УДК 004.9

О. М. ЯШИНА

Хмельницький національний університет, м. Хмельницький

СТРУКТУРНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ТОРГІВЕЛЬНОЇ МЕРЕЖІ СУПЕРМАРКЕТУ

Анотація. В даній статті обґрунтована структурна схема моделі ієрархічного рольового управління доступом до інформаційної системи торгівельної мережі супермаркету. Запропоновано аналітичний опис процесу управління доступом до інформаційних ресурсів торгівельної мережі супермаркету.

Ключові слова: ієрархічне рольове управління доступом, розподілена структура інформаційної мережі, система безпеки інформаційної мережі, атрибути керування доступом.

Аннотация. В статье обоснована структурная схема модели иерархического ролевого управления доступом к информационной системе торговой сети супермаркета. Предложено аналитическое описание процесса управления доступом к информационным ресурсам торговой сети супермаркета.

Ключевые слова: иерархическое ролевое управление доступом, распределенная структура информационной сети, система безопасности информационной сети, атрибуты управления доступом.

Abstract. In this article a model structural scheme of hierarchical role management access to information system of trading supermarket network has been grounded. The analytical description of the management access process to information resources of trading supermarket network has been offered.

Keywords: information system, hierarchical role management access, divided structure of information network system, safety system of information network, attribute of access control.

Вступ

Розвиток сучасних підприємств різноманітних сфер економіки, як правило, супроводжується синтезом корпоративних інформаційно-комунікаційних мереж, функціонування яких ґрунтується на використанні сучасних інформаційних технологій. Одним із завдань щодо сталого (безпечного з точки зору захисту інформації) функціонування інформаційно-комунікаційних мереж (ІКМ) вважається контроль і управління за доступом до баз даних та інформації, що в них міститься.

На сьогодні відома значна кількість робіт, що присвячені розробці інформаційних технологій забезпечення безпеки та управління доступом до інформаційних мереж (систем) [1,2]. Як на думку автора, управління доступом до інформаційних систем (ІС) сучасних торгівельних мереж супермаркетів доцільно організувати з використанням смарт-технологій [2]. Однак, наукових робіт, присвячених застосуванню смарт-технологій для ідентифікації користувачів інформаційних систем торгівельних мереж недостатньо. Так в роботах Фороузана Б.А., Шнайера Б., Шоріна Д.В., Шкурка М.І., Борисенка О.В., Стасенка Л., Кулікова А.Л. та інш. висвітлені окремі аспекти застосування як криптографії, так і смарт-технологій для забезпечення інформаційної безпеки інформаційних систем загального, або конкретного призначення, що ускладнює їх використання для управління доступом до ІС торговельних мереж супермаркетів [3,4]. Це пов’язано із необхідністю врахування специфіки функціонування ІС торговельної мережі супермаркету, а саме: обсягів інформації, що в них утримується, а також особливості її утримання, оновлення, циркуляції, що в свою чергу обумовлює особливості допуску до цієї інформації.

Усі ключові бізнес-процеси в торгівельній мережі, такі як фінансовий і бухгалтерський облік, управління кадрами, клієнтами, товаром і складом, документообіг, автоматизуються відповідним класом систем. Процес впровадження великої кількості інформаційних систем, при всій їх незаперечній корисності, несе в собі нові витрати і ризики для торгівельної мережі. Обов'язковою умовою високої конкурентоспроможності супермаркету стає захист інформації.

У таких умовах надання доступу до інформаційних систем тільки уповноваженим співробітникам – одна з найважливіших завдань ІТ та підрозділів служб безпеки. Основний крок у вирішенні даного завдання – побудова системи надійної аутентифікації користувачів. Класичний спосіб аутентифікації з використанням статичного пароля не забезпечує адекватного рівня захисту [2]. Необхідно використання сучасних надійних технологій. Застосування технологій строгої аутентифікації є фундаментом для побудови надійних і безпечних систем управління доступом.

Таким чином, викладене вище обумовлює необхідність синтезу інформаційної технології управління доступом до інформаційної системи торгівельної мережі супермаркету, що являє собою актуальне науково-прикладне завдання.

Відомо, що управління доступом до інформаційних ресурсів направлено на забезпечення політики інформаційної безпеки шляхом встановлення порядку доступу суб’єктів до відповідних баз даних. Для встановлення порядку та пріоритетів доступу до інформаційної мережі (ІМ) супермаркету наочна необхідність обґрунтування структури ІС торгівельної мережі та відповідної структури управління

доступом до її баз даних з урахуванням ієрархічного розподілу функцій персоналу (рольового управління). Наявність таких структур відкриє можливість аналітичного опису процесу управління доступом до ІС торговельних мереж і синтезу математичної моделі доступу. Сутність математичної моделі управління доступом до ІС торговельних мереж полягає в формальному визначенні безпеки системи при певних умовах і обґрунтуванні кількісної міри безпеки. При цьому слід відмітити, що математична модель управління доступом повинна адаптивно відображувати стан всієї ІС торгівельної мережі, її переходи з одного стану в інший, реакцію на зовнішні та внутрішні впливи, а також визначати безпечні стани і переходи впродовж управління доступом до інформаційних ресурсів системи.

Метою статті є обґрунтування структури ІС торгівельної мережі та відповідної їй структурної схеми ієрархічного, рольового управління доступом. Побудова математичної моделі управління доступом до ІС торгівельної мережі супермаркету у вигляді множинно-формалізованого опису процедури управління доступом до інформаційних ресурсів та обґрунтуванні рівня безпеки.

Результати дослідження

Зазвичай у структурі підрозділів торгівельної мережі супермаркету притаманна ієрархічна побудова, що обумовлює розподілену структуру її інформаційної системи, як це показано на рис.1.

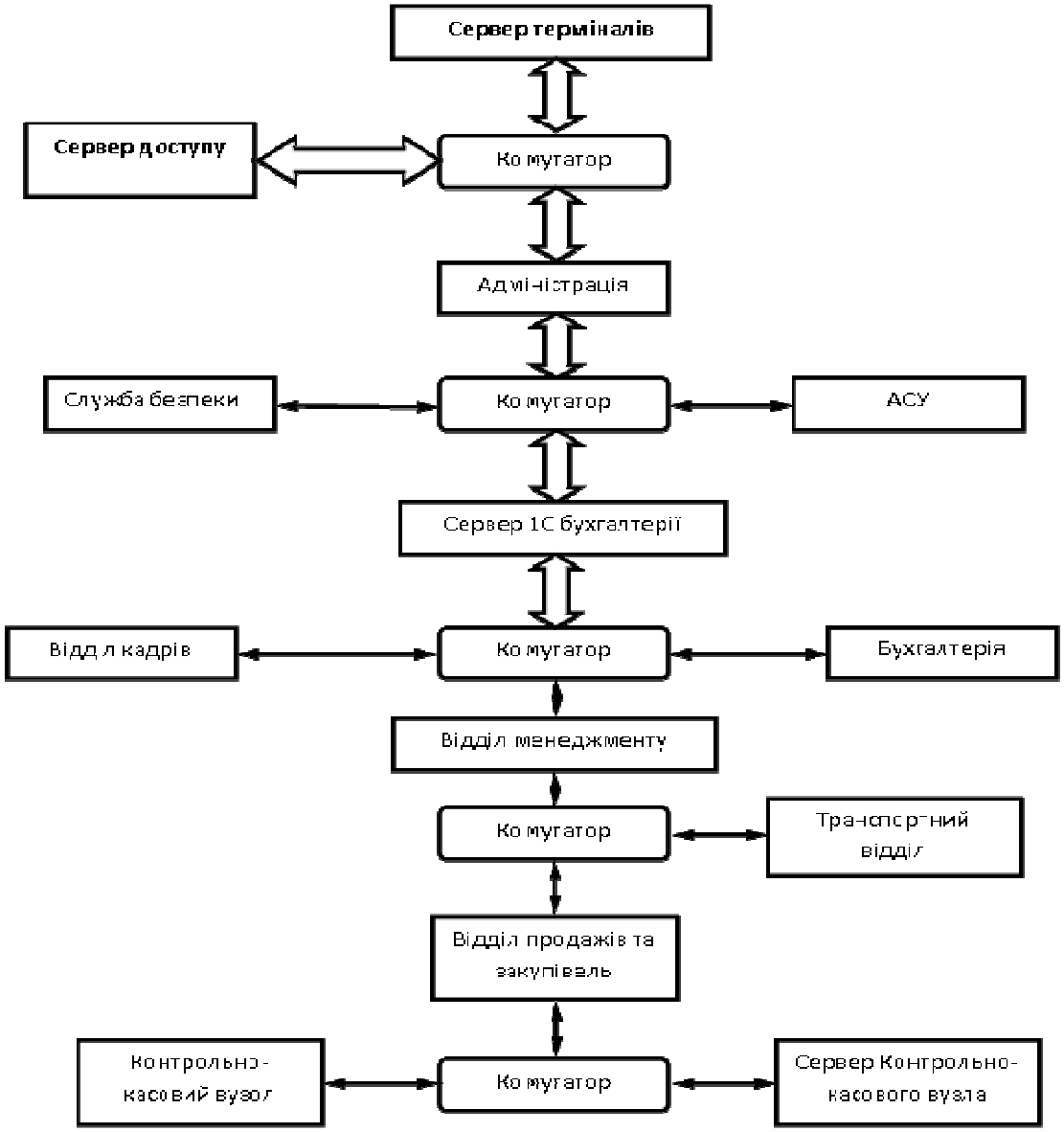

Рисунок 1 – Структурна схема розподіленої інформаційної системи торгівельної мережі супермаркету

У відповідності зі встановленими організаційно-управлінськими відносинами та заданою політикою безпеки ІС торгівельної мережі супермаркету (ТМСМ) користувачам надаються деякі види прав доступу

до даних свого підрозділу, що визначаються функціональними та посадовими обов’язками. При цьому співробітники вищої ланки по організаційно-штатній структурі підрозділів повинні мати доступ до даних підлеглих нижчої ланки. Разом з тим співробітники нижчої ланки не повинні отримувати права доступу до даних вищої ланки та топ-менеджерів. Отже, у відповідності із вимогами політики безпеки управління доступом до відповідних баз даних, надання прав доступу залежить від рівня сутностей в ієрархії ІС торгівельної мережі супермаркету.

Припустимо, що торгівельна мережа, а саме інформаційна система в цій мережі має деревовидну ієрархічну структуру (як це показано на рис.1) і для кожної сутності визначений певний рівень ієрархії. Така побудова дає підстави розглядати рівень ієрархії сутності якості одного з атрибутів, що використовуються при керуванні доступом. На основі цього атрибуту визначена політика управління доступом до системи: призначення всім сутностям рівнів ієрархії у відповідності зі структурою інформаційної системи та надання суб’єкту права доступу до сутності тільки в тому випадку, якщо рівень ієрархії суб’єкта не менший рівня ієрархії сутності (на множині ієрархій сутностей повинна бути задана верхня напіврешітка [5].

Враховуючи основні вимоги управління доступом до інформаційної системи ТМСК запропоновано ієрархічну структуру рольового управління доступом у вигляді рис.2.

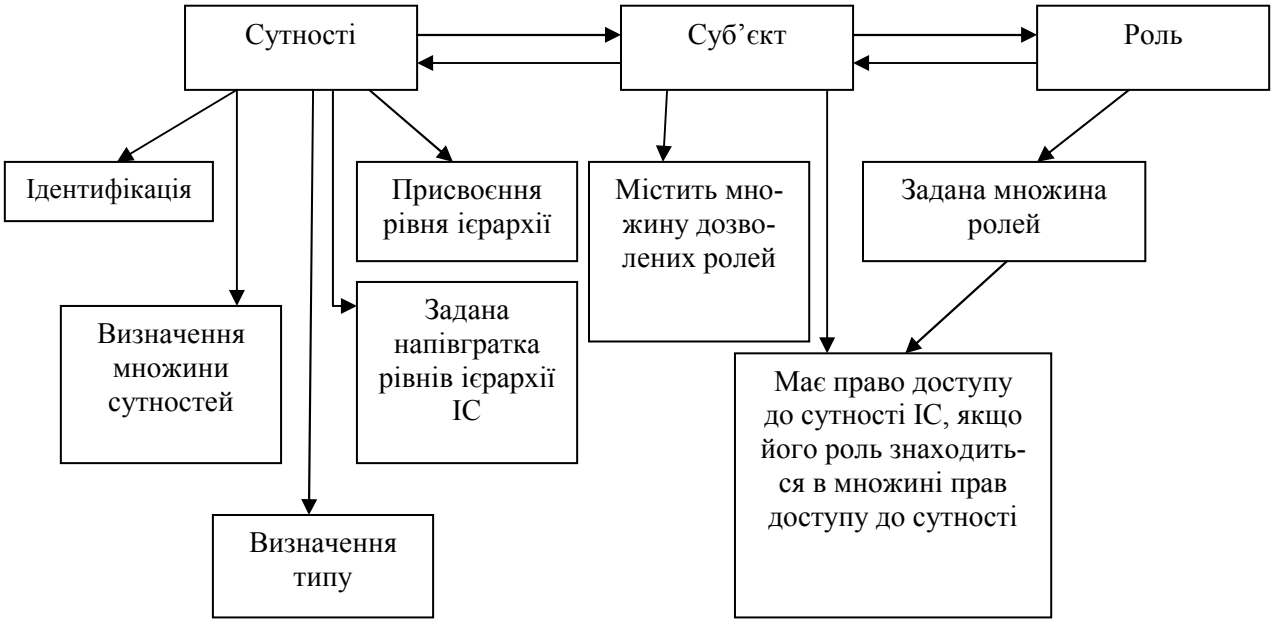

Рисунок 2 – Структура інформаційної технології ієрархічного рольового управління доступом до ІС торгівельної мережі

Для побудови формальних моделей інформаційна система, як правило, представляється у вигляді сукупності взаємодіючих сутностей – суб’єктів (S) та об’єктів (O). Суб’єкт безпеки – активна системна складова, до якої застосовується політика безпеки, а об’єкт – пасивна. Користувачі, данні, файли, системні таблиці, периферійні пристрої – це суб’єкти. З точки зору формалізованого подання інформаційної технології управління доступом (ІТУД) в даній роботі під суб’єктами слід розуміти підмножину сукупності об’єктів. На практиці реалізація політики безпеки (ПБ) інформаційної системи ТМСМ полягає у присвоєнні суб’єктам та об’єктам ідентифікаторів та фіксації набору правил, що дозволяють визначити дозвіл даного суб’єкта на авторизацію, достатню для надання до певного об’єкту вказаного типу доступу.

Модель, що описує політику ієрархічного рольового управління доступом до інформаційної системи торгівельної мережі є ієрархічною рольовою моделлю управління доступом та позначається RBAC-M. Основними елементами цієї моделі, згідно із [5,6,7], слід вважати:

$E = O \cup C$ – множина сутностей, де O – множина суб’єктів, C – множина об’єктів та $O \cap C = \varnothing$;

U – множина користувачів, при цьому користувачі не є сутностями $(U \cap E = \varnothing)$;

$S \subseteq E$ – множина суб’єкт-сесій користувачів;

T – множина типів сутностей;

L – множина рівнів ієрархії сутностей;

R_1 – множина видів прав доступу;

R – множина ролей.

Згідно із [5] отримаємо:

$P \subseteq (R_r \times T) \cup (R_r \times E)$ – множина прав доступу до всіх сутностей одного типу та окремих сутностей;

$PA : R \to 2^P$ – функція прав доступу ролей, що задає для кожної ролі множину прав доступу до сутностей, при цьому для кожного права доступу $p \in P$ існує роль $r \in R$, при якій виконується умова $p \in PA(r)$;

$UA : U \to 2^R$ – функція авторизованих ролей користувачів, що задає для кожного користувача множину ролей, на які він може бути авторизований;

$type : E \to T$ – функція типів сутностей;

$f_c E \to L$ – функція, що задає рівень ієрархії кожної сутності;

$user : S \to U$ – функція приналежності суб'єкт-сесії користувачу, що задає для кожної суб'єкт-сесії користувачі, від імені якого вона авторизована;

$roles : S \to 2^R$ – дана функція задає для користувача множину ролей, на які він авторизований поточній сесії, при цьому в кожному стані комп'ютерної системи для кожної суб'єкт-сесії $s \in S$ виконується умова $roles(s) \subseteq U\ A(user(s))$.

Введемо ще одне значення X, яке будемо називати розбиттям множини E у відповідності із заданою ієрархією сутностей, при цьому $|X| = |L|$. Доменом d сутностей множини E будемо називати будь-який клас із X. Ієрархією доменів назвемо задане на множині X відношення часткового порядку $\leq$, що задовольняє таким вимогам:

– якщо для $d \in X$ існують $d_1, d_2 \in X$, такі, що $d \leq d_1, d \leq d_2, mo\ d_1 \leq d_2\ або\ d_2 \leq d_1$;

в X існує найбільший елемент.

описана ієрархія доменів відповідає ІС із ієрархічною деревовидною структурою, що відображає організаційно-управлінські відносини, та задаю верхню напіврешітку ($X, \leq$).

Нехай L – задана множина рівнів ієрархії сутностей та існує бієктивне відображення X на L [8]. Визначимо на множині L відношення часткового порядку $\leq$, де для будь-яких $l_1, l_2 \in L$ буде вірним вираз тоді і тільки тоді, коли для відповідних $d_1, d_2 \in X$ тоді $(L, \leq)$ – верхня напіврешітка рівнів ієрархії сутностей.

Будемо вважати, що множини U, X, T, L, P, R, R_r та функції не змінюються з часом.

Нехай є множини $E, S, X, U, T, L, P, R, R_r$, функції $PA, UA, type, user, roles, (L, \leq)$ – напіврешітка рівнів ієрархії. Визначимо предикат $can\_access(s, e, p)$, що істинний тоді і тільки тоді, коли виконується такі умови:

1) $f_e(e) \leq f_e(s)$;

2) $(p, type(e)) \in PA(roles(s))$.

Будемо вважати, що в ІС реалізовано рольове управління доступом RBAC-M, якщо будь-яка суб'єкт-сесія $s \in S$ користувача $user(s) \in U$ може мати право доступу $p \in R_r$, тоді і тільки тоді коли істинним є предикат $can\_access(s, e, p)$.

Одним із важливих механізмів сімейства моделей управління доступом є обмеження , що накладаються на множину ролей, на які може бути авторизований користувач або на які він авторизується протягом однієї сесії. Основні обмеження, визначені в рамках моделей рольового управління доступом сімейства RBAC можуть бути перенесені у запропоновану модель. Разом з тим для більшої відповідності ієрархічного управління доступом процедурам обробки даних, що використовуються у торгівельній мережі необхідно визначити нові види обмежень, суттєві саме для даного виду управління доступом.

Визначимо функцію $h : E \to X$, таку, що $h(e) = d$, якщо $e \in d, e \in E$ та $d \in X$.

В моделі RBAC-M задано обмеження на область доступу користувача в ієрархії сутностей при виконання таких умов:

1. Визначена функція $UD : U \to 2^X$.

2. Для будь-яких $s \in S, e \in E, p \in R_r$, якщо предикат $can\_access(s, e, p)$ та $user(s) = u$, то $h(e) \in UD(u)$.

Будемо вважати, що в моделі RBAC-M задані обмеження на область авторизації ролей в ієрархії сутностей, якщо виконуються такі умови:

визначено функцію $RD: R \to 2^X$;

для будь-яких $s \in S, e \in E, p \in R_r$, якщо є істинним предикат $can\_access(s, e, p)$ та $r \in roles(s), mo\,h(c) \in RD(r)$.

Будемо вважати також, що в моделі RBAC-M задані обмеження на область застосування прав доступу в ієрархії сутностей, якщо виконуються такі вимоги:

визначена функція $URD: U \times R \to 2^X$.

для будь-яких $s \in S, e \in E, p \in R_r$, якщо є істинним предикат $can\_access(s, e, p)$, $user(s) = u,\ r \in roles(s),\ mo\,h(e) \in URD(u, r)$.

Будемо вважати, що в моделі RBAC-M задані обмеження на область застосування прав доступу в ієрархії сутностей, якщо виконуються наступні вимоги:

визначена функція $PD: P \to 2^X$;

для будь-яких $s \in S, e \in E, p \in R_r$ якщо є істинним предикат $can\_access(s, e, p)$, то $h(e) \in PD(p)$.

Вважатимемо, що в моделі RBAC-M задані обмеження на область доступу до типу сутностей в ієрархії сутностей, якщо виконуються такі умови:

визначена функція $TD: T \to 2^X$;

для будь-яких $s \in S, e \in E, p \in R_r$ якщо істинним є предикат $can\_access(s, e, p)$, то $h(c) \in TD(type(c))$.

Отже, загальна структура моделі ієрархічного рольового управління доступом торгівельної мережі матиме вигляд, як це показано на рисунку 3.

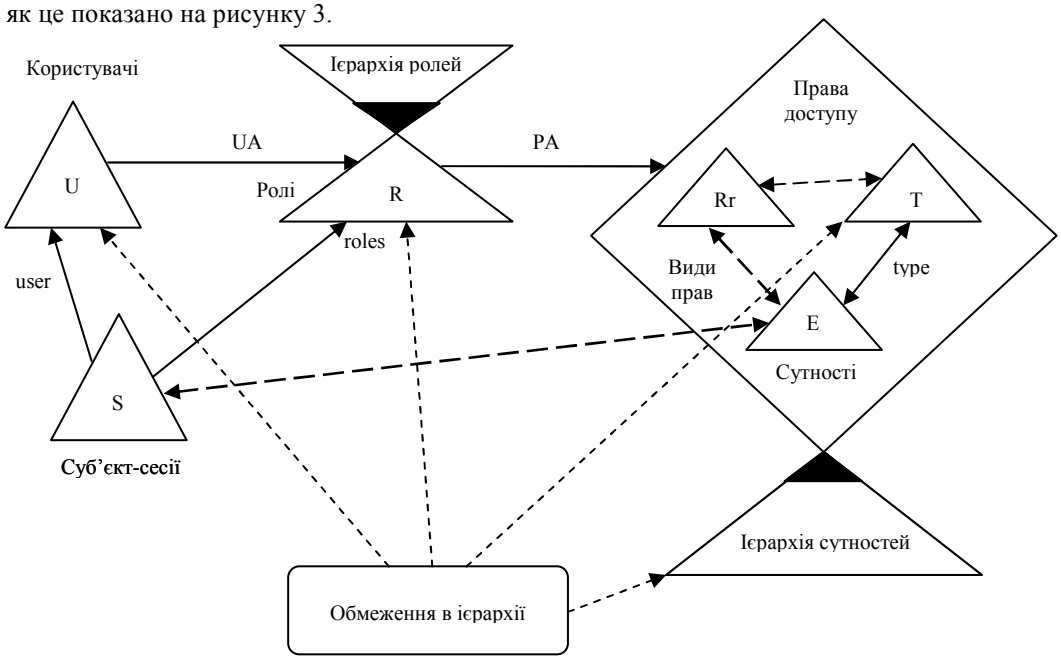

Рисунок 3 – Модель ієрархічного рольового управління доступом до ІС торгівельної мережі

Висновки

На підставі обґрунтованих структурної схеми розподіленої інформаційної системи торгівельної мережі супермаркету та структури інформаційної технології ієрархічного рольового доступу до інформаційної системи торгівельної мережі проведено формалізований опис політики безпеки доступу до відповідної інформаційної системи.

Встановлено, що для інформаційної системи, яка характеризується ієрархією сутностей, адекватною математичною моделлю керування доступом слід вважати рольову модель керування доступом виду RBAC-M. Саме така модель здатна відобразити встановлені організаційно-управлінські відносини, що реалізуються в інформаційних системах торгівельних мереж супермаркетів. При цьому запропоновані атрибути ієрархії інформаційної

системи торгівельної мережі та типи сутностей до елементів моделей RBAC, що дозволяє адаптувати їх до умов функціонування ІС торгівельних мереж. Це в свою чергу спрощує реалізацію рольового управління доступом до ІС торгівельних мереж та відкриває можливість апаратно-програмної реалізації інформаційної технології процесу керування доступом до ІС торгівельної мережі.

Література

1. Куликов А. Л. Информационная система университета с управлением приоритетами доступа к ресурсам на основе СМАРТ-технологий: Дис. ... канд. техн. наук: 05.13.10: Астрахань, 2005. – 197 с.
2. Шинкарук О.М., Яшина О.М. Використання смарт-карт для ідентифікації користувачів інформаційних систем. // Вісник Хмельницького національного університету. Хмельницький: ХНУ. – №1, 2013. С.114-116.
3. Фороузан Б. А. Математика криптографии и теория шифрования информация. Режим доступу – http://www.intuit.ru/department/security/mathcryptet/14/3.html.
4. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с.
5. Колегов Д.Н. Построение иерархического ролевого управления доступом // Математические основы компьютерной безопасности: ТГУ. – №3(17), 2012. С.71-76.
6. Девянин П. Н. Формирование словаря терминов теории моделирования безопасности управления доступом и информационными потоками в компьютерных системах // Прикладная дискретная математика. 2011. №2. С. 17-39.
7. Коньков А.К. Разработка и реализация моделей защищенности в рабочих группах и доменах Windows. [Электронный ресурс]: дис. …канд. тех. наук: 05.13.18. – М.:РГБ, 2007.
8. Ершов Ю. Л., Палютин Е. А. Математическая логика: Учебное пособие. – 3-е, стереотип. изд. – СПб.: «Лань», 2004 – 336 с.

Стаття надійшла: 14.02.2014.

Інформація про автора

Яшина Оксана Миколаївна – ст. викладач кафедри програмної інженерії, аспірант Хмельницького національного університету.