DOI: https://doi.org/10.17721/ISTS.2019.1.19-26
УДК 004.056

МЕТОД РОЗРАХУНКУ ЙМОВІРНОСТІ РЕАЛІЗАЦІЇ ЗАГРОЗ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ВІД ВНУТРІШНЬОГО ПОРУШНИКА

Бойченко Олег [1]
orcid.org/ 0000-0003-3048-4184

Зюбіна Руслана [2]
orcid.org/0000-0002-8654-6981

[1] м. Житомир, Житомирський військовий інституту імені С.П. Корольова, bos_2006@ukr.net
[2] м. Київ, Київський національний університет ім. Тараса Шевченка, ziubina@knu.ua

Історія статті:
Надійшла до редакції 21.07.2019
Прийнято 29.07.2019

Ключові слова:
внутрішній порушник;
інформаційна безпека;
модель загроз;
модель порушника.

Анотація: У статті проведено аналіз нормативно-правових документів, які регламентують питання захисту інформації в інформаційно-телекомунікаційній системі. За результатами проведеного аналізу сформовано мету наукового дослідження, яке полягає в удосконаленні методу розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника. Для досягнення поставленої мети були розроблені перелік загроз інформації з обмеженим доступом, які можуть надходити від внутрішнього порушника та модель внутрішнього порушника. Розроблено метод розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника, який має наступні етапи: визначення рівня знань внутрішнього порушника та оцінка можливості реалізації загрози; формування моделі внутрішнього порушника; формування моделі появи мотиву поведінки внутрішнім порушником; розрахунок імовірності реалізації загроз інформації з обмеженим доступом внутрішнім порушником. Проведено перевірку працездатності розробленого методу для наступних співробітників установи (організації): системний адміністратор, оператор автоматизованого робочого місця, інженер з телекомунікацій та співробітника, який не є користувачем інформаційно-телекомунікаційної системи та не належить до технічного персоналу. Результати перевірки дозволяють зробити висновок про те, що найбільш імовірна реалізація загроз інформації з обмеженим доступом від співробітників установи (організації) йде від тих співробітників, які є користувачами інформаційно-телекомунікаційної системи, мають високий рівень знань щодо можливості реалізації загроз та які мають мотив поведінки – помста. Розроблений метод розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника, крім загальноприйнятої класифікації рівнів можливостей, використовуваних методів і способів здійснення дій та місця здійснення дій, враховує мотив неправомірних дій з боку внутрішнього порушника та оцінку його знань щодо можливості реалізації загроз інформації з обмеженим доступом в інформаційно-телекомунікаційній системі.

Abstract: In the article analyzed regulatory documents which regulate the question of information security in the information and telecommunication system. According the results of the analysis the aim of scientific research, which consists in the improvement of method of calculation of probability of realization of threats of information with the limited access from an internal user violator was formed. To achieve this aim, a list of threats of information with limited access which could come from an internal user violator and the internal user violator model was developed. The method of calculation of probability of realization of threats of information with the limited access from an internal user violator was developed and has the followings stages: determination of level of knowledge's of internal user violator and assessment of the possibility of realizing the threat; forming of model of internal user violator; forming of model of the appearance of the motive of behavior by the internal user violator; calculation of probability of realization of threats of information with the limited access from an internal user violator. The work of the developed method has been tested for the following employees of the institution (organization): the system administrator, the operator of the automated workplace, the

telecommunications engineer and the employee who is not the user of the information and telecommunication system and does not belong to the technical personnel. The results of the verification allow conclude that the most probable realization of the threats of information with limited access from the employees of the institution (organization) comes from those employees who are users of the information and telecommunication system, have a high level of knowledge about the possibility of realizing threats and having a motive of behavior – revenge. The developed method of calculation of probability of realization of threats of information with the limited access from an internal user violator in addition to the generally accepted classification of levels of opportunities, methods used of action and place of action, takes into account the motive of wrongful acts by the internal user violator and assessment of his knowledge about the possibility of realizing the threats of information with limited access in the information and telecommunication system.

1. ВСТУП

Сьогодні на сучасному етапі розвитку інформаційних технологій, які надають змогу проводити автоматизацію процесів обробки інформації в інформаційно-телекомунікаційних системах (ІТС), особливо актуальним стає питання захисту інформації в ІТС.

Відповідно до "Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [1] для забезпечення захисту інформації в ІТС створюється комплексна система захисту інформації (КСЗІ). В цьому ж документі вказано, що організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізації системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

Вимоги та порядок створення КСЗІ визначаються наступними нормативними документами системи технічного захисту інформації:

1. "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [2], в якому визначено, що для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації.

2. "Типове положення про службу захисту інформації в автоматизованій системі" [3], в якому визначено, що служба захисту інформації здійснює свою роботу з реалізації основних організаційних та організаційно-технічних заходів з створення та забезпечення функціонування КСЗІ у відповідності з Планом захисту інформації в автоматизованій системі.

Наведені документи надають методичні вказівки щодо структури та змісту Плану захисту інформації в автоматизованій системі. Одним з розділів цього Плану є розділ, у якому визначаються загрози для інформації в ІТС. На даний час немає єдиного методологічного забезпечення щодо розробки моделі загроз для інформації та моделі порушника.

З метою удосконалення існуючого методологічного забезпечення процесу розробки моделі загроз для інформації та моделі порушника, які адекватно описують процес захисту інформації в ІТС за рахунок визначення ймовірності реалізації загроз інформації в ІТС, існує потреба у розробленні методу розрахунку ймовірності реалізації загроз інформації в ІТС. Виникнення цього важливого науково-практичного завдання обумовлено існуючим протиріччям між високими вимогами до захисту інформації в ІТС та принциповою неможливістю оцінки ймовірності реалізації загроз інформації в ІТС за рахунок застосування існуючих методів оцінки інформаційних ризиків, що й визначає актуальність та своєчасність досліджень.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дослідженню наукових проблем захисту інформації в ІТС присвячено багато наукових праць, основним спрямуванням яких є вирішення задачі оцінювання інформаційних ризиків в ІТС.

Авторами у наукових дослідженнях [4, 5] було запропоновано розглядати загальну структуру системи захисту інформації автоматизованої системи управління технологічними процесами об'єктів критичної інфраструктури з двох компонентів: технічного та соціокультурного; а також проведено аналіз загроз захисту інформації в даній системі.

У роботі [6] авторами було описано модель порушника безпеки інформації для захищеного вузла інтернет доступу.

Результатом наукового дослідження, наведеного у роботі [7], є модель ймовірних погроз і захисту інформації в мережах загального користування, що містить у собі модель ймовірного порушника, модель об'єкта захисту, засобу захисту, а також можливі пасивні та активні канали витоку інформації.

Автори у роботі [8] навели модель реалізації загроз інформаційній безпеці вищого навчального закладу, яка ґрунтується на результатах аналізу уразливості інформаційного ресурсу.

У ряді наукових досліджень, результати яких опубліковано у наукових працях [9-16], наведені методи та способи оцінювання ризиків інформаційної безпеки в ІТС, які ґрунтуються не лише на вітчизняних нормативно-правових документах з технічного захисту інформації, але й на міжнародних стандартах у сфери інформаційної безпеки.

Таким чином, у наукових дослідженнях, які спрямовані на розв'язання наукової задачі оцінювання інформаційних ризиків в ІТС, опис моделі порушника проводиться для внутрішніх та зовнішніх джерел загроз. Але результати останніх досліджень у сфері інформаційної безпеки [17-22] свідчать про те, що найбільшу загрозу інформаційної безпеки в ІТС становлять внутрішні джерела загроз.

Розробці моделі внутрішнього порушника, яким може бути співробітник установи (організації), у відкритих джерелах на даний час не приділено належної уваги.

Тому **метою наукової роботи** є удосконалення методу розрахунку ймовірності реалізації загроз інформації з обмеженим доступом (ІзОД) від внутрішнього порушника.

Для реалізації мети були визначені наступні завдання дослідження:

розробка переліку загроз ІзОД, які можуть надходити від внутрішніх порушників;

розробка моделі внутрішнього порушника;

розробка методу розрахунку ймовірності реалізації загроз ІзОД від внутрішнього порушника на основі його моделі та переліку загроз.

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Відповідно до "Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [2] під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Відповідно до "Типового положення про службу захисту інформації в автоматизованій системі" [3] основою для проведення аналізу ризиків є модель загроз для інформації та модель порушника.

У даному науково-практичному дослідженні модель загроз для ІзОД в ІТС представляє собою перелік загроз, які можуть надходити від внутрішніх порушників. Враховуючи вимоги [2] та рекомендації [3] запропоновано визначити наступні загрози ІзОД:

1. Несанкціоноване ознайомлення з ІзОД – одержання користувачем ІТС або процесом ІзОД, що міститься в об'єкті з порушенням правил розмежування доступу.

2. Неконтрольоване ознайомлення з ІзОД – одержання користувачем ІТС або процесом ІзОД, що міститься в об'єкті з порушенням прав доступу до об'єктів.

3. Випадкова модифікація ІзОД – зміна користувачем ІТС ІзОД, що міститься в об'єкті, внаслідок його недбалості, некомпетентності, неуважності та яка не має на меті нанесення збитків ІТС.

4. Навмисна модифікація ІзОД – цілеспрямована зміна користувачем ІТС ІзОД, що міститься в об'єкті, з метою нанесення збитків ІТС.

5. Випадкове знищення ІзОД – недбала, некомпетентна або неуважна дія користувача ІТС, внаслідок якої ІзОД в ІТС зникає та яка не має на меті нанесення збитків ІТС.

6. Навмисне знищення ІзОД – цілеспрямована дія користувача ІТС з метою нанесення збитків ІТС, внаслідок якої ІзОД в ІТС зникає.

7. Несанкціоноване копіювання ІзОД – копіювання ІзОД з порушенням правил розмежування доступу, внаслідок якого відбувся витік ІзОД.

8. Випадкове поширення ІзОД – розповсюдження, обнародування ІзОД користувачем ІТС шляхом порушення політики безпеки інформації в ІТС внаслідок його недбалості, некомпетентності, неуважності та яке не має на меті нанесення збитків ІТС.

9. Навмисне поширення ІзОД – цілеспрямоване розповсюдження, обнародування ІзОД користувачем ІТС шляхом свідомого порушення політики безпеки інформації в ІТС з метою нанесення збитків ІТС.

Другою складовою для проведення аналізу ризиків є модель порушника, яка повинна бути адекватна реальному порушнику для даної ІТС.

Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та

теоретичні можливості, апріорні знання, час та місце дії і т.ін [2].

У межах даного наукового дослідження будуть розглядатися лише внутрішні порушники, які є співробітниками установи (організації).

1. Користувачі ІТС:

1.1 Адміністратор безпеки.

1.2 Адміністратор обчислювальної мережі.

1.3 Системний адміністратор.

1.4 Адміністратори баз даних.

1.5 Оператори АРМ.

1.6 Керівники структурних підрозділів.

1.7 Інші співробітники установи (організації).

2. Співробітники установи (організації):

2.1 Технічні співробітники, які забезпечують експлуатацію ІТС (технік-монтажник, інженер з телекомунікацій, електрик та інші).

2.2 Технічні співробітники (прибиральниці, сантехніки та інші).

2.3 Інші співробітники установи (кухар, медична сестра та інші).

Метою внутрішнього порушника є реалізація однієї або більшої кількості загроз ІзОД. Саме розрахунок імовірності реалізації загроз ІзОД від внутрішнього порушника є метою пропонованого методу, який має наступні етапи:

1. *Визначення рівня знань внутрішнього порушника та оцінка можливості реалізації загрози* проводиться за допомогою анкетування та подальшого аналізу отриманих результатів. Тематика для проведення анкетування визначається керівником установи (організації). Результатом проведення анкетування є відносна оцінка знань внутрішнього порушника щодо можливості реалізації загроз K, яку можна розрахувати за формулою:

$$K = \frac{\sum_{i=1}^{N} k_i}{N}, \qquad (1)$$

де N – кількість анкет;

$k_i = \frac{N_r}{N_\Sigma}$ – відносна оцінка знань внутрішнього користувача за i-ю анкетою;

N_r – кількість вірних відповідей в анкеті;

N_Σ – загальна кількість питань в анкеті.

2. Формування моделі внутрішнього порушника.

Внутрішній порушник має наступні рівні можливостей, які надаються їм засобами ІТС:

1. Запуск фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки ІзОД – читання (перегляд).

2. Створення і запуск власних програм з новими функціями обробки ІзОД (проектів документів) – модифікація, видалення та копіювання.

3. Створення і запуск власних програм з новими функціями обробки ІзОД (діючі документи) – модифікація, видалення та копіювання.

4. Управління функціонуванням ІТС – надання прав доступу.

5. Управління конфігурацією ІТС та політикою безпеки.

Слід зауважити, що й для співробітників установи (організації), які не є користувачами ІТС, наведені рівні можливостей також застосовуються. Це пояснюється тим припущенням, що внутрішній порушник може маскуватися під зареєстрованого користувача ІТС.

Внутрішній порушник може здійснити свої дії щодо реалізації загроз ІзОД у наступних місцях:

1. У межах контрольованої зони.

2. У межах режимного приміщення без доступу до технічних та програмних засобів ІТС.

3. У межах режимного приміщення з доступом до технічних та програмних засобів ІТС.

Внутрішні порушники можуть використовувати наступні методи і способи здійснення дій щодо реалізації загрози ІзОД:

1. Використання агентурних методів (підкуп, шантаж та інші).

2. Використання пасивних технічних засобів перехоплення інформаційних сигналів.

3. Використання штатних апаратних або програмних засобів ІТС.

4. Використання додаткових апаратних або програмних засобів ІТС.

5. Маскування під зареєстрованого користувача ІТС.

6. Використання сторонніх програмних засобів щодо управління безпекою ІТС.

Модель внутрішнього порушника наведено в таблиці 1.

В таблиці 1 наведено окремі ознаки внутрішнього порушника, які характеризують його місце, методи і способи здійснення дій, а також рівень можливостей, що надаються йому ІТС.

Імовірність реалізації загроз внутрішнім порушником за ознаками, наведеними у моделі порушника, представлена у вигляді відношення суми кількості ознак, якими характеризується внутрішній порушник до загальної кількості цих ознак:

Таблиця 1. Модель внутрішнього порушника

№	Внутрішні порушники	Рівень можливостей					Місце дії			Методи і способи дій						Σ	Імовірність реалізації загроз
		r1	r2	r3	r4	r5	a1	a2	a3	s1	s2	s3	s4	s5	s6		
1	**Користувачі ІТС**																
1.1	Адміністратор безпеки	1	1	1	1	1	1	1	1	0	0	1	1	1	1	12	0,857
1.2	Адміністратор обчислювальної мережі	1	1	1	1	1	1	0	1	0	0	1	1	1	1	11	0,786
1.3	Системний адміністратор	1	1	1	1	0	1	0	1	0	0	1	1	1	1	10	0,714
1.4	Адміністратори баз даних	1	1	1	1	0	1	0	1	0	0	1	1	1	1	10	0,714
1.5	Оператори АРМ	1	1	1	0	0	1	0	1	1	0	1	0	1	0	8	0,571
1.6	Керівники структурних підрозділів	1	1	1	0	0	1	0	1	1	0	1	0	1	0	8	0,571
1.7	Інші співробітники установи (організації)	1	0	0	0	0	1	1	1	1	1	1	0	0	0	7	0,5
2	**Співробітники установи (організації)**																
2.1	Технічні співробітники, які забезпечують експлуатацію ІТС (технік-монтажник, інженер з телекомунікацій, електрик та інші)	0	0	0	0	0	1	1	1	1	1	1	0	0	0	6	0,429
2.2	Технічні співробітники (прибиральниці, сантехніки та інші)	0	0	0	0	0	1	1	0	1	1	0	0	0	0	4	0,286
2.3	Інші співробітники установи (кухар, медична сестра та інші)	0	0	0	0	0	1	0	0	1	1	0	0	0	0	3	0,214

$$R = \frac{\sum_{i=1}^{M} r_i + \sum_{i=1}^{N} a_i + \sum_{i=1}^{L} s_i}{M + N + L}, \qquad (2)$$

де M, N, L – кількість ознак внутрішнього порушника за рівнями можливостей, що надає ІТС, місцем здійснення дії та методом (способом) здійснення дії відповідно;

r_i – ймовірність отримання внутрішнім порушником i-го рівня можливостей. Якщо рівень можливостей отримано – $r_i = 1$, в іншому випадку $r_i = 0$;

a_i – ймовірність здійснення дій внутрішнім порушником з i-го місця. Якщо дія здійснена з i-го місця – $a_i = 1$, в іншому випадку $a_i = 0$;

s_i – ймовірність здійснення дій внутрішнім порушником i-м методом (способом). Якщо дія здійснюється – $s_i = 1$, в іншому випадку – $s_i = 0$.

3. Формування моделі появи мотиву поведінки внутрішнім порушником.

Результати аналізу сучасних підходів щодо формалізованого опису внутрішнього порушника свідчать про те, що у моделі поведінки внутрішнього порушника не враховуються його ознаки, які характеризують мотиви його поведінки при здійсненні певного виду порушень політики безпеки [17-22]. Для врахування можливих мотивів дії внутрішнього порушника проведено розробку ознак за наступними групами:

1. Кар'єрне зростання.

1.1 На посаді в установі (організації) більше двох років.

1.2 Призначений на нижчу посаду в установі (організації).

2. Рівень виплат.

2.1 Підвищений (премії, підняття зарплатні).

2.2 Згідно норм.

2.3 Зменшений (штрафні санкції).

3. Кількість дисциплінарних стягнень.

3.1 Менше 2.

3.2 Від 2 до 4.

3.3 Більше 4.

За результатами аналізу мотивів дії внутрішнього порушника розроблено наступні мотиви поведінки:

1. Помста.

2. Отримання матеріальної вигоди (збагачення).

3. Самореалізація.

Модель появи мотиву поведінки внутрішнього порушника представлено у вигляді таблиці 2.

Імовірність появи мотиву неправомірної поведінки внутрішнім порушником представлена у вигляді відношення суми кількості ознак, яким він найбільш відповідає, до загальної кількості цих ознак:

$$M = \frac{\sum_{i=1}^{C} z_i + \sum_{i=1}^{J} q_i + \sum_{i=1}^{Y} d_i}{C + J + Y}, \quad (3)$$

де C, J, Y – кількість ознак внутрішнього порушника за кар'єрним зростанням, рівнем виплат та кількістю дисциплінарних стягнень відповідно;

z_i – показники кар'єрного зростання;

q_i – показники рівня виплат;

d_i – показники кількості дисциплінарних стягнень.

Таблиця 2. Модель появи мотиву

№	Мотиви поведінки	Кар'єрний зріст		Виплати			Дисципліна			Σ	Імовірність появи мотиву
		z1	z2	q1	q2	q3	d1	d2	d3		
1	Помста	1	1	0	1	1	0	1	1	6	0,75
2	Збагачення	1	0	0	1	1	1	0	0	4	0,5
3	Самореалізація	1	0	0	0	1	1	0	0	3	0,375

4. Розрахунок імовірності реалізації загроз ІзОД внутрішнім порушником.

Для оцінки можливості реалізації загроз ІзОД в ІТС з боку внутрішніх порушників враховано появу трьох подій:

А – реалізація як мінімум однієї з загроз ІзОД відповідно до знань (кваліфікації);

В – реалізація як мінімум однієї з загроз ІзОД відповідно до характеру здійснення дій;

С – поява мотиву поведінки.

Тоді ймовірність реалізації загроз ІзОД внутрішнім порушником згідно з теоремою додавання подій представлено у наступному вигляді:

$$P(A+B+C) = R + M + K - R \cdot M - \\ -R \cdot K - M \cdot K + R \cdot M \cdot K. \quad (4)$$

Перевірку працездатності розробленого методу проведено на прикладах.

Приклад 1. Розрахувати ймовірність реалізації загроз ІзОД від системного адміністратора.

1. Відносна оцінка знань щодо можливості реалізації загроз $K = 0,9$.

2. З таблиці 1 визначено, що $R = 0,714$.

3. Мотиви поведінки обрано з таблиці 2.

Підставляючи отримані дані до формули 4 отримані ймовірності реалізації хоча б однієї загрози ІзОД від системного адміністратора ІТС для різних мотивів поведінки, значення яких наведено в таблиці 3.

Приклад 2. Розрахувати ймовірність реалізації загроз ІзОД від оператора АРМ.

1. Відносна оцінка знань щодо можливості реалізації загроз $K = 0,6$.

2. З таблиці 1 визначено, що $R = 0,571$.

3. Мотиви поведінки обрано з таблиці 2.

Підставляючи отримані дані до формули 4 отримані ймовірності реалізації хоча б однієї загрози ІзОД від оператора АРМ для різних мотивів поведінки, значення яких наведено в таблиці 3.

Приклад 3. Розрахувати ймовірність реалізації загроз ІзОД від інженера з телекомунікацій.

1. Відносна оцінка знань щодо можливості реалізації загроз $K = 0,6$.

2. З таблиці 1 визначено, що $R = 0,429$.

3. Мотиви поведінки обрано з таблиці 2.

Підставляючи отримані дані до формули 4 отримані ймовірності реалізації хоча б однієї загрози ІзОД від інженера з телекомунікацій для різних мотивів поведінки, значення яких наведено в таблиці 3.

Приклад 4. Розрахувати ймовірність реалізації загроз ІзОД від співробітників установи (організації), які не є користувачами ІТС.

1. Відносна оцінка знань щодо можливості реалізації загроз $K = 0,1$.

2. З таблиці 1 визначено, що $R = 0,214$.

3. Мотиви поведінки обрано з таблиці 2.

Підставляючи отримані дані до формули 4 отримані ймовірності реалізації хоча б однієї загрози ІзОД від співробітників установи (організації), які не є користувачами ІТС, для різних мотивів поведінки, значення яких наведено в таблиці 3.

Узагальнення прикладів наведено в таблиці 3.

Таблиця 3. Узагальнення результатів прикладів

№	Співробітники/мотиви	Імовірність реалізації
1 Системний адміністратор		
	помста	0,992
	збагачення	0,986
	самореалізація	0,982
2 Оператор АРМ		
	помста	0,957
	збагачення	0,914
	самореалізація	0,893
3 Інженер з телекомунікацій		
	помста	0,943
	збагачення	0,886
	самореалізація	0,857
4 Співробітник установи (організації), які не є користувачами ІТС		
	помста	0,823
	збагачення	0,646
	самореалізація	0,375

Результати розрахунку ймовірностей реалізації загроз ІзОД від співробітників установи (організації) у приведених прикладах дають змогу зробити наступні висновки:

1. Найбільш імовірна реалізація загроз ІзОД від співробітників установи (організації) йде від тих співробітників, які є користувачами ІТС, мають високий рівень знань щодо можливості реалізації загроз.

2. Найбільш імовірна реалізація загроз ІзОД від співробітників установи (організації) йде від тих співробітників, які мають мотив поведінки – помста.

4. ВИСНОВКИ

Проведена перевірка працездатності методу розрахунку ймовірності реалізації загроз ІзОД від внутрішнього порушника дозволяє зробити висновки про те, що при застосуванні запропонованого методу отримуються кількісні значення загроз ІзОД для кожного співробітника установи (організації).

Розроблений метод розрахунку ймовірності реалізації загроз ІзОД від внутрішнього порушника, крім загальноприйнятої класифікації рівнів можливостей, використовуваних методів і способів здійснення дій та місця здійснення дій, враховує мотив неправомірних дій з боку внутрішнього порушника та оцінку його знань щодо можливості реалізації загроз ІзОД в ІТС.

Метод розрахунку ймовірності реалізації загроз ІзОД від внутрішнього порушника може застосовуватись як на етапі проектування КСЗІ, так і під час її експлуатації.

Подальші наукові дослідження будуть спрямовані розробку математичної моделі оцінки ризику ІзОД в ІТС від внутрішніх порушників.

5. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова Кабінету Міністрів України від 29.03.2006 № 373 [Електронний ресурс]. Режим доступу: http://www.zakon.rada.gov.ua/laws/show/373-2006-%DO%BF.

[2] 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 [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074.

[3] 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 [Електронний ресурс]. Режим доступу: http://www.tzi.com.ua/downloads/1.4-001-2000.pdf.

[4] В. О. Хорошко, В. В. Єрмошин, М. В. Капустян, "Методика оцінки інформаційних ризиків системи управління інформаційною безпекою", *Сучасний захист інформації*, № 3, с. 95-104, 2010.

[5] С. Гончар, Г. Леоненко, О. Юдін, "Загальна модель загроз безпеці інформації АСУ ТП", *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, вип. 1 (29), с. 78-82, 2015.

[6] С. Ф. Гончар, "Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом", *Захист інформації*, Том 16, № 1, с. 40-46, 2014.

[7] М. Ю. Комаров, А. В. Ониськова, С. Ф. Гончар, "Аналіз дослідження

моделі порушника безпеки інформації для захищеного вузла інтернет доступу", *Вчені записки ТНУ імені В. І. Вернадського. Серія: технічні науки*, Том 29 (68) Ч. 1 № 5, с. 138-142, 2018.
[8] А. О. Петров, "Системи захисту інформації в мережах загального користування", *Сучасна спеціальна техніка*, № 2 (25), с. 118-123, 2011.
[9] О. О. Ільїн, В. В. Вишнівський, С. О. Сєрих, "Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки", *Сучасний захист інформації*, № 1, с. 66-72, 2017.
[10] С. С. Бучик, С. В. Мельник, "Методика оцінювання інформаційних ризиків в автоматизованій системі", *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*, Вип. 11, с. 33-43, 2015.
[11] О. Г. Пузиренко, С. О. Івко, О. О. Лаврут, О. К. Климович, "Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах", *Системи обробки інформації*, Вип. 3 (128), с. 75-79, 2015.
[12] С. С. Бучик, О. К. Юдін, Р. В. Нетребко, "Теоретичні основи визначення рівня гарантій автоматизованих систем від несанкціонованого доступу", *Наукоємні технології*, № 2 (34), с. 119-125, 2017.
[13] С. С. Бучик, О. К. Юдін, *Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія*, К. : НАУ, 2015, 214 с.
[14] Р. В. Грищук, Ю. Г. Даник, *Основи кібернетичної безпеки: монографія*, Житомир: ЖНАЕУ, 2016, 636 с.
[15] Р. М. Хмелевський, "Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності", *Сучасний захист інформації,* № 4, с. 55-70, 2016.
[16] В. Н. Дереко, "Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки", *Інформаційна безпека людини, суспільства, держави*, № 2 (18), с. 16-22, 2015.
[17] Т. Ткачук, "Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз", *Підприємство, господарство і право*, № 10, с. 182-186, 2017.
[18] В. О. Панченко, "Механізм протидії інсайдерам у системі кадрової безпеки", *Науковий вісник Львівського державного університету внутрішніх справ*, №1, с. 219-227, 2018.
[19] С. Ф. Гончар, "Модель імовірних деструктивних дій персоналу АСУ ТП в умовах наявності дестабілізуючих впливів в аспекті інформаційної безпеки", *Наукоємні технології,* №3, с. 250-253, 2015.
[20] Ю. П. Рак, Р. Ю. Сукач, "Математична модель оцінки ризику в проектах захисту об'єктів потенційної небезпеки", *Управління проектами та розвиток виробництва*, №2(54), с. 12-17, 2015.
[21] М. Г. Романюков, "Критерії оцінки ймовірності витоку інформації через технічні канали", *Інформатика та математичні методи в моделюванні*, Том 5, № 3, с. 240–248, 2015.
[22] О. Я. Матов, В. С. Василенко, М. М. Будько, "Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-телекомунікаційних системах", *Методи захисту інформації в комп'ютерних системах і мережах*, Т. 6, № 2, с. 62-74, 2004.

Бойченко Олег Сергійович, *Вищу освіту здобув у Житомирському військовому інституті радіоелектроніки імені С. П. Корольова у 2004 році. Закінчив ад'юнктуру ЖВІ імені С. П. Корольова у 2016 році. У 2017 році захистив дисертацію на здобуття наукового ступеня кандидат технічних наук за спеціальністю "Озброєння і військова техніка".*
Посада: начальник НДЛ наукового центру ЖВІ імені С. П. Корольова.
Наукові інтереси: моделювання інформаційних систем; системи передачі даних; криптографічний захист інформації.

Зюбіна Руслана Віталіївна, *Вищу освіту здобула у Національному авіаційному університеті у 2013 році. , Зараз працює асистентом кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченко. Наукові інтереси: інформаційна безпека, кібербезпека, інформаційні технології.*