід застосувати ієрархічне нечітке логічне виведення.

Для оцінки рівня незахищеності інформаційних систем пропонується використати стандарт CVSS [7] і розрахувати показник вразливості інформаційних систем $ISP_{ij}$ операції $p_{ij} \in P_i$. На основі цього показника запропонована лінгвістична змінна $LevelISP_{ij}$, опис якої відповідно до методики інфологічного моделювання [8] наведено у вигляді фрейму на рисунку 2.

| **Рівень незахищеності інформаційних систем $LevelISP_{ij}$ при використанні оцінок вразливостей за CVSS** | |
|---|---|
| Тип | Input |
| **Блок змінних** | |
| Оцінка вразливостей по стандарту CVSS | Множина допустимих значень {1…10} |
| **Блок термів** | |
| None | Лінійна z-образна функція належності $\mu(x, 0, 0.1)$ |
| Low | Трикутна функція належності $\mu(x, 0.1, 3.9, 4)$ |
| Medium | Трапецевидна функція належності $\mu(x, 3.9, 4.0, 6.9, 7)$ |
| High | Трапецевидна функція належності $\mu(x, 6.9, 7.0, 8.9, 9)$ |
| Critical | трикутна функція належності $\mu(x, 8.9, 9, 10)$ |
| Опис процедури формування нових термів відсутня | |
| Опис процедури формування функцій належності термів відсутня | |

Рис. 2. Опис лінгвістичної змінної рівня незахищеності інформаційних систем

З метою формування функцій належності термів лінгвістичної змінної $LevelISP_{ij}$ використана обробка експертних оцінок на основі методу аналізу ієрархій Сааті [8].

Для кількісної оцінки рівня зацікавленості в порушені конфіденційності документа $IntConf\_d_i$ пропонується застосувати метод аналізу ієрархій, спираючись на експертні оцінки на основі трирівневої ієрархії в вигляді дерева декомпозицій по акторам загроз та видам документів, представленої на рисунку 3. Оцінювати рівень зацікавленості в порушенні конфіденційності за замовчуванням запропоновано для виду документу. В тих випадках, коли це припущення не може бути застосовано, рівень зацікавленості встановлюється експертом.

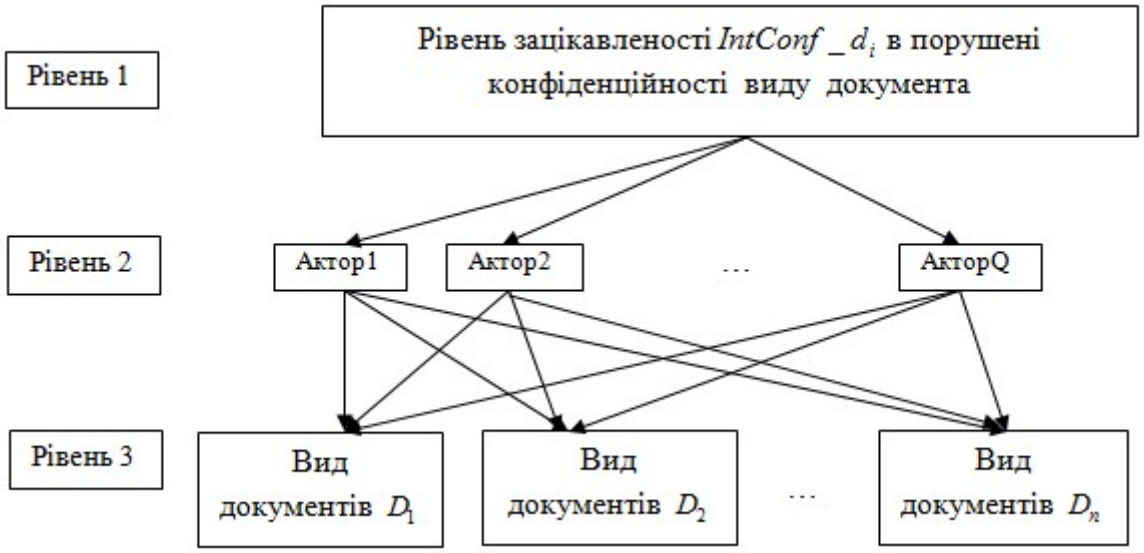


Рис. 3. Дерево критеріїв оцінки рівня зацікавленості в порушенні конфіденційності документу

Розрахунок оцінки $UConf^i$ шкоди від загрози порушення конфіденційності документа $d^i$ вимагає введення множини частинних показників, що впливають на даний збиток/шкоду. Узагальнений перелік частинних показників розроблено і представлено у таблиці 1. Показники розподілені за трьома групами: зовнішній збиток/шкода організації, внутрішній збиток/шкода організації, фінансові збитки організації. Для розрахунку оцінки $UConf^i$ пропонується використати метод аналізу ієрархій на основі дерева критеріїв, яке складається з рівня частинних показників шкоди, видів документів проекту та документів, розподілених по видам. Шкода від порушення конфіденційності оцінюється в грошовому еквіваленті або у балах, які можуть бути використані при прийнятті рішень стосовно заходів кібербезпеки.

*Таблиця 1*

Перелік частинних показників збитку/шкоди

| № | Назва показника | Група показників |
|---|---|---|
| 1 | Збиток авторитету організації | Зовнішня збиток/шкода |
| 2 | Збиток авторитету України на міжнародній арені | |
| 3 | Судові витрати | |
| 4 | Негативна реакція на рівні уряду України | |
| 5 | Публікація негативних матеріалів у пресі | |
| 6 | Можливість здійснення терористичних актів | |
| 7 | Можливість звершення техногенних катастроф | |
| 8 | Звільнення фахівців організації | Внутрішній збиток/шкода |
| 9 | Зниження рівня інформаційної безпеки | |
| 10 | Втрата або руйнування активів організації | |
| 11 | Вплив на прийняті персоналом організації рішення в бізнес-процесів | |
| 12 | Необхідність перевірки і відновлення цілісності активу | |
| 13 | Погіршення емоційного клімату в колективі | |
| 14 | Дезорганізація діяльності | |
| 15 | Необхідність ручного виконання робіт | |

*Продовження таблиці 1*

| № | Назва показника | Група показників |
|---|---|---|
| 16 | Зниження конкурентоспроможності організації | Фінансовий збиток |
| 17 | Втрати вигоди при укладанні договорів | |
| 18 | Зниження ліквідності і курсової вартості акцій | |
| 19 | Неможливість організації виконати свої зобов'язання перед клієнтами і постачальниками | |
| 20 | Необхідність проведення додаткових досліджень | |
| 21 | Можливість розкрадання активів і проведення неврахованих операцій | |
| 22 | Зниження цін на продукцію, обсягів продажів | |
| 23 | Втрата можливостей патентування, продажу ліцензій | |
| 24 | Випередження конкурентами виведення аналогічної продукції на ринок | |
| 25 | Відмова від стратегічних рішень, що стали неефективними | |
| 26 | Погіршення умов отримання кредитів | |
| 27 | Падіння рентабельності виробництва | |
| 28 | Зниження рівня співпраці з діловими партнерами | |
| 29 | Масові крадіжки, шахрайства | |

**Висновки.** В роботі наведено підхід для оцінки ризиків порушення конфіденційності документів при вирішенні задач інформаційної безпеки проектів. Формалізовано набір документів проекту в вигляді узагальненої ієрархічної структури та визначено зв'язок документів з операціями та інформаційними системами, які використовуються під час операцій над документами. На основі формалізованої структури документів розроблено модель для оцінки ризику від порушення конфіденційності документа на засадах нечіткої логіки, яка дозволяє врахувати неповноту та розмитість даних.

Результати роботи можуть бути використані при прийнятті рішень щодо заходів інформаційної безпеки проектів на підприємствах, які мають проектні види діяльності, в тому числі на підприємствах критичної інфраструктури, IT- підприємствах, в будівельних компаніях та інших. Запропоновані підходи можуть слугувати основою для розробки інформаційних технологій автоматизації оцінки ризиків проектів.

**Список використаних джерел**

1. 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.

2. 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.

3. 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.

4. 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.

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

6. 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.

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

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

9. Oleksii Shushura, Liudmyla Asieieva, Iryna Husyeva, Mykhailo Stepanov, Oksana Datsiuk. Construction of Membership Functions in Fuzzy Modeling Tasks Using the Analytic Hierarchy Process. International Journal of Advanced Trends in Computer Science and Engineering. Volume 9, No.3, May - June 2020/ p.2702-2707. Https://DOI.org/10.30534/ijatcse/2020/33932020.

**References**

1. 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.

2. 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.

3. 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.

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

5.Zadeh L.A. “Fuzzy sets”. *Information and Control*. 1965. Vol. 8. PP. 338–353.

6. 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 c.142-151.

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

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

9. Oleksii Shushura, Liudmyla Asieieva, Iryna Husyeva, Mykhailo Stepanov, Oksana Datsiuk. “Construction of Membership Functions in Fuzzy Modeling Tasks Using the Analytic Hierarchy Process”. *International Journal of Advanced Trends in Computer Science and Engineering*. Volume 9, No.3, May - June 2020/ p.2702-2707. Https://DOI.org/10.30534/ijatcse/2020/33932020.