УДК 004.942

В. В. ГЛУШАК, О. М. НОВІКОВ

Національний технічний університет України "Київський політехнічний інститут"

ПІДХІД ДО АНАЛІЗУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ БАЙЄССІВСЬКИХ МЕРЕЖ

Анотація. Робота присвячена розробці підходу до аналізу та оцінки ймовірностей реалізації загроз інформації з ефективним поєднанням експертного досвіду та емпіричних даних. В якості апарату для отримання ймовірнісних характеристик загроз обрано апарат байєссівських мереж.

Ключові слова: загрози інформаційної безпеки, вразливості інформаційної безпеки (ІБ), механізми захисту, Байєссівська мережа.

Аннотация. Работа посвящена разработке подхода к анализу и оценке вероятностей реализации угроз информации с эффективным сочетанием экспертного опыта и эмпирических данных. В качестве аппарата для получения вероятностных характеристик угроз избраны подходы на основе байесовских сетей.

Ключевые слова: угрозы информационной безопасности, уязвимости информационной безопасности (ИБ), механизмы защиты, байесовского сеть.

Annotation. The article is devoted to developing an approach to analyze and assess the probability of information threat with an effective combination of expertise and empirical data. To determine probabilities of threat it has been chosen approach based on Bayesian networks.

Keywords: threats to information security, information security vulnerability (IB) protection mechanisms Bayesian network.

Вступ

Проектування сучасних систем захисту інформації (СЗІ) та створення їх політик безпеки вимагає забезпеченням їх високоточними вихідними даними. Важливим етапом, що передує аналізу ризиків інформаційної безпеки (ІБ), як ключового кроку побудови політики СЗІ, є створення моделі порушників та загроз. Від коректності побудованої моделі загроз залежать рішення, що будуть прийматися на наступних етапах, а також стійкість створеної СЗІ до атак зловмисників.

На сьогоднішній день, розроблено ряд емпіричних та формальних методів, що вирішують задачу синтезу (побудови) СЗІ. При цьому використовуються логіко-ймовірнісний підхід, теорія ігор, методи математичного програмування та інші підходи. Результати використання даних підходів наведені в роботах О.М. Новікова, А. Тимошенко, А.М. Родіонова та інших [3-5].

Аналіз сучасного стану досліджень в області захисту інформації свідчить про існування недоліків, пов'язаних, в першу чергу, з ефективним використанням накопичених статистичних даних разом з суб'єктивними експертними оцінками та розробленими математичними моделями. Проте, досі не існує підходів, що об'єднують переваги із кожної групи методів. На практиці, для аналізу ймовірності реалізації загроз ІБ використовуються або методи на основі експертних оцінок (метод аналізу ієрархій Сааті, метод узгоджених оцінок «Делфі», критерій переваги) або статистичні методи (аналіз часових рядів). Кожна група методів має свої переваги, проте для складних систем ймовірність похибки експерта збільшується, в той час як статистичні дані можуть бути непридатними для використання через свою неповноту.

Вказані аспекти побудови СЗІ можна врахувати в підході що ґрунтується на застосовувані байєссівських мереж. У порівнянні з існуючими методами аналізу данних, вони надають зрозуміліше пояснення своїх висновків, припускають логічну інтерпретацію і модифікацію структури відношень між змінними задачі, а також можливість використання у якості вихідних даних емпіричні частоти появи різних значень змінних, суб'єктивні оцінки експертів та теоретичні уявлення про математичні ймовірності тих чи інших наслідків із апріорної інформації.

Представлення байєсової мережі у вигляді графа робить її зручним інструментом для розв'язання задачі оцінки ймовірностей реалізації загроз.

Постановка задачі

Метою роботи є підвищення якості оцінок ймовірності реалізації загроз зловмисника шляхом розробки підходу що базується на застосуванні байєсівських мереж.

Для досягнення мети необхідно розв'язати такі задачі:

- виконати аналіз змінних, що мають відношення до створення інформаційних загроз;
- побудувати ймовірнісну модель у формі байєсівської мережі для оцінювання ймовірності виникнення загрози;
- виконати обчислювальні експерименти з дослідження адекватності побудованих ймовірнісних моделей.

Побудова ймовірнісної моделі

Байєсівська мережа (БМ) – це орієнтований ациклічний граф $G = (V, E)$, вершинами якого є випадкові змінні, а ребра описують впливи між ними [1]. Побудова БМ починається з визначення змінних

$a_i \in V$, що приймають участь в задачі. Серед множини всіх змінних необхідно вибрати ті, що відносяться до цільових та описати їх можливі значення. На наступному кроці, на основі досвіду та наявної інформації, експертами визначаються апріорні ймовірності значень цих змінних $p(a_i)$. Далі необхідно описати причинно-наслідкові зв’язки між змінними у вигляді орієнтованих ребер графа $\{a_i, a_j\} \in E$, розмістивши у вузлах змінні задачі. Для кожного вузла графа, що має вхідні ребра вказати умовні ймовірності різних значень змінних для набору батьківських змінних на графі. Стан всіх батьківських змінних для вершини a_i будемо позначати через $pa(a_i)$. Для множини змінних графа виконується марківська умова, кожна змінна a_i в графі не залежить від усіх інших змінних, окрім батьківських $pa(a_i)$ [6].

Цільовими змінними в БМ $x_k \in V$, що розробляється, є потенційні загрози, до яких може бути вразлива ІКС. Всі змінні, в моделі, що розробляється, будуть дискретними. Кожна змінна-загроза може приймати одне із п’яти значень, що відповідає ймовірності її реалізації: trivial, low, medium, high, critical (несуттєва, низька, середня, висока, критична).

Інші змінні в БМ є характеристиками, набір яких дозволить ідентифікувати загрозу та визначити її ймовірність. Дані змінні були поділені на категорії, що класифікують загрози інформаційної безпеки або описують різні види зловмисників:

1. Мета несанкціонованого досутпу (НСД). Розглядається порушення конфіденційності (*p_confidentiality*), цілісності (*p_integrity*) чи доступності (*p_availability*) інформації.
2. Положення джерела НСД (*n_network*). Розподілено на 3 категорії: внутрішньосегментне, міжсегментне, зовнішнє.
3. Необхідність автентифікації для реалізації загрози (*a_auth*).
4. Підготовка зловмисника (*a_complexity*): висока, середня, низька.

Визначивши всі змінні мережі, необхідно описати причинно-наслідкові зв’язки між ними. Треба визначити які характеристики на які загрози впливають, а також взаємозв’язки між характеристиками, якщо є такі.

Кожній змінній потомку y_l, з батьківськими змінними $b_1,...,b_i,...,b_n$ приписується таблиця умовних ймовірностей $p(y_l \mid b_1,...,b_i,...,b_n)$. Якщо змінна не має предків, то замість умовної ймовірності використовується безумовна $p(y_l)$.

В якості потомків і батьківських змінних можуть виступати як цільові змінні x_k, так і змінні характеристики a_i, залежно від топології байєсової мережі.

При обранні загроз для моделювання використовувалися практичні класифікатори загроз за їх наслідками. В тому числі класифікація, запропонована Пітером Меллом та методика STRIDE, що розроблена, обґрунтована і активно пропагується фахівцями з компанії Microsoft [2].

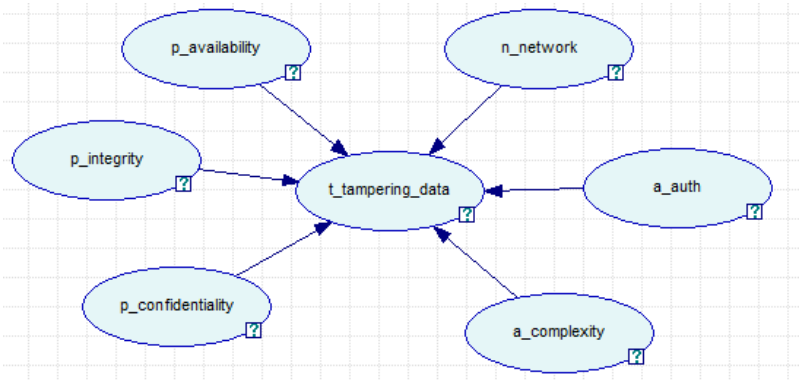


Рисунок 1 – Приклад Баєсової мережі для загрози «модифікація даних»

Після визначення всіх змінних та причинно наслідкових зв’язків між ними (рис. 1) необхідно визначити ймовірності різних значень змінних для множини батьківських змінних. Існує ряд методів для визначення вказаних ймовірностей, серед яких:

експертний (задання ймовірностей кваліфікованим фахівцем);
статистичний (навчання мережі на основі накопичених даних про реалізовані загрози);
математичний (визначення формальних співвідношень між змінними).

При побудові вказаної мережі застосовувалися емпіричний та статистичний підходи до отримання вихідних даних, проте основним варто виділити статистичний. В даній роботі таблиці умовних ймовірностей визначаються через навчання мережі з використанням алгоритму максимізації математичного сподівання (expected maximization) [8].

Алгоритми навчання мережі

Навчання баєсівської мережі відбувається на основі статистичних даних. Навчання моделі можна розділити на два етапи: навчання параметрів мережі та її структури.

Для навчання параметрів мережі з фіксованою структурою застосовано EM-алгоритм. Метою застосування даного алгоритму є уточнення апріорних припущень експерта щодо значень параметрів, а задача зводиться до визначення найбільш ймовірного рівня загрози $t \in T$ при відомій множині факторів $a_1 ... a_n \in A$, що можуть призвести до реаліації цієї загрози. Математично це можна записати таким чином:

$$t = \arg \max_{T} P(T \mid A_i) \quad (1)$$

EM алгоритм використовується для знаходження оцінок максимальної вірогідності параметрів ймовірнісної моделі та дає можливість досягти глобального екстремуму. При цьому за основу береться формула Байєса (2), що вирішує задачу пошуку $P(T \mid A_i)$ шляхом переходу до непрямих ймовірностей.

$$P(T \mid A_i) = \frac{P(A_i \mid T)P(T)}{P(A_i)} \quad (2)$$

Алгоритми навчання структури мережі передбачають пошук умовної незалежності між змінними та підбір відповідної структури графу. В роботі розглядаються такі алгоритми: байєсівський пошук, PC-алгоритм та наївний баєсівський класифікатор[8-9].

Таблиця 1 – Частина таблиці умовних ймовірностей для загрози «Модифікація даних», розрахована за EM-алгоритмом

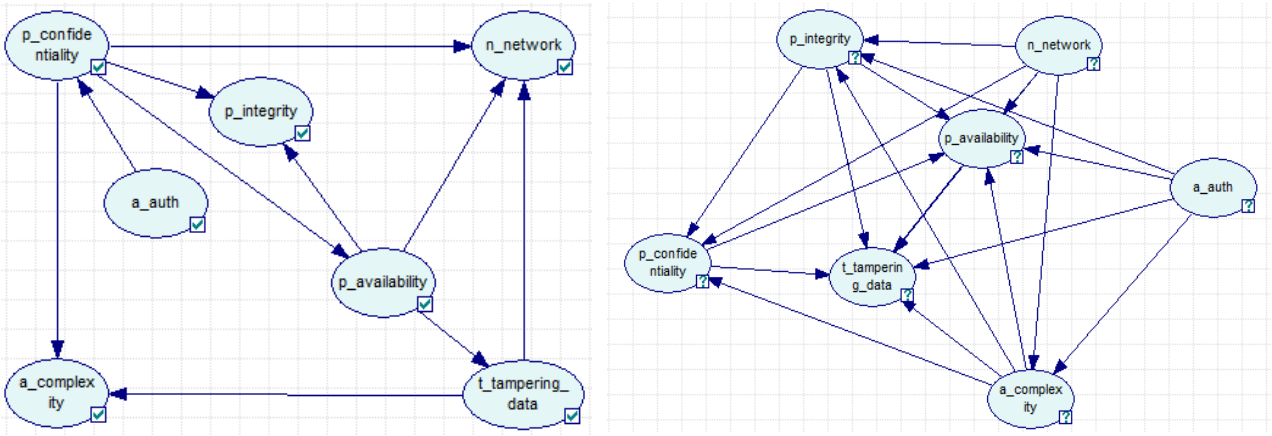
фактори	p_availability	повна					
	p_integrity	повна					
	p_confidentiality	повна					
	n_network	міжсегментна					
	a_auth	відсутня			слабка		
	a_complexity	низька	середня	висока	низька	середня	висока
рівень загрози	trivial	0,00058	0,00058	0,02500	0,00741	0,00741	0,02500
	minor	0,00058	0,00058	0,02500	0,00741	0,00741	0,02500
	medium	0,00058	0,00058	0,90000	0,00741	0,00741	0,90000
	major	0,99767	0,99767	0,02500	0,97037	0,97037	0,02500
	critical	0,00058	0,00058	0,02500	0,00741	0,00741	0,02500

Обчислювальний експеримент

Для створення мережі задано апріорні умовні ймовірності виникнення тих чи інших подій. Після чого було проведено навчання мережі на основі статистичних даних, отриманих з Національної Бази Вразливостей США (версія 2.2), де є інформація про вразливості, умови їх виникнення та наслідки (загрози), до яких вони можуть призвести.

В статті наведено результати моделювання для однієї з загроз — модифікація даних.

В таблиці 1 подано результати навчання мережі з використанням EM-алгоритму. Як видно із таблиці, деякі ситуації є рівноймовірними, що свідчить про неповноту статистичність даних. Також було проведено навчання структури мережі для прогнозування ймовірності реалізації загроз з використанням алгоритмів, вказаних вище. Отримані мережі подано на рис. 2 а та 2 б. Структура мережі, навченої наївним класифікатором співпадає з рис. 1, крім того факту, що ребра спрямовані в протилежний бік.

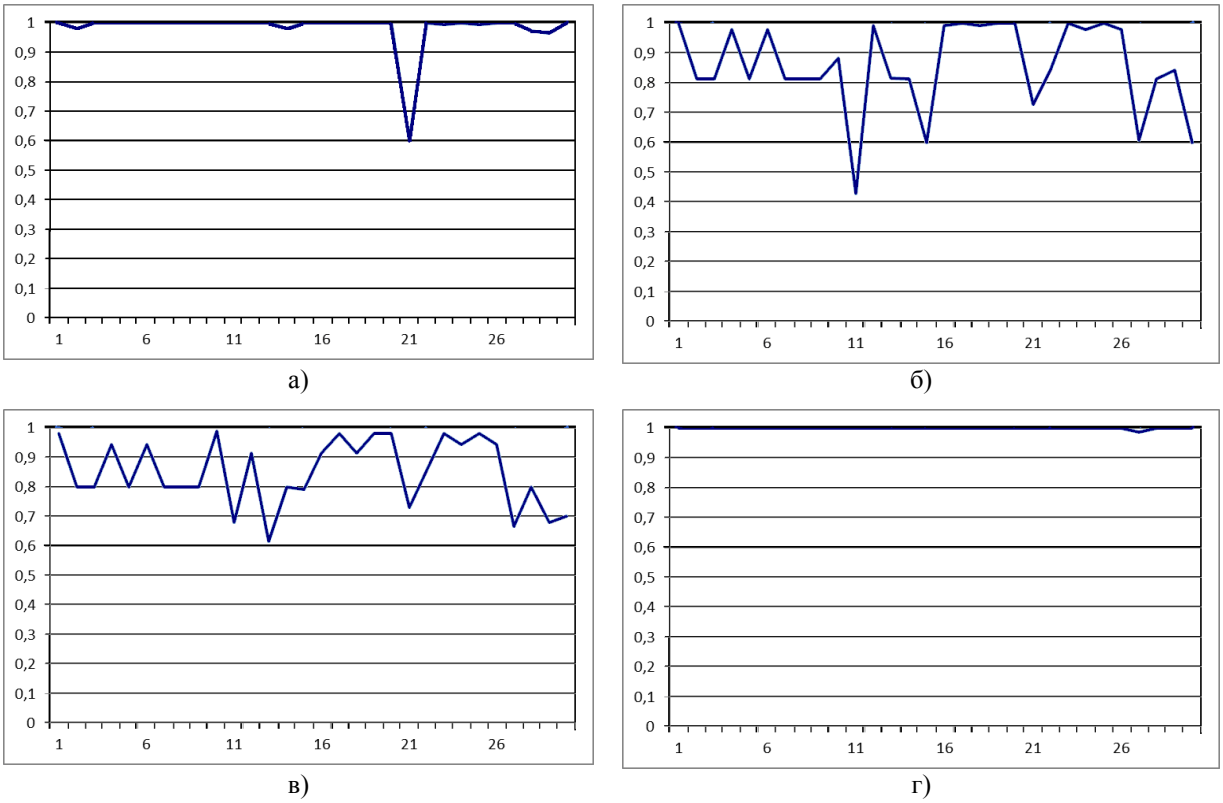


а) б)

Рисунок 2 – Мережі: а) Байєсівський пошук; б) PC алгоритм

При побудові байєсових мереж та їх навчанні було використано програмне забезпечення Genie версії 2.0, що дає можливість визначати змінні та зв’язки між ними, проводити навчання параметрів та структури мережі, а також робити ймовірнісні висновки на основі отриманих даних.

Як видно із згенерованих мереж (рис. 2 а та рис. 2 б), між змінними існує складніша залежність ніж це було задано експертним методом, рис. 1. Виділимо деякі особливості. Необхідно зауважити, що атаки на цілісність призводять до порушення конфіденційності та доступності, що ніяк не відображено в експертній моделі. Також варто зазначити, що майже 75 % атак з локальної мережі призводять до порушення доступності, в той час як з віддаленої мережі тільки 45 %. Атаки, які прості в реалізації приносять, більшість збитків (де необхідна підготовка зловмисника – низька).



а) б)

в) г)

Рисунок 3 – Ймовірність коректного визначення загрози (похибки 2-го роду) для мереж навчених PC алгоритмом (а), наївним байєсівським класифікатором (б), Байєсівським пошуком (в) та EM-алгоритмом

Подальший аналіз отриманих мереж проведено на тестовій вибірці в 60 записів, що не приймали участі в навчанні. Перші 30 записів – це коректні дані, для перевірки пропуску наявної загрози (помилка 2го роду), інші 30 – для перевірки помилкового спрацювання (помилка 1го роду).

На рис.4 та рис. 5 подано помилки 2го та 1го роду відповідно. Найбільш ефективними виявилися РС та ЕМ алгоритми, які більш ніж з 95% точністю вірно визначали ймовірність реалізації загрози.

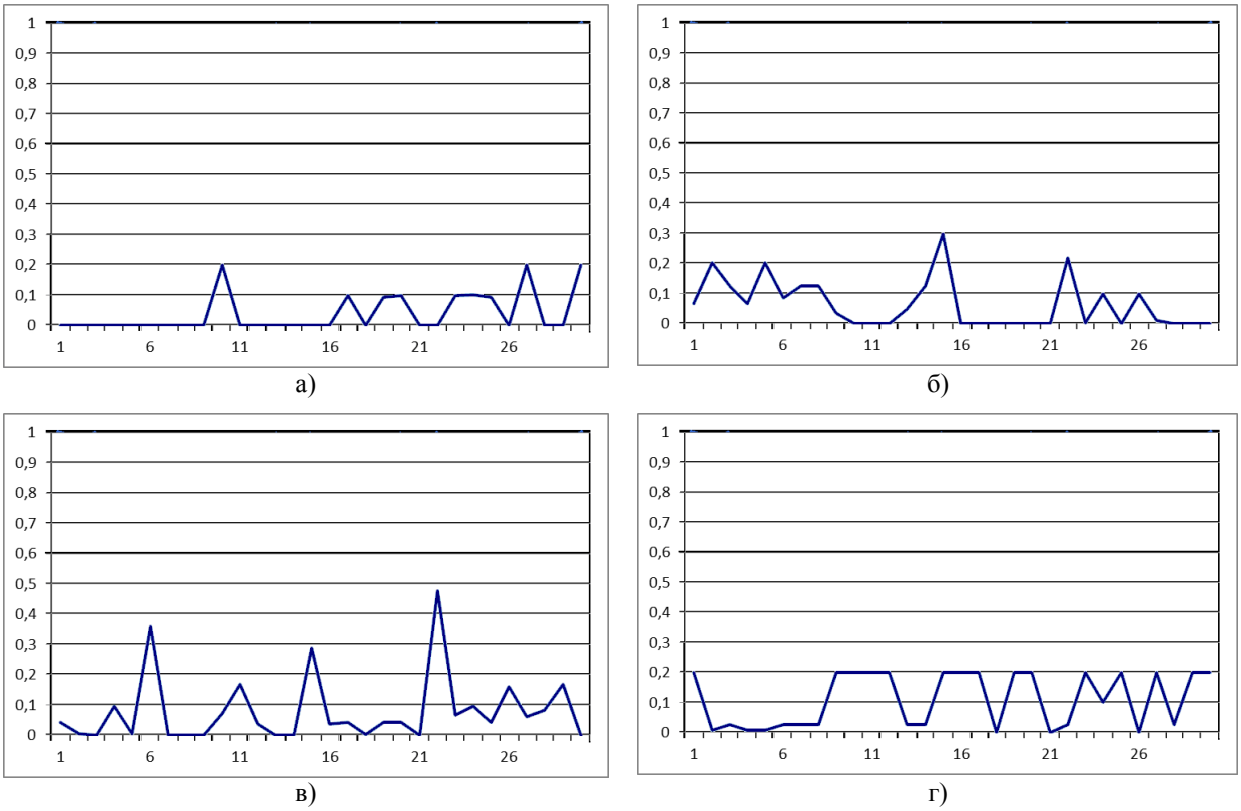


Рисунок 4 – Помилки 1-го роду для мереж навчених РС алгоритмом (а), наївним байєсівським класифікатором (б), Байєсівським пошуком (в) та ЕМ-алгоритмом (г)

В таблиці 2 наведено порівняння ефективності алгоритмів навчання мережі.

Таблиця 2 – Зведена таблиця порівняння алгоритмів навчання Байєсівської мережі для прогнозування ймовірності реалізації загроз

	ЕМ алгоритм	РС алгоритм	Байєсівський пошук	Наївний класифікатор
Помилка 1го роду	0,11	0,04	0,08	0,06
Помилка 2го роду	0,01	0,02	0,15	0,14
Загальна точність	0,97	0,95	0,83	0,83

В результаті виконаної роботи отримано Байєсову мережу для моделювання загроз, що дає можливість прогнозувати ймовірність виникнення тих чи інших загроз безпеки при заданих особливостях навколишнього середовища та вказаних характеристиках зловмисника.

Висновки

На основі проведеного аналізу методів побудови моделей зловмисника та загроз, обгрунтовано ефективність застосування апарату байєсівських мереж.

Розроблено байєсівську мережу прогнозування загроз в ІКС, що оперує множиною випадкових змінних та визначає ймовірність реалізації загроз при заданих умовах. Для підвищення ефективності прогнозування проведено навчання параметрів мережі за ЕМ-алгоритмом на основі наявних статистичних даних. Також створено альтернативні мережі завдяки оцінюванню структури мережі за трьома різними алгоритмами.

Ефективність розроблених моделей перевірено на тестових вибірках, що не приймали участь в навчанні. Отримані результати свідчать про доцільність використанні ЕМ та РС алгоритмів для отримання високоякісного результату розпізнавання загроз.

Подальший розвиток роботи передбачає розширення моделі, шляхом введення додаткових критеріїв та факторів, що впливають на виникнення загрози ІБ.

Список літератури

1. Ю.В. Тюменцев Научная сессия МИФИ-2003. V Всероссийская научно-техническая конференция "Нейроинформатика-2003": лекции по нейроинформатике. Часть 1. - М.: МИФИ, 2003. - 188с.
2. М.В. Грайворонський, О.М. Новіков Безпека інформаційно-комунікаційних систем. – Київ.: BHV, 2009. – 608 с.
3. В.В. Глушак, О.М. Новіков Метод проектування систем захисту інформації з використанням детермінованої гри «захисник-зловмисник». // Наукові вісті НТУУ «КПІ». – 2011. – №2. – С. 46-53.
4. Новіков О.М., Родіонов А.М. Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем // Інформаційні технології та комп`ютерна інженерія. – 2008. – № 1 (11). – С. 170-175.
5. Новиков А., Тимошенко А. Определение множества механизмов защиты, обеспечивающих оптимальный уровень защищенности информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2002. – Вип. 4. – с.98-105.
6. Бідюк П.І. Аналіз ефективності функціонування мережі Байєса [електронний ресурс]. / П.І. Бідюк, В.І. Литвиненко, А.В. Кроптя // ААЭКС Моделирование объектов и систем управления. – 2007. - №2 (20). – Режим доступу: http://aaecs.org
7. Cooper G. F. The computational complexity of probabilistic inference using Bayesian belief networks // Artificial Intelligence. 1990. – 42, (2-3). – pp. 393-405
8. David Heckerman A Tutorial on Learning With Bayesian Networks // Tecnical Report. – Redmond: Microsoft Research. – 1995. – 58p.
9. Denver Dash, Marek J. Druzdzel A Hybrid Anytime Algorithm for the Construction of Causal Models From Sparse Data. – Proceedings of the Fifteenth Annual Conference on Uncertainty in Artificial Intelligence (UAI-99), pages 142-149, Morgan Kaufmann Publishers, Inc., San Francisco, CA, 1999.

Відомості про авторів

Глушак Володимир Володимирович – аспірант, асистент кафедри Інформаційної безпеки ФТІ НТУУ «КПІ». Адреса: м. Київ, вул. Пугачова 19а, кв. 4. Телефон: (068)373-5374, e-mail: vglushak@gmail.com.

Новіков Олексій Миколайович - доктор технічних наук, професор, директор ФТІ НТУУ «КПІ». Адреса: 03056, м. Київ, пр. Перемоги 37, корпус №1, 3 поверх, кім. 308-1. Телефон: (044)236-7098.