УДК 004.056.53::511.52

ДИОФАНТОВ МЕТОД ОПРЕДЕЛЕНИЯ ЧАСТОСТИ НАНЕСЕНИЯ УЩЕРБА ВСЛЕДСТВИЕ РЕАЛИЗАЦИИ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Виталий Безштанько, Василий Цуркан

Перспективным подходом к обеспечению конфиденциальности, целостности и доступности государственных информационных ресурсов является внедрение систем управления информационной безопасностью на основе оценивания рисков. Оценка риска выражается как комбинация частости нанесения ущерба вследствие реализации угрозы и его абсолютной величины. Поэтому выбор метода определения его оценок в конечном итоге сводится к выбору метода определения частости. Использование традиционных подходов к решению этой задачи ограничено сложностью накопления статистики нанесения ущерба. Для преодоления этого ограничения разработан метод определения частости на основе линейного, неоднородного диофантового уравнения в положительных целых числах. Он позволяет путем корректировки допустимых значений величины ущерба и приемлемого значения риска получать гарантированные решения как модельные оценки рисков. На основе полученных результатов возможно принятие решения о необходимости их обработки в системах управления информационной безопасностью.

***Ключевые слова**: диофантов метод, частость нанесения ущерба, угроза информационной безопасности, государственный информационный ресурс, определение оценок риска.*

Одним из перспективных подходов к обеспечению конфиденциальности, целостности и доступности государственных информационных ресурсов является внедрение систем управления информационной безопасностью. Такой подход предполагает оценивание рисков для принятия решения о необходимости их обработки и, как следствие, о выборе соответствующих средств и мероприятий. Для этого руководством организации выбирается метод определения оценок риска и устанавливается для него приемлемое значение [7, 8].

В большинстве случаев оценка риска выражаются качественно или количественно как комбинация частости нанесения ущерба вследствие реализации угрозы и его абсолютной величины. Поэтому выбор метода определения оценок риска в конечном итоге сводиться к выбору метода определения частости [9]. Вместе с тем применение вероятностного, статистического и экспертного подходов для решения этой задачи ограничено сложностью выполнения условий [4, 10]:

а) стационарности наблюдений за реализациями угроз для накопления статистики нанесения ущерба;

б) использования заимствованной статистики нанесения ущерба вследствие реализации угроз, а именно:

– объекты, к которым предполагается применять статистику, и объекты, на которых собрана статистика, являются эквивалентными (требование эквивалентности объектов);

– условия, при которых предполагается применять статистику и условия ее сбора являются эквивалентными (требование эквивалентности условий);

– объемы выборок статистики являются достаточными, методы обработки – корректными, а источники сведений – заслуживающие доверия (требование убедительности).

Таким образом, получение соответствующих частостных характеристик осуществляется на основе статистики недостаточного объема, то есть в условиях неопределенности. В связи с этим целью данной работы является разработка метода определения частости нанесения ущерба вследствие реализации угрозы информационной безопасности для получения модельных оценок рисков в условиях неопределенности.

Для достижения поставленной цели предположим [2 – 3], что установлено приемлемое значение величины риска $r_{пр}$. Это значение является оценкой возможности обеспечения требуемого уровня информационной безопасности и целей деятельности организации [1, 8]. Тогда сума допустимых значений величины риска нанесения ущерба вследствие реализации угроз для n информационных активов должна быть меньшей или равной $r_{пр}$, то есть

$$r_1 + r_2 + ... + r_j + ... + r_n \le r_{пр},\ j \in (1;n). \qquad (1)$$

Исходя из этого предположения, выразим r_j через произведение ущерба a_j на частость x_j его нанесения [2, 5]

$$a_j \cdot x_j \le r_j, \qquad (2)$$

где $a_j \in Z_+,\ x_j \in Z_+,\ r_j \in Z_+,\ Z_+$ – множество положительных целых чисел.

Путем подстановки (2) в (1) получим

$$a_1 \cdot x_1 + a_2 \cdot x_2 + ... + a_j \cdot x_j + ... + a_n \cdot x_n \le r_{пр}. \qquad (3)$$

Вследствие этого, предельную форму записи (3) можно интерпретировать как линейное, неоднородное диофантовое уравнение относительно x_j в положительных целых числах

$$a_1 \cdot x_1 + a_2 \cdot x_2 + ... + a_j \cdot x_j + ... + a_n \cdot x_n = r_{пр}. \quad (4)$$

В общем виде (4) имеет бесконечное множество решений. Поэтому для сокращения их полного перебора целесообразно использовать дополнительные ограничения, наложение которых предполагает учет особенностей методов решения (4) [3]. Тогда нахождение частостей x_j нанесения ущерба в положительных целых числах предполагает выполнение таких этапов:

Определение приемлемого значения величины риска $r_{пр}$ в организации, которое не должно превышать среднеквадратического отклонения $\sigma_{A_{ср}}$ от среднего значения ущерба $A_{ср}$ за рассматриваемый период времени (например: месяц, год) [1]

$$r_{пр} \le \sigma_{A_{ср}}, \quad (5)$$

$$\sigma_{A_{ср}} = \sqrt{\frac{\sum_{i=1}^{m}(A_i - A_{ср})^2}{m}},$$

где A_i – значение ущерба за рассматриваемый период времени, $A_i = P_{план,i} - P_{пол,i}$, $P_{план,i} > P_{пол,i}$; $P_{план,i}$ – планируемое значение прибыли в организации; $P_{пол,i}$ – полученное значение прибыли в организации; i – номер рассматриваемого периода времени, $i \in (1, m)$; m – количество рассматриваемых периодов времени.

Определение значений a_j величины ущерба вследствие реализации угроз для n информационных активов организации с учетом следующих условий [2]:

– сумма значений a_j величины ущерба вследствие реализации угроз для n информационных активов меньше или равна значению приемлемого риска $r_{пр}$

$$(a_1 + a_2 + ... + a_j + ... + a_n) \le r_{пр}; \quad (6)$$

существует наибольший общий делитель d для значений $a_1,..,a_j,..,a_n$, $d \ge 1$;

– приемлемое значение риска $r_{пр}$ делится без остатка на наибольший общий делитель d значений величины ущерба $a_1,..,a_j,..,a_n$.

В случае необходимости, выполнение этих условий достигается путем изменения значений a_j и $r_{пр}$ владельцем j информационного актива или руководством организации с учетом (5) и (6).

Формирование линейного, неоднородного диофантового уравнения в положительных целых числах для n информационных активов.

Решение линейного, неоднородного диофантового уравнения относительно x_j в положительных целых числах путем выбора соответствующего метода и характерных для него ограничений [2 – 3].

Предположим, что по результатам выполнения 1 и 2 этапов для 3 информационных активов определены приемлемое значение риска $r_{пр}$ и значения a_1, a_2, a_3 величины ущерба. Тогда линейное, неоднородное диофантовое уравнение запишется в таком виде

$$a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot x_3 = r_{пр}. \quad (7)$$

Для определения частостей x_1, x_2, x_3 нанесения ущерба воспользуемся комбинацией методов, которые изложены в [3, 6]. Их применение предполагает выбор наименьшего коэффициента в уравнении (7) среди a_1, a_2, a_3. Без ограничения общности можно считать, что это a_1 [6]. Поэтому справедливо следующее неравенство $a_1 < \{a_2, a_3\}$.

Разделим коэффициенты a_2 и a_3 на a_1 и, как следствие, получим

$$\begin{aligned} a_2 &= q_2 \cdot a_1 + w_1, \\ a_3 &= q_3 \cdot a_1 + w_2, \end{aligned} \quad (8)$$

где q_2 и q_3 – целочисленные результаты деления коэффициентов a_2 и a_3 на a_1; w_1 и w_2 – целочисленные остатки от деления a_2 и a_3 на a_1, $0 \le w_1 < a_1$ и $0 \le w_2 < a_2$.

Путем подстановки (8) в (7) запишем

$$a_1 \cdot x_1 + (q_2 \cdot a_1 + w_2) \cdot x_2 + (q_3 \cdot a_1 + w_3) \cdot x_3 = r_{пр}.$$

В этом выражении раскроем скобки

$$a_1 \cdot (x_1 + q_2 \cdot x_2 + q_3 \cdot x_3) + w_2 \cdot x_2 + w_3 \cdot x_3 = r_{пр} \quad (9)$$

и сделаем замену переменных

$$\begin{cases} y_1 = x_1 + q_2 \cdot x_2 + q_3 \cdot x_3; \\ y_2 = x_2; \\ y_3 = x_3. \end{cases} \quad (10)$$

Перепишем (9) с учетом (10)

$$a_1 \cdot y_1 + w_2 \cdot y_2 + w_3 \cdot y_3 = r_{пр} \quad (11)$$

и приравняем коэффициент w_3 к нулю

$$a_1 \cdot y_1 + w_2 \cdot y_2 = r_{пр}. \quad (12)$$

Для решения полученного уравнения (12) предположим [3], что известно частное решение $\{y_1', y_2'\}$

$$a_1 \cdot y_1' + w_2 \cdot y_2' = r_{пр}. \quad (13)$$

В результате вычитания (13) из (12) получим

$$a_1 \cdot (y_1 - y_1') + w_2 \cdot (y_2 - y_2') = 0. \quad (14)$$

Из (14) выразим $(y_1 - y_1')$

$$a_1 \cdot (y_1 - y_1') = -w_2 \cdot (y_2 - y_2'),$$

$$(y_1 - y_1') = \frac{-w_2 \cdot (y_2 - y_2')}{a_1}. \quad (15)$$

Как следствие, условием целочисленности (15) будет отсутствие остатка от деления $-w_2 \cdot (y_2 - y_2')$ на a_1, то есть $y_2 - y_2' = a_1 \cdot t$, где t – целочисленный результат деления $-w_2 \cdot (y_2 - y_2')$ на a_1, $t \in Z_+$.

Тогда все решения $\{y_1, y_2\}$ уравнения (12) в целых положительных числах запишем в таком виде

$$\begin{cases} y_1 = y_1' - w_2 \cdot t, \\ y_2 = y_2' + a_1 \cdot t, \end{cases} \quad (16)$$

$$y_1' > w_2 \cdot t, \quad y_2' > a_1 \cdot t.$$

Учитывая (10) и (16), из (7) найдем выражение для x_3

$$x_3 = \frac{r_{пр} - a_1 \cdot x_1 + a_2 \cdot x_2}{a_3}.$$

Рассмотрим использование предложенного диофантового метода на примере определения частостей x_1, x_2, x_3 нанесения ущерба вследствие реализации угроз для трех информационных активов. Пускай приемлемое значение величины риска $r_{пр} = 54$ и определены значения величины ущерба, а именно: $a_1 = 2, a_2 = 3, a_3 = 4$. Эти значения удовлетворяют условиям (а) – (в):

– сумма значений $a_1 = 2, a_2 = 3, a_3 = 4$ величины ущерба вследствие реализации угроз для трех информационных активов меньше или равна значению приемлемого риска $r_{пр} = 54$

$$(2 + 3 + 4) \le 54;$$

– существует наибольший общий делитель $d = 1$ для значений $a_1 = 2, a_2 = 3, a_3 = 4$ величины ущерба;

– $r_{пр} = 54$ делится без остатка на наибольший общий делитель $d = 1$ значений $a_1 = 2, a_2 = 3, a_3 = 4$.

Поскольку существует наибольший общий делитель $d = 1$, то линейное, неоднородное диофантовое уравнение

$$2x_1 + 3x_2 + 4x_3 = 54 \quad (17)$$

разрешимо во множестве Z_+ положительных целых чисел.

Разделим коэффициенты 3 и 4 на 2 и, как следствие, запишем

$$\begin{aligned} 3 &= 1 \cdot 2 + 1, \\ 4 &= 2 \cdot 2 + 0. \end{aligned} \quad (18)$$

Путем подстановки (18) в (17) получим

$$2 \cdot x_1 + (1 \cdot 2 + 1) \cdot x_2 + (2 \cdot 2 + 0) \cdot x_3 = 54.$$

В этом выражении раскроем скобки

$$2 \cdot (x_1 + x_2 + 2 \cdot x_3) + w_2 \cdot x_2 = 54 \quad (19)$$

и сделаем замену переменных

$$\begin{cases} y_1 = x_1 + x_2 + 2 \cdot x_3, \\ y_2 = x_2. \end{cases} \quad (20)$$

Благодаря этому, перепишем (19) с учетом (20)

$$2 \cdot y_1 + y_2 = 54. \quad (21)$$

Частным решением уравнения (21) будет пара положительных целых чисел $\{y_1' = 26, y_2' = 2\}$, которые используем для определения частостей x_1 и x_3 нанесения ущерба на основе (20)

$$\begin{aligned} y_1' &= x_1 + y_2' + 2 \cdot x_3, \\ 26 &= x_1 + 2 + 2 \cdot x_3, \\ x_1 &+ 2 \cdot x_3 = 24. \end{aligned} \quad (22)$$

Частным решением уравнения (22) будет пара чисел $\{x_1' = 10, x_3' = 7\}$

$$a_1 \cdot x_1' + a_3 \cdot x_3' = 24. \quad (23)$$

В результате вычитания (23) из (22) получим

$$2 \cdot (x_1 - 10) + 2 \cdot (x_3 - 7) = 0. \quad (24)$$

Из (24) выразим $(x_1 - 10)$

$$(x_1 - 10) = -2 \cdot (x_3 - 7). \quad (25)$$

Как следствие, условием целочисленности (25) будет целочисленность выражения $(x_3 - 7)$, то есть $x_3 - 7 = a_1 \cdot t$.

Тогда все целые решения $\{x_1, x_3\}$ уравнения (22) запишем в таком виде

$$\begin{cases} x_1 = 10 - 2 \cdot t, \\ x_3 = 7 + t, \end{cases} \quad (26)$$

$$-7 < t < 5. \quad (27)$$

Изменяя значения переменной t в (26) с учетом условия (27) найдем значения x_1, x_3. И, путем их подстановки в уравнение (17), решим его относительно переменной x_2

$$x_2 = \frac{54 - 2 \cdot x_1 - 4 \cdot x_3}{3}.$$

Тогда частными решениями уравнения (17) будут значения частостей нанесения ущерба вследствие реализации угроз для трех информационных активов, которые приведены в табл. 1.

Для рассмотренного примера оценена эффективность предложенного метода относительно полного перебора по количеству операций умножения/деления и сложения/вычитания путем использования таких коэффициентов (табл. 2)

$$h_u = \frac{K_{pu} - K_{du}}{K_{pu}} \cdot 100\%, \; h_s = \frac{K_{ps} - K_{ds}}{K_{ps}} \cdot 100\%,$$

где h_u и h_s – коэффициенты эффективности предложенного метода по количеству операций умножения/деления и сложения/вычитания; K_{du} и K_{pu} – количество операций умножения / деления для диофантового метода и полного перебора; K_{ds} и K_{ps} – количество операций сложения/вычитания для диофантового метода и полного перебора.

Таблица 1

Частости нанесения ущерба

t / x_j	- 6	- 5	- 4	- 3	- 2	- 1	0	1	2	3	4
x_1	22	20	18	16	14	12	10	8	6	4	2
x_2	2	2	2	2	2	2	2	2	2	2	2
x_3	1	2	3	4	5	6	7	8	9	10	11

Таблица 2

Результаты оценки эффективности диофантового метода

$r_{пр}$	Диофантов метод		Полный перебор		h_u, %	h_s, %
	K_{du}	K_{ds}	K_{pu}	K_{ps}		
18	83	132	165	165	49,69	20,00
36	269	1042	3470	3470	92,24	69,97
54	650	4286	15560	15560	95,82	72,45
129	3431	61774	272011	272011	98,73	77,28
183	6803	177182	800890	800890	99,15	77,87
237	11327	385902	1365388	1365388	99,17	71,73
291	17003	715582	3355675	3355675	99,49	78,67
345	23831	1193870	5686204	5686204	99,58	79,00
399	31811	1848414	8746061	8746061	99,63	78,86
453	40943	2706862	13033386	13033386	99,68	79,23
507	51227	3796862	18276127	18276127	99,71	79,22
561	62663	5146062	24943621	24943621	99,74	79,37

Графическое изображение результатов оценки эффективности диофантового метода относительно полного перебора для разных значений приемлемого риска показано на рисунке.

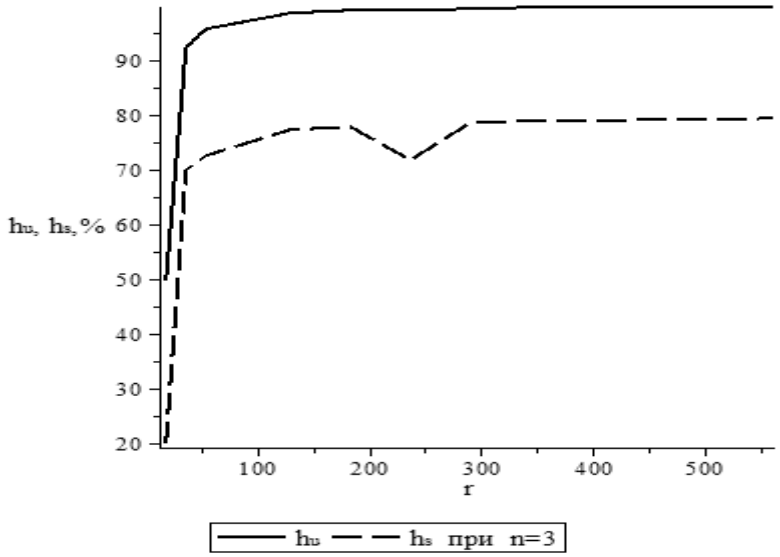

Рис. Зависимость эффективности диофантового метода относительно полного перебора

Таким образом, в работе разработан метод определения частости нанесения ущерба вследствие реализации угрозы информационной безопасности на основе линейного, неоднородного диофантового уравнения в положительных целых числах. Для сокращения полного перебора множества решений этого уравнения использованы дополнительные ограничения, что позволяет уменьшить количество операций умножения/деления, сложения/вычитания относительно полного перебора. Об этом свидетельствуют результаты оценки эффективности предложенного метода для рассмотренного примера.

В конечном итоге, диофантов метод позволяет путем корректировки допустимых значений величины ущерба и приемлемого значения риска получать гарантированные решения как модельные оценки рисков в условиях неопределенности. Благодаря этому возможно принятие решения о необходимости их обработки в системах управления информационной безопасностью.

ЛИТЕРАТУРА

[1]. Безштанько В. М. Определение приемлемого значения риска для информационных активов организации / В. М. Безштанько // Збірник наукових праць ІПМЕ ім. Г.Є. Пухова НАН України. – 2013 (в друку).

[2]. Безштанько В. М. Анализ условий разрешимости неоднородного положительного диофантового уравнения при моделировании рисков безопасности информации / В. М. Безштанько // Моделювання та інформаційні технології. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2012. – Вип. 66. – С. 92 – 96.

[3]. Безштанько В. М. Анализ методов решения неоднородных положительных диофантовых уравнений в контексте моделирования рисков / В. М. Безштанько// Информационные технологии и безопасность. – 2012. – Вип. 2. – С. 96 – 106.

[4]. Вишняков Я. Д. Общая теория рисков: учеб.пособие для студ. высш. учеб. заведений / Я. Д. Вишняков, Н. Н. Радаев. – М.: Издательский центр «Академия», 2007. – 368 с.

[5]. Качинський А. Б. Безпека загрози і ризик: наукові концепції та математичні моделі / А. Б. Качинський. – К., 2003. – 472.

[6]. Колесников П. С. Теория чисел [Электронный ресурс] / П. С. Колесников. – Режим доступа: http://math.nsc.ru/LBRT/a1/pavelsk/Num_Theory.pdf. – Дата доступа: июнь 2013. – Название с экрана.

[7]. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги: (ISO/IEC 27001:2005, MOD): СОУ Н НБУ 65.1 СУІБ 1.0:2010 – Чинний з 2010-10-28. – К.: Національний банк України, 2010. – 59 с. – (Стандарт організації України).

[8]. Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою: (ISO/IEC 27002:2005, MOD): СОУ Н НБУ 65.1 СУІБ 2.0:2010 – Чинний з 2010-10-28. – К. : Національний банк України, 2010. – 195 с. – (Стандарт організації України).

[9]. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [Электронный ресурс]: (ISO/IEC 27005:2008, IDT): ГОСТ Р ИСО/МЭК 27005-2010 – Действующий с 2010-11-30. – М.: Стандартинформ, 2011. – Режим доступа: http://docs.cntd.ru/document/1200084141. – Дата доступа: май. 2013. – Название с экрана.

[10]. Мохор В. В. Построение оценок рисков безопасности информации на основе динамического множества актуальных угроз / В. В. Мохор, А. М. Богданов, О. Н. Крук, В. В. Цуркан // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова. – К.: ІПМЕ ім. Г. Є. Пухова НАН України, 2010. – Вип. 56. – С. 87–99.

REFERENCES

[1]. Bezshtanko V.M Determining an acceptable level of risk for the organization's information assets / V. M. Bezshtanko // Collection of Scientific Papers of Pukhov Institute for Modeling in Energy Engineering, National Academy of Sciences of Ukraine, K: Pukhov Institute for Modeling in Energy Engineering, National Academy of Sciences of Ukraine, 2013 (in printing)

[2]. Bezshtanko V. M. Analysis of the conditions of the solvability of the positive inhomogeneous diophantine equation for modeling information security risks / V. M. Bezshtanko // Simulations and IT, K: Pukhov Institute for Modeling in Energy Engineering, National Academy of Sciences of Ukraine, 2012, Issue 66, P. 92 - 96.

[3]. Bezshtanko V. M. Analysis of the methods of solutions of inhomogeneous positive diophantine equations in the context of risk modeling / V. M Bezshtanko/ Information technology and security., 2012, Issue 2, P. 96 - 106.

[4]. Vishnjakov Y. General theory of risks : manual for the students at higher education institutions / Y. D. Vishnyakov, N.N. Radaev., M.: Publishing Center "The Academy", 2007., 368 p.

[5]. Kachynskiy A. B. Security of threats and risk: scientific concepts and mathematical models / A. B. Kachynskiy., K, 2003, 472 p.

[6]. Kolesnikov P. S. Number Theory [electronic resource] / P. S Kolesnikov., Access mode: http://math.nsc.ru/LBRT/a1/pavelsk/Num_Theory.pdf. Date of access: June 2013., The screen title.

[7]. Methods of protection in banking. Information Security Management System. Requirements: (ISO / IEC 27002:2005, MOD): N Bank JMA 65.1 ISMS 2.0:2010, Valid from 2010-10-28., Kyiv: National Bank of Ukraine, 2010., 195 p. (Organization standard of Ukraine).

[8]. Methods of protection in banking. Code of Rules for Information Security Management: (ISO / IEC

27002:2005, MOD): N Bank JMA 65.1 ISMS 2.0:2010., Valid from 2010-10-28., Kyiv: National Bank of Ukraine, 2010., 195 p. (Organization standard of Ukraine).
[9]. The methods and means to ensure security. Information security risk management [electronic resource]: (ISO / IEC 27005:2008, IDT): GOST R ISO / IEC 27005-2010., Valid from 2010-11-30. Moscow: Standartinform, 2011., Access mode : http://docs.cntd.ru/document/1200084141., Date of access: May 2013., The screen title.
[10]. Mokhor V. Building a risk assessment of information security based on a dynamic set of actual threats / V. Mokhor, A. Bogdanov, O. Cruk, V. Tsurkan// Collection of Scientific Papers of Pukhov Institute for Modeling in Energetics, National Academy of Sciences of Ukraine., K: Pukhov Institute for Modeling in Energy Engineering, National Academy of Sciences of Ukraine, 2010, Issue. 56, P. 87 - 99.

ДІОФАНТОВИЙ МЕТОД ВИЗНАЧЕННЯ ЧАСТОСТІ НАНЕСЕННЯ ЗБИТКУ ВНАСЛІДОК РЕАЛІЗАЦІЇ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ

Перспективним підходом стосовно забезпечення конфіденційності, цілісності та доступності державних інформаційних ресурсів є впровадження систем менеджування безпекою інформації на основі оцінювання ризику. Оцінка ризику виражається як комбінація частості нанесення збитку внаслідок реалізації загрози та його абсолютної величини. Тому вибір методу отримання його оцінок зводиться до вибору методу визначення частості. Використання традиційних підходів стосовно розв'язання цього завдання обмежене складністю накопичення статистики нанесення збитку. Для подолання цього обмеження розроблено метод визначення частості на основі лінійного, неоднорідного діофантового рівняння в додатних цілих числах. Він дозволяє шляхом корегування значень величини збитку та прийнятного значення ризику отримувати гарантовані розв'язки як модельні оцінки ризиків. На основі отриманих результатів можливе прийняття рішення про необхідність їх оброблення в системах менеджування безпекою інформації.

Ключові слова: діофантовий метод, частість нанесення збитку, загроза безпеці інформації, державний інформаційний ресурс, визначення оцінок ризику.

DIOPHANTUS METHOD OF DETERMINING OF FREGUENCY DAMAGES AS A RESULT OF IMPLEMENTATIONS INFORMATION SECURITY THREAT

Implementation of information security management systems based on risk assessments is a promising approach of ensuring the confidentiality, integrity and availability of state information resources. Risk assessment is expressed as a combination of frequency of damage occurrence as a result of the threat and its absolute value. Therefore the choice of the method for determining of its assessment leads to the choice of the method of determining the frequency of damage occurrence. Using traditional approaches to solving this problem is limited to the complexity of the statistics accumulation of damage. To overcome this limitation developed a method of determining the relative frequency of a linear inhomogeneous Diophantine equation in positive integers. It allows through adjusting acceptable values the amount of damage and acceptable risk values to get guaranteed solutions as model risk assessments. Making a decision on the necessity of their treatment in the management of information systems security is possible basing on received results.

Keywords: diophantus method, frequency of damage, information security threat, government information resource, risk evaluation.

Безштанько Віталій Михайлович, начальник лабораторії кафедри кібербезпеки та застосування автоматизованих інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: v.bezshtanko@gmail.com
Безштанько Виталий Михайлович, начальник лаборатории кафедры кибербезопасности и применения информационных систем и технологий, Институт специальной связи и защиты информации НТУУ «КПИ».
Bezshtanko Vitaliy, Head of Laboratory of Academic Department of Cybersecurity and the use of Information Systems and Technologies, Institute of Special Communication and Information Security of NTUU «KPI».

Цуркан Василь Васильович, кандидат технічних наук, старший викладач кафедри кібербезпеки та застосування автоматизованих інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: v.v.tsurkan@gmail.com
Цуркан Василий Васильевич, кандидат технических наук, старший преподаватель кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации НТУУ «КПИ».
Tsurkan Vasyl, Ph. D. in Eng., senior teacher of Academic Department of Cybersecurity and the use of Information Systems and Technologies, Institute of Special Communication and Information Security of NTUU «KPI».