УДК 681.3:519.872

В.А. Козачок, М.В. Діхтяр, О.В. Семко

ОСОБЛИВОСТІ ІДЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ В СУЧАСНИХ КОРПОРАТИВНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В статті розглянуто особливості ідентифікації та авторизації в сучасних корпоративних інформаційно-телекомунікаційних системах. Обгрунтована необхідність створення систем ідентифікації та авторизації в корпоративних інформаційно-телекомунікаційних системах. Розглянуті сучасні засоби ідентифікації/автонтефікації. Обгрунтована стратегія ідентифікації та авторизації в інформаційно-телекомунікаційних ситемах. Показана необхідність використання прогресивних та перспективних технологій інформаційної безпеки.

Ключові слова: Корпоративна інформаційно-комунікаційна система, система ідентифікації та авторизації в інформаційно-телекомунікаційних ситемах, характеристика об'єктів захисту

Постановка проблеми.

Необхідність створення комплексних систем захисту інформації визначається законодавчими та нормативними вимогами [1, 2, 3].

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.

Актуальність питання полягає в особливостях, які притаманні корпоративним інформаційно-телекомунікаційним системам, а саме: велика кількість споживачів; велика різноманітність вирішуємих завдань та наявність розгалужених зв'язків.

Аналіз останніх досліджень та публікацій. В [1, 2, 3, 5] регламентовані загальні вимоги щодо необхідності створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. Основні концептуальні питання інформаційної безпеки викладені в [4]. На теперішній час, нажаль, недостатньо приділяється уваги питанням ідентифікації та авторизації в сучасних розподілених корпоративних мережах.

Метою статті є розробка стратегії ідентифікації та авторизації в сучасних інформаційно-комунікаційних системах.

Виклад основного матеріалу.

При виборі стратегії авторизації та автонтифікації для інформаційних сервісів компанії, слід представляти принципові відмінності технологій і їх реалізацій в плані адекватності розв'язуваної задачі. Ввівши три основних критерії, які дозволяють розрізняти технології аутентифікації - рівень безпеки, зручність використання і вартісні параметри, можна розглянути "трикутник" технологій аутентифікації [6] (рис. 1)

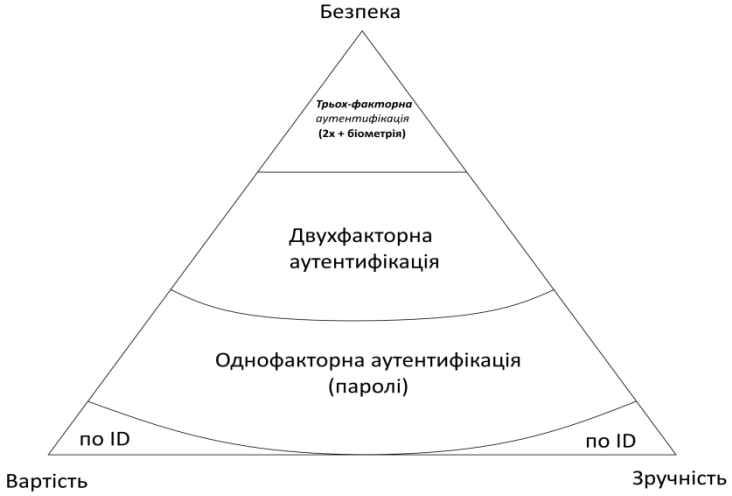

Рис.1. Трикутник технологій аутентифікації

Видно, що немає одночасно безкоштовних, прозорих для користувача і абсолютно надійних технологій. Кожна займає своє місце на діаграмі.

Інформаційна інфраструктура компанії перестала бути суто внутрішньою. IT-інфраструктури відділень компанії і навіть різних компаній стають все більш пов'язаними між собою. Повноваження делегуються на місця, посилюються вимоги до гнучкості та віддалених робочих місць, відбувається надання доступу до інформаційних систем для клієнтів і постачальників.

Компанії часто віддають на субпідряд зовнішнім фірмам завдання непрофільного бізнесу - HR, Call Center, логістику. У зв'язку з цим, питання ідентифікації стає дуже важливим для забезпечення інформаційної безпеки. Контроль доступу, шифрування, міжмережеві екрани, VPN - все засновано на аутентифікації користувача, пристрою або програми, з яким встановлюється з'єднання, і якщо вона має недоліки, то перераховані засоби захисту втрачають свою доцільність.

Ідентифікацію та аутентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація та аутентифікація - це перша лінія оборони, "прохідна" інформаційного простору організації. Ідентифікація дозволяє суб'єкту (користувачеві, процесу, що діє від імені певного користувача, чи іншого апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "аутентифікація" іноді використовують словосполучення "перевірка справжності". Аутентифікація буває односторонньою (зазвичай клієнт доводить свою справжність серверу) і двосторонньою (взаємною). Приклад односторонньої аутентифікації - процедура входу користувача в систему. В мережевому середовищі, коли сторони ідентифікації/аутентифікації територіально рознесені, у розглянутого сервісу є два основних аспекти [6]:

- що служить аутентифікатором (тобто використовується для підтвердження автентичності суб'єкта);
- як організований (і захищений) обмін даними ідентифікації/аутентифікації.

Суб'єкт може підтвердити свою автентичність, пред'явивши принаймні одну з наступних сутностей:

- щось, що він знає (пароль, особистий ідентифікаційний номер, криптографічний ключ і т.ін.);
- щось, чим він володіє (особисту картку або інший пристрій аналогічного призначення);
- щось, що є частина його самого (голос, відбитки пальців і т.ін., тобто свої біометричні характеристики).

У відкритому мережевому середовищі між сторонами ідентифікації/аутентифікації не існує довіреного маршруту; це означає, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманими і використаними для перевірки автентичності. Необхідно забезпечити захист від пасивного і активного прослуховування мережі, тобто від перехоплення, зміни та/або відтворення даних. Передача паролів у відкритому вигляді, очевидно, є незадовільною; не рятує становище і шифрування паролів, так як воно не захищає від відтворення. Потрібні більш складні протоколи аутентифікації.

Надійна ідентифікація ускладнена не тільки через мережевиі загрози, а й по цілому ряду причин. По-перше, майже всі аутентифікаційні сутності можна дізнатися, вкрасти або підробити. По-друге, є протиріччя між надійністю аутентифікації, з одного боку, і зручностями користувача і системного адміністратора з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити аутентифікаційну інформацію (адже на його місце могла сісти інша людина), а це не тільки клопітно, але і підвищує ймовірність того, що хтось може підглянути за введенням даних. По-третє, чим надійніший засіб захисту, тим він дорожче.

Сучасні засоби ідентифікації/аутентифікації повинні підтримувати концепцію єдиного входу в мережу. Єдиний вхід в мережу - це, в першу чергу, вимога зручності для

користувачів. Якщо в корпоративній мережі багато інформаційних сервісів, що допускають незалежне звернення, то багаторазова ідентифікація/аутентифікація стає занадто обтяжливою. На жаль, поки не можна сказати, що єдиний вхід в мережу став нормою, домінуючі рішення поки не сформувалися.

Таким чином, необхідно шукати компроміс між надійністю, доступністю за ціною і зручністю використання й адміністрування засобів ідентифікації і аутентифікації.

Цікаво відзначити, що сервіс ідентифікації/аутентифікації може стати об'єктом атак на доступність. Якщо система налаштована так, що після певного числа невдалих спроб пристрій введення ідентифікаційної інформації (наприклад, термінал) блокується, то зловмисник може зупинити роботу легального користувача буквально декількома натисканнями клавіш.

Головна перевага парольної аутентифікації - простота і звичність. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, за сукупністю характеристик їх слід визнати найслабшим засобом перевірки автентичності.

Щоб пароль запам’ятовувався, його часто роблять простим (ім'я подруги, назва спортивної команди і т.ін.). Однак простий пароль неважко вгадати, особливо якщо знати пристрасті даного користувача. Іноді паролі з самого початку не зберігаються в таємниці, так як мають стандартні значення, зазначені в документації, і далеко не завжди після установки системи проводиться їх зміна. Введення пароля можна підглянути. Іноді для підглядання використовуються навіть оптичні прилади.

Паролі нерідко повідомляють колегам, щоб ті могли, наприклад, підмінити на деякий час власника пароля. Теоретично в подібних випадках більш правильно задіяти засоби управління доступом, але на практиці так ніхто не чинить; а таємниця, яку знають двоє, це вже не таємниця.

Пароль можна вгадати "методом грубої сили", використовуючи, скажімо, словник. Якщо файл паролів зашифрований, але доступний для читання, його можна завантажити до себе на комп'ютер і спробувати підібрати пароль, запрограмувавши повний перебір (передбачається, що алгоритм шифрування відомий). Проте, такі заходи дозволяють значно підвищити надійність парольного захисту:

- накладення технічних обмежень (пароль повинен бути не надто коротким, він повинен містити літери, цифри, знаки пунктуації тощо);
- управління терміном дії паролів, їх періодична зміна;
- обмеження доступу до файлу паролів;
- обмеження числа невдалих спроб входу в систему (це утруднить застосування "методу грубої сили");
- навчання користувачів;
- використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може створювати тільки благозвучні і, отже, не складні для запам’ятання паролі).

Перераховані заходи доцільно застосовувати завжди, навіть якщо разом з паролями використовуються інші методи аутентифікації.

Розглянуті вище паролі можна назвати багаторазовими; їх розкриття дозволяє зловмисникові діяти від імені легального користувача. Набагато більш сильним засобом, стійким до пасивного прослуховування мережі, є одноразові паролі.

Найбільш відомим програмним генератором одноразових паролів є система S/KEY компанії Bellcore. Ідея цієї системи полягає в наступному. Нехай є одностороння функція f (тобто функція, обчислити зворотну якої за прийнятний час не представляється можливим). Ця функція відома і користувачеві, і серверу аутентифікації. Нехай, далі, є секретний ключ K, відомий тільки користувачеві. На етапі початкового адміністрування користувача функція f застосовується до ключу K n раз, після чого результат зберігається на сервері. Після цього процедура перевірки автентичності користувача виглядає наступним чином:

- сервер надсилає на призначену для користувача систему число (n-1);

- користувач застосовує функцію f до секретного ключа K (n-1) раз і відправляє результат по мережі на сервер аутентифікації;

- сервер застосовує функцію f до отриманого від користувача значенням і порівнює результат з раніше збереженої величиною. У разі збігу справжність користувача вважається встановленою, сервер запам'ятовує нове значення (надісланий користувачем) і зменшує на одиницю лічильник (n). Насправді реалізація влаштована трохи складніше (крім лічильника, сервер посилає перевірочне значення, яке використовується функцією f). Оскільки функція f необоротна, перехоплення пароля, так само як і отримання доступу до сервера аутентифікації, не дозволяють дізнатися секретний ключ K і передбачити наступний одноразовий пароль. Система S/KEY має статус Internet-стандарту (RFC 1938).

Інший підхід до надійної аутентифікації складається в генерації нового пароля через невеликий проміжок часу (наприклад, кожні 60 секунд), для чого можуть використовуватися програми або спеціальні інтелектуальні карти (з практичної точки зору такі паролі можна вважати одноразовими). Серверу аутентифікації повинен бути відомий алгоритм генерації паролів і асоційовані з ним параметри; крім того, годинник клієнта і сервера повинні бути синхронізовані.

Біометрія являє собою сукупність автоматизованих методів ідентифікації та/або аутентифікації людей на основі їх фізіологічних і поведінкових характеристик. До числа фізіологічних характеристик належать особливості відбитків пальців, сітківки та рогівки очей, геометрія руки та обличчя тощо [7]. До поведінкових характеристик відносяться динаміка підпису (ручний), стиль роботи з клавіатурою. На стику фізіології і поведінки знаходяться аналіз особливостей голосу і розпізнавання мови.

Біометрією у всьому світі займаються дуже давно, проте довгий час все, що було пов'язано з нею, відрізнялося складністю і великою вартістю. Останнім часом попит на біометричні продукти, в першу чергу в зв'язку з розвитком електронної комерції, постійно і дуже інтенсивно росте. Це зрозуміло, оскільки з точки зору користувача набагато зручніше пред'явити себе самого, ніж щось запам'ятовувати. Попит народжує пропозицію, і на ринку з'являються відносно недорогі апаратно-програмні продукти, орієнтовані в основному на розпізнавання відбитків пальців.

У загальному вигляді робота з біометричними даними організована таким чином. Спочатку створюється і підтримується база даних характеристик потенційних користувачів. Для цього біометричні характеристики користувача знімаються, обробляються, і результат обробки (званий біометричним шаблоном) заноситься в базу даних (вихідні дані, такі як результат сканування пальця або рогівки, як правило, не зберігаються). Надалі для ідентифікації (і одночасно аутентифікації) користувача процес зняття і обробки повторюється, після чого проводиться пошук в базі даних шаблонів. У разі успішного пошуку особистість користувача і її справжність вважаються встановленими. Для аутентифікації досить зробити порівняння з одним біометричним шаблоном, обраним на основі попередньо введених даних.

Зазвичай біометрію застосовують разом з іншими аутентифікаторами, такими, наприклад, як інтелектуальні карти. Іноді біометрична аутентифікація є лише першим рівнем захисту і служить для активізації інтелектуальних карт, що зберігають криптографічні секрети; в такому випадку біометричний шаблон зберігається на тій же карті.

Активність в області біометрії дуже велика. Організовано відповідний консорціум, активно ведуться роботи по стандартизації різних аспектів технології (формату обміну даними, прикладного програмного інтерфейсу і т.ін.), публікується багато рекламних статей, в яких біометрія підноситься як засіб забезпечення найкращого захисту, що став доступним великій кількості користувачів[8].

Необхідно враховувати, що біометрія схильна до тих же загроз, що і інші методи аутентифікації. *По-перше*, біометричний шаблон порівнюється не з результатом первісної обробки характеристик користувача, а з тим, що прийшло до місця порівняння. А, як відомо, за час шляху багато чого може статися. *По-друге*, біометричні методи не більш надійні, ніж

база даних шаблонів. *По-третє*, слід враховувати різницю між застосуванням біометрії на контрольованій території, під пильним оком охорони, і в "польових" умовах, коли, наприклад до пристрою сканування рогівки можуть піднести муляж і т.ін. *По-четверте*, біометричні дані людини змінюються, так що база шаблонів потребує супроводу, що створює певні проблеми і для користувачів, і для адміністраторів.

Але головна небезпека полягає в тому, що будь-яка "пробоїна" для біометрії виявляється фатальною. Паролі, при всій їх ненадійності, в крайньому випадку можна змінити. Загублену аутентифікаційну карту можна анулювати і завести нову. Відбиток пальця, "малюнок" очей або голос змінити не можна. Якщо біометричні дані виявляться скомпрометовані, доведеться як мінімум проводити істотну модернізацію всієї системи.

З традиційної точки зору засоби управління доступом дозволяють специфікувати і контролювати дії, які суб'єкти (користувачі і процеси) можуть виконувати над об'єктами (інформацією та іншими комп'ютерними ресурсами).

Логічне управління доступом - це основний механізм багатокористувацьких систем, покликаний забезпечити конфіденційність і цілісність об'єктів і, до певної міри, їх доступність (шляхом заборони обслуговування неавторизованих користувачів).

Розглянемо формальну постановку задачі в традиційному трактуванні. Є сукупність суб'єктів і набір об'єктів. Завдання логічного управління доступом полягає в тому, щоб для кожної пари "суб'єкт-об'єкт" визначити безліч допустимих операцій (що можливо залежить від деяких додаткових умов) і контролювати виконання встановленого порядку.

Відношення "суб'єкти-об'єкти" можна представити у вигляді матриці доступу, в рядках якої перераховані суб'єкти, в стовбцях - об'єкти, а в клітинах, розташованих на перетині рядків і стовпців, записані додаткові умови (наприклад, час і місце дії) і дозволені види доступу . Фрагмент матриці може виглядати, наприклад, так [9]:

	Файл	Програма	Зв'язок	Реляційна таблиця
Користувач №1	orw з системної консолі	e	rw з 08:00 до 18:00	
Користувач №2				a

"o" - позначує дозвіл на передачу прав доступу іншим користувачам

"r" - зчитування

"w" - запис

"e" - виконання

"a" - додавання інформації

Тема логічного управління доступом - одна з найскладніших в області інформаційної безпеки. Справа в тому, що саме поняття об'єкта (а тим більше видів доступу) змінюється від сервісу до сервісу. Для операційної системи до об'єктів відносяться файли, пристрої та процеси. Стосовно до файлів і пристроїв зазвичай розглядаються права на читання, запис, виконання (для програмних файлів), іноді на видалення та додавання. Окремим правом може бути можливість передачі повноважень доступу іншим суб'єктам (так зване право володіння). Процеси можна створювати і знищувати. Сучасні операційні системи можуть підтримувати і інші об'єкти.

Для систем керування базами даних об'єкт - це база даних, таблиця, подання, процедура що зберігається. До таблиць застосовують операції пошуку, додавання, модифікації і видалення даних, у інших об'єктів інші види доступу. Різноманітність об'єктів і застосовних до них операцій призводить до принципової децентралізації логічного управління доступом. Кожен сервіс повинен сам вирішувати, чи дозволити конкретному суб'єкту ту чи іншу операцію. Теоретично це узгоджується з сучасним об'єктно-орієнтованим підходом, на практиці ж призводить до значних труднощів.

Головна проблема в тому, що до багатьох об'єктів можна отримати доступ за допомогою різних сервісів (можливо, при цьому доведеться подолати деякі технічні

труднощі). Так, до реляційних таблиць можна добратися не тільки засобами СУБД, але і шляхом безпосереднього читання файлів або дискових розділів, підтримуваних операційною системою (розібравшись попередньо в структурі зберігання об'єктів бази даних). В результаті при завданні матриці доступу потрібно брати до уваги не тільки принцип розподілу привілегій для кожного сервісу, але і існуючі зв'язки між сервісами (доводиться дбати про узгодженість різних частин матриці). Аналогічні труднощі виникають при експорті/імпорті даних, коли інформація про права доступу, як правило, втрачається. Отже, обмін даними між різними сервісами представляє особливу небезпеку з точки зору управління доступом, а при проектуванні і реалізації різнорідної конфігурації необхідно подбати про узгоджений розподілі прав доступу суб'єктів до об'єктів і про мінімізацію числа способів експорту/імпорту даних.

При прийнятті рішення про надання доступу зазвичай аналізується наступна інформація [10]:

- ідентифікатор суб'єкта (код користувача, мережева адреса комп'ютера і т.ін.). Подібні ідентифікатори є основою довільного (або дискреційного) управління доступом;
- атрибути суб'єкта (мітка безпеки, група користувача і т.ін.). Мітки безпеки - основа примусового (мандатного) управління доступом.

Матрицю доступу, з огляду на її розрідженості (більшість клітин - порожні), нерозумно зберігати у вигляді двомірного масиву. Зазвичай її зберігають за стовпцями, тобто для кожного об'єкта підтримується список "допущених" суб'єктів разом з їх правами. Елементами списків можуть бути імена груп і шаблони суб'єктів, що служить великою підмогою адміністратору. Деякі проблеми виникають тільки при видаленні суб'єкта, коли доводиться видаляти його ім'я з усіх списків доступу; втім, ця операція проводиться нечасто.

Списки доступу - виключно гнучкий засіб. За їх допомогою легко виконати вимогу що до гранулярності прав з точністю до користувача. За допомогою списків нескладно додати права або явним чином заборонити доступ (наприклад, щоб покарати кількох членів групи користувачів). Безумовно, списки є найкращим засобом довільного управління доступом.

Переважна більшість операційних систем і систем управління базами даних реалізують саме довільне керування доступом. Основна перевага довільного управління - гнучкість. Взагалі кажучи, для кожної пари "суб'єкт-об'єкт" можна незалежно задавати права доступу (особливо легко це робити, якщо використовуються списки управління доступом). На жаль, у "довільного" підходу є ряд недоліків. Розосередження управління доступом веде до того, що довіреними повинні бути багато користувачів, а не тільки системні оператори або адміністратори. Через неуважність або некомпетентність співробітника, який володіє секретною інформацією, цю інформацію можуть дізнатися і всі інші користувачі. Отже, довільність управління повинна бути доповнена жорстким контролем за реалізацією обраної політики безпеки.

Другий недолік, який є головним, полягає в тому, що права доступу існують окремо від даних. Ніщо не заважає користувачеві, що має доступ до секретної інформації, записати її в доступний всім файл або замінити корисну утиліту її "троянським" аналогом. Подібна "розділеність" прав і даних істотно ускладнює проведення декількома системами узгодженої політики безпеки і, головне, робить практично неможливим ефективний контроль узгодженості.

Повертаючись до питання подання матриці доступу, можна використовувати також функціональний спосіб, коли матрицю не зберігають в явному вигляді, а кожен раз обчислюють вміст відповідних клітин. Наприклад, при примусовому управлінні доступом застосовується порівняння міток безпеки суб'єкта та об'єкта.

Зручною надбудовою над засобами логічного управління доступом є обмежуючий інтерфейс, коли користувача позбавляють самої можливості спробувати зробити несанкціоновані дії, включивши в число видимих йому об'єктів тільки ті, до яких він має доступ. Подібний підхід зазвичай реалізують в рамках системи меню (користувачеві показують лише допустимі варіанти вибору) або за допомогою обмежуючих оболочок, таких як restricted shell в ОС Unix [11].

На закінчення необхідно підкреслити важливість управління доступом не тільки на рівні операційної системи, але і в рамках інших сервісів, що входять до складу сучасних додатків, а також, наскільки це можливо, на "стиках" між сервісами. Тут на перший план виходить існування єдиної політики безпеки організації, а також кваліфіковане і узгоджене системне адміністрування.

Висновок

На даний час неможливо уявити наш «сучасний» світ без комп'ютерних систем і технологій пов'язаних з ними. Оскільки системи авторизації, аутентифікації та ідентифікації присутні майже у всіх галузях промисловості, сферах діяльності і у повсякденному житті, то можна зробити висновок, що ці системи будуть у майбутньому лише покращуватись і на базі існуючих розроблятимуться більш досконалі та надійні способи та методи.

Список використаної літератури

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 5 липня 1994 року № 80/94-ВР, Відомості Верховної Ради України (ВВР), 1994, № 31, - с.286

2. Постанова КМ України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" № 373 від 29 березня 2006 року. [Електронний ресурс]: - Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=47960&cat_id=38834

3. НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі". [Електронний ресурс] - Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835

4. Методика информационной безопасности. / [Уфимцев Ю.С., Буянов В.П., Ерофеев Е.А и др.] – М.: Издательство "Экзамен", 2004. – 544 с.

5. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу". [Електронний ресурс] - Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835

6. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. М.: ДМК Пресс, 2002.

7. Матвеев И.А., Ганькин К.А. Распознавание человека по радужке // Системы безопасности, 2004, № 5, с. 72.

8.Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие.– СПб.: Изд-во СПбГУЭФ, 2010.– 267 с.

9. Тихонов И.А. Информативные параметры биометрической аутентификации пользователей информационных систем по инфракрасному изображению сосудистого русла Биомедицинская техника и радиоэлектроника. 2010. № 9. С. 26–32.

10. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. – Феникс, 2008 г.

11. Галатенко В.А. Идентификация и аутентификация, управление доступом лекция из курса «Основы информационной безопасности». – Интернет Университет Информационных Технологий, 2010г.

Надійшла 25.04.2017 р. Рецензент: д.т.н., проф. Горбенко І.Д.