## INFORMATION SECURITY RISK MANAGEMENT

DOI 10.20535/2411-1031.2020.8.2.222608
УДК 004[056.53+413.4]

ВОЛОДИМИР МОХОР,
АНДРІЙ ДАВИДЮК

# СПОСІБ ОЦІНЮВАННЯ РИЗИКІВ ПОРУШЕННЯ ВЛАСТИВОСТЕЙ ІНФОРМАЦІЇ ЗА КОЛІРНОЮ ШКАЛОЮ

Одним з актуальних завдань сьогодення є захист інформації, що визначено нормативними документами нашої держави в сфері інформаційної безпеки та кібербезпеки. Захист інформації полягає у забезпеченні збереження таких її властивостей як конфіденційність цілісність та доступність. У процесі оцінювання захищеності інформації визначаються пріоритети її захисту з урахуванням ступеня обмеження доступу до неї. Для вибору ефективних заходів та засобів захисту здійснюється оцінювання ризиків інформаційної безпеки. Тому проаналізовано існуючі методи оцінювання, що базуються на знаходженні величин можливого збитку від настання інциденту інформаційної безпеки та ймовірності або вірогідності його виникнення. Однак, жодною з форм формалізації рівня ризику не відображається, які саме властивості можуть бути порушені в межах інциденту. Тобто загальне представлення ризику не дає можливості оперативного його оброблення. З використанням сучасних комп'ютерних технологій стало можливим створення динамічних зображень рівня ризику. Насамперед адитивної моделі передавання червоного, зеленого та синього кольорів. З огляду на це, розроблено спосіб оцінювання ризиків порушення властивостей інформації. Його використання дозволить розрізняти властивості інформації за встановленим кольором. З появою інформації про нові вразливості інформаційно-телекомунікаційних систем колір може змінюватися, що сигналізуватиме про зміну рівня ризику для конкретної властивості інформації. Такий підхід до управління ризиками інформаційної безпеки сприяє оперативному прийманню рішень щодо оброблення ризиків та підтриманню процесу забезпечення інформаційної безпеки на належному рівні. Водночас використання запропонованого способу дозволить фіксувати змінення числових значень кольорів і, як наслідок, знаходити швидкість змінення рівня ризику інформаційної безпеки. Її усереднене значення може використовуватися для прогнозування стійкості системи захисту до інцидентів інформаційної безпеки. Тому швидкістю змінення рівня ризику інформаційної безпеки можна розширити перелік параметрів визначення індексу розвитку інформаційної системи та підставою для актуалізації запланованих витрат організації на забезпечення інформаційної безпеки.

**Ключові слова:** властивості інформації, інформаційна безпека, ризик інформаційної безпеки, оцінювання ризиків, колірна шкала.

**Постановка проблеми.** Процес оцінювання ризиків є невід'ємною частиною впровадження системи управління інформаційною безпекою організації (СУІБ) [1]. Нормативними документами нашої держави визначено вимоги щодо забезпечення збереженості властивостей інформації шляхом побудови СУІБ та/або комплексної системи захисту інформації з підтвердженою відповідністю [2]. У свою чергу оцінювання ризиків інформаційної безпеки здійснюється відповідальними співробітниками за процес розроблення таких систем. Саме від коректності результатів оцінювання ризиків та форм їхнього представлення керівництву залежить його участь у процесі оброблення неприйнятних ризиків інформаційної безпеки (ІБ) та підвищення захищеності інформаційних активів. Однак, серед проаналізованих способів представлення рівнів ризику ІБ відсутні ознаки розмежування щодо порушень конкретних властивостей інформаційних активів. Вони дають лише загальне уявлення про рівень захищеності інформації (див., наприклад [3], рис. 1-3).

© В. Мохор, А. Давидюк, 2020

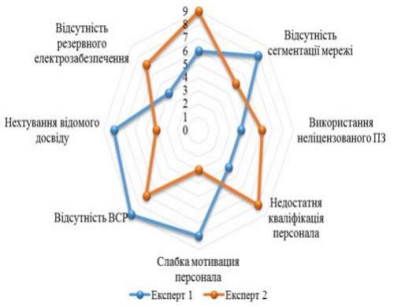


Рисунок 1 – Представлення рівнів ризику ІБ “трояндою”

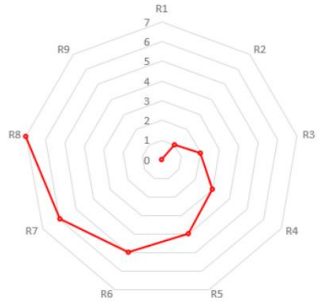


Рисунок 2 – Представлення аналізу груп ризиків за ймовірністю реалізації ризику “Спіраллю”

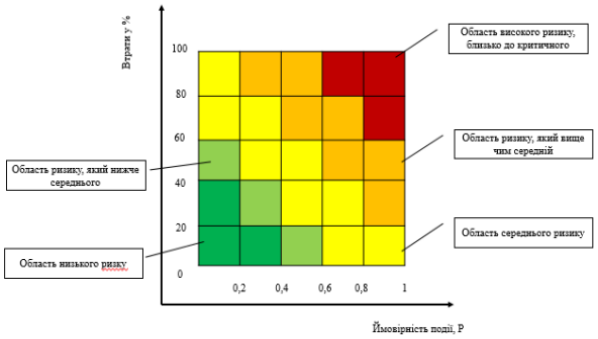


Рисунок 3 – Представлення рівнів ризику “картою ризику”

Інформація щодо ризику порушення однієї з трьох властивостей інформації може вказуватися у його паспорті. Дане представлення є незручним, зокрема, за великої кількості загроз безпеці інформаційних активів. Тому виникає потреба зручного представлення рівнів ризику ІБ. При цьому важливим є адаптування його для використання засобами візуальної аналітики. Це дозволить оперативно приймати рішення щодо його оброблення з урахуванням пріоритетів забезпечення ІБ. Під візуальною аналітикою розумітимемо напрям аналізування, що сфокусований на винесенні аналітичного рішення за допомогою візуальних інтерактивних користувацьких інтерфейсів [4].

Отже, розроблення способу оцінювання ризиків порушення властивостей інформації за колірною шкалою є актуальним завданням.

**Аналіз останніх досліджень і публікації.** Аналіз основних способів представлення результатів оцінювання ризиків ІБ наведено в [3]. Серед них виокремлюються такі розповсюджені варіанти представлення з дискретними шкалами оцінок як дерево ризиків, кругові діаграми, карти ризиків з дискретними шкалами оцінок рівня ризику та інші способи представлені в публікаціях [5] - [10]. Однак, ними складно врахувати порушення конкретних властивостей інформації та специфіку середовища у якому проявляється ризик. Також варто звернути увагу на те, що дані способи базуються на основі методів експертних оцінок та статистичних методах. Це призводить до наявності певної невизначеності вибору заходів та засобів забезпечення ІБ з урахуванням пріоритету збереження властивостей інформації.

**Метою статті є** підвищення ефективності оброблення ризиків ІБ завдяки розробленню способу їхнього оцінювання за колірною шкалою.

**Виклад основного матеріалу дослідження.** На сьогодні використання кольору у аналізуванні даних є доволі розповсюдженим, зокрема його застосування у програмах оркестраторах для аналізування фінансових даних, для проєктування обладнання (Siemens PLM Software), обчисленнях гідродинаміки (Computional Fluid Dynamics), аналізу даних з соціальних мереж [4]. Не виключенням є і представлення рівнів ризику ІБ, що обмежене зеленим, жовтим та червоним кольорами та їх відтінками на карті ризиків. Тому колір можна

використати й для відображення порушень окремих властивостей інформації як інформаційного активу організації. Для представлення стану інформаційного активу з прийнятним рівнем ризику використаємо колірну модель RGB (англ. “red, green, blue”), представлену у вигляді куба (див., наприклад [11], рис. 4), де на осі *X* відображені відтінки червоного, на осі *Y* – зеленого, на осі *Z* – синього.

На даній моделі можна побачити щонайбільше 3 сторони з 6. І, як би не рухали цей геометричний об’єкт їхня кількість залишиться без змін. Це можна використати для представлення кожною з них окремого кольору після чого присвоїти кожній видимій стороні певного кольору по одній з властивостей інформації. Наприклад, червоний – конфіденційність, зелений – доступність, синій – цілісність. Інші три невидимі сторони будуть білого кольору і відображатимуть невизначеність. Тоді представлене на рис. 4 зображення буде формально відповідати інформаційному активу у якого однаково захищені всі три властивості інформації. Однак, у реальному житті такого стану досягти складно. Тому ним відображатиметься актуальний стан захищеності інформаційного активу.

Уявимо, що кожен ряд цього куба може рухатися на $360^{o}$ за аналогією з іграшкою “кубик Рубік” (див., наприклад, рис. 5). Тоді при виникненні інциденту ІБ, що призвів до впливу на певну властивість інформації, поточний ряд замінюватиметься білим. Це відображатиме проблему збереженості конкретної властивості інформаційного активу. Одночасно може виникати певна множина таких проблем забезпечення ІБ. І не завжди вирішення однієї проблеми дозволятиме подолати інші або може призводити до появи нових.

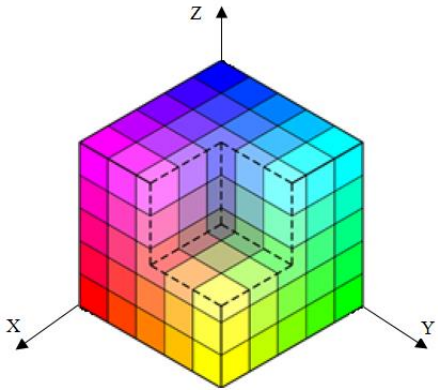


Рисунок 4 – Представлення колірної моделі “RGB” кубом

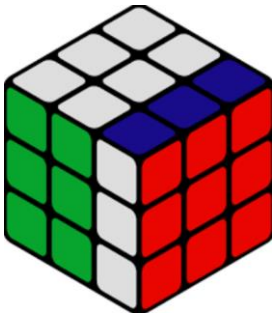

Рисунок 5 – Приклад візуалізування забезпечення збереженості властивостей інформації

З огляду на рис. 5, потрібно виконати завдання вибору порядку збирання цього “куба”. Зокрема, отримання очікуваного результату за мінімальну кількість кроків. Однак, за малий проміжок часу зазвичай зробити це складно, тоді як комп’ютер справиться з цим значно швидше і знайде найбільш точний результат. Шляхи пошуку такого рішення, яким можливе забезпечення збереженості властивостей інформаційного активу у найкоротші строки насамперед важливе для об’єктів критичної інформаційної інфраструктури. Оскільки нештатні зміни в їхній роботі можуть мати катастрофічні наслідки. Це обумовлено тим, що основними критеріями до функціонування об’єктів критичної інформаційної інфраструктури є їхня відмовостійкість та неперервність операцій [12].

Також необхідно сформувати для комп’ютера завдання з пошуку шляху з найменшою кількістю кроків до повернення інформаційного активу у захищений стан. Для цього можна використати математичний апарат логіки предикатів першого порядку, що дасть змогу зв’язати об’єкти певної множини з їхніми властивостями. Такий підхід дасть змогу використати трикластеризацію як спосіб виявлення об’єктів зі схожими властивостями в контексті з трьох видів сутностей (властивостей інформації) [4]. Наприклад, розділити

інформаційні активи за пріоритетами захисту їх трьох властивостей. Використання трикластеризації дозволить знайти групи активів з однаковими пріоритетами та врахувати це при пошуку найкоротшого вектору досягнення стану захищеності. У даному випадку графічно пропонується до кожного квадрату на стороні куба, який має певний колір вписати по одній загрозі порушення відповідної властивості інформаційного активу. Для кращого інтуїтивного сприйняття їм будемо присвоювати відтінки відповідно до величини можливих збитків від найменшої для блідого до найбільшої для насичених відтінків. Це пояснюється фізіологічними якостями людини звертати більшу увагу на щось яскраве, аніж на бліде. Тобто градієнт кожного кольору являтиме колірну шкалу оцінок ризиків ІБ для кожної з властивостей інформаційного активу за величиною можливих збитків. Завдяки цьому кожну зі сторін можна тлумачити як карту ризиків для певної властивості інформаційного активу. Комп'ютер, маючи координати кожного квадрату на стороні і знаючи принцип обертання кожного ряду (див., наприклад, рис. 5), зможе знайти найменшу кількість ітерацій, що відповідатиме найкоротшому шляху для повернення його у вихідний стан. Знаходження найкоротшого шляху для кожного квадрату на стороні куба, що змістився, дасть змогу отримати послідовність з найменшою кількістю кроків для повернення сторони куба у вихідний стан. Звісно, це рішення не є способом модернізації системи з метою підвищення рівня захисту, проте воно здатне значно підвищити "живучість" системи до впливу невизначеностей за тлумаченням ризику через вплив невизначеності на досягнення мети.

Враховуючи це, можливо математично обґрунтувати пріоритети оброблення ризиків та побудувати стратегію забезпечення ІБ. З огляду на те, що такий куб має обмежену кількість комбінацій розміщення його елементів, реально знайти всі можливі комбінації відсортувавши їх за кількістю кроків повернення стану забезпечення ІБ у вихідне положення. Додатково можна оцінити час на стабілізацію ситуації, визначивши які зі загроз (квадратики, що змінюють своє положення) найчастіше зустрічаються серед комбінацій і, як наслідок, спрогнозувати найбільш вірогідні типи атак. Отримані результати від застосування такого способу можуть виявитися більш точними на відміну від існуючих підходів на основі статистичних даних або оцінок експертів. Зокрема, враховуючи те, що для статистичного методу досі не вирішеним залишається питання формування вибірки інцидентів ІБ. Так як в умовах динамічного розвитку інформаційних систем вкрай складно віднайти однакові умови виникнення подій безпеки та необхідну кількість таких випадків, щоб отримати коректні статистичні дані. На даний момент такі дані не є повною мірою статистичними, і описуються таким поняттям як частість [13]. Експертний метод вважається більш продуктивним, проте його основою є суб'єктивні знання та досвід експертів, що не завжди можуть бути універсальними для кожного конкретного середовища функціонування інформаційної системи.

Беззаперечно, точність прогнозування атак буде залежати від коректності розстановки загроз по квадратах "кубіка Рубіка" з відповідними відтінками та їх попереднього оцінювання. Однак, даний спосіб можливо зробити більш точним з використанням систем штучного інтелекту. Вони здатні за кількістю та оцінками наявних у відкритих базах вразливостей оцінити рівень критичності загроз, що пов'язані з використанням конкретного програмного або апаратного забезпечення. Це дасть змогу забезпечити підтримку прийняття рішень з оптимальної стратегії оброблення ризиків [14].

Додатково до переваг такого способу можна віднести можливість відслідковування швидкості зміни стану кожної властивості інформаційного активу на конкретному рівні існування загроз. Показник цієї швидкості відображатиме стійкість інформаційного активу до впливу невизначеності. Тоді можна ввести додаткове поняття до управління ризиками – "стійкість до ризику". Воно буде відображати відношення швидкості зміни стану захищеності властивостей інформаційного активу до мінімально необхідного часу на відновлення цього стану. Використання таких фізичних величин як швидкість та час у оцінюванні ризиків дасть можливість розширити можливості аналітичних механізмів обробки даних з використанням систем на основі нейронних мереж (штучного інтелекту), що здатні навчатися як з учителем так і без.

Варто також зазначити, що оцінювання ризиків повинно враховувати те, що величина збитків може змінюватися в часі і є відносною. Коли мова йде про оцінку вартості (наприклад, дорого, дешево), порівнюється вартість з сумою наявних коштів і в залежності на скільки відрізняються вартість і сума коштів, приймається рішення щодо можливості організації дозволити собі той чи інший актив або його втрату. Тоді стала величина збитків при збільшенні капіталу організації все менше впливатиме на досягнення нею її цілей і навпаки при збільшенні величини збитку і сталому капіталі компанії – вплив буде більшим. В умовах реальної діяльності організації і величина можливих збитків, і величина капіталу постійно змінюються. Отже, необхідно визначати відношення швидкості росту/падіння капіталу організації до швидкості росту/падіння величини збитку за якого втрати не призведуть до банкротства компанії – коефіцієнт допустимої зміни.

$$K = \left(H_2 - H_1\right) / \left(H_4 - H_3\right)$$

де $K$ – коефіцієнт допустимої зміни;

$H_1$ – початкова величина капіталу;

$H_2$ – прогнозована величина капіталу;

$H_3$ – початкова величина збитку;

$H_4$ – прогнозована величина збитку.

При цьому ймовірність реалізації загрози може визначатися за значенням коефіцієнта допустимої зміни. Його значення у більшості випадків за наявності договірних відносин легше передбачити, ніж вірогідність появи кіберінциденту з використанням вразливості нульового дня.

Тоді при значенні $K < 1$ ризик потребує оброблення, а при $K > 1$ є прийнятним. Отже, у даному випадку можемо узагальнити, що при оцінюванні ризику ІБ також можна використовувати відношення швидкості росту величини капіталу до швидкості росту величини збитку. Зокрема, такий спосіб поводження з ризиками ІБ може бути універсальним та доповнений урахуванням природи ризику індивідуально для кожного окремого інформаційного активу – фізична, інформаційна, геопросторова, процедурна, соціальна [15], де фізична – визначає технічну взаємозалежність між елементами системи захисту; інформаційна – залежність від інформаційного обміну між елементами системи захисту; геопросторова – взаємозалежність між елементами системи захисту, що виникає внаслідок взаємного розміщення елементів системи захисту; процедурна – виникає внаслідок якогось інциденту на одному з елементів системи захисту і провокує вплив на інші складові системи захисту; соціальна – виникає через соціальні фактори; суспільна думка, довіра, страх. Для більш точної характеристики ризику з урахуванням специфіки зв'язків між елементами системи захисту пропонується їх класифікувати за сферами – інформаційна, інфраструктурна, економічна, політична, соціальна.

**Висновки.** Запропоновано застосування колірної моделі "RGB" для представлення ризиків ІБ за допомогою куба. Для позначення ризиків порушення таких властивостей інформації як конфіденційність, цілісність та доступність використано червоний, зелений та синій кольори і введено градієнт кольору як шкалу оцінювання можливих збитків унаслідок реалізації загроз. Використання моделі за аналогією з "кубіком Рубіком" дозволить відображати зміни стану ІБ, прогнозування найбільш вірогідних типів атак, вибору оптимальної стратегії оброблення ризиків та обчислення швидкості зміни властивостей інформації. На основі значень швидкості зміни стану захищеності властивостей інформації та мінімального часу на відновлення її початкового стану введено поняття "стійкість до ризику".

Результати даного дослідження можуть математично обґрунтувати вектори захисту, зменшивши вплив суб'єктивізму та некоректності вибірки при оцінюванні ризиків ІБ. Підвищити ефективність обраних механізмів захисту інформації не залежно від галузі використання.

У перспективах подальших досліджень планується розробити систему підтримки прийняття рішень для оброблення ризиків інформаційної безпеки та моніторингу захищеності інформації з використанням нейронних мереж. Зокрема, вибору оптимальних алгоритмів пошуку найкоротшого шляху у тривимірному просторі та сортування великого масиву даних у реальному часі.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


[1] ДП "УкрНДНЦ". (2015, Груд. 18). *ДСТУ ISO/IEC 27001, Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги* (ISO/IEC 27001:2013; Cor 1:2014, IDT). Київ, 2016, 22 с.

[2] Верховна рада України (1994, Лип. 05) *Закон 80/94-ВР, Про захист інформації в інформаційно-телекомунікаційних системах.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/ laws/ show/80/94-%D0%B2%D1%80#Text. Дата звернення: Трав. 19, 2020.

[3] В. Мохор, О. Бакалинський та В. Цуркан, "Аналіз способів представлення оцінок ризиків інформаційної безпеки", *Information Technology and Security*, Vol. 6, iss. 1, pp. 75-84, 2018, doi: 10.20535/2411-1031.2018.6.1.153189.

[4] Ю. С. Кашницкий, "Визуальная аналитика в задаче трикластеризации", *Труды МФТИ*, том 6, № 3, с. 43-56, 2014.

[5] O. Latvala, J. Toivonen, A. Evesti, M. Sihvonen, and V. Jordan "Security Risk Visualization with Semantic Risk Model", *Procedia Computer Science*, vol. 83, pp. 1194-1199, 2016, doi: 10.1016/ j.procs.2016.04.247.

[6] М. В. Буйневич, В. В. Покусов, и К. Е. Израилов, "Способ визуализации модулей системы обеспечения информационной безопасности". [Електронный ресурс]. Доступно: https://cyberleninka.ru/article/n/sposob-vizualizatsii-moduley-sistemy-obespecheniya-informatsionnoy-bezopasnosti/viewer. Дата обращения: Авг. 08, 2020.

[7] В. Мохор, О. Бакалинський, та В. Цуркан, "Представлення оцінок ризиків інформаційної безпеки картою ризиків", *Information Technology and Security*, vol. 6, iss. 2, pp. 94-104, 2018, doi: 10.20535/2411-1031.2018.6.2.153494.

[8] М. В. Коломеец, А. А. Чечулин, Е. В. Дойникова, и И. В. Котенко "Методика визуализации метрик кибербезопасности", *Вычислительная техника,* том 61, № 10, 2018, doi: 10.17586/0021-3454-2018-61-10-873-880.

[9] J. Muchagata, and A. Ferreira, "How can visualization affect security", *SCITEPRESS*, pp. 503-510, 2018, doi: 10.5220/0006695505030510.

[10] S. Yoo, H. Ryu, H. Yeon, T. Kwon, and Y. Jang, "Visual analytics and visualization for android security risk", *Journal of computer languages*, vol. 53, pp. 9-21, 2019, doi: 10.1016/ j.cola.2019.03.004.

[11] Wikipedia (2020, листопад). RGB. 2020. [Online]. Available: https://ru.wikipedia.org/wiki/ RGB#/ media/%D0%A4%D0%B0%D0%B9%D0%BB:RGBCube_b.svg. Accessed on: Aug. 08, 2020.

[12] Кабінет Міністрів України, (2019, Чер. 19). *Постанова № 518, Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури*. [Електронний ресурс]. Доступно: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-zagalnih-vimog-do-kiberzahistu-obyektiv-kritichnoyi-infrastrukturi-i190619. Дата звернення: Серп. 08, 2020.

[13] В. М. Безштанько, та В. В. Цуркан, "Діофантовий метод визначення частості нанесення збитку внаслідок реалізації загрози безпеці інформації", *Захист інформації*, том 15, № 4, 2013, doi: 10.18372/2410-7840.15.5707.

[14] National vulnerability database. [Онлайн]. Доступно: https://nvd.nist.gov/. Дата звернення: Серп. 08, 2020.

[15] Б. Д. Леонов, Р. М, Шостак, та В. С. Серьогін, “Розвиток методичного забезпечення антитерористичноъ захищеності об’єктів критичної інфраструктури (На прикладі США)”, *Інформація і право,* № 3, с. 88-96, 2020.

Стаття надійшла до редакції 09.08.2020

**REFERENCE**

[1] SE “UkrNDNC”. (2015, Dec. 18). *DSTU ISO/IEC 27001, Information Technologies. Methods of protection. Information security management systems. Requirements* (ISO / IEC 27001: 2013; Cor 1: 2014, IDT). Kyiv, 2016, 22 p.

[2] The Verkhovna Rada of Ukraine (1994, Jul. 05) *Law 80/94-BP, On the Protection of Information in Information and Telecommunication Systems.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text. Accessed on: May 19, 2020.

[3] V. Mokhor, O. Bakalinsky, and V. Tsurkan, “Analysis of ways to present information security risk assessments”, *Information Technology and Security*, Vol.6, pp. 75-84, 2018, doi: 10.20535/2411-1031.2018.6.1.153189.

[4] U. S. Kashnitsky, “Visual analytics in the problem of triclustering”, *Works of MIPT*, vol. 6, no. 3, pp. 43-56, 2014.

[5] O. Latvala, J. Toivonen, A. Evesti, M. Sihvonen, and V. Jordan “Security Risk Visualization with Semantic Risk Model”, *Procedia Computer Science*, vol. 83, pp. 1194-1199, 2016, doi: 10.1016/ j.procs.2016.04.247.

[6] M. V. Buinevich, V. V. Pokusov, and K. E. Izrailov, “Method of visualization of information security system modules”, [Online]. Available: https://cyberleninka.ru/article/n/sposob-vizualizatsii-moduley-sistemy-obespecheniya-informatsionnoy-bezopasnosti/viewer. Accessed on: Aug. 08, 2020.

[7] V. Mokhor, O. Bakalinsky, and V. Tsurkan, “Presentation of information security risk assessments by a risk map”, *Information Technology and Security*, vol. 6, iss. 2, pp. 94-104, 2018, doi: 10.20535/2411-1031.2018.6.2.153494.

[8] M. V. Kolomeets, A. A. Chechulin, E. V. Doinikova, and I. V. Kotenko, “Methods of visualization of cybersecurity metrics”, *Computing*, vol. 61, no. 10, 2018, doi: 10.17586/ 0021-3454-2018-61-10-873-880.

[9] J. Muchagata, and A. Ferreira, “How can visualization affect security”, *SCITEPRESS*, pp. 503-510, 2018, doi: 10.5220/0006695505030510.

[10] S. Yoo, H. Ryu, H. Yeon, T. Kwon, and Y. Jang, “Visual analytics and visualization for android security risk”, *Journal of computer languages*, vol. 53, pp. 9-21, 2019, doi: 10.1016/ j.cola.2019.03.004.

[11] Wikipedia (2020, листопад). RGB. 2020. [Online]. Available: https://ru.wikipedia.org/wiki/ RGB#/media/%D0%A4%D0%B0%D0%B9%D0%BB:RGB Cube_ b.svg. Accessed on: Aug. 08, 2020.

[12] Cabinet of Ministers of Ukraine, (2019, June 19). *Resolution № 518, On approval of the General requirements for cyber protection of critical infrastructure*. [Online]. Available: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-zaganih-vimog-do-kiberzahistu-obyektiv-kritichnoyi-infrastrukturi-i190619. Accessed on: Aug. 08, 2020.

[13] V. M. Bezshtanko, and V. V. Tsurkan, “Diophantine method for determining the frequency of damage due to the implementation of information security threats”, *Ukrainian Information Security Research Journal*, vol. 15, no. 4, 2013, doi: 10.18372 / 2410-7840.15.5707.

[14] NIST (2021) National vulnerability database. [Online]. Available: https://nvd.nist.gov/. Accessed on: Aug. 08, 2020.

[15] B. D. Leonov, R. M. Shostak, and V. S. Seryogin, “Development of methodological support for anti-terrorist protection of critical infrastructure facilities (on the example of the United States)”, *Information and Law*, № 3, pp. 88-96, 2020.

VOLODYMYR MOKHOR,
ANDRII DAVYDIUK

**APPROACH OF THE INFORMATION PROPERTIES DESTRUCTION RISKS ASSESSING BASED ON THE COLOR SCALE**

One of the urgent tasks of today is information protection as defined by the regulations of our state in the field of information security and cybersecurity. The protection of information is to ensure the preservation of its properties such as confidentiality, integrity, and accessibility. In the process of assessing the information security, the priorities of its protection are determined, taking into account the degree of restriction of access to it. Information security risks are assessed to select effective measures and remedies. The existing assessment methods are analyzed, based on estimates of the magnitude of possible damage from the occurrence of an information security incident and the probability or probability of its occurrence. However, none of the forms of formalizing the risk level reflects which properties may be violated within the incident. That is, the general presentation of the risk does not allow its prompt processing. With the use of modern computer technology, it has become possible to create dynamic images of the level of risk. The basis of computer graphics is an additive model of the transfer of red, green, and blue. With this in mind, a method has been developed to assess the risks of violating the properties of information. Its use will distinguish the properties of information by the set color. With the advent of information about new vulnerabilities in information and telecommunications systems, the color may change, which will signal a change in the level of risk for a particular property of information. This approach to information security risk management facilitates prompt decision-making on risk management and maintains the information security process at the appropriate level. At the same time, the use of the proposed method will allow to record changes in the numerical values of colors and, as a consequence, to find the rate of change of the level of information security risk. Its average value can be used to predict the resilience of the protection system to information security incidents. Therefore, the speed of change in the level of information security risk can expand the list of parameters for determining the index of information system development and the basis for updating the planned costs of the organization to ensure information security.

**Keywords:** information properties, information security, information security risk, risk assessment, color scale.

**Мохор Володимир Володимирович**, член-кореспондент Національної академії наук України, доктор технічних наук, професор, директор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

ORCID: 0000-0001-5419-9332.

E-mail: v.mokhor@gmail.com.

**Давидюк Андрій Вікторович**, аспірант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

ORCID: 0000-0003-1238-2598.

E-mail: andrey19941904@gmail.com.

**Mokhor Volodymyr**, corresponding member of the National Academy of Sciences of Ukraine, doctor of technical sciences, professor, director, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.

**Davydiuk Andrii**, postgraduate student, Pukhov Institute for Modeling in Energy Engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.