ISSN 2076-1546

УДК 004.056.5 DOI: 10.46972/2076-1546.2022.22.03

О. С. Бойченко, Д. С. Костерев, І. Ю. Маковський, О. М. Грищук

МАТЕМАТИЧНА МОДЕЛЬ РОЗРАХУНКУ ЦІННОСТІ ІНФОРМАЦІЇ УСТАНОВИ

Статтю присвячено вирішенню актуального науково-практичного завдання – розробці математичної моделі розрахунку цінності інформації установи. Наведено тлумачення таких понять: цінність, рівень важливості, час остаточного старіння інформації та вид права власності на неї, – які застосовують у ході досліджень самого об'єкта захисту. Детально розглянуто показники, за якими пропонується визначати цінність інформації, та доведено її залежність від них. Запропоновано розраховувати цінність інформації як середнє значення суми відповідних коефіцієнтів, кожен з яких обирається за допомогою методу ранжування. Важливість відповідного показника інформації визначається згідно з вимогами керівних документів щодо організації інформаційної безпеки або спеціально створеною групою експертів. Запропоновано використовувати такі коефіцієнти впливу: рівня доступу до інформації, часу остаточного її старіння, важливості інформації та виду права на неї. Проведено перевірку адекватності математичної моделі розрахунку цінності інформації установи. Встановлено, що інформація, яка має найвищий рівень обмеження доступу, найвищий рівень важливості та найвищий рівень права на неї (належать державі), має найбільшу цінність для установи. Наведено приклад, у якому складено список документів, у яких міститься інформація, що потребує захисту в установі, та розраховано значення її цінності. Математична модель розрахунку цінності інформації установи дозволяє обґрунтувати необхідність вжиття додаткових заходів для вдосконалення комплексної системи захисту інформації в автоматизованих системах установи та більш якісно підійти до питання формування моделі загроз інформації в інформаційно-комунікаційних системах.

Ключові слова: *цінність інформації; право власності на інформацію; час остаточного старіння інформації; рівень важливості інформації.*

Постановка проблеми в загальному вигляді. Діджиталізація сучасного суспільства спричинила широке використання інформаційних технологій у всіх сферах людської діяльності. Поява інформаційно-комунікаційних систем (ІКС), за допомогою яких автоматизовано процеси накопичення, модифікації, обміну, зберігання інформації, значно спрощує процеси управління повсякденною діяльністю установ за рахунок використання систем електронного документообігу. Такий рівень автоматизації роботи з інформацією в установі зумовлює ризики несанкціонованого доступу (НСД) до неї. Відповідно до [1] захист інформації від НСД в ІКС полягає в забезпеченні додержання правил розмежування доступу шляхом створення і підтримки в дієздатному стані системи заходів із захисту інформації. Із цією метою в ІКС установ створюються комплексні системи захисту інформації (КСЗІ).

© О. С. Бойченко, Д. С. Костерев, І. Ю. Маковський, О. М. Грищук, 2022

У сучасних КСЗІ в моделі загроз не завжди враховується цінність інформації, а більша увага приділяється порушенню її таких властивостей, як: цілісність, доступність, конфіденційність тощо. Тому в ході обстеження інформаційного середовища під час створення КСЗІ постає важливе науково-практичне завдання щодо розрахунку цінності інформації установи з метою своєчасного проведення організаційно-технічних заходів для забезпечення її захисту.

Виникнення цього важливого науково-практичного завдання зумовлено наявною об’єктивною суперечністю між вимогами до зменшення потенційних збитків від загроз для інформації та принциповою неможливістю їх врахування через чинний порядок обстеження інформаційного середовища, що й визначає своєчасність та актуальність досліджень.

Аналіз останніх досліджень і публікацій. Нормативні документи з технічного захисту інформації (НД ТЗІ) визначають вимоги до захисту інформації від несанкціонованого доступу в ІКС [1−5]. Зокрема, у цих документах окремо визначено характеристики фізичного середовища, обчислювальної системи, оброблюваної інформації та користувачів.

У НД ТЗІ [6] наведено порядок обстеження інформаційного середовища, у якому визначено, що аналізу підлягає вся інформація, яка обробляється та зберігається в ІКС. Під час аналізу вона повинна бути класифікована за режимом доступу, правовим режимом, мають бути визначені й описані види її подання в ІКС.

У НД ТЗІ [7] вказано, що вихідними даними для визначення вимог до заходів, методів та засобів захисту інформації є: завдання та функції ІКС, результати аналізу середовищ функціонування ІКС, модель загроз та модель порушників, а також результати аналізу ризиків.

Отже, у НД ТЗІ не приділено належної уваги питанню впливу цінності інформації на визначення вимог до заходів, методів та засобів її захисту.

У науковій праці [8] автори висвітлили результати аналізу методів визначення цінності та старіння інформації. У роботі встановлено взаємозв’язок між цими поняттями.

У [9, 10] цінність інформації розглядається як міра досягнення мети користувача після її отримання, тобто рівень реалізації цільової функції.

Цінність інформації з погляду захисту інформації визначається ступенем її корисності для власника [11].

На сьогоднішній день відомо чимало підходів до формалізації процесу розрахунку цінності інформації, однак дотепер у цьому процесі залишається значна частка суб'єктивізму. У відкритих джерелах не було запропоновано математичних моделей, які б описували у формалізованому вигляді кількісне значення цінності інформації.

Формулювання завдання дослідження. Метою статті є розроблення математичної моделі розрахунку цінності інформації з урахуванням таких критеріїв, як: рівень важливості інформації, вид права власності на неї, рівень обмеження доступу до інформації та, відповідно, час остаточного її старіння.

Виклад основного матеріалу. Під цінністю інформації установи в цьому дослідженні слід розуміти кількісну міру, яка визначає ступінь її корисності для

володільця інформації. Функціональну залежність цінності інформації від її показників можна подати за допомогою такого виразу:

$$VOI = \frac{\sum_{i=1}^{n} \alpha_i}{n}, \quad (1)$$

де n – кількість показників інформації, що мають вплив на її цінність;

α_i – коефіцієнт, який характеризує кількісну міру впливу i-го показника інформації на її цінність.

Розрахунок цінності інформації ґрунтується на методах та способах сучасної теорії системного аналізу, яка надає інструментарій для визначення відповідних коефіцієнтів, що приймають значення з відрізка [0…1].

Для розрахунку цінності інформації установи пропонуємо математичну модель, яка дозволяє отримати її числове значення шляхом розрахунку середнього значення суми відповідних коефіцієнтів, кожен з яких розраховується за допомогою методу ранжування. Важливість відповідного показника інформації визначається з керівних документів щодо організації інформаційної безпеки або спеціально створеною групою експертів.

Результати аналізу сучасних підходів до визначення цінності інформації свідчать про те, що в математичних моделях її розрахунку не враховано показників інформації, які характеризують ступінь важливості та вид права власності на неї. Тому в даному дослідженні характеризувати цінність інформації пропонуємо за певними показниками. Розглянемо їх детальніше.

1. Рівень обмеження доступу. За цим показником пропонуємо оцінювати вплив грифа обмеження доступу до інформації та часу остаточного старіння інформації на її цінність. Під старінням інформації розуміється втрата достовірності внаслідок змін і появи нових даних.

Відповідно до Закону України “Про інформацію” інформація за порядком доступу поділяється на відкриту та з обмеженим доступом, яка, у свою чергу, може бути конфіденційною, службовою або таємною. Чинним законодавством України передбачено час, через який переглядається інформація щодо віднесення її до таємної чи службової або зняття обмеження доступу до неї. Що стосується конфіденційної інформації, то законодавством України не встановлено терміну обмеження доступу до неї та не встановлено порядку віднесення інформації до конфіденційної. Правила доступу до конфіденційної інформації встановлюють фізичні та юридичні особи, у володінні яких вона перебуває. Конфіденційна інформація може мати велику цінність, втрата або передача якої іншим особам може завдати установі значних збитків [7]. З метою встановлення правил розмежування доступу до конфіденційної інформації необхідно її класифікувати шляхом поділу на декілька категорій за ступенем цінності. Але в дослідженні питання впливу категорій цінності конфіденційної інформації не розглядалося. Тому в статті запропоновано застосовувати рівні обмеження доступу до інформації r_i, зокрема й до конфіденційної інформації, та часу її остаточного старіння (табл. 1).

За допомогою відомого методу ранжування отримано коефіцієнт впливу грифа обмеження рівня доступу до інформації на цінність інформації β_1 та проведено його нормування за таким виразом:

$$\beta_1 = \frac{r_i}{\sum_{i=1}^{n} r_i}, \tag{2}$$

де n – кількість рівнів доступу до інформації;

r_i – коефіцієнт, який характеризує важливість i-го рівня доступу до інформації.

Для отримання коефіцієнта впливу часу остаточного старіння інформації на її цінність для відповідного рівня доступу до інформації β_2 пропонуємо використати вираз

$$\beta_2 = \frac{t_i}{\sum_{i=1}^{n} t_i}, \tag{3}$$

де n – кількість рівнів доступу до інформації;

t_i – час остаточного старіння інформації i-го рівня доступу.

Коефіцієнт, який характеризує вплив показника "Рівень обмеження доступу" на цінність інформації, α_1 складається з двох рівнозначних коефіцієнтів β_1 та β_2, а його значення є середнім арифметичним значень цих двох коефіцієнтів.

Результати розрахунку коефіцієнта, який характеризує вплив показника "Рівень обмеження доступу" на цінність інформації, α_1 наведено в табл. 1.

Таблиця 1

Показник "Рівень обмеження доступу"

Інформація за порядком доступу	r_i	β_1	Час остаточного старіння (діб)	β_2	α_1
Особливої важливості	6	0,286	10860	0,566	0,426
Цілком таємно	5	0,238	3620	0,189	0,213
Таємно	4	0,190	1810	0,094	0,142
Для службового користування	3	0,143	1810	0,094	0,119
Конфіденційна	2	0,095	1086	0,057	0,076
Відкрита	1	0,048	1	0,000	0,024

2. Рівень важливості інформації. Під важливою слід розуміти таку інформацію, втрата або несанкціонований доступ до якої завдадуть значних збитків установі або повністю зупинять її роботу. Важливість інформації та рівень її важливості запропоновано визначати групою експертів з установи, а кількісне значення отримувати шляхом нормування рівнів важливості за допомогою такого виразу:

$$\alpha_2 = \frac{im_j}{\sum_{j=1}^{k} im_j}, \tag{4}$$

де k – кількість рівнів доступу до інформації;

im_j – j-й рівень важливості інформації.

3. Вид права власності на інформацію. Право власності на інформацію визначається Законом України "Про інформацію". Відповідно до цього документа є такі види права власності на інформацію: персональна, колективна та державна. Рівень виду права власності на інформацію, яка циркулює в установі та підлягає захисту, пропонуємо визначати групою експертів з установи, а кількісне значення отримувати шляхом нормування рівнів виду права на інформацію за допомогою такого виразу:

$$\alpha_3 = \frac{o_i}{\sum_{i=1}^{m} o_i}, \tag{5}$$

де m – кількість рівнів виду доступу до інформації;

o_i – i-й рівень виду доступу до інформації.

Перевірку працездатності математичної моделі розрахунку цінності інформації проведено на прикладі.

Групою експертів для установи розроблено показники інформації та відповідно до виразів (2)–(5) проведено їх розрахунок, результати якого наведено в табл. 2–3.

Таблиця 2

Показник "Рівень важливості інформації"

Інформація за рівнем важливості	im_j	α_2
Життєво необхідна	5	0,333
Дуже важлива	4	0,267
Важлива	3	0,200
Корисна	2	0,133
Несуттєва	1	0,067

Таблиця 3

Показник "Рівень виду права власності на інформацію"

Інформація за видом права власності на інформацію	o_j	α_3
Державна	4	0,4
Колективна (установа)	3	0,3
Колективна (відділ установи)	2	0,2
Персональна	1	0,1

В установі складено групою її експертів перелік тієї інформації, яка потребує захисту. Отримані дані наведено в табл. 4.

Таблиця 4

Список інформації

Назва інформації	Рівень обмеження доступу	Остаточний час старіння (діб)	Рівень важливості	Рівень виду права власності
Індивідуальний план роботи начальника установи на 2022 рік	Відкрита	1	Несуттєва	Персональна
План роботи відділу 1 установи на 2022 рік	Конфіденційна	1086	Корисна	Колективна (відділ установи)
План роботи відділу 2 установи на 2022 рік	Конфіденційна	1086	Важлива	Колективна (відділ установи)
План роботи установи на 2022 рік	Для службового користування	1810	Важлива	Колективна (установа)
План розвитку міністерства на 2022 рік	Цілком таємно	3620	Дуже важлива	Державна
План розвитку держави на 2020–2025 роки	Особливої важливості	10860	Життєво необхідна	Державна
Звіт за результатами діяльності держави за 2021 рік	Таємно	1810	Важлива	Державна
Звіт за результатами діяльності міністерства за 2021 рік	Для службового користування	1810	Важлива	Державна
Звіт за результатами діяльності установи за 2021 рік	Конфіденційна	1086	Корисна	Колективна (установа)
Звіт за результатами діяльності відділу 1 установи за 2021 рік	Конфіденційна	1086	Корисна	Колективна (відділ установи)
Звіт за результатами діяльності відділу 2 установи за 2021 рік	Конфіденційна	1086	Важлива	Колективна (відділ установи)
Звіт за результатами діяльності начальника установи за 2021 рік	Відкрита	1	Несуттєва	Персональна

Використовуючи запропоновану математичну модель розрахунку цінності інформації, отримано кількісні значення цінності інформації та коефіцієнтів, які характеризують вплив показників інформації на її цінність. Результати розрахунків наведено в табл. 5.

Таблиця 5

Результати розрахунків

Назва інформації	α_1	α_2	α_3	*VOI*
Індивідуальний план роботи начальника установи на 2022 рік	0,024	0,067	0,1	0,064
План роботи відділу 1 установи на 2022 рік	0,076	0,133	0,2	0,136
План роботи відділу 2 установи на 2022 рік	0,076	0,2	0,2	0,159
План роботи установи на 2022 рік	0,119	0,2	0,3	0,206
План розвитку міністерства на 2022 рік	0,214	0,267	0,4	0,294
План розвитку держави на 2020–2025 роки	0,426	0,333	0,4	0,386
Звіт за результатами діяльності держави за 2021 рік	0,142	0,2	0,4	0,247
Звіт за результатами діяльності міністерства за 2021 рік	0,119	0,2	0,4	0,240
Звіт за результатами діяльності установи за 2021 рік	0,076	0,133	0,3	0,170
Звіт за результатами діяльності відділу 1 установи за 2021 рік	0,076	0,133	0,2	0,136
Звіт за результатами діяльності відділу 2 установи за 2021 рік	0,076	0,2	0,3	0,192
Звіт за результатами діяльності начальника установи за 2021 рік	0,024	0,067	0,1	0,064

Відповідно до отриманих результатів з’ясовано, що цінність інформації зростає залежно від:

рівня обмеження доступу до інформації: чим вищим є рівень обмеження доступу, тим цінніша інформація для установи;

рівня важливості інформації: чим вищим є рівень важливості інформації, тим більшою є цінність інформації;

рівня виду права на інформацію: чим більшою є кількість суб'єктів, які мають право на володіння інформацією, тим ціннішою є інформація.

Усі рівні обмеження доступу до інформації, її важливості та виду права на неї визначаються групою експертів.

Висновки. Проведена перевірка адекватності математичної моделі розрахунку цінності інформації установи дозволяє зробити висновки про те, що інформація, яка має найвищий рівень обмеження доступу, найвищий рівень важливості та права на яку належать державі, є найбільш цінною в установі.

Розроблена математична модель розрахунку цінності інформації установи доповнює модель загроз інформації в установі. Саме врахування цінності інформації дозволить вжити додаткових заходів для вдосконалення комплексної системи захисту інформації в автоматизованих системах установи.

Математична модель розрахунку цінності інформації установи може застосовуватися як на етапі проєктування комплексної системи захисту інформації в автоматизованих системах установи, так і під час експлуатації з метою зниження рівня потенційних загроз.

Подальші наукові дослідження будуть спрямовані на розроблення методичних рекомендацій щодо застосування математичної моделі розрахунку цінності інформації установи для розробки моделі загроз.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22. URL: http://dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden-1&art_id-102106&cat_id=46556&ctime=1344502446343 (дата звернення: 10.02.2022).
2. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-002-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22. URL: http://dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340 (дата звернення: 10.02.2022).
3. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. НД ТЗІ 2.5-008-2002 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.12.2002 № 84. URL: https://www.dsszzi.gov.ua/dsszzi/doccatalog/document/id=106343 (дата звернення: 10.02.2022).
4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/articleshowHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407 (дата звернення: 10.02.2022).
5. Критерії захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22. URL: https://www.dsszzi.gov.ua/dsszzi/doccatalog/document/id=106342 (дата звернення: 10.02.2022).
6. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 08.11.2005 № 125. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 07.02.2022).
7. Типове положення про службу захисту інформації в автоматизованій системі. НД ТЗІ 1.4-001-2000 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04.12.2000 № 53. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення: 08.02.2022).
8. Мороз Б., Молотков О., Ульяновська Ю. Методи визначення цінності інформації для організації її захисту // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. Вип. 2. С. 46–53.

9. Заяць В. М., Рибицька О. М., Заяць М. М. Підхід до оцінювання цінності та кількості інформації в системах масового обслуговування на основі теорії розпізнавання образів та нечітких множин // Кібернетика і системний аналіз. 2019. № 4 (55). С. 133–144. https://doi.org/10.1007/s10559-019-00172-1
10. Заяць В. М., Заяць М. М. Образний підхід до кількісної оцінки цінності інформації // Доповіді Національної академії наук України. 2018. № 6. С. 32–39. https://doi.org/10.15407/dopovidi2018.06.032
11. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки : підручник. Київ : Вид-во НА СБ України, 2020. 256 с.

Стаття надійшла до редакції 21.02.2022.

REFERENCES

1. Terminolohiia v haluzi zakhystu informatsii v komp'iuternykh systemakh vid nesanktsionovanoho dostupu. ND TZI 1.1-003-99 : nakaz Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy vid 28.04.1999 № 22 [Terminology in the field of information protection in computer systems against unauthorized access. ND TZI 1.1-003-99: order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine dated April 28, 1999 No. 22]. Retrieved from http://dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden-1&art_id-102106&cat_id=46556&ctime=1344502446343 [in Ukrainian].
2. Zahalni polozhennia shchodo zakhystu informatsii v komp'iuternykh systemakh vid nesanktsionovanoho dostupu. ND TZI 1.1-002-99 : nakaz Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy vid 28.04.1999 № 22 [General provisions on the protection of information in computer systems against unauthorized access. ND TZI 1.1-002-99: order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine dated April 28, 1999 No. 22]. Retrieved from http://dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340 [in Ukrainian].
3. Vymohy iz zakhystu sluzhbovoi informatsii vid nesanktsionovanoho dostupu pid chas obroblennia v avtomatyzovanykh systemakh klasu 2. ND TZI 2.5-008-2002 : nakaz Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy vid 13.12.2002 № 84 [Requirements for the protection of official information from unauthorized access during processing in automated class 2 systems. ND TZI 2.5-008-2002: order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine dated December 13, 2002 No. 84]. Retrieved from https://www.dsszzi.gov.ua/dsszzi/doccatalog/document/id=106343 [in Ukrainian].
4. Klasyfikatsiia avtomatyzovanykh system i standartni funktsionalni profili zakhyshchenosti obrobliuvanoi informatsii vid nesanktsionovanoho dostupu. ND TZI 2.5-005-99 : nakaz Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy vid 28.04.1999 № 22 [Classification of automated systems and standard functional profiles of protection of processed information from unauthorized access. ND TZI

2.5-005-99: order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine dated April 28, 1999 No. 22]. Retrieved from http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/articleshowHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407 [in Ukrainian].

5. Kryterii zakhyshchenosti informatsii v komp'iuternykh systemakh vid nesanktsionovanoho dostupu. ND TZI 2.5-004-99 : nakaz Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy vid 28.04.1999 № 22 [Information security criteria in computer systems against unauthorized access. ND TZI 2.5-004-99: order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine dated April 28, 1999 No. 22]. Retrieved from https://www.dsszzi.gov.ua/dsszzi/doccatalog/document/id=106342 [in Ukrainian].

6. Poriadok provedennia robit iz stvorennia kompleksnoi systemy zakhystu informatsii v informatsiino-telekomunikatsiinii systemi. ND TZI 3.7-003-05 : nakaz Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy vid 08.11.2005 № 125 [The procedure for the creation of a comprehensive information protection system in the information and telecommunications system. ND TZI 3.7-003-05: order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine dated November 8, 2005 No. 125]. Retrieved from https://tzi.com.ua/downloads/3.7-003-2005.pdf [in Ukrainian].

7. Typove polozhennia pro sluzhbu zakhystu informatsii v avtomatyzovanii systemi. ND TZI 1.4-001-2000 : nakaz Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy vid 04.12.2000 № 53 [A typical provision on the information protection service in an automated system. ND TZI 1.4-001-2000: order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine dated December 4, 2000 No. 53]. Retrieved from https://tzi.com.ua/downloads/1.4-001-2000.pdf [in Ukrainian].

8. Moroz, B., Molotkov, O., & Ulianovska, Yu. (2001). Metody vyznachennia tsinnosti informatsii dlia orhanizatsii yii zakhystu [An approach to evaluating the value and amount of information in mass service systems based on the theory of pattern recognition and fuzzy sets]. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini [Cybernetics and system analysis]*, *2*, 46–53 [in Ukrainian].

9. Zaiats, V. M., Rybytska, O. M., & Zaiats, M. M. (2019). Pidkhid do otsiniuvannia tsinnosti ta kilkosti informatsii v systemakh masovoho obsluhovuvannia na osnovi teorii rozpiznavannia obraziv ta nechitkykh mnozhyn [An approach to evaluating the value and amount of information in mass service systems based on the theory of pattern recognition and fuzzy sets]. *Kibernetyka i systemnyi analiz [Cybernetics and system analysis]*, *4* (55), 133–144. https://doi.org/10.1007/s10559-019-00172-1 [in Ukrainian].

10. Zaiats, V. M., & Zaiats, M. M. (2018). Obraznyi pidkhid do kilkisnoi otsinky tsinnosti informatsii [Figurative approach to quantitative assessment of the value of information]. *Dopovidi Natsionalnoi akademii nauk Ukrainy [Reports of the National Academy of Sciences of Ukraine]*, *6*, 32–39. https://doi.org/10.15407/dopovidi2018.06.032 [in Ukrainian].

11. Hulak, H. M. (2020). *Metodolohiia zakhystu informatsii. Aspekty kiberbezpeky [Information protection methodology. Aspects of cyber security]*. Kyiv [in Ukrainian].

O. S. Bojchenko, D. S. Kosterev, I. Yu. Makovskyi, O. M. Hryshchuk

MATHEMATICAL MODEL OF CALCULATION THE VALUE OF INFORMATION OF THE INSTITUTION

The article is devoted to solving a relevant scientific and practical problem - the development of a mathematical model for calculating the value of information of the institution. The following concepts are interpreted: the value of information, the level of importance of information, the time of final aging of information and the level of ownership of information used in research on the object of information protection. The indicators by which it is proposed to determine the value of information are considered in detail and its dependence on such indicators is shown. It is proposed to calculate the value of information as the average value of the sum of the relevant coefficients. Each of the selected coefficients is calculated using the ranking method. The importance of the relevant information indicator is determined in accordance with the requirements of the guidance documents on the organization of information security or a specially created group of experts. It is proposed to use the following coefficients: the coefficient of influence of the level of access to information, the coefficient of influence of the time of final aging of information, the coefficient of influence of information importance and the coefficient of influence of the right to information. The adequacy of the mathematical model for calculating the value of information of the institution was checked. It is established that the information that has the highest level of restriction of access, the highest level of importance and the right to information belongs to the state, has the greatest value for the institution. An example is given in which a list of information that needs protection in the institution is compiled and the value of information from this list is calculated. The mathematical model of calculating the value of the institution's information allows you to justify the need to take additional measures to improve the comprehensive system of information protection in the institution's automated systems and to better approach the issue of forming a model of information threats in information and telecommunication systems.

Keywords: *value of information; ownership of information; time of final aging of information; level of importance of information.*