DOI: <https://doi.org/10.15407/emodel.43.01.017>
УДК 004.056

І.А. Пількевич, д-р техн. наук,
О.С. Бойченко, канд. техн. наук, **В.В. Лобода**, **Р.І. Гладич**
Житомирський військовий інститут ім. С.П. Корольова
Україна, 10004, м. Житомир, проспект Миру, 22
тел. +38(067) 39 787 39, e-mail: igor.pilkevich@meta.ua;
тел. +38(068) 17 025 02, e-mail: bos_2006@ukr.net;
тел. +38(063) 52 711 95, e-mail: veronichkaloboda@gmail.com;
тел. +38(068) 98 664 51, e-mail: roman.hladych@gmail.com

Математична модель оцінювання рівня знань користувачів інформаційно-телекомунікаційної системи

На основі нормативно-правових документів, які регламентують захист інформації в інформаційно-телекомунікаційних системах, розроблено математичну модель оцінювання рівня знань користувачів інформаційно-телекомунікаційної системи за результатами виконання ними тестових завдань. Застосовано методи сучасної теорії тестів та визначено вихідні дані. Для оцінювання рівня знань користувачів інформаційно-телекомунікаційної системи запропоновано використання шкали результатів виконання тесту та визначено її межі, які залежать від кількості якісних показників рівня знань. Показано математичну залежність складності тесту від кількості завдань різного рівня складності. Проведено перевірку адекватності моделі для трьох користувачів, за результатами якої встановлено, що якісна відповідь на завдання вищого рівня складності забезпечує більшу кількісну оцінку рівня знань. Наведено приклад визначення меж шкали результатів виконання тесту для трьох якісних показників рівня знань користувачів інформаційно-телекомунікаційної системи.

Ключові слова: внутрішній порушник, модель порушника, захист інформації, математична модель.

Захист інформації від витоку та несанкціонованого доступу в інформаційно-телекомунікаційних системах (ІТС) є одним з головних завдань щодо забезпечення ефективного виконання установами своїх основних функцій. На сучасному етапі розвитку інформаційних технологій захист інформації умовно поділяється на захист від зовнішніх та внутрішніх загроз. Якщо захист інформації від зовнішніх загроз має потужний тех-

© Пількевич І.А., Бойченко О.С., Лобода В.В., Гладич Р.І., 2021

нічний інструментарій, обґрунтований результатами наукових досліджень у сфері криптографічного та технічного захисту інформації, то захист від внутрішніх загроз полягає здебільшого у виконанні організаційних заходів при створенні комплексної системи захисту інформації [1—4].

Аналіз літературних даних та постановка проблеми. Для захисту інформації від внутрішніх загроз розробляють модель порушника та модель загроз інформації. Перша відображає практичні та теоретичні можливості порушника, апіорні знання, час та місце дії [2]. Під внутрішнім порушником слід розуміти персонал установи, який має доступ до інформаційних ресурсів її ІТС, тобто є авторизованими користувачами даної ІТС [5—8]. При розробці моделі внутрішнього порушника враховують лише апіорні знання користувачів ІТС, а не знання, реально оцінені. Тому існує потреба в оцінюванні рівня знань користувачів ІТС за результатами виконання ними тестових завдань. Виникнення цього важливого науково-практичного завдання обумовлено протиріччям між високими вимогами до адекватності математичної моделі внутрішнього порушника та принциповою неможливістю оцінювання його рівня знань за допомогою застосування відомих моделей, які використовують апіорні знання, що й визначає актуальність та своєчасність досліджень.

Для оцінювання рівня знань користувача ІТС застосовують методи та способи сучасної теорії тестів IRT (Item Response Theory), яка надає інструментарій для визначення рівня знань тестованого за результатами виконання ним тестових завдань. Ці завдання оцінюють певною неперервною величиною, значення якої лежать на відрізку $[0...1]$. Зв'язок між рівнем знань та виконанням тестових завдань визначається деякою нелінійною залежністю [9—12].

Відповідно до основної гіпотези теорії тестів імовірність виконання тестового завдання є функцією латентного параметра рівня знань тестованого та латентного параметра складності тестового завдання. Під латентним параметром слід вважати властивість особистості, яка недоступна для безпосереднього спостереження. Відповідно до математичної теорії параметричної оцінки тестових завдань, а саме математичної моделі Раша, оцінка рівня знань тестованого визначається у шкалі логітів. Логіт рівня знань — натуральний логарифм відношення частки правильних відповідей на всі завдання до частки неправильних [13—16].

У моделі контролю знань (логістичній моделі) наведено вимогу щодо складності завдань: одне завдання вважається складнішим за друге, якщо ймовірність правильної відповіді на нього менша, ніж на інше, незалежно від того, хто його виконує [17—20].

Недоліком наведених вище моделей є відсутність оцінки якості відповіді на завдання. Тому метою дослідження є розробка математичної

моделі оцінювання рівня знань користувачів ІТС за допомогою шкали результатів виконання тесту.

Постановка задачі і алгоритм розрахунку. Дано: тест із n завдань, які мають m рівнів складності. На кожне завдання є k варіантів відповідей. Необхідно за результатами виконання тестових завдань провести оцінювання рівня знань тестованого. Для цього визначено такі кроки:

1. Розрахунок складності тесту (complexity of the test). Складність тесту C визначається кількістю завдань різного рівня складності та дозволяє отримати максимальну оцінку тестованого за умови надання всіх правильних відповідей на завдання тесту:

$$C = \frac{\sum_{i=1}^m n_i tc_i}{m}, \quad (1)$$

де m — кількість рівнів складності завдань; n_i — кількість завдань i -го рівня складності, $i = 1 \dots m$; tc_i — складність завдання (task complexity),

$$tc_i = \frac{m+1-i}{m}.$$

2. Розрахунок якості відповіді (quality of answer). Якість відповіді qa є неперервною випадковою величиною, розподіленою на проміжку $[0 \dots 1]$, яка характеризує повноту правильної відповіді:

$$qa_i = \frac{k-i}{k-1}, \quad (2)$$

де k — кількість варіантів відповідей на тестове завдання; $i = 1 \dots k$.

3. Розрахунок імовірності правильної відповіді (probability of the correct answer). Імовірність правильної відповіді залежить від кількості рівнів складності завдань m , яку визначають за допомогою співвідношення

$$pca_i = i / m, \quad (3)$$

де $i = 1 \dots m$.

4. Розрахунок рівня відповіді (answer level). Рівень відповіді Al є неперервною випадковою величиною, розподіленою на проміжку $[0 \dots 1]$, яка характеризує повноту правильної відповіді, отриманої на завдання відповідного рівня складності. При цьому рівень відповіді враховує не ймовірність правильної відповіді на завдання, а складність самого завдання: $Al_i = qa_{i,l} tc_{i,j}$, де $i = 1 \dots n$; $l = 1 \dots k$; $j = 1 \dots m$; n — кількість тестових завдань.

5. Розрахунок частки правильних відповідей (share of correct answers). Частка правильних відповідей Sca є неперервною випадковою величиною, розподіленою на проміжку $[0...1]$, яка характеризує рівень знань на основі якості відповідей, отриманих на завдання різного рівня складності:

$$Sca = \frac{\sum_{i=1}^n Al_i}{n}.$$

6. Вибір шкали результатів виконання тестів та розрахунок її числових значень. Межі шкали результатів виконання тесту LS залежать від кількості якісних показників оцінки результатів виконання тестів Ret , а саме

$$LS_i = Sca_{\min} + i \frac{Sca_{\max}}{Ret}, \quad (4)$$

де $i = 1...Ret$; $Sca_{\min} = 0$; $Sca_{\max} = Sca$, якщо $qa=1$.

Для перевірки адекватності розробленої моделі розглянемо приклад оцінювання рівня знань користувачів ІТС. Під час оцінювання було використано тест, який складався з 30 завдань чотирьох рівнів складності та мав чотири варіанти відповідей на кожне завдання. Тест має 10 завдань четвертого (найнижчого) рівня складності; 10 завдань третього (середнього) рівня складності; 6 завдань другого (високого) рівня складності; 4 завдання першого (найвищого) рівня складності.

На першому кроці проведено розрахунок складності тесту за виразом (1). У табл. 1. наведено розподіл номерів завдань за рівнем складності. Складність тесту $C = 0,625$.

На другому кроці проведено розрахунок за виразом (2) значень якості відповіді, результати якого наведено в табл. 2.

На третьому кроці за виразом (3) розраховано імовірності правильної відповіді на завдання різної складності (табл. 3).

На четвертому кроці отримано відповіді на завдання та оцінено їх якість. Відповіді згруповано за рівнем складності та наведено в табл. 4—7.

Таблиця 1

Номери завдань	Рівень складності	Складність завдання tc_i	Кількість завдань n_i
27—30	1 — найвищий	1	4
21—26	2 — високий	0,75	6
11—20	3 — середній	0,5	10
1—10	4 — найнижчий	0,25	10

Таблиця 2

Відповідь	qa_i
Правильна, точна, повна	1,0
Правильна, точна, неповна	0,667
Правильна, неточна, неповна	0,333
Неправильна	0

Таблиця 3

Рівень складності	pca_i
1 — найвищий	0,25
2 — високий	0,5
3 — середній	0,75
4 — найнижчий	1,0

Таблиця 4

Користувач	Номер завдання четвертого рівня складності	1	2	3	4	5	6	7	8	9	10
1	qa	1	1	1	0,667	0,667	1	0	0,333	0,667	1
	Al	0,25	0,25	0,25	0,167	0,167	0,25	0	0,083	0,167	0,25
2	n	1	1	1	1	1	1	1	1	1	1
	Al	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25
3	qa	1	1	1	1	1	1	1	1	1	1
	Al	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25

Таблиця 5

Користувач	Номер завдання третього рівня складності	11	12	13	14	15	16	17	18	19	20
1	qa	1	1	0,667	0,667	0,667	1	0	0,333	0,333	0
	Al	0,5	0,5	0,334	0,334	0,334	0,5	0	0,167	0,167	0
2	qa	1	1	0,667	0,667	0,667	0,667	0,667	0,333	0,333	0
	Al	0,5	0,5	0,334	0,334	0,334	0,334	0,334	0,167	0,167	0
3	qa	1	1	1	1	1	1	1	1	1	1
	Al	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5

Таблиця 6

Користувач	Номер завдання другого рівня складності	21	22	23	24	25	26
1	<i>qa</i>	1	0,667	0,667	0,333	0,667	0
	<i>Al</i>	0,75	0,5	0,5	0,25	0,5	0
2	<i>qa</i>	1	0,667	0,667	0,333	0,333	0
	<i>Al</i>	0,75	0,5	0,5	0,25	0,25	0
3	<i>qa</i>	1	1	1	1	1	1
	<i>Al</i>	0,75	0,75	0,75	0,75	0,75	0,75

Таблиця 7

Користувач	Номер завдання першого рівня складності	27	28	29	30
1	<i>qa</i>	1	0,667	0,333	0
	<i>Al</i>	1	0,667	0,333	0
2	<i>qa</i>	0,667	0,333	0	0
	<i>Al</i>	0,667	0,333	0	0
3	<i>qa</i>	1	1	1	1
	<i>Al</i>	1	1	1	1

Таблиця 8

Користувач	Рівень складності завдання	<i>Sca</i>	Рівень знань
1	1	0,500	0,333 — середній
	2	0,375	0,333 — середній
	3	0,283	0,333 — середній
	4	0,175	0,333 — середній
2	1	0,250	0,294 — середній
	2	0,375	0,294 — середній
	3	0,300	0,294 — середній
	4	0,250	0,294 — середній
3	1	1,000	0,625 — високий
	2	0,750	0,625 — високий
	3	0,500	0,625 — високий
	4	0,250	0,625 — високий

На п'ятому кроці розраховано частку правильних відповідей Sca для різних рівнів складності (табл. 8).

На шостому кроці оцінювання результатів виконання тесту було обрано якісну шкалу з трьох рівнів знань ($Ret = 3$): низький, середній та високий. Відповідно до (4) розраховано наступні межі шкали результатів виконання тесту: низький — від 0 до 0,21; середній — від 0,22 до 0,42; високий — від 0,43 до 0,625. Відповідно до розрахованих меж шкали оцінено рівень знань користувачів ІТС за якісними показниками.

З табл. 8 випливає, що користувач 2 у порівнянні з користувачем 1 відповів краще на завдання тесту третього та четвертого рівнів складності та гірше — на завдання першого рівня складності. Отже, рівень знань користувача 2 нижчий за рівень знань користувача 1, але результати виконання тесту оцінюємо однаковим якісним показником — середній.

Таким чином, при оцінюванні рівня знань користувачів ІТС враховується рівень складності завдань тесту, а також якість відповіді. Отримані результати свідчать про те, що вірні відповіді на тести більш високого рівня дають більш високу оцінку знань користувача.

Висновки

Математична модель оцінювання рівня знань користувачів ІТС може бути використана для оцінювання рівня складності тесту і рівня знань тестованого. Вона враховує не апріорні знання, а ті, рівень яких оцінено за допомогою тестів із відповідним рівнем складності та якістю відповіді на завдання. Результати виконання тестів надають якісну оцінку рівня знань користувачів ІТС і в подальшому можуть бути використані для розробки моделі внутрішнього порушника. Застосування розробленої математичної моделі спрямовано на обґрунтування числових значень у методиці побудови моделі внутрішнього порушника в ІТС, розробці якої будуть присвячені подальші наукові дослідження.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 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: 12.05.2020).
2. Порядок проведення робіт зі 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: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074 (дата звернення: 12.05.2020).

3. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова Кабінету Міністрів України від 29.03.2006 № 373. URL: <http://www.zakon.rada.gov.ua/laws/show/373-2006-%DO%BF> (дата звернення: 12.05.2020).
4. 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: <http://www.tzi.com.ua/downloads/1.4-001-2000.pdf> (дата звернення: 12.05.2020).
5. *Панченко В.О.* Механізм протидії інсайдерам у системі кадрової безпеки// *Наук. вісник Львівського державного університету внутрішніх справ*, 2018, №1, с. 219—227.
6. *Бойченко О.С., Гуменюк І.В., Гладич Р.І.* Математична модель оцінки ризику несанкціонованого доступу до інформації користувачами інформаційно-телекомунікаційної системи // *Зб. наук. праць «Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем»*. Вип. 16. Житомир : ЖБІ, 2019, с. 124—135.
7. *Бойченко О.С., Зюбіна Р.В.* Метод розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника // *Безпека інформаційних систем та технологій*, 2019, № 1 (1), с. 19 – 26.
8. *Комаров М.Ю., Ониськова А.В., Гончар С.Ф.* Аналіз дослідження моделі порушника безпеки інформації для захищеного вузла інтернет доступу // *Вчені записки ТНУ ім. В.І. Вернадського. Серія: технічні науки*, 2018, **29** (68), ч. 1, № 5, с. 138—142.
9. *Лісова Т.В.* Моделі та методи сучасної теорії тестів /Нав.-метод. посіб. Ніжин: Видавець ПП Лисенко М.М., 2012, 112 с.
10. *Федорук П.І.* Адаптивні тести: статистичні методи аналізу результатів тестового контролю знань//*Математичні машини і системи*, 2007, № 3, 4, с. 122—138.
11. *Rasch G.* Probabilistic Models for Some Intelligence and Attainment Tests. With a Foreword and Afteword by B.D. Wright. The Univ. of Chicago Press. Chicago & London, 1980, 199 p.
12. *Погребнюк І.М., Томашевський В.М.* Моделювання сценаріїв адаптивного навчання з використанням мереж Петрі // *Вісник НТУУ «КПІ» Інформатика, управління та обчислювальна техніка*, 2013, № 55, с. 38—45.
13. *Івохін Є.В., Махно М.Ф.* Розробка засобів адаптивного тестування та автоматичного оцінювання знань // *Вісник Київського національного університету ім. Тараса Шевченка. Серія фізико-математичні науки*, 2015, №1, с. 130—133.
14. *Пасєка М.С.* Опрацювання даних адаптивного навчання і тестування студентів вищого навчального закладу // *Наук. вісник НЛТУ України*, 2015, вип. 25(4), с. 400—407.
15. *Фетісов В.С., Чернишова Е.О.* Програмні засоби для обґрунтування якості тестових завдань// *Наукові записки НДУ ім. М. Гоголя. Психолого-педагогічні науки*, 2011, № 10, с. 106—110.
16. *Соколов А.Ю., Молчанова О.Г.* Методы оценивания результатов тестирования в автоматизированных системах обучения // *Радиоэлектронні і комп'ютерні системи*, 2011, № 1 (49), с. 117—123.
17. *Раков С.А., Мазорчук М.С., Бондаренко Е.О.* Алгоритм корректировки тестовых баллов на основе анализа сложности заданий// *Інформаційні технології в освіті*, 2013, № 16, с. 49—56.
18. *Шумейко О.О., Іскандарова-Мала А.О., Лимар Н.М.* Про обчислення складності завдань // *Математичне моделювання*, 2018, № 2 (39), с. 58—65.

19. Алексеев О.М., Коновалова Н.А., Лозова К.А., Трофименко П.С. Значущість і складність тестових завдань під час оцінювання діяльності викладачів ВНЗ // Вісник КНУТД, Серія Технічні науки, 2015, № 2 (84), с. 240—246.
20. Мельник А.М., Пасічник Р.М., Шевчук Р.П. Інформаційна технологія автоматичної генерації тестових завдань з керованою складністю // Системи обробки інформації, 2011, № 3(93), с. 57—61.

Отримано 03.11.2020

REFERENCES

1. Order of the Department of Special Telecommunication Systems and Information Protection Security Services of Ukraine № 22 dated April 28, 1999, “General provisions to protect information in computer systems from unauthorized access”, ND TZI 1.1-002-99, available at: <http://dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340>, (accessed: May 12, 2020).
2. Order of the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine № 125 dated November 08, 2005, “Procedure for work on the creation of an integrated information protection system in the information and telecommunications system”, LP TSO 3.7-003-05, available at: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074, (accessed: May 12, 2020).
3. Resolution of the Cabinet of Ministers of Ukraine № 373 dated March 29, 2020, “On approval of the Rules for Ensuring the Protection of Information in Information, Telecommunication and Information-Telecommunication Systems”, available at: <http://www.zakon.rada.gov.ua/laws/show/373-2006-%DO>, (accessed: May 12, 2020).
4. Order of the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine № 53 dated December 04, 2000, “Standard provision on the information protection service in an automated system”, LP TSO 1.4-001-2000, available at: <http://www.tzi.com.ua/downloads/1.4-001-2000.pdf>, (accessed: May 12, 2020).
5. Panchenko, V.A. (2018), “Mechanism against insiders in the personnel security system”, *Naukovyy visnyk L'vivs'koho derzhavnoho universytetu vnutrishnikh sprav*, Vol. 1, pp. 219-227.
6. Boychenko, A.S., Gumenyuk, I.V. and Gladich, R.I. (2019), “Mathematical model for assessing the risk of unauthorized access to information by users of the information and telecommunications system”, *Problemy stvorenniya, vyprobuvannya, zastosuvannya ta ekspluatatsiyi skladnykh informatsiynykh system*, Vol. 16, pp. 124-135.
7. Boychenko, A.S. and Zyubina, R.V. (2019), “Method of calculating the probability of implementing restricted access information threats from an internal violator”, *Bezpeka informatsiynykh system ta tekhnolohiy*, Vol. 1, № 1, pp. 19-26.
8. Komarov, M.Yu., Oniskova, A.V. and Gonchar, S.F. (2018), “Analysis of the study of the model of an information security violator for a secure Internet access node”, *Vcheni zapysky TNU im. V.I. Vernads'koho. Seriya: tekhnichni nauky*, Vol. 29, № 68, pp. 138-142.
9. Lisova, T.V. (2012), Models and methods of modern test theory, Vydavets' PP Lysenko M.M., Nizhyn, Ukraine.
10. Fedoruk, P.I. (2007), “Adaptive tests: statistical methods for analyzing the results of test knowledge control”, *Matematychni mashyny i systemy* Vol. 3, № 4, pp. 122-138.
11. Rasch, G. (1980), Probabilistic Models for Some Intelligence and Attainment Tests, The University of Chicago Press, Chicago, US.

12. Pogrebnyuk, I.M. and Tomashevsky, V.M. (2013), "Modeling of adaptive learning scenarios using Petri networks", *Visnyk NTUU «KPI» Informatyka, upravlinnya ta obchyslyuv-al'na tekhnika*, Vol. 55, pp. 38-45.
13. Ivokhin, E.V. and Makhno, M.F. (2015), "Development of adaptive testing and automatic assessment of knowledge", *Visnyk Kyivsk'oho natsional'noho universytetu im. Tarasa Shevchenka. Seriya fizyko-matematychni nauky*, Vol. 1, pp. 130-133.
14. Paseka, M.S. (2015), "Processing data of adaptive training and testing of students of a higher educational institution", *Naukovyy visnyk NLTU Ukrainy*, Vol. 25, № 4, pp. 400-407.
15. Fetisov, V.S. and Chernysheva, E.A. (2011), "Software tools for substantiating the quality of test tasks", *Naukovi zapysky NDU im. M. Hoholya. Psykholoho-pedahohichni nauky*, Vol. 10, pp. 106-110.
16. Sokolov, A.Yu. and Molchanova, A.G. (2011), "Methods of evaluating test results in automated training systems", *Radioelektronni i komp'yuterni systemy*, Vol. 1, № 49, pp. 117-123.
17. Rakov, S.A., Mazorchuk, N.S. and Bondarenko, E.A. (2013), "Algorithm for adjusting test scores based on the analysis of the complexity of tasks", *Informatsiyi tekhnolohiyi v osviti*, Vol. 16, pp. 49-56.
18. Shumeyko, A.O., Iskandarova-Malaya, A.O. and Limar, N.M. (2018), "On calculating the complexity of tasks", *Matematychne modelyuvannya*, Vol. 2, № 39, pp. 58-65.
19. Alekseev, O.M., Konovalova, N.A., Lozovaya, K.A. and Trofimenko, P.E. (2015), "The significance and complexity of test tasks in assessing the activities of university teachers", *Visnyk KNUVD, Seriya Tekhnichni nauky*, Vol. 2, № 84, pp. 240-246.
20. Melnik, A.M., Pasechnik, R.M. and Shevchuk, R.P. (2011), "Information technology for automatic generation of test tasks with controlled complexity", *Systemy obrobky informat-siyi*, Vol. 3, № 93, pp. 57-61.

Received 03.11.20

I.A. Pilkevych, O.S. Boychenko, V.V. Loboda, R.I. Gladich

MATHEMATICAL MODEL ASSESSMENT OF KNOWLEDGE LEVEL USERS INFORMATION AND TELECOMMUNICATION SYSTEM

The regulatory documents regulating issues of information protection in information and telecommunication systems have been analyzed. The purpose of scientific research is to assess the level knowledge of users the information and telecommunication system based on the results of their test tasks. To achieve it, methods modern test theory were applied and initial data were determined. It is proposed for assessment level knowledge of users information-telecommunication system using scale of test results. The limits the test results scale are defined, which depend on the number of qualitative measures level knowledge assessment. The mathematical dependence test complexity on the number of tasks different level complexity is shown. A mathematical model for assessing the level knowledge of users information and telecommunication system has been developed, which takes into account the quality of response to tasks different levels complexity. The adequacy of the developed mathematical model for three users was checked, according to the results test, it was established that a qualitative response to tasks of the highest level complexity provides a large quantitative assessment of the level knowledge. An example of determining the limits the test results scale for three qualitative indicators of the knowledge level users the information and telecommunication system is given.

Key words: internal intruder, model of intruder, information protection, mathematical model.

ПЛІКЕВИЧ Ігор Анатолійович, д-р техн. наук, професор, професор кафедри комп'ютерних інформаційних технологій Житомирського військового інституту ім. С.П. Корольова. У 1982 р. закінчив Житомирське військове училище радіоелектроніки ППО. Область наукових досліджень — математичне моделювання складних систем, інформаційна безпека.

БОЙЧЕНКО Олег Сергійович, канд. техн. наук, начальник науково-дослідного відділу наукового центру Житомирського військового інституту ім. С.П. Корольова, який закінчив у 2004 р. Область наукових досліджень — захист інформації, моделювання інформаційно-телекомунікаційних систем.

ЛОБОДА Вероніка Вікторівна, молодший науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту ім. С.П. Корольова. Область наукових досліджень — захист інформації, моделювання інформаційно-комунікаційних систем.

ГЛАДИЧ Роман Іванович, науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту ім. С.П. Корольова. У 2006 р. закінчив Житомирський військовий інститут радіоелектроніки ім. С.П. Корольова. Область наукових досліджень — захист інформації, моделювання інформаційно-комунікаційних систем.