УДК 004.056:338
DOI: 10.25140/2411-5363-2021-1(23)-62-68

Іван Карпович, Олена Гладка, Юрій Бухало

ТЕХНОЛОГІЇ МОДЕЛЮВАННЯ І ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Виконано моделювання, аналіз і оцінювання ризиків інформаційної безпеки на основі прикладних аспектів теорії графів в поєднанні з експертними методами оцінювання. Проаналізовано сучасні підходи до моделювання заходів та методики оцінки ризиків в інформаційній безпеці. Сформульовано рекомендації щодо підвищення ефективності системи захисту інформації. Запропонована модель може бути застосована на етапі аудиту безпеки організації для виявлення слабких місць системи захисту, а також для удосконалення діючої системи кіберзахисту.

Ключові слова: *загроза; захист інформації; засоби захисту; аналіз ризиків інформаційної безпеки; експертне оцінювання; управління інформаційною безпекою; модель оцінки ризиків.*

Рис.: 3. Бібл.: 12.

Актуальність теми дослідження. Діяльність практично будь-якої організації чи підприємства пов'язана з необхідністю застосування сучасних технологій збору, опрацювання та зберігання інформації. У зв'язку з цим неминучі виникнення загроз інформаційній безпеці, які необхідно своєчасно усувати, щоб уникнути втрати цілісності, конфіденційності та доступності інформації і нанесення збитку діяльності організації. Зростання уваги до проблем захисту інформації зумовлене збільшенням кількості інцидентів, пов’язаних із втратою і розголошенням інформації чи втратою контролю над нею. Тому актуальним завданням є розробка фундаментальних основ інформаційної безпеки та проведення прикладних досліджень у цьому напрямку.

Постановка проблеми. У загальному вигляді предмет захисту інформації можна подати у вигляді наступної схеми (рис. 1), де взаємодія компонентів відбувається під впливом заходів із захисту інформації. Захист інформації поєднує в собі як застосування технічних засобів, так і проведення певного виду організаційних заходів.

Рис. 1. Схема предмету захисту інформації

Створення системи інформаційної безпеки вимагає розв’язування задач, які спрямовані на захист як формалізованої, так і неформалізованої інформації. У першому випадку можна сформувати і за допомогою методів теорії інформації розрахувати точні параметри, що відображають ступінь захищеності об'єкта або системи. Однак у другому випадку, а також для комплексної оцінки рівня захищеності нерідко доводиться застосовувати експертні методи оцінювання тих параметрів, які неможливо розрахувати за допомогою теоретико-інформаційного підходу. Загалом, моделювання заходів інформаційної безпеки повинно враховувати як наявність невизначеності, обумовленої відсутністю інформації або складністю системи, так і наявність інформації якісного характеру про систему [1].

Аналіз останніх досліджень і публікацій. Оцінка ризиків інформаційної безпеки в проблемі управління на сьогодні – одна зі складних і актуальних задач. Складність полягає в тому, що відсутні загальноприйняті підходи і методики для оцінки ризиків. Фактори ризику (загроза, вразливість, збиток) аналізуються за допомогою евристичних методів, у результаті чого можна отримати дані, які значно відрізняються, якщо експертиза проводилася різними експертами [2]. Крім того, процедура оцінювання ризиків є трудомістким завданням. Проводити аналіз, застосовуючи офісні інструменти, завдання практично нездійсненне у зв'язку із великими обсягами інформації і ймовірністю отримати помилковий результат. Тому необхідно застосовувати сукупність методів аналізу та обробки інформації, що дозволяють оцінити ризики інформаційної безпеки й на основі отриманих даних здійснювати управління інформаційною безпекою.

© Карпович І. М., Гладка О. М., Бухало Ю. П., 2021

Аналіз підходів до математичного моделювання систем захисту інформації показує, що широкого поширення набувають методи моделювання, які ґрунтуються на неформальній теорії систем: методи структурування, методи оцінювання та методи пошуку оптимальних рішень [3–6]. Методи структурування є розвитком формального опису, що поширюється на організаційно-технічні системи. Методи оцінювання дозволяють визначити значення характеристик системи, які не можуть бути виміряні або отримані з використанням аналітичних виразів чи в процесі статистичного аналізу (ймовірності реалізації загроз, ефективність елементів системи захисту та ін.). Комбінування перелічених методів дозволяє розширити можливості застосування формальних теорій для проведення повноцінного моделювання систем захисту.

Виділення недосліджених частин загальної проблеми. Формування системи інформаційної безпеки об'єкта потребує вирішення низки завдань, пов'язаних з формалізованою інформацією – інформацією взаємодії у формі документів або обмінних сигналів технічних систем. У цьому випадку можна застосувати методи математичної теорії інформації і вдається сформувати досить точні значення параметрів, що характеризують захищеність системи. Однак для повної оцінки захищеності ці параметри доводиться порівняти з оцінками зовнішнього впливу, інформація про який безпосередньо недоступна. Отримати таку оцінку можна лише експертним шляхом. Застосовувати методи теорії інформації в цьому випадку неефективно, тому що результат повністю визначається вхідними припущеннями, які формуються зазвичай довільно.

Одним із найважливіших етапів у процесі управління інформаційною безпекою є етап аналізу та оцінки ризиків інформаційної безпеки. Методики оцінки ризиків в інформаційній безпеці з'явилися для прогнозування можливого збитку, пов'язаного з реалізацією загроз, і, відповідно, оцінки необхідного обсягу інвестицій на створення систем захисту інформації. Кількісний розрахунок величини ризиків ускладнюється насамперед відсутністю достатнього обсягу статистичних даних про ймовірності реалізації тієї чи іншої загрози. У результаті значного поширення набула якісна оцінка інформаційних ризиків. Задача розрахунку можливого збитку й економічне обґрунтування розміру необхідних інвестицій в інформаційну безпеку для запобігання реалізації ризиків не втратила своєї важливості.

Постановка завдання. Управління інформаційною безпекою організації може бути реалізовано за допомогою математичного моделювання в поєднанні з експертними методами оцінювання. У цій роботі розглянуто методику аналізу й оцінки ризиків інформаційної безпеки з використанням елементів теорії графів.

Виклад основного матеріалу. Математичне моделювання, як відомо, дозволяє отримати формальний опис системи та сформулювати в подальшому кількісні і якісні оцінки її показників. Для створення і дослідження систем захисту інформації використовують теорію випадкових процесів, теорію графів, теорію нечітких множин, теорію ігор, еволюційне моделювання тощо. Відмінності моделей здебільшого полягають у змісті й характеристиках вхідних і вихідних параметрів.

Ризик інформаційної безпеки будемо визначати як добуток фінансових втрат (збитків), пов'язаних з інцидентами безпеки, на ймовірності того, що вони будуть реалізовані [7]. Це визначення підходить при розгляді різних архітектур інформаційних систем. Інформація може існувати в різних формах. Але яких би форм інформація не набувала, вона завжди повинна бути захищена відповідним чином.

З погляду управління ризиками, оцінка ризиків інформаційної безпеки – це аналіз інформаційних систем і технологій, які систематично піддаються загрозам та наявним вразливостям, науковими методами і засобами. На підставі проведеного оцінювання потенційних збитків у разі загрозливих подій розгортаються контрзаходи проти загроз для запобігання чи врегулювання ризиків інформаційної безпеки, а також здійснюється контроль ризиків на прийнятному рівні таким чином, щоб максимально підтримати безпеку інформації.

Оцінювання ризиків інформаційної безпеки складається з трьох основних етапів: ідентифікація загроз, ідентифікація вразливостей, ідентифікація активів (рис. 2) [8]. Процес оцінки ризику інформаційної безпеки виглядає наступним чином:

1) визначення інформаційних активів, встановлення цінності активів;
2) аналіз загроз, визначення ймовірності загроз;
3) ідентифікація вразливостей інформаційних активів, визначення міри вразливості;
4) обчислення ймовірності настання події щодо реалізації загроз (використання вразливостей);
5) поєднуючи важливість інформаційних активів і можливість виникнення інцидентів, виконується розрахунок значення ризику інформаційної безпеки для інформаційного активу.

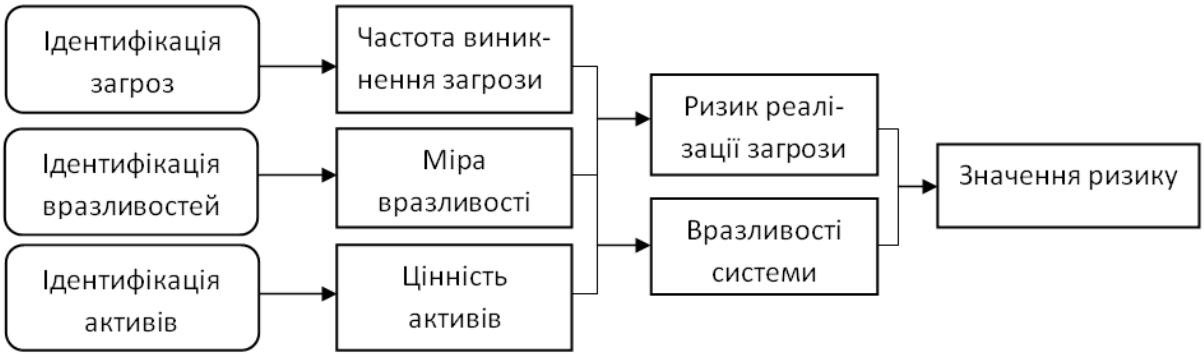

Рис. 2. Елементи оцінки ризиків інформаційної безпеки

Множина вразливостей V системи може бути подана у вигляді декартового добутку множини I рівнів порушників, які можуть реалізувати загрозу, і множини станів S системи, в яких вразливості існують: $V \subseteq I \times S$.

Відповідно до теорії графів [9], граф атаки – це граф, що представляє всі можливі послідовності дій порушника для реалізації загрози. Такі послідовності дій називають шляхами атак (рис. 3).

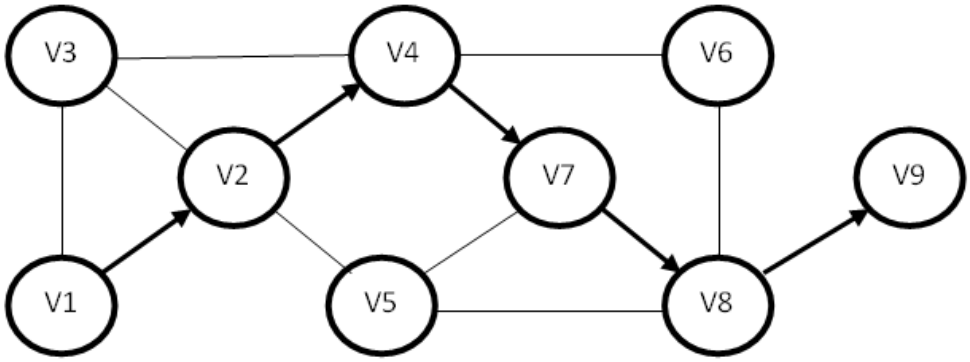

Рис. 3. Граф атаки

Під елементарної атакою (atomic attack) розуміють використання порушником вразливості. Прикладом елементарної атаки може бути, наприклад, переповнення буфера служби SSH, що дозволяє віддалено отримати права адміністратора системи тощо.

Розрізняють наступні види графів атак [10]:

• state enumeration graph (граф переліку станів) – у таких графах вершинам відповідають трійки (s, d, a), де s – джерело атаки, d – мета атаки, a – елементарна атака (або використання вразливості); дуги позначають переходи з одного стану в інший;

• condition-oriented dependency graph (граф умово-орієнтованих залежностей) – вершинам відповідають результати атак, а дугам – елементарні атаки, що призводять до таких результатів;

• exploit dependency graph (граф реалізації залежностей) – вершини відповідають результатам атак або елементарним атакам, дуги відображають залежності між вершинами – умови, необхідні для виконання атаки, і наслідок атаки.

Побудований граф містить сценарії атак, які порушник може реалізувати. У результаті аналізу такого графа можна визначити [11]:

• перелік успішних атак, які не виявляються системою виявлення атак (вторгнень) IDS (англ. Intrusion Detection System);

• співвідношення реалізованих заходів безпеки й рівня захищеності мережі (інформаційної системи);

• перелік найбільш критичних вразливостей;

• перелік заходів, що дозволяють запобігти використанню вразливостей у програмному забезпеченні, для якого відсутні оновлення;

• мінімальна кількість заходів, реалізація яких зробить інформаційну систему чи мережу захищеною.

Систему захисту інформації, за аналогією з рис. 3, можна подати у вигляді орієнтованого графа $G = (T, S)$, де вершинами $T = \{t_i\}$, $i = 1, 2, 3, ..., n$ будуть загрози активам з боку зловмисників, а дугами S – їх зв'язки [12]. Зауважимо, що загроза, розміщена в певній вершині графа, може бути спрямована як на один, так і на декілька активів; у свою чергу, один актив може бути розміщений своїми частинами в кількох вершинах. Дуга (t_k, t_{k+1}) позначає зв'язок загрози t_k із загрозою t_{k+1}, ймовірна реалізація якої є прямим наслідком реалізації загрози t_k. Кожен зв'язок характеризується величиною ймовірності вибору зловмисником шляху реалізації пов'язаної загрози – $p(t_k, t_{k+1})$.

Відмітимо, що не всі загрози можуть бути реалізовані безпосередньо. Здійснення деяких атак стає можливим лише за умови реалізації "батьківських" загроз. Прикладом може служити несанкціонований доступ до конфіденційної інформації, що вимагає фізичного втручання в мережеву інфраструктуру. Множина загроз і зв'язків, а також їхні параметри визначаються експертним способом. Завдяки використанню такого набору даних і описаної структури з'являється можливість усунути недоліки моделі безпеки, в якій кожній загрозі протиставлено свій засіб захисту.

Кожній загрозі поставимо у відповідність параметри:

ω_{t_i} – частота виникнення загрози t_i;

p_{t_i} – ймовірність реалізації загрози, наприклад, унаслідок успішного використання деякої вразливості.

Спочатку за допомогою формули розрахунку вартості ризику обчислимо ймовірні втрати від реалізації окремих загроз:

$$R_{t_i} = \sum_{k=1}^{k1} \omega_{t_i} p_{t_i} d_{t_i} c(a_k), \qquad (1)$$

де $k1$ – кількість активів, на які спрямована загроза t_i, $i = 1, 2, 3, ..., n$;

A_{t_i} – набір активів або ресурсів, на які спрямована загроза t_i;

$c(a_k)$ – вартість активу $a_k \in A_{t_i}$.

Коефіцієнт пошкодження (руйнування) $d_{t_i} \in [0;1]$, що виражає рівень руйнівної дії загрози t_i на актив чи активи [12], може служити критерієм відбору (селектором) тих активів, на які поширюється руйнівна дія загрози t_i.

Імовірні втрати від реалізації загроз, що реалізуються одна за одною на деякому шляху $M(t_\alpha, t_\beta)$, розраховуємо за формулою:

$$R_{M(t_\alpha, t_\beta)} = R_{t_\alpha} + \sum_{i=1}^{m} \sum_{j=1}^{r} p(t_i, t_j) R_{t_j}, \quad (2)$$

де m, r – кількість "батьківських" і "дочірніх" загроз відповідно на шляху $M(t_\alpha, t_\beta)$.

Для $t_i \in M(t_\alpha, t_\beta)$ знаходимо витрати на забезпечення захисту від реалізації загроз на шляху $M(t_\alpha, t_\beta)$:

$$F_{M(t_\alpha, t_\beta)} = \sum_{i=1}^{n} F_{t_i} \quad (3)$$

де F_{t_i} – витрати на забезпечення захисту від реалізації загрози t_i.

Далі виконується порівняння вартості ризику з витратами на забезпечення інформаційної безпеки і приймається рішення щодо цього ризику на основі відомих рекомендацій. Ризик може бути проігноровано, якщо його величина незначна, або визнано прийнятним, якщо $R_{t_i} = F_{t_i}$. Якщо $R_{t_i} < F_{t_i}$, можна оптимізувати витрати на засоби захисту. Ризик можна усунути, якщо є можливість відмовитися від використання активу, який піддається ризику або передати його третій стороні, наприклад, застрахувати. Якщо ж $R_{t_i} > F_{t_i}$, то ризик необхідно знижувати за рахунок впровадження нових засобів захисту.

Висновки. Використання моделі, що поєднує в собі застосування формальної математичної теорії і неформальних методів, зокрема, експертного оцінювання та пошуку оптимальних розв'язків, дозволить вирішити прикладну задачу з мінімізації ризиків можливих збитків у сфері інформаційної безпеки. Такі моделі можуть бути застосовані на етапі аудиту безпеки інформаційної системи чи мережі для виявлення слабких місць системи захисту і прогнозування дій порушника, а також для удосконалення діючої системи кіберзахисту підприємства чи організації. Хоча однією з основних цілей моделювання систем захисту інформації є створення найбільш ефективної системи. Оскільки абсолютно неперебороного захисту створити не можна, необхідно дотримуватися балансу між витратами на захист і одержуваним ефектом, у тому числі економічним: пам'ятаючи, що вартість засобів захисту не повинна перевищувати вартості активів, досягнути максимально можливого зменшення втрат від порушення інформаційної безпеки.

Список використаних джерел

1. Зайченко Ю. П. Нечеткие модели и методы в интеллектуальных системах : учебник для вузов. Киев : Слово, 2008. 344 с.

2. Булдакова Т. И., Миков Д. А. Реализация методики оценки рисков информационной безопасности в среде Matlab. *Вопросы кибербезопасности*. 2015. № 4 (12). С. 53–61.

3. Карпович І. М., Гладка О. М., Наконечна Ю. А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* Серія: Технічні науки. 2020. Т. 31 (70), № 5. С. 69–74.

4. Герасименко В. А. Защита информации в автоматизированных системах обработки данных : в 2 кн. Москва: Энергоатомиздат, 1994.

5. Stepashko V., Bulgakova O., Zosimov V. Construction and research of the generalized iterative GMDH algorithm with active neurons. *Advances in Intelligent Systems and Computing*. Springer Verlag. 2018. Vol. 689. Pp. 492–510.

6. Шуляр С. Методи виявлення ризиків безпеки у життєвому циклі розробки ПЗ. *Прикладні науково-технічні дослідження* : матеріали V Міжнар. наук.-прак. конф., 5–7 квітня 2021 р. Івано-Франківськ, 2021. С. 96–98.

7. Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві : монографія. Київ : КНЕУ, 2004. 480 с.

8. Астахов А. Искусство управления информационными рисками. Москва : ДМК Пресс, GlobalTrust, 2006. 312 с.

9. Іглін С. П. Теорія графів : навч. посіб. Харків : НТУ «ХПІ», 2017. 146 с.

10. Jajodia S., Noel S. Managing Attack Graph Complexity Through Visual Hierarchical Aggregation. In *1st International Workshop on Visualization and Data Mining for Computer Security*, Washington, DC, USA. October 2004. Pp. 109–118.

11. Колегов Д. Н. Проблемы синтеза и анализа графов атак. URL: https://www.securitylab.ru/contest/299868.php.%202007?R=1.

12. Курилов Ф. М. Моделирование систем защиты информации. Приложение теории графов. *Технические науки: теория и практика* : материалы III Международ. науч. конф. (г. Чита, апрель 2016 г.). Чита : Изд-во «Молодой ученый», 2016. С. 6–9.

References

1. Zaichenko, Yu. P. (2008). *Nechetkie modeli i metody v intellektualnykh sistemakh [Fuzzy models and methods in intelligent systems].* Slovo.

2. Buldakova, T. I., Mikov, D. A. (2015). Realizatsiia metodiki otsenki riskov informatsionnoi bezopasnosti v srede Matlab [Implementation of information security risk assessment methodology in Matlab environment]. *Voprosy kiberbezopasnosti – Cybersecurity issues*, (4(12)), pp. 53–61.

3. Karpovych, I. M., Hladka, O. M., Nakonechna, Yu. A. (2020). Analiz ryzykiv bezpeky informatsiinoi systemy IT-pidpryiemstva [Analysis of security risks of information system of IT-enterprise]. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky – Scientific notes of V. I. Vernadsky Tavriya National University. Series: Technical Sciences. K.: TNU. V. I. Vernadsky, 31(70)*(5), pp. 69–74.

4. Gerasimenko, V. A. (1994). *Zashchyta ynformatsyy v avtomatyzyrovannыkh systemakh obrabotky danniakh [Information protection in automated data processing systems].* Energoatomizdat.

5. Stepashko, V., Bulgakova, O., Zosimov, V. (2018). Construction and research of the generalized iterative GMDH algorithm with active neurons. *Advances in Intelligent Systems and Computing*, (689), pp. 492–510.

6. Shulyar, S. (2021). Metody vyiavlennia ryzykiv bezpeky u zhyttievomu tsykli rozrobky PZ [Methods for identifying security risks in the software development life cycle]. *Prykladni naukovo-tekhnichni doslidzhennia : materialy V Mizhnar. nauk.-prak. konf. – Applied scientific and technical research: materials V International scientific-practical Conf.* (pp. 96–98).

7. Vitlinsky, V. V., Velykoivanenko, G. I. (2004). *Ryzykolohiia v ekonomitsi ta pidpryiemnytstvi [Riskology in economics and entrepreneurship]*. KNEU.

8. Astakhov, A. (2006). *Iskusstvo upravleniia informatsionnymi riskami [The art of information risk management].* DMK Press, GlobalTrust.

9. Iglin, S. P. (2017). *Teoriia hrafiv [Theory of graphs]*. NTU “KhPI”.

10. Jajodia, S., Noel, S. (2004). Managing Attack Graph Complexity Through Visual Hierarchical Aggregation. In 1st International Workshop on *Visualization and Data Mining for Computer Security* (pp. 109–118).

11. Kolegov, D. N. (2007). *Problemy sinteza i analiza grafov atak [Problems of synthesis and analysis of attack graphs]*. https://www.securitylab.ru/contest/299868.php.%202007?R=1.

12. Kurilov, F. M. (April, 2016). Modeling of information security systems. Graph theory application. *Technical sciences: theory and practice: materials III International scientific conf.* (pp. 6-9). Young Scientist Publishing.

UDC 004.056:338

Ivan Karpovych, Olena Hladka, Yuriy Bukhalo

TECHNOLOGIES OF MODELING AND ASSESSMENT OF THE INFORMATION SECURITY RISKS

The growing focus on information security is due to the increasing number of incidents involving the loss and disclosure of information or the loss of control over it. Therefore, the urgent task is to develop the fundamentals of information security and applied research.

Today, the activities of almost any organization is associated with the need to use modern technologies for collecting, processing and storing information. This creates threats to information security, which must be addressed in a timely manner to avoid loss of integrity, confidentiality and availability of information.

Modern approaches to modeling measures and methods of risk assessment in information security are analyzed. The difficulty of qualitative assessment of information risks is that there are no generally accepted methods of such assessment. Risk factors analyzed by different experts using heuristic methods can differ significantly, and therefore the assessment of information security risks in the problem of management today is one of the most difficult and urgent tasks.

Information security management is implemented using mathematical modeling in combination with expert evaluation methods. The purpose of this work is to develop methods for analyzing and assessing information security risks using elements of graph theory.

We consider building a model that combines the application of formal mathematical theory and informal methods, in particular, expert evaluation and search for optimal solutions, which allows to solve the applied problem of minimizing the risk of possible damage in the field of information security. The proposed model can be used during the security audit of the organization to identify weaknesses in the security system, as well as to improve the existing cyber security system.

Based on the applied aspects of graph theory, modeling, analysis and assessment of information security risks are performed. Recommendations for improving the efficiency of the information protection system are formulated.

Keywords: *threat; information protection; means of protection; information security risk analysis; expert evaluation; information security management; risk assessment model.*

Fig.: 3. References: 12.

Карпович Іван Миколайович – кандидат фізико-математичних наук, доцент, доцент кафедри комп'ютерних технологій та економічної кібернетики, Національний університет водного господарства і природокористування (вул. Соборна, 11, м. Рівне, 33028, Україна).
Karpovych Ivan – PhD on Physics and Mathematics Science, Associate Professor, Assistant Professor in Department of Computer Technology and Economic Cybernetics, National University of Water and Environmental Engineering (11 Soborna Str., 33028 Rivne, Ukraine).
E-mail: karpivan@ukr.net
Scopus Author ID: 7005525002

Гладка Олена Миколаївна – кандидат технічних наук, доцент, доцент кафедри комп'ютерних технологій та економічної кібернетики, Національний університет водного господарства і природокористування (вул. Соборна, 11, м. Рівне, 33028, Україна).
Hladka Olena – PhD in Engineering Science, Associate Professor, Assistant Professor in Department of Computer Technology and Economic Cybernetics, National University of Water and Environmental Engineering (11 Soborna Str., 33028 Rivne, Ukraine).
E-mail: o.m.hladka@nuwm.edu.ua
ORCID: https://orcid.org/0000-0003-4728-0663
ResearcherID: AAE-3216-2019
Scopus Author ID: 57191967048

Бухало Юрій Петрович – здобувач вищої освіти, Національний університет водного господарства і природокористування (вул. Соборна, 11, м. Рівне, 33028, Україна).
Bukhalo Yuriy – student, National University of Water and Environmental Engineering (11 Soborna Str., 33028 Rivne, Ukraine).
E-mail: bukhalo_ak19@nuwm.edu.ua

Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. *Технічні науки та технології.* 2021. № 1(23). С. 62-68.