УДК 510.649

Н. В. Лысак, к. т. н., доц.; Ю. В. Миронова, к. е. н.; О. Л. Рудковская

МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИЯХ

В работе рассмотрено влияние значений показателей отдельных параметров на общее состояние защищенности информации. В результате исследования разработана математическая модель оценки уровня защиты информации на предприятии средствами математического аппарата нечеткой логики.

Ключевые слова: *защита информации, математическая модель, нечеткая логика.*

Введение

Защита информационных ресурсов является одной из приоритетных задач безопасности предприятий Украины, поскольку переход к информационному обществу изменил статус информации. Сейчас она может быть как средством обеспечения безопасности, так и угрозой, и опасностью. В условиях постиндустриального этапа информация превратилась в стратегический ресурс экономического и научно-технологического прогресса. Следовательно, защита информации на предприятиях требует достаточной теоретико-методологической основы [1]. Исследование возможности применения математических методов для оценки защиты информации на предприятии является достаточно актуальным вопросом в современных условиях развития экономики Украины.

Использование различных методик для оценки защиты информации на предприятиях рассматривали многие ученые, а именно: В. В. Бут, В. В. Микитенко, А. В. Гребенюк, М. А. Живко, А. А. Сроковский, В. С. Цымбалюк, А. М. Чёрная. Однако нерешенным вопросом в сфере защиты информации остается обоснование необходимости использования математических моделей и методов исследования. Существующие методы не всегда являются доступными и удобными в использовании, требуют значительных материальных затрат.

Целью работы является разработка методического подхода к оценке уровня защиты информации на предприятии, которому свойственна упрощенная процедура идентификации защищенности за счет использования аппарата нечеткой логики.

Объектом исследования является процесс совершенствования системы оценки уровня защиты информации на предприятиях.

Изложение основного материала

В экономике Украины после длительных реформационных, кризисных и посткризисных периодов наблюдаем модификацию условий функционирования предприятий. Результатом этого является насущная необходимость обеспечения информационной безопасности, отражающей защищенность информационной среды и эффективность информационного обеспечения процесса управления на предприятии. Следовательно, защита информации является составной частью общей социально-экономической безопасности предприятия.

Для освещения дискуссионности ключевых моментов коротко предоставим трактовки основных категорий.

Защита информации (англ. *data protection*) – совокупность методов и средств, обеспечивающих целостность, доступность и конфиденциальность информации в условиях воздействия на нее угроз естественного или искусственного характера, реализация которых может повредить владельцам и пользователям информации [2; 3].

Защищают информацию для поддержки таких свойств:

- целостность (англ. *integrity*) – защита информации от несанкционированной модификации или удаления ее части;
- доступность (англ. *availability*) – защита (обеспечение) доступа к информации, а также возможности ее санкционированного использования с любого места и в любое время;
- конфиденциальность (англ. *confidentiality, privacy*) – защита информации от несанкционированного ознакомления с ней [4]. Это достаточно сложный процесс, ведь он требует учета всех значимых факторов и установления правильных функциональных зависимостей. Однако важно профильтровать множество факторов, чтобы избежать среди них коллинеарных, обращенных друг к другу, взаимосвязанных, взаимодополняющих и таких, которые дублируют друг друга.

Для оценки информационной безопасности часто используют методы рентабельности затрат на осуществление мероприятий по защите информации, методы оценки ущерба от угрозы хакерских атак. Широкое распространение получил метод нечетких множеств. При этом экспертным путем оценивают вероятность преодоления системы защиты информации, вероятность доставки единицы информации к потребителю, время доставки и аппаратурную сложность. Иногда используют показатели части работников информационных отделов в общем количестве работников, части расходов на обеспечение информационной безопасности в общей величине расходов.

Кроме того, некоторые ученые анализируют следующие показатели:

– производительность информации;

– коэффициент информационной вооруженности;

– коэффициент защищенности информации [4; 5].

Перечень параметров оценки уровня защиты информации и степень их конкретизации определяют таким методическим условием: количество оцениваемых параметров должно быть достаточно ограниченным с целью обеспечения оперативности управленческих решений, которые принимают. Формирование и группировка параметров опирается на анализ широкого комплекса проблем экономического и социального характера, поэтому множество входных факторов должно удовлетворять условия полноты, эффективности и минимальности. По критерию полноты необходимо определить такое количество параметров, которое охватывало бы все аспекты деятельности предприятия, но удаление хотя бы одного из них не меняло результат. На базе сформированного множества по критерию полноты необходимо выделить группу с максимальной степенью результативности по критерию действенности. По критерию минимальности нужно уменьшить количество параметров, исключив те, которые являются обратными, взаимозависимыми, взаимодополняющими и дублирующими друг друга.

На основе анализа зарубежных и отечественных работ [2 – 7] определены ключевые факторы, которые определяют уровень защиты информации на предприятии. Можно установить функциональную зависимость между уровнем защиты информации и факторами влияния на него в виде структурно-логической схемы. Таким образом, была разработана структурно-логическая схема защиты информации на предприятии (рис. 1).

Предлагаем множество входных параметров l_c (с $=\overline{1,C}$); совокупность показателей, рассчитываемых на основе оценочных параметров x_i (i $=\overline{1,n}$); функцию преобразования входных параметров на оценочные показатели $F_1 : L \to X$; множество функций, на основе которых осуществляется идентификация уровня эффективности политики информационной безопасности $F_2 = F(f_1,\ldots,f_i)$; множество выходных параметров $E = (e_j),\ j = \overline{1,J}$.

Итак, математическая модель такого процесса приобрела вид:

$$L \xrightarrow{F_1} X \xrightarrow{F_2} E, \partial e\, L = (l_c), c = \overline{1,C}, X = (x_i), i = \overline{1,4}, E = (e_j), j = \overline{1,J}$$
$$F_1 = f(x_{11}, x_{12}); F_2 = f(x_{21}, x_{22}); F_3 = f(x_{31}, \ldots, x_{36}); F_4 = f(x_{41}, \ldots, x_{43}). \quad (1)$$

На основе множества X параметров x_i сформирована совокупность функций преобразования:

F_1 – функция эффективности работы технического обеспечения; F_2 – функция эффективности кадровой составляющей; F_3 – функция эффективности управления информационными потоками, F_4 – функция эффективности программного обеспечения.

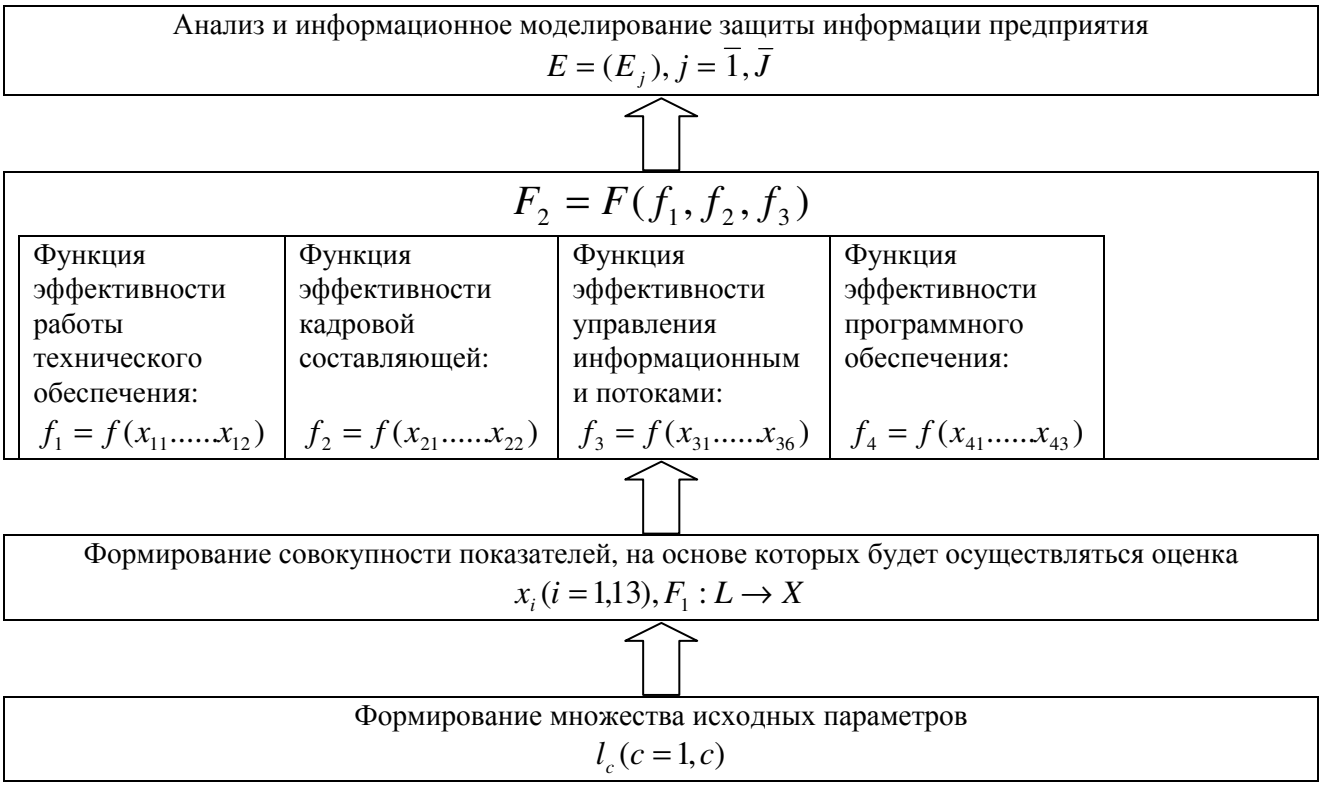

Рис. 1. Структура схемы оценки уровня защиты информации на предприятии

Как было отмечено выше, использование отдельных показателей (рентабельности, защищенности информации), а также методов экспертных оценок не позволяет эффективно идентифицировать уровень защиты информации на предприятии. Для эффективного оценивания защиты информации предприятий необходимо использовать современные математические аппараты, которые позволят совместить не только разные по содержанию показатели и модели, но и различные по своей природе – количественные и качественные параметры. Именно таким инструментом выступает аппарат нечетких множеств [8]. Важным преимуществом нечетких моделей является их прозрачность, которая позволяет им успешно конкурировать с различными индуктивными методами обработки данных [9].

Создание модели оценивания предполагает 7 этапов.

Первый этап предусматривает определение множества Т лингвистических термов, которые состоят из совокупности лингвистических переменных. Необходимо отметить, что лингвистической считается переменная, которая приобретает свое значение из перечня слов (словосочетаний) естественной или искусственной речи. При совокупности из трех лингвистических термов имеем: Н – низкий, С – средний, В – высокий. При совокупности из пяти термов: Н – низкий, НС – ниже среднего; С – средний, ВС – выше среднего; В – высокий. Такое количество лингвистических термов учитывает тот факт, что наиболее

точные и адекватные решения эксперты принимают при 7 анализированных факторах.

Для оценки параметров (x_{11}, x_{12}, x_{21}, x_{22}, x_{31},…, x_{36}, x_{41}, …, x_{43}) целесообразно использовать три нечетких терма, поскольку диапазон изменения параметров не очень большой. Необходимо отметить, что диапазон изменения параметров находится в пределах от 0 до 1, поскольку предварительно было проведено нормирование значений. Таким образом были получены функции принадлежности μ^{E_j}, $j=\overline{1,J}$ трех нечетких термов. Учитывая мнения экспертов о специфике природы выбранных параметров, был избран вид функций принадлежности. Для всех параметров была использована Гауссова функция принадлежности, которая в наибольшей степени соответствует специфике выбранных параметров [8].

Целью второго этапа является определение графиков функций принадлежности. Графики определяют для совокупности параметров (x_{ij}). Для каждого лингвистического терма отдельно определяют функцию принадлежности на основе существующего перечня функций принадлежности [10 – 12].

Общий вид функции принадлежности для различных параметров приведен на рис. 2, рис. 3 и рис. 4.

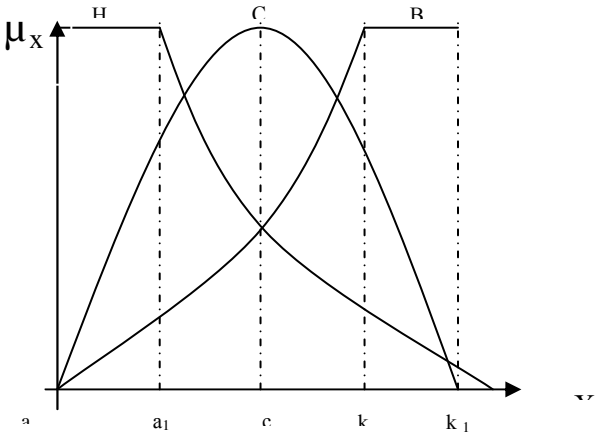

Рис. 2. Общий вид функции принадлежности трех нечетких термов для параметров x_{21}, x_{42}, x_{43}

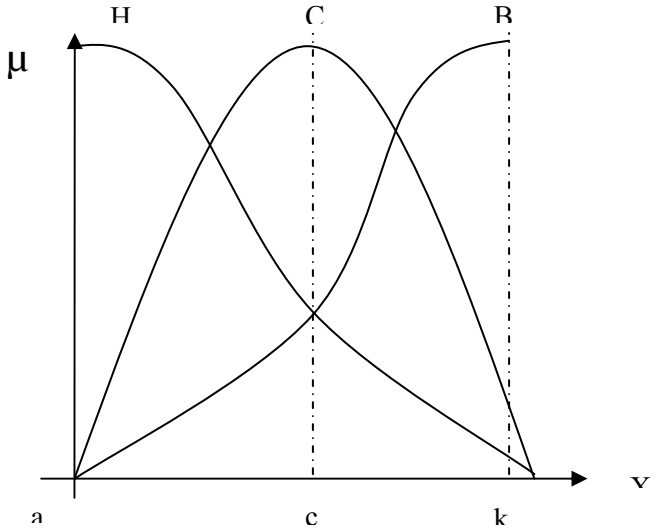

Рис. 3. Общий вид функции принадлежности трех нечетких термов для параметров x_{11}, x_{31}

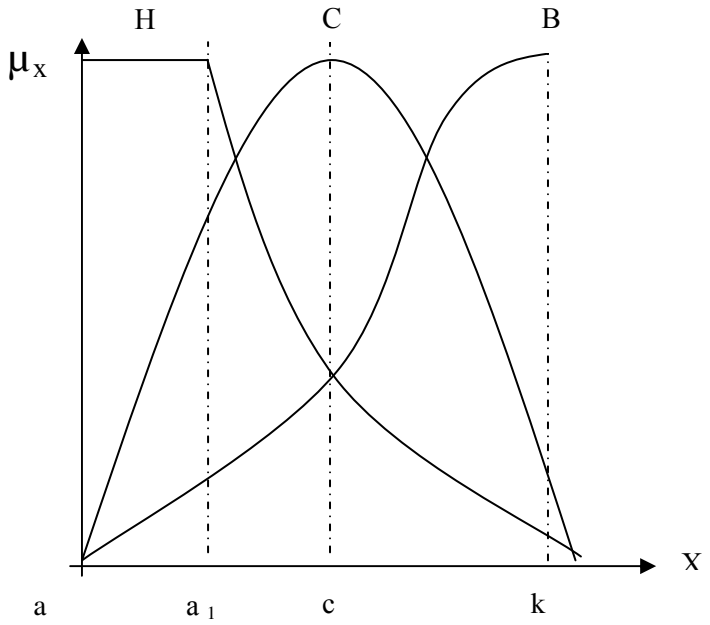

Рис. 4. Общий вид функции принадлежности трех нечетких термов для параметров $x_{12,}$ x_{22}, x_{32}, x_{33}, $x_{34,}$ x_{35}, x_{36}, x_{41}

Таблица 1

Входные показатели модели оценки уровня защиты информации предприятия

Сокращенное название показателя	Полное название показателя
1. Эффективность работы технического обеспечения предприятия	
X_{11}	коэффициент технической защиты информации
X_{12}	уровень вооруженности техническими средствами
2. Эффективность кадровой составляющей предприятия	
X_{21}	коэффициент финансирования информационных служб предприятия
X_{22}	коэффициент надежности персонала
3. Эффективность управления информационными потоками предприятия	
X_{31}	коэффициент правовой защищенности информации
X_{32}	коэффициент полноты информации
X_{33}	коэффициент точности информации
X_{34}	коэффициент противоречивости информации
X_{35}	коэффициент своевременности предоставления информации
X_{36}	коэффициент надежности информации
4. Эффективность программного обеспечения предприятия	
X_{41}	коэффициент программной защищенности информации
X_{42}	степень обеспечения программными средствами для защиты информации
X_{43}	уровень эффективности работы программного обеспечения

Ниже приведены пояснения к избранным показателям и зависимости, по которым необходимо их рассчитывать:

1) коэффициент технической защиты информации (x_{11}):

$$K_{m.з.}=l_3/l_4, \qquad (2)$$

где l_4 – количество информационных атак, на которые не среагировала техническая защита;

2) уровень вооруженности техническими средствами (x_{12}). Исчисляют как отношение количества имеющихся технических средств к необходимым;

3) коэффициент финансирования информационных служб предприятия (x_{21}):

$$K_{фин} = \frac{l_1}{l_2}, \tag{3}$$

где l_1 – затраты на финансирование информационных служб предприятия; l_2 – общие затраты предприятия [3];

4) коэффициент надежности персонала, обеспечивающего информационную безопасность предприятия (x_{22}):

$$K_{н.п} = \frac{l_7 - l_8}{l_7}, \tag{4}$$

где l_7 – общая численность уволенных работников; l_8 – численность работников, уволенных по причине утечки информации;

5) коэффициент правовой защищенности информации (x_{31}):

$$K_{пр.з} = \frac{l_5}{l_6}, \tag{5}$$

где l_5 – объем информации, разглашение которой может привести к негативным последствиям для предприятия; l_6 – общий объем юридически защищенной информации [5];

6) коэффициент полноты информации (x_{32}):

$$K_{п.ин.} = \frac{l_{10}}{l_9}, \tag{6}$$

где l_9 – объем информации, которой располагают, $l_{10.}$ – объем информации, необходимой для принятия обоснованного решения;

7) коэффициент точности информации (x_{33}):

$$K_{т.ин.} = \frac{l_{11}}{l_{12}}, \tag{7}$$

где l_{11} – объем релевантной информации, l_{12} – объем информации, которой располагают;

8) коэффициент противоречивости информации (x_{34}):

$$K_{п.ин.} = \frac{l_{13}}{l_{14}}, \tag{8}$$

где l_{13} – количество независимых свидетельств в пользу принятия решения, l_{14} – общее количество независимых свидетельств в суммарном объеме релевантной информации;

9) коэффициент своевременности предоставления информации (x_{35}):

$$K_{с.п.ин.} = \frac{l_{15.}}{l_{16}}, \tag{9}$$

где $l_{15.}$ – объем своевременно предоставленной информации, l_{16} – объем информации, необходимой для принятия обоснованного решения;

10) коэффициент надежности информации (x_{36}):

$$K_{н.ин.} = \frac{l_{17}}{l_{18}}, \tag{10}$$

где l_{17} – объем информации, предоставляемой из надежных источников, l_{18} – общий объем предоставленной информации;

11) коэффициент программной защищенности информации (x_{41}):

$$K_{п.з.} = \frac{l_{19}}{l_{20}}, \tag{11}$$

где l_{19} – время бесперебойного функционирования корпоративной информационной системы, l_{20} – нормативное время функционирования корпоративной информационной системы [6];

12) степень обеспечения программными средствами для защиты информации (x_{42}). Исчисляют как отношение количества имеющихся программных средств к необходимым;

13) уровень эффективности работы программного обеспечения (x_{43}).

На третьем этапе осуществим определение математических формул, описывающих функции принадлежности μ^{E_j}, $j=\overline{1,J}$, предварительно избранные.

Для первой функции принадлежности, изображенной на рис. 2, математическая формула имеет вид:

$$\mu^{H}(x) = \begin{cases} 1, x \in [a; a_1) \\ \left(\dfrac{k-x}{k_1-a_1}\right)^n, x \in [a_1; k] \end{cases}, \tag{12}$$

$$\mu^{C}(x) = \frac{1}{1+\left(\dfrac{x-c}{n}\right)^n}, \tag{13}$$

$$\mu^{B}(x) = \begin{cases} \left(\dfrac{x-a}{k-a}\right)^n, x \in [a; k] \\ 1, x \in (k; k_1] \end{cases}. \tag{14}$$

Для функции принадлежности, график которой изображен на рис. 3, математическая формула имеет вид:

$$\mu^{H}(x)=\frac{1}{1+\left(\frac{k_1-x}{k_1-a}\right)^{n}}, \tag{15}$$

$$\mu^{C}(x)=\frac{1}{1+\left(\frac{x-c}{n}\right)^{n}}, \tag{16}$$

$$\mu^{B}(x)=\frac{1}{1+\left(\frac{x-k_1}{n}\right)^{n}}. \tag{17}$$

Для функции принадлежности, изображенной на графике рис. 4, математическая формула имеет вид:

$$\mu^{H}(x)=\begin{cases}1, x\in[a;a_1)\\ \left(\frac{k-x}{k_1-a_1}\right)^{n}, x\in[a_1;k]\end{cases}, \tag{18}$$

$$\mu^{C}(x)=\frac{1}{1+\left(\frac{x-c}{n}\right)^{n}}, \tag{19}$$

$$\mu^{B}(x)=\frac{1}{1+\left(\frac{x-k_1}{n}\right)^{n}}. \tag{20}$$

На следующем этапе формируем группы показателей и устанавливаем числовые пределы для трех термов (табл. 2). В зависимости от природы экономического явления выбираем для каждого параметра одну из трех функций (графиков).

Таблица 2

Формулирование показателей по шкале нечетких термов «0 – 1»

Полное название показателя	Сокращенное название показателя	График	Значение показателей для термов		
			Н	С	В
I. Эффективность работы технического обеспечения предприятия					
коэффициент технической защиты информации	X_{11}	Рис. 3	0	0,2	1
уровень вооруженности техническими средствами	X_{12}	Рис. 4	0 – 0,2	0,5	1
II. Эффективность кадровой составляющей предприятия					
коэффициент финансирования информационных служб предприятия	X_{21}	Рис. 2	0 – 0,3	0,5	0,7 – 1
коэффициент надежности персонала	X_{22}	Рис. 4	0 – 0,3	0,5	1
III. Эффективность управления информационными потоками предприятия					
коэффициент правовой защищенности информации	X_{31}	Рис. 3	0	0,5	1
коэффициент полноты информации	X_{32}	Рис. 4	0 – 0,2	0,4	1
коэффициент точности информации	X_{33}	Рис. 4	0 – 0,2	0,4	0,6-1
коэффициент противоречивости информации	X_{34}	Рис. 4	0 – 0,1	0,5	1
коэффициент своевременности предоставления информации	X_{35}	Рис. 4	0 – 0,1	0,5	1
коэффициент надежности информации	X_{36}	Рис. 4	0 – 0,1	0,5	1
IV. Эффективность программного обеспечения предприятия					
коэффициент программной защищенности информации	X_{41}	Рис. 4	0 – 0,1	0,5	1
степень обеспечения программными средствами для защиты информации	X_{42}	Рис. 2	0 – 0,3	0,5	0,6 – 1
уровень эффективности работы программного обеспечения	X_{43}	Рис. 2	0 – 0,3	0,5	0,6 – 1

На следующем этапе разработки математической модели оценки эффективности политики информационной безопасности на предприятии, используя предварительно полученную информацию о значениях параметров, были составлены матрицы знаний для оценки групп параметров оценки. Построенные матрицы были описаны логическими уравнениями, которые устанавливают связь между f_i.

Результатом является сформированный методический подход к оценке уровня защиты информации на отечественных предприятиях, что позволяет значительно сократить расходы от потерь информации и безопасности информационного пространства предприятий [13].

Выводы

Проведенные исследования методологического инструментария построения математической модели позволили построить комплексную модель оценки эффективности защиты информации, что дало возможность учесть основные факторы, влияющие на уровень защиты информации и определить слабые места в политике информационной безопасности.

Разработанная модель оценки уровня защиты информации на предприятии помогает осуществлять оценку, учитывая четыре группы показателей отображения особого уровня

количественных и качественных сторон эффективности защиты информации: на уровне технической защиты, на уровне эффективности работы кадров, обеспечивающих защиту информации, на уровне эффективности управления информационными потоками и на уровне эффективности программной составляющей. Модель состоит из логических уравнений, описывающих связь между факторами, влияющими на уровень защиты информации.

Соблюдение предоставленных рекомендаций позволяет отечественным предприятиям поддерживать уровень информационной безопасности в соответствии с требованиями современности.

СПИСОК ЛИТЕРАТУРЫ

1. Сорокіна І. В. Теоретико-методологічні аспекти формування системи економічної безпеки підприємства / І. В. Сорокіна // Актуальні проблеми економіки. – 2009. – №12 (102). – С. 114 – 122.

2. Архипов А. Е. Технологии экспертного оценивания в задачах защиты информации / А. Е. Архипов, С. А. Архипова, С. А. Носок // Інформаційні технології та комп'ютерна інженерія : міжнар. наук.-техн. журн. – 2005. – № 1. – С. 89 – 94.

3. Степанов А. В. Характерные особенности задачи построения комплексной системы защиты информации распределенных корпоративных ресурсов / А. В. Степанов // Захист інформації. – 2007. – Спец. вип. – С. 131 – 134.

4. Дудикевич В. Б. Ієрархічна модель захисту даних в інформаційних технологіях / В. Б. Дудикевич, Г. В. Микитин, Ю. Р. Гарасим // Проблеми і перспективи Роозвитку ІТ-індустрії : зб. тез. доп. ІІ Міжнар. наук.-практ. конф. – Харків : Вид-во ХНУРЕ, 2010. – С. 212 – 213.

5. Ілляшенко С. М. Економічний ризик : навч. посіб. 2-ге вид., доп., перероб. / С. М. Ілляшенко. – К. : Центр навчальної літератури, 2004. – 220 с.

6. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур : монографія / Н. Й. Реверчук. – Львів: ЛБІ НБУ, 2004. – 195 с.

7. Ермошин В. В. Методика оценки информационных рисков предприятия / В. В. Ермошин // Захист інформації. – 2009. – №4 (45). – С. 80 – 88.

8. Ротштейн А. П. Інтелектуальні технології ідентифікації: нечіткі множини, генетичні алгоритми, нейронні мережі : монографія / А. П. Ротштейн. – Вінниця : Універсум-Вінниця, 1999. – 320 с.

9. Штовба С. Д. Порівняння критеріїв навчання нечіткого класифікатора / С. Д. Штовба // Вісник ВПІ. – 2007. – № 6. – С. 84 – 91.

10. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – К. : "МК-Прес", 2006. – 320 с

11. Самарский А. А. Математическое моделирование : Идеи. Методы. Примеры / А. А. Самарский, А. П. Михайлов. – М. : Физматлит, 2001. – 213 с.

12. Сергеева Л. Н. Нелинейная экономика: модели и методы / Л. Н. Сергеева. – Запорожье : Полиграф, 2003. – 217 с.

13. Стасюк А. И. Анализ методов выполнения нечетких операций над нетолерантными числами для использования в системах защиты информации / А. И. Стасюк, А. Г. Корченко, В. В. Душеба, В. А. Рындюк, Н. В. Семенова // Зб. наук. пр. Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова. – 2002. – Вип. 18. – С. 27 – 30.

Лысак Наталия Владимировна – доцент кафедры менеджмента и безопасности информационных систем.

Миронова Юлия Владимировна – старший преподаватель кафедры менеджмента и безопасности информационных систем.

Рудковская Ольга Леонидовна – ассистент кафедры финансов.

Винницкий национальный технический университет.