ISSN 2076-1546

УДК 004.056 DOI: 10.46972/2076-1546.2019.16.12

О. С. Бойченко, І. В. Гуменюк, Р. І. Гладич

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ РИЗИКУ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ КОРИСТУВАЧАМИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Стаття присвячена вирішенню актуального науково-практичного завдання – розробці математичної моделі оцінки ризику несанкціонованого доступу до інформації користувачами інформаційно-телекомунікаційної системи. Наведено тлумачення таких понять: несанкціонований доступ до інформації, ризик та оцінка ризику, – які застосовують у ході досліджень внутрішніх загроз. Визначено ознаки користувача інформаційно-телекомунікаційної системи, які впливають на величину ймовірності несанкціонованого доступу до інформації. Показано, що врахування теоретичних та практичних знань користувача інформаційно-телекомунікаційної системи характеристик фізичного середовища, обчислювальної системи, оброблюваної інформації, які він може використовувати для свідомого порушення правил розмежування доступу з метою отримання несанкціонованого доступу до інформації, дозволить більш точно оцінити даний ризик.

Проведено перевірку адекватності розробленої математичної моделі оцінки ризику несанкціонованого доступу до інформації користувачами інформаційно-телекомунікаційної системи за допомогою спеціального програмного забезпечення. Встановлено, що користувачі, які мають найбільший стаж і досвід роботи з інформаційно-телекомунікаційними системами (не тільки в установі, що розглядається), найвищий рівень допуску до інформації з обмеженим доступом, займають відповідальні посади та є недисциплінованими, становлять найбільш імовірну внутрішню загрозу щодо несанкціонованого доступу до інформації. Саме використання математичної моделі оцінки ризику несанкціонованого доступу до інформації користувачами інформаційно-телекомунікаційної системи дозволить удосконалити комплексну систему захисту інформації відповідної інформаційно-телекомунікаційної системи.

Ключові слова: *внутрішні загрози; модель порушника; несанкціонований доступ; потенційні збитки; ризик.*

Постановка проблеми в загальному вигляді. Стрімкий розвиток інформаційних технологій спричинив появу інформаційно-телекомунікаційних систем (ІТС), за допомогою яких автоматизовано процеси накопичення, модифікації, обміну, зберігання інформації. Такий рівень автоматизації роботи зумовлює ризики несанкціонованого доступу (НДС) до неї. Під НДС до інформації в контексті даного дослідження слід розуміти отримання доступу до неї особою, яка має право на це, але в обсязі, що перевищує необхідний для виконання службових обов'язків.

Відповідно до [1] захист інформації від НСД в ІТС полягає в забезпеченні додержання правил розмежовування доступу шляхом створення і підтримки в дієздатному стані системи заходів із захисту інформації.

У сучасних комплексних системах захисту інформації (КСЗІ) модель порушника не враховує в необхідному обсязі можливостей внутрішньої загрози. Тому в ході розробки моделі порушника під час створення КСЗІ постає важливе науково-практичне завдання щодо оцінювання ризику НСД до інформації користувачами ІТС з метою зменшення потенційних збитків від реалізації внутрішніх загроз.

Виникнення цього важливого науково-практичного завдання обумовлено наявною об'єктивною суперечністю між вимогами до зменшення потенційних збитків від внутрішніх загроз та принциповою неможливістю їх врахування через реальну модель порушника, що й визначає своєчасність та актуальність досліджень.

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

Так, у НД ТЗІ [3] наведено категорії користувачів за рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконують у процесі функціонування ІТС. Даний розподіл доцільно враховувати в ході розробки моделі порушника в частині, що стосується внутрішніх загроз.

У відкритих джерелах питанню оцінки ризику НСД до інформації користувачами ІТС не приділено належної уваги, а саме не було запропоновано математичні моделі, які б описували у формалізованому вигляді ймовірність виникнення внутрішніх загроз.

Формулювання завдання дослідження. Метою статті є розробка математичної моделі оцінки ризику НСД до інформації користувачами ІТС з урахуванням таких критеріїв, як: рівень освіти, стаж роботи загальний та в установі (організації), наявність допуску до державної таємниці, посада та кількість дисциплінарних стягнень за поточний рік.

Виклад основного матеріалу. Розмежування доступу користувачів до інформації здійснюється адміністратором безпеки та/або уповноваженим на це співробітником установи (організації) на основі розробленої політики безпеки. При цьому не враховується той факт, що від самого адміністратора безпеки може надходити загроза. Для запобігання цьому пропонуємо математичну модель, яка дозволяє оцінювати ризик НСД до інформації шляхом розрахунку ймовірності реалізації певної загрози від користувача ІТС з належними йому ознаками.

Під ризиком у даному науковому дослідженні слід розуміти кількісну міру безпеки, яка дорівнює добутку ймовірності НСД до інформації користувачем ІТС на ймовірність потенційних збитків унаслідок цього [6, 7]:

$$r = \sum_{i=1}^{N} p_i \cdot w_i, \qquad (1)$$

де N – кількість ознак користувача;

p_i – імовірність НСД до інформації користувачем ІТС за його i -ю ознакою;

w_i – імовірність потенційних збитків унаслідок НСД до інформації відповідним користувачем ІТС з i-ю ознакою.

Відповідно до методології оцінювання ризиків OWASP [8] для визначення втрат використовують якісну шкалу (малий/посередній/великий). Тоді ймовірність потенційних збитків унаслідок НСД до інформації відповідним користувачем ІТС з i-ю ознакою можна описати шляхом ранжування шкали від 0 до 1, отримавши значення, наведені в табл. 1.

Таблиця 1

Імовірність потенційних збитків

Величина потенційних збитків	Імовірність
Мала	$w_1 = 0,33$
Посередня	$w_2 = 0,66$
Велика	$w_3 = 0,99$

Результати аналізу сучасних підходів до формалізованого опису внутрішнього порушника (інсайдера) свідчать про те, що в моделі поведінки внутрішнього порушника не враховані його ознаки, які характеризують мотиви поведінки під час певного виду порушень політики безпеки. При цьому не розглядаються також його теоретичні та практичні знання характеристик фізичного середовища, обчислювальної системи, оброблюваної інформації, які він може використовувати для свідомого порушення правил розмежування доступу з метою отримання НСД до інформації в ІТС [9−11]. Тому в даному дослідженні характеризувати користувача ІТС пропонуємо за певними ознаками. Розглянемо їх детальніше.

1. Рівень освіти. За цією ознакою пропонуємо оцінювати теоретичні знання користувача щодо можливості отримання ним НСД до інформації. Запропоновані рівні освіти користувача ІТС та відповідні їм числові значення, які характеризують імовірність НСД до інформації, наведено в табл. 2.

Таблиця 2

Ознака “Рівень освіти”

Освіта	Значення
Середня	$Ed_1 = 0,1$
Середня спеціальна	$Ed_2 = 0,3$
Середня спеціальна (технічна)	$Ed_3 = 0,7$
Вища	$Ed_4 = 0,5$
Вища (технічна)	$Ed_5 = 0,9$

2. Стаж роботи. За цією ознакою пропонуємо оцінювати знання користувача з організації роботи в ІТС інших установ (організацій). При цьому слід враховувати його досвід роботи з ІТС. Запропоновані рівні трудового стажу та відповідні їм числові значення, які характеризують імовірність НСД до інформації, наведено в табл. 3.

Таблиця 3

Ознака “Стаж роботи”

Стаж	Значення
Відсутній	$Tw_1 = 0,1$
До 1 року (ІТС відсутня)	$Tw_2 = 0,2$
До 1 року (ІТС)	$Tw_3 = 0,5$
До 5 років (ІТС відсутня)	$Tw_4 = 0,3$
До 5 років (ІТС)	$Tw_5 = 0,7$
Більше 5 років (ІТС відсутня)	$Tw_6 = 0,4$
Більше 5 років (ІТС)	$Tw_7 = 0,9$

3. Стаж роботи в установі (організації). За цією ознакою пропонуємо оцінювати ризик НСД до інформації на основі знань користувача з організації роботи в ІТС установи (організації). При цьому потрібно враховувати його досвід праці з ІТС. Запропоновані рівні стажу роботи та відповідні їм числові значення, які характеризують імовірність НСД до інформації, наведено в табл. 4.

Таблиця 4

Ознака “Стаж роботи в установі (організації)”

Стаж	Значення
Відсутній	$Twg_1 = 0,1$
До 6 місяців (ІТС відсутня)	$Twg_2 = 0,2$
До 6 місяців (ІТС)	$Twg_3 = 0,7$
До 1 року (ІТС відсутня)	$Twg_4 = 0,4$
До 1 року (ІТС)	$Twg_5 = 0,8$
Більше 1 року (ІТС відсутня)	$Twg_6 = 0,5$
Більше 1 року (ІТС)	$Twg_7 = 0,9$

4. Допуск до державної таємниці. За цією ознакою пропонуємо оцінювати обізнаність користувача щодо можливості отримання ним НСД до інформації шляхом свідомого порушення організаційних заходів, спрямованих на забезпечення захисту інформації в ІТС. Запропоновані форми допуску до державної таємниці та відповідні їм числові значення, які характеризують імовірність НСД до інформації, наведено в табл. 5.

Таблиця 5

Ознака “Допуск до державної таємниці”

Форма допуску	Значення
Форма 1	$Ts_1 = 0,9$
Форма 2	$Ts_2 = 0,8$
Форма 3	$Ts_3 = 0,7$
Без допуску	$Ts_4 = 0,5$

5. Рівень допуску до інформації з обмеженим доступом установи (організації). За цією ознакою потрібно оцінювати обізнаність користувача щодо характеристик фізичного

середовища, обчислювальної системи, оброблюваної інформації, які він може використовувати для свідомого порушення правил розмежування доступу з метою отримання НСД до інформації в ІТС. Запропоновані рівні допуску до інформації з обмеженим доступом установи та відповідні їм числові значення наведено в табл. 6.

Таблиця 6

Ознака "Допуск до інформації з обмеженим доступом установи (організації)"

Гриф інформації	Значення
Відкрита	$Tsg_1 = 0,2$
Для службового користування	$Tsg_2 = 0,4$
Таємно	$Tsg_3 = 0,6$
Цілком таємно	$Tsg_4 = 0,8$
Особливої важливості	$Tsg_5 = 0,9$

6. Кількість дисциплінарних стягнень за останній рік. За цією ознакою оцінюють стан користувача щодо можливості отримання ним НСД до інформації з метою завдання навмисної шкоди установі (організації). Запропоновані кількість дисциплінарних стягнень за останній рік та відповідні їм числові значення наведено в табл. 7.

Таблиця 7

Ознака "Кількість дисциплінарних стягнень за останній рік"

Кількість	Значення
0	$Dis_1 = 0,1$
1	$Dis_2 = 0,4$
2	$Dis_3 = 0,7$
3 та більше	$Dis_4 = 0,9$

7. Посада користувача в установі (організації). За цією ознакою пропонуємо оцінювати можливості отримання НСД до інформації користувачем відповідно до його владних повноважень в установі (організації). Запропоновані типові посади та відповідні їм числові значення наведено в табл. 8.

Таблиця 8

Ознака "Посада користувача в установі (організації)"

Назва	Значення
Адміністратор безпеки ІТС	$Ra_1 = 0,9$
Адміністратор операційних систем, баз даних, мережевих додатків	$Ra_2 = 0,8$
Начальник структурного підрозділу	$Ra_3 = 0,7$
Технічний обслуговуючий персонал ІТС	$Ra_4 = 0,6$
Розробник програмних засобів для модифікації ІТС	$Ra_5 = 0,6$
Розробник апаратних засобів для модифікації ІТС	$Ra_6 = 0,5$
Технічний персонал (електрики, технічний персонал з обслуговування будівель, ліній зв'язку тощо)	$Ra_7 = 0,3$
Інший персонал установи (організації)	$Ra_8 = 0,1$

У роботі [11] доведено, що інтегровану оцінку можливих втрат за всіма варіантами вибору дає середній ризик. Враховуючи ці результати, середній ризик НСД до інформації користувачем ІТС розраховано за таким виразом:

$$R = \frac{\sum_{i=1}^{N} p_i \cdot w_i}{N}, \tag{2}$$

Для перевірки адекватності математичної моделі оцінки ризику НСД до інформації користувачами ІТС розроблено програмне забезпечення, екранну форму якого наведено на рис. 1.

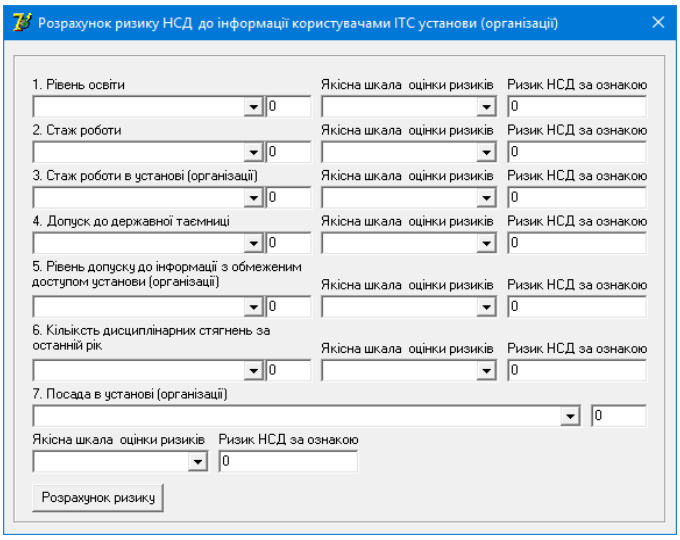

Рис. 1. Екранна форма програмного забезпечення

Перевірку працездатності математичної моделі проведено на прикладах.

Приклад 1. Оцінити ризик НСД до інформації користувачем ІТС, який має певні ознаки, та потенційні збитки:

1. Рівень освіти – “Середня”; величина потенційних збитків – “Мала”.

2. Стаж роботи – “Відсутній”; величина потенційних збитків – “Посередня”.

3. Стаж роботи в установі (організації) – “Відсутній”; величина потенційних збитків – “Посередня”.

4. Допуск до державної таємниці – “Без допуску”; величина потенційних збитків – “Посередня”.

5. Рівень допуску до інформації з обмеженим доступом установи (організації) – “Відкрита”; величина потенційних збитків – “Велика”.

6. Кількість дисциплінарних стягнень за останній рік – “0”; величина потенційних збитків – “Посередня”.

7. Посада в установі (організації) – “Технічний персонал з обслуговування ліній зв’язку”; величина потенційних збитків – “Велика”.

Відповідно до математичної моделі для користувача були обрані числові значення його ознак та розраховано ризик НСД до інформації (рис. 2).

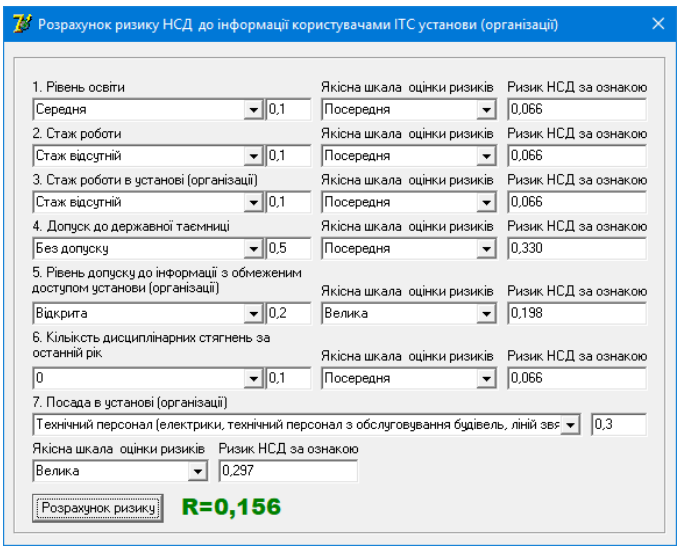

Рис. 2. Результати розрахунку для прикладу 1

Приклад 2. Оцінити ризик НСД до інформації користувачем ІТС, який має такі ознаки:

1. Рівень освіти – “Середня спеціальна технічна”; величина потенційних збитків – “Мала”.

2. Стаж роботи – “До 1 року в іншій установі, де був користувачем ІТС”; величина потенційних збитків – “Посередня”.

3. Стаж роботи в установі – “Відсутній”; величина потенційних збитків – “Посередня”.

4. Допуск до державної таємниці – “Форма 3”; величина потенційних збитків – “Посередня”.

5. Рівень допуску до інформації з обмеженим доступом установи (організації) – “Таємно”; величина потенційних збитків – “Велика”.

6. Кількість дисциплінарних стягнень за останній рік – “2”; величина потенційних збитків – “Посередня”.

7. Посада в установі (організації) – “Технічний обслуговуючий персонал ІТС”; величина потенційних збитків – “Велика”.

Відповідно до математичної моделі для користувача були обрані числові значення його ознак та розраховано ризик НСД до інформації (рис. 3).

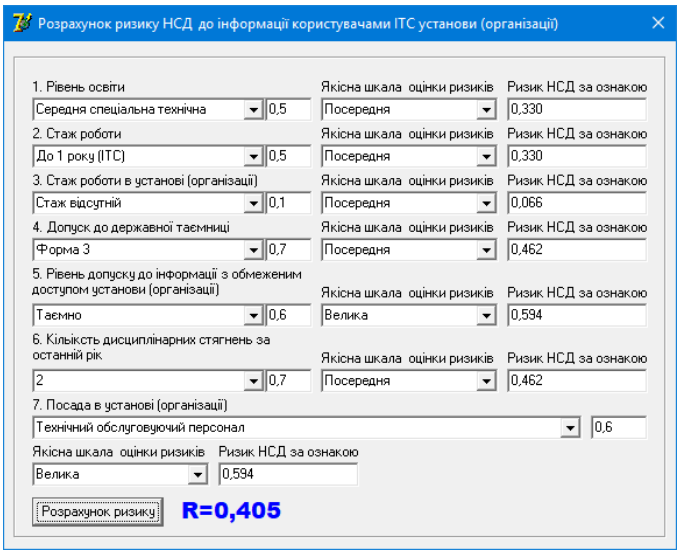

Рис. 3. Результати розрахунку для прикладу 2

Приклад 3. Оцінити ризик НСД до інформації користувачем ІТС, який має такі ознаки:

1. Рівень освіти – “Вища технічна”; величина потенційних збитків – “Посередня”.

2. Стаж роботи – “Більше 5 років в іншій установі, де був користувачем ІТС”; величина потенційних збитків – “Посередня”.

3. Стаж роботи в установі (організації) – “Більше 1 року, користувач ІТС”; величина потенційних збитків – “Посередня”.

4. Допуск до державної таємниці – “Форма 1”; величина потенційних збитків – “Посередня”.

5. Рівень допуску до інформації з обмеженим доступом установи (організації) – “Особливої важливості”; величина потенційних збитків – “Велика”.

6. Кількість дисциплінарних стягнень за останній рік – “3 та більше”; величина потенційних збитків – “Посередня”.

7. Посада в установі (організації) – “Адміністратор безпеки ІТС”; величина потенційних збитків – “Велика”.

Відповідно до математичної моделі для користувача були обрані числові значення його ознак та розраховано ризик НСД до інформації (рис. 4).

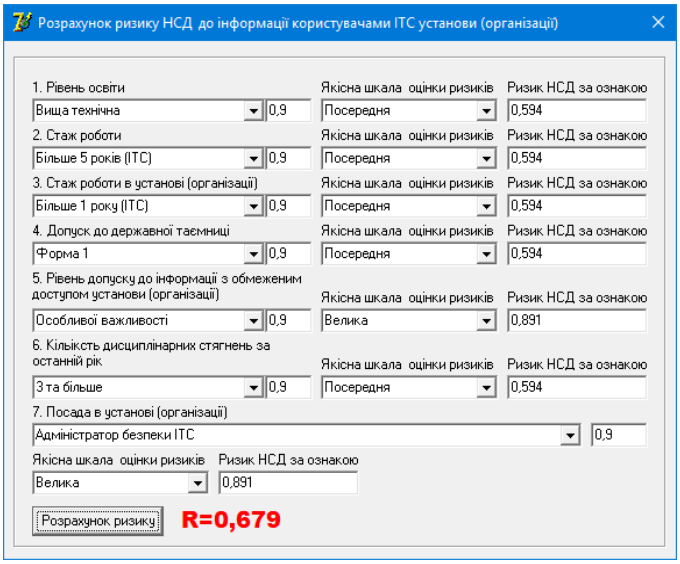

Рис. 4. Результати розрахунку для прикладу 4

Відповідно до отриманих результатів ризик НСД до інформації користувачами ІТС зростає залежно від:

рівня освіти: чим вищий рівень освіти, тим імовірніша загроза від цього користувача;

стажу роботи: чим більший стаж роботи, тим імовірніша загроза від цього користувача;

рівня допуску до державної таємниці та інформації з обмеженим доступом установи (підприємства): чим вище гриф секретності, тим імовірніша загроза;

кількості дисциплінарних стягнень за останній рік: чим їх більше, тим вища ймовірність загрози.

Імовірність виникнення загрози залежно від посади визначають за допомогою методу експертних оцінок.

Висновки. Проведена перевірка адекватності математичної моделі оцінки ризику НСД до інформації користувачами ІТС дозволяє зробити висновки про те, що ті, хто мають найбільший стаж роботи і досвід роботи з ІТС (не тільки в установі, що розглядається), мають найвищий рівень допуску до інформації з обмеженим доступом установи (організації), займають відповідальні посади та є недисциплінованими становлять найбільш імовірну внутрішню загрозу щодо НСД до інформації.

Розроблена математична модель оцінки ризику НСД до інформації користувачами ІТС доповнює модель порушника, зокрема внутрішнього. Саме врахування внутрішніх загроз дозволить вжити додаткові заходи щодо вдосконалення комплексної системи захисту інформації в ІТС.

Математична модель оцінки ризику НСД до інформації користувачами ІТС може застосовуватися як на етапі проєктування КСЗІ в ІТС, так і під час експлуатації з метою зниження рівня внутрішніх загроз.

Подальші наукові дослідження будуть спрямовані на розроблення методичних рекомендацій щодо зниження внутрішніх загроз в ІТС.

СПИСОК ЛІТЕРАТУРИ

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: 03.06.2019).
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: 03.06.2019).
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: 03.06.2019).
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/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407 (дата звернення: 03.06.2019).
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: 03.06.2019).

6. Rowe W. Ananatomy of risk. New York : Iohn Wiley, 1997. 488 p.
7. Качинський А. Безпека, загрози і ризик: наукові концепції та математичні методи. Київ : Поліграфконсалтінг, 2004, 472с.
8. Managing information security risk: organization, mission, and information system view / Joint task force transformation initiative. URL: http://csrc.nist.gov/publications/detail/sp/800-39/final (last accessed: 25.06.2019).
9. Панченко В. О. Механізм протидії інсайдерам у системі кадрової безпеки // Науковий вісник Львів. держ. ун-ту внутрішніх справ. 2018. № 1. С. 219–227.
10. Рак Ю. П., Сукач Р. Ю. Математична модель оцінки ризику в проектах захисту об'єктів потенційної небезпеки // Управління проектами та розвиток виробництва. 2015. № 2 (54). С. 12–17.
11. Романюков М. Г. Критерії оцінки ймовірності витоку інформації через технічні канали // Інформатика та математичні методи в моделюванні. 2015. Т. 5, № 3. С. 240–248.

Подано 26.06.2019

О. С. Бойченко, И. В. Гуменюк, Р. И. Гладич

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ РИСКА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЯМИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ

Статья посвящена решению актуальной научно-практической задачи – разработке математической модели оценки риска несанкционированного доступа к информации пользователями информационно-телекоммуникационной системы. Приведены толкования таких понятий: несанкционированный доступ к информации, риск и оценка риска, применяемые в ходе исследований внутренних угроз. Определены признаки пользователя информационно-телекоммуникационной системы, которые влияют на величину вероятности несанкционированного доступа к информации. Показано, что учет теоретических и практических знаний пользователя информационно-телекоммуникационной системы о характеристиках физической среды, вычислительной системы, обрабатываемой информации, которые он может использовать для сознательного нарушения правил разграничения доступа с целью получения несанкционированного доступа к информации, позволит более точно оценить данный риск.

Проведена проверка адекватности разработанной математической модели оценки риска несанкционированного доступа к информации пользователями информационно-телекоммуникационной системы с помощью специального программного обеспечения. Установлено, что пользователи, которые имеют самый большой стаж и опыт работы с информационно-телекоммуникационными системами (не только в рассматриваемом учреждении), самый высокий уровень допуска к информации с ограниченным доступом, занимают ответственные должности и являются недисциплинированными, составляют наиболее вероятную внутреннюю угрозу несанкционированного доступа к информации. Именно использование математической модели оценки риска несанкционированного доступа к информации пользователями информационно-телекоммуникационной системы позволит усовершенствовать

комплексную систему защиты информации соответствующей информационно-телекоммуникационной системы.

***Ключевые слова**: внутренние угрозы; модель нарушителя; несанкционированный доступ; потенциальные убытки; риск.*

O. S. Boychenko, I. V. Gumenyuk, R. I. Hladych

MATHEMATICAL MODEL OF ASSESSMENT OF RISK UNAUTHORIZED ACCESS TO INFORMATION BY USERS OF INFORMATION AND TELECOMMUNICATION SYSTEM

The article is devoted to the solution of the actual scientific and practical task – to develop a mathematical model for assessing the risk of unauthorized access to information by users of the information and telecommunication system. Interpretations of such concepts are given: unauthorized access to information, risk and risk assessment used in the course of internal threat research. The characteristics of the user of the information and telecommunication system that affect the value of the probability of unauthorized access to information are determined. It is shown that taking into account the theoretical and practical knowledge of the user of the information and telecommunication system about the characteristics of the physical environment, the computing system, the processed information, which he can use to deliberately violate the rules of demarcation in order to gain unauthorized access to information, will provide a more accurate assessment of this risk.

A verification of the adequacy of the developed mathematical model of risk assessment of unauthorized access to information by users of information and telecommunication system with the help of special software is carried out. It is established that the users who have the most experience and experience with information and telecommunication systems (not only in the institution under consideration), the highest level of access to information with restricted access of the institution (organization), occupy responsible positions and are undisciplined are the most likely internal threat of unauthorized access to information. It is the use of a mathematical model for assessing the risk of unauthorized access to information by users of the information and telecommunication system that will improve the comprehensive information protection system of the corresponding information and telecommunication system.

***Keywords**: internal threats; user violator model; unauthorized access; potential damage; risk.*