Александр Потий, Дмитрий Пилипенко*
*Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков, *Харьковский национальный университет радиоэлектроники, Харьков*

УДК 681.3.06

МЕТОДИКА ФОРМИРОВАНИЯ МНОЖЕСТВА ПОКАЗАТЕЛЕЙ КАК СОСТАВЛЯЮЩАЯ МЕТОДА ОЦЕНКИ УРОВНЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: **Рассматривается методика формирования множества показателей в рамках метода оценки уровня культуры информационной безопасности. Сформированное множество показателей позволяет оценить наиболее значимые аспекты культуры информационной безопасности**.
Summary: **The technique of formation of a set of indicators within a method of an assessment of level of culture of information security is considered. The set of indicators allows to estimate the most significant aspects of culture of information security.**
Ключевые слова: **Показатель безопасности, система показателей безопасности, оценивание, культура информационной безопасности.**

I Введение

Сегодня можно с уверенностью утверждать, что понимание проблем управления процессами и деятельностью по защите информации (ЗИ) претерпевает качественные изменения. Ученые, исследователи и практики, работающие в области информационной безопасности, утверждают, что организационным аспектам ЗИ должно уделяться не меньшее внимание, чем техническим аспектам.

Обилие готовых программных, аппаратных и программно-аппаратных решений безопасности позволяет сократить число инцидентов безопасности, причиной которых являются внешние угрозы. Однако, как показывают аналитические отчеты (например, отчеты InfoWatch [1]), основные финансовые потери по причине инцидентов безопасности заключаются в утечке данных, причем соотношение умышленных и случайных утечек примерно равно. Это говорит о том, что организации страдают от действий собственных сотрудников в той же мере, как и от действий злоумышленников.

Инциденты безопасности, возникающие по причине человеческого фактора, не всегда связаны с неадекватностью (или нехваткой) политик, практик и процедур безопасности. Зачастую причина заключается в их несоблюдении, что может случаться при неверном понимании целей и задач ЗИ рядовыми сотрудниками. Нередко сотрудники воспринимают политику безопасности (ПБ) как ограничение и неудобство, которое препятствует выполнению их профессиональных обязанностей [2]. Подобное отношение к задачам обеспечения безопасности информации приводит к формированию низкого уровня культуры информационной безопасности (КИБ) [3]. Здесь под «культурой информационной безопасности» будем понимать набор норм, ценностей и установок, которые формируют допустимое поведение в контексте деятельности по защите информации.

Поскольку носителями КИБ являются все члены организации, а сама КИБ зависит от результатов их *деятельности*, процесс формирования КИБ напрямую связан с управлением нормами и ограничениями (ПБ, правила, процедуры и т. д.). С этой позиции КИБ предпочтительно рассматривать в рамках институционального управления, где КИБ является механизмом побуждения, в то время как ПБ является механизмом принуждения. Управляющий субъект деятельности по ЗИ (руководитель, начальник службы безопасности и т. д.), осуществляя управляющие воздействия, не должен опираться исключительно на субъективные факторы (опыт, знания, интуицию), поскольку более обоснованные решения могут быть приняты на основе показателей безопасности. Таким образом, целью данной работы является представление методики формирования множества показателей оценки уровня КИБ, которую следует рассматривать в рамках метода оценки уровня КИБ.

II Общая характеристика метода оценки уровня КИБ

Краткое описание метода оценки уровня КИБ позволит сформировать общее представление о разработанном методе оценки уровня КИБ и том, такое место занимает в нем методика формирования показателей оценки уровня КИБ. Для удобства визуального представления разработанного метода оценки уровня КИБ воспользуемся нотацией алгоритмического языка [4] (Рисунок 1). Данное средство позволяет разрабатывать эргономичные схемы, описывающие структуру человеческой деятельности, служит для систематизации, структуризации, наглядного представления и формализации императивных знаний, что обуславливает выбор данного алгоритмического языка для визуализации метода оценки уровня КИБ.

На рис. 1 представлена схема-примитив, содержащая основные этапы метода оценки уровня КИБ. Как видно из схемы, на первом этапе формируется множество показателей оценки КИБ. Отметим, что методика позволяет получить в определенном смысле универсальное множество показателей, поскольку данное множество может использоваться как в рамках различных механизмов комплексного оценивания, так и самостоятельно.

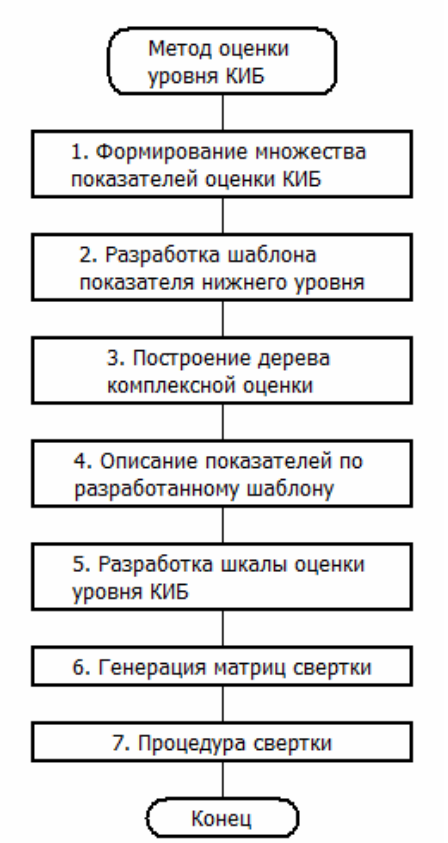

Рисунок 1 – Схема метода оценки уровня КИБ в общем виде

На втором этапе разрабатывается шаблон показателя оценки КИБ нижнего уровня. Далее, на третьем этапе осуществляется построение дихотомического дерева комплексной оценки. Описание показателей нижнего уровня (четвертый этап) следует после построения дерева комплексной оценки, поскольку множество показателей, получаемое на первом шаге, неупорядочено. Показатели нижнего уровня (листья дерева) определяются из иерархической структуры построенного дерева комплексной оценки и описываются по заранее разработанному шаблону. В данном случае необходимость построения дерева комплексной оценки обусловлена выбором матриц свертки как механизма комплексного оценивания.

На пятом этапе определяется размерность и тип шкалы оценки уровня КИБ. Размерность шкалы напрямую влияет на размерность матриц свертки, поскольку матрицу свертки можно рассматривать как таблицу, номера строк и столбцов которой означают оценку по сворачиваемым критериям (показателям). В рамках данного метода число строк равно числу столбцов и определяется размерностью шкалы.

На шестом этапе осуществляется генерация матриц свертки с учетом весовых коэффициентов и минимальных пороговых значений, которые определяются экспертно. На последнем, седьмом, этапе

осуществляется сама свертка значений показателей оценки КИБ. Таким образом, выполнение данного алгоритма позволяет получить комплексную оценку уровня КИБ.

III Методика формирование множества показателей безопасности оценки уровня КИБ

В [5] был проведен анализ следующих систем показателей безопасности: Vaughn-Hennig-Siraj [6], OCTAVE [7], CISWG [8], Erkan Kahraman [9] и NIST [10]. Результаты анализа позволяют сформулировать следующий вывод: несмотря на то, что показатели безопасности организационного характера присутствуют в том или ином виде в каждой из проанализированных систем, целостной системы (набора) показателей, позволяющей количественно или качественно оценить уровень КИБ, на данный момент не существует. Таким образом, возникает задача сформировать целостное множество показателей, позволяющих осуществить комплексную оценку уровня КИБ.

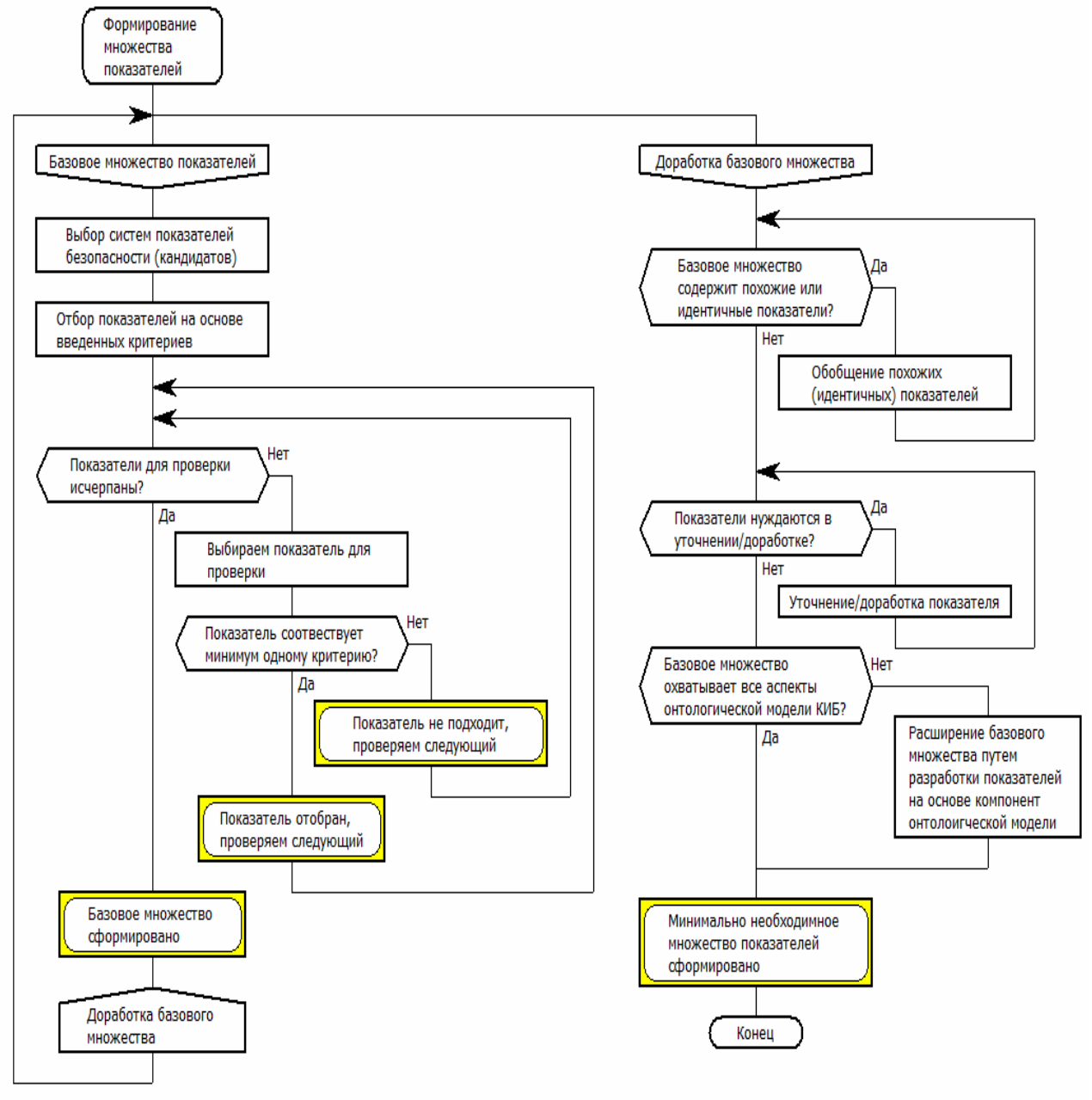

Рисунок 2 – Алгоритм (методика) формирования множества показателей оценки КИБ

Алгоритм (методика) формирования множества показателей оценки КИБ состоит из главной ветки «Базовое множество показателей» и вспомогательной ветки «Доработка базового множества» (рис. 2). Отбор показателей для оценки КИБ осуществляется из показателей, входящих в состав систем-кандидатов. В качестве систем-кандидатов были выбраны наиболее известные системы показателей безопасности: Vaughn-Hennig-Siraj [6], OCTAVE [7], CISWG [8], Erkan Kahraman [9] и NIST [10]. Введем следующие критерии отбора показателей:

– критерий пригодности (показатель отбирается, если он может быть использован для оценки КИБ);

– критерий назначения (назначение показателя определяется на основании прямых указаний разработчиков, характеристики показателя и т. д.).

В ходе анализа систем-кандидатов было отобрано 24 показателя оценки КИБ, формирующих базовое множество показателей безопасности $P^{base} = \{P_n \mid n = \overline{1,24}\}$. В табл. 1 содержатся элементы данного множества с указанием иерархии оригинальной системы показателей. Следующим этапом является доработка полученного множества (рис. 2).

Анализ табл. 1 показывает, что некоторые элементы множества P^{base}, несмотря на отличия в названии, обладают схожей (в некоторых случаях – идентичной) сущностью. Например, показатели 2.1.1 «Информирование и обучение» [7], 4.1.1 «Информирование, тренинг и обучение» [9] и 5.1.1 «Информирование и обучение (AT)» [10] предназначены для оценки компетентности членов организации и имеют одно назначение.

Таблица 1 – Результаты анализа систем-кандидатов

Система показателей	**Иерархия и название показателя**	
1. Vaughn-Hennig-Siraj	1.1 Кадровое и мат.-техн. Обеспечение	1.1.1 Персонал
		1.1.2 Ресурсы
	1.2 Операционные показатели	1.2.1 Готовность → Управленческая готовность
2. OCTAVE	2.1 Стратегическая деятельность	2.1.1 Информирование и обучение
		2.1.2 Политика и нормы безопасности
		2.1.3 Совместное управление безопасностью
	2.2 Кадровая безопасность	2.2.1 Управление инцидентами
		2.2.2 Общая деятельностью персонала
3. CISWG	3.1 Стратегическое управление	3.1.1 Сотрудничество с менеджментом среднего звена
		3.1.2 Аудит
	3.2 Оперативное управление	3.2.1 Роли и ответственность в процессе ОБИ
		3.2.2 Сотрудничество с персоналом службы безопасности
4. Erkan Kahraman	4.1 Человеческий фактор	4.1.1 Информирование, тренинг, обучение
		4.1.2 Компетенция персонала
5. NIST	5.1 Оперативное управление	5.1.1 Информирование и обучение (AT)
		5.1.2 Кадровая безопасность (PS)

Поскольку множество показателей P^{base} не является оптимальным в силу наличия идентичных по назначению показателей, представляется рациональным пренебречь сохранением оригинальной иерархии и провести обобщение (в ряде случаев уточнение) элементов множества P^{base} с целью формирования множества $\tilde{P}^{base}$, содержащего уникальные элементы. Таким образом, во избежание путаницы, похожие показатели будут обобщены, т. е. приведены к единому виду, название которого ясно отражает сущность и

назначение показателя. Обобщаемые показатели исходного множества P^{base} и итоговый результат (элементы множества $\tilde{P}^{base}$) представлены в табл. 2.

Необходимо отметить, что в некоторых случаях существуют заметные расхождения в иерархии анализируемых систем показателей безопасности. Например, показатель 2.2 «Кадровая безопасность» в системе OCTAVE [7] представляет собой группу (класс) показателей, в то время как в системе показателей NIST [10] 5.1.2 «Кадровая безопасность» является показателем нижнего уровня и глубже не детализируется. Это свидетельствует о том, что при создании подобных систем показателей безопасности точка зрения разработчиков относительно некоторых аспектов защиты информации может отличаться. Иными словами, подобные системы показателей безопасности строятся с определенной долей субъективности и зависят от предпочтений разработчика. Можно предположить, что при решении подобного рода задач (построения таксономий) полностью избежать субъективизма невозможно.

Следует подчеркнуть, что анализ существующих систем показателей безопасности не позволил выявить некоторый формализованный подход или методику построения подобных систем. Очевидно, что иерархия рассмотренных систем и выбор показателей определялись разработчиками системы главным образом на основе принципа логического обоснования.

Таблица 2 – Результаты обобщения/уточнения базового множества P^{base}

Обобщение/уточнение показателей безопасности, P^{base}	**Итоговые показатели, $\tilde{P}^{base}$**
1.1 Кадровое и мат.-техн. обеспечение 1.1.2 Ресурсы	Выделение человеческих, материальных и технических ресурсов на обеспечение ЗИ
1.1.1 Персонал 4.1.2 Компетенция персонала	Компетентность персонала
1.2 Операционные показатели 3.2 Оперативное управление 5.1 Оперативное управление	Оперативность управления
	Точность управления
	Стабильность управления
1.2.1 Готовность -> Управленческая готовность	Управленческая готовность
2.1 Стратегическая деятельность 3.1 Стратегическое управление	Управление деятельностью персонала
2.1.1 Информирование и обучение 4.1.1 Информирование, тренинг, обучение 5.1.1 Информирование и обучение (AT)	Степень информированности персонала
	Доля персонала, прошедшего тренинг по информационной безопасности
2.1.3 Совместное управление безопасностью	Координированность
3.1.1 Сотрудничество с менеджментом среднего звена	Сотрудничество с руководством
3.2.2 Сотрудничество с персоналом службы безопасности	Сотрудничество с отделом ИБ
2.2 Кадровая безопасность 5.1.2 Кадровая безопасность (PS)	Кадровая безопасность
2.1.2 Политика и нормы безопасности	Соответствие стандартам поведения
3.1.2 Аудит	Аудит безопасности
3.2.1 Роли и ответственность в процессе ОБИ 2.2.2 Общая деятельность персонала	Доля утвержденных ролей и ответственностей
2.2.1 Управление инцидентами	Эффективность обратной связи
4.1 Человеческий фактор	Доля инцидентов безопасности по вине персонала

КИБ является в достаточной мере сложным и глубоким понятием и, как видно из онтологической модели предметной области КИБ [3], полученное множество показателей $\tilde{P}^{base}$ не способно охватить все необходимые аспекты формирования КИБ. Аспекты КИБ, которые не были охвачены показателями множества $\tilde{P}^{base}$, предлагается учесть посредством расширения данного множества. Опираясь на разработанную онтологическую модель предметной области КИБ [3], расширим множество $\tilde{P}^{base}$ дополнительными показателями, разработанными с учетом компонент модели (аспектов КИБ).

Табл. 3 содержит множество показателей P^{om} оценки КИБ, разработанные на основе онтологической модели предметной области КИБ. Пусть множество показателей безопасности P^{final} является результатом объединения множеств $\tilde{P}^{base}$ и P^{om}, выражение (1).

$$P^{final} = \tilde{P}^{base} \cup P^{om}, \tag{1}$$

где P^{final} – универсальное множество показателей оценки уровня КИБ, $\tilde{P}^{base}$ – уточненное базовое множество показателей, P^{om} – множество показателей, разработанных на основе компонент онтологической модели предметной области КИБ.

Таблица 3 – Результат преобразования множества $P^{concept}$

Предлагаемые показатели оценки КИБ, P^{om}	1. Степень принятия КИБ	1.1 Степень понимания КИБ
		1.2 Охват персонала КИБ
	2. Уровень КИБ	2.1 Вклад персонала
		2.2 Вклад руководства
	3. Дисциплина	
	4. Провозглашаемые ценности и нормы	
	5. Поддержка руководства	

Таким образом, в результате анализа существующих систем показателей безопасности было сформировано базовое множество показателей P^{base}, элементы которого были доработаны, уточнены и обобщены. Опираясь на онтологическую модель предметной области КИБ было разработано дополнительное множество показателей оценки КИБ P^{om}, благодаря которому были охвачены аспекты КИБ, не затронутые элементами базового множества P^{base}. Объединение данных множеств позволило получить множество P^{final}, содержащее минимально необходимое число показателей для оценки уровня КИБ. Отметим, что множество показателей P^{final} не является окончательно определенным и может быть дополнено новыми показателями для оценки уровня КИБ.

IV Выводы

В работе предложена методика формирования множества показателей оценки КИБ, которая является составляющей метода оценки уровня КИБ. Путем анализа существующих систем показателей безопасности информации на основании сформулированных критериев было сформировано базовое множество показателей оценки уровня КИБ, состоящее из 24 показателей. После доработки базового множества (уточнения и обобщения показателей) число уникальных показателей составило 18 штук. Однако анализ онтологической модели позволил сделать вывод, что многие ключевые аспекты не были охвачены. По этой причине доработанное базовое множество показателей было расширено показателями, разработанными на основе компонент онтологической модели. Финальное множество состоит из 27 показателей оценки КИБ и охватывает все ключевые аспекты КИБ. Однако следует заметить, что полученное в итоге множество

показателей не является окончательно определенным и может быть дополнено новыми показателями для оценки уровня КИБ.

Список использованной литературы: ***1.*** *Сайт http://infowatch.com [Электрон. ресурс]. – Режим доступа: http://infowatch.com/analytics.* ***2.*** *Alfawaz, Salahuddin M. Information security management: a case study of an information security culture. PhD thesis, Queensland University of Technology, 2011.* ***3.*** *Potiy A.V. The prerequisites of information security culture developmen and an approach to complex evaluation of its level / A.V. Potiy, D.Y. Pilipenko, I.N. Rebriy // Науково-технічний журнал "Радіоелектронні і комп'ютерні системи" № 5(57). Харків "ХАІ". – 2012 р. – С. 72 – 77.* ***4.*** *Пароңджанов В. Д. Как улучшить работу ума? Алгоритмы без программистов – это очень просто! / В. Д. Пароңджанов. – М.: Дело, 2001. – 360 с.* ***5.*** *Потій О. В. Аналіз систем показників безпеки інформації / О. В. Потій, Д. Ю. Пилипенко // Научно-технический журнал «Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности». Харьков, ХНУРЭ, 2010. – Том 9. – №3. – С. 435-443.* ***6.*** *Rayford Vaughn Jr., Ronda Henning, Ambareen Siraj, Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, 30th Hawaii International Conference on System Sciences, Big Island, Hawaii, January 7- 10, 2002.* ***7.*** *Alberts C., Dorofee A. Managing Information Security Risks "The OCTAVE Approach" Addison-Wesley Publishing 2003.* ***8.*** *Corporate Information Security Working Group (CISWG). November 17, 2004 (Revised January 10, 2005). Report of the Best Practices and Metrics Teams, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Government Reform Committee, United States House of Representatives.* ***9.*** *Erkan Kahraman. Evaluating it security performance with quantifiable metrics. Master's thesis, DSV SU/KTH, 2005.* ***10.*** *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Aug. 2009.* ***11.*** *Stemler, S., and Bebell, D. (1998). An Empirical Approach to Understanding and Analyzing the Mission Statements of Selected Educational Institutions. Paper presented at the annual meeting of the New England Educational Research Organization. Portsmouth, New Hampshire.*

Володимир Бурячок, Анатолій Шиян*
*Військова частина А1906, *Вінницький національний технічний університет*

УДК: 004.056:159.95

ТЕОРІЯ ІГОР ЯК МЕТОД УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Анотація: **Проаналізовано теорію ігор як кількісний метод, який суттєво розширює можливості при управлінні інформаційною безпекою, та визначено основні особливості його застосування. Описано характеристики теорії ігор, які є перспективними для застосування в управлінні інформаційною безпекою, та наведено приклади застосування для задач управління інформаційною безпекою. Проаналізовано розвиток теорії ігор в Україні.**

Summary: **The paper analyzes the game theory as a quantitative method, which significantly expands the possibilities in the information security management, and describes the main features of its application. We describe the characteristics of game theory, which are promising for use in the information security management, and are presented the solutions of problems for information security management. The development of game theory in Ukraine is described.**

Ключові слова: **Інформаційна безпека, теорія ігор, управління, узгодження інтересів, рівновага Неша.**

І Вступ

Управління інформаційною безпекою включає в себе управління людськими, інформаційними, технічними, програмними, фінансовими та іншими ресурсами [1]. Саме людина, сукупність людей (як організована – підприємство, організація тощо, так і неорганізована – сукупність футбольних фанатів чи хакерів), суспільство і держава (та їх інститути) складають суб'єкти управління інформаційною безпекою.

Все зростаюче поширення інформаційних технологій, зростання числа користувачів Інтернету, створення та структурування міжнародного та регіонального кіберпросторів приводить до все зростаючої ролі процесу узгодження інтересів різних суб'єктів. Саме рівень узгодженості інтересів суб'єктів інформаційних процесів, який визначає *мотивацію* суб'єктів, сьогодні часто визначає і рівень інформаційної безпеки.