УДК 004.056.5:004.7

В. А. Струзік, О. В. Харкянен, С. В. Грибков
Національний університет харчових технологій,
кафедра інформаційних систем

АНАЛІЗ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ДОДАТКОВОГО ЗАХИСТУ КОРПОРАТИВНИХ БАЗ ДАНИХ

Розглянуто проблеми захисту корпоративних баз та сховищ даних. Виявлено основні проблеми, що виникають під час захисту інформації у базах та сховищах даних при використанні стандартних засобів захисту систем управління базами даних. Проведено огляд та порівняння функціональності та принципів роботи програмних продуктів для підвищення ефективності захисту корпоративних баз та сховищ даних під час їх роботи та рефакторингу.

Ключові слова: захист інформації, сховища та бази даних, засоби захисту.

The problems of protection of corporate databases and data warehouses are considered. The main problems that arise when multiple data are stored in data bases and data stores and secured by standard data base management systems are identified. The review and comparison of functionality and operating principles of software products was performed to improve the efficiency of protecting corporate databases and data warehouses during their operation and refactoring.

Keywords: information protection, databases and data warehouses, protection.

Вступ

Сучасне підприємство має розвинену мережеву інфраструктуру, в якій працюють корпоративні інформаційні системи, що забезпечують підтримку всіх бізнес-процесів організації. Головним джерелом бізнес-інформації в таких мережевих інфраструктурах є сховища та бази даних, в яких зберігається внутрішня оперативна та фінансова інформація, персональні дані співробітників, інформація про замовників та клієнтів, інтелектуальна власність, дослідження ринку та аналіз діяльності конкурентів, платіжна інформація.

За деякими даними, в промислово розвинених країнах середній збиток від одного злочину в сфері комп`ютерної інформації становить приблизно 450 тис. дол., а щорічні сумарні втрати в США і Західній Європі, за даними, що наводять В. Гайкович та А. Прешин, досягають 100 млрд. і 35 млрд. дол. В останні десятиріччя зберігалася стійка тенденція до зростання збитків, пов’язаних із злочинністю в сфері комп’ютерної інформації. В пресі та літературі наведено багато подібних прикладів [1].

Сьогодні більшість фірм виробників систем управління сховищами та базами даних намагаються удосконалити засоби захисту, але їхні зусилля, як правило, скеровані тільки на усунення відомих вразливостей власних продуктів.

Основними напрямками розвитку технологій систем управління базами даних (СУБД) є реляційні та нереляційні СУБД.

Аналіз досліджень та публікацій

В умовах тотальної комп'ютеризації та інформаційної революції питання захисту даних повинні цікавити кожну компанію, яка має власні сховища даних.

У публікації [1] досліджено загальні принципи захисту даних в інформаційних системах та висвітлені актуальні проблеми захисту інформації. Автор роботи [2] розглянув та проаналізував основні методи захисту баз даних. У звіті [3] компанія "InfoWatch" навела статистичні дані дослідження витоків конфіденційної інформації з фінансових компаній за 2015 рік. У праці [4] розглянуто п'ять найбільших сьогодні загроз безпеці баз даних. У роботі [5] описані засоби та методи захисту даних в інформаційних системах.

Проблема захисту інформації у корпоративних базах та сховищах даних сьогодні є дуже гострою, і ситуація ускладнюється з кожним роком, незважаючи на швидкий розвиток технологій. Це означає, що цим питанням приділяють замало уваги.

Формулювання цілі статті

Враховуючи все вищезазначене, актуальною задачею є комплексне дослідження і систематизація питань захисту сховищ та баз даних з урахуванням загальних тенденцій розвитку підходів до забезпечення інформаційної безпеки та усунення загроз з використанням додаткових програмних засобів.

Основні типи атак на корпоративні інформаційні системи

Розвиток інформаційних технологій сприяє вдосконаленню корисних інформаційних ресурсів та дає поштовх для розвитку різноманітних шкідливих програмних засобів для нанесення цілеспрямованих пошкоджень та атак, що спричиняють неабиякий збиток. Найпоширенішими типами атак та загроз для корпоративних інформаційних систем є: аналізатори трафіку (sniffer) – перехват та прослуховування мережевого трафіку; повний перебір (brute force) – метод грубої сили; SQL-ін'єкції; DDOS-атаки (Distributed Denial of Service – "відмова від обслуговування"); оновлення програмного забезпечення без перевірки підпису або з неавторитативних джерел.

Аналізатори трафіку – це програмні або апаратні засоби перехвату та аналізу мережевого трафіку. Їх використовують шахраї для втручання до протоколу передавання даних між контрагентами задля викривлення або підміни вихідної інформації. Захистом корпоративних джерел інформації від такого виду атак є використання шифрованих SSL-з'єднань (Secure Sockets Layer). Цю опцію захисту, як правило, реалізовано в усіх найпопулярніших СУБД, наприклад, у MySQL [6]. За її відсутності необхідно організовувати окреме шифроване підключення між серверами з використанням додаткових засобів, що реалізують технологію віртуальної приватної мережі OpenVPN (Virtual Private Network). Вона дає змогу встановлювати захищене з'єднання між комп'ютерами без необхідної зміни їх налаштувань. Для організації ефективного захисту корпоративних баз та сховищ даних доцільно приховувати їхні порти, а самі джерела інформації розміщувати у захищеному сегменті мережі. За потреби підключення до корпоративної інформації інших серверів вони повинні мати адресу із захищеного сегменту мережі. Підтвердженням доцільності саме такого підходу є здійснена у 2017 році масштабна атака за назвою WannaCry. Хакери діяли через комп'ютери з відкритим TCP-портом 445 та використовували класичну схему вимагання грошових коштів за дешифрування інформації.

У разі перебування клієнта поза захищеним сегментом його необхідно підключити через захищений VPN, а аутентифікація має відбуватись з використанням сертифікатної аутентифікації (сертифікат при цьому може бути "зашитий" у захищеному сховищі – такому, як eToken) [7].

Повний перебір скерований на підбирання логінів та паролів перебором усіх варіантів та їх модифікацій. Особливістю такого виду атаки є можливість застосування проти шифру будь-якої складності, але вона може вимагати нереалістичних часових та ресурсних витрат.

Як і у випадку попереднього виду атаки, найефективнішим засобом є приховування портів баз даних та використання шифрованих з'єднань, як описано вище, а також використання складних паролів, при формуванні яких задіяно всі типи допустимих символів, букви верхніх та нижніх регістрів, спеціальні символи.

SQL-ін'єкції є найпоширенішим видом атак на SQL бази даних. Ін'єкції шкідливого коду призводять до втрати маніпуляції операціями, що здійснюються в базі даних кінцевими користувачами додатка, тобто відбуваються анулювання транзакцій, зміни та знищення вихідних даних, розкриття конфіденційної корпоративної інформації.

DdoS-атака призначена на цілenаправлене надсилання запитів до серверу у такій кількості, щоб він не зміг їх обробити. В результаті такої атаки сервер починає працювати повільно, обробляючи надмірний обсяг помилкових запитів, а потім може вийти з ладу.

Оновлення програмних засобів без перевірки підпису або з неперевірених джерел є видом атаки, за якого здійснюється самостійне завантаження шкідливих оновлень. Основним захистом від такого виду атак є кваліфіковані адміністратори баз даних, але і вони не можуть забезпечити повної безпеки – підтвердженням є відома атака віруса Petya.A.

Проблеми захисту корпоративних сховищ та баз даних

Проаналізувавши засоби забезпечення безпеки даних, реалізовані у СУБД, архітектуру сховищ та баз даних, інтерфейси систем, відомі вразливості та інциденти безпеки, було виділено основні проблеми захисту сховищ та баз даних:

– на належному рівні проблемами захисту інформації займаються тільки провідні фірми-виробники промислових, великих СУБД;

– при створенні програмних продуктів розробники намагаються використовувати лише стандартні засоби захисту, що надаються СУБД;

– різновид масштабів та виду інформації, що зберігається, потребує різних підходів до безпеки;

– майже кожна СУБД використовує різні лінгвістичні конструкції для доступу до даних, що організовані на основі однієї моделі.

Актуальність захисту повністю пов’язана із розвитком ІТ-технологій, що зумовлює зростання можливостей комп’ютерної техніки. Розвиток засобів, методів і форм автоматизації процесів обробки інформації, а також масове застосування персональних комп’ютерів роблять інформацію набагато вразливішою.

Основними чинниками вразливості інформації є [1]: збільшення обсягів та видів інформації, що обробляється за допомогою комп’ютерів, її збереження в електронному вигляді; накопичення інформації у сховищах та базах даних різнорідного призначення; розширення кола користувачів, що мають безпосередній доступ до ресурсів обчислювальної системи та масивів даних; ускладнення режимів роботи технічних засобів обчислювальних систем; обмін інформацією в локальних та глобальних мережах.

Основними загрозами корпоративного рівня є: використання прав доступу іншої особи; несанкціонована зміна або копіювання даних; зміна (підміна) програмного забезпечення; непродумані методики і процедури, що допускають змішування конфіденційних і звичайних даних в одному документі чи місці зберігання; підключення до кабельних мереж без вживання заходів захисту; введення кіберзлочинцями некоректних даних; шантаж; створення “лазівок” у системі; викрадення інформації, програмного забезпечення та обладнання; відмова систем захисту; недостатній рівень знань та недотримання правил безпеки персоналом; надання доступу до засекречених даних третім особам; електронні перешкоди і радіація; руйнування даних у результаті відключення або перенапруження в мережі електроживлення; пожежі, повені, диверсії; фізичне пошкодження обладнання та елементів інфраструктури; зараження комп’ютерними вірусами.

Як показує практика, загрози бувають комбінованими та призводять до таких наслідків: викрадення і фальсифікація даних; втрата конфіденційності; порушення недоторканності особистих даних; втрата цілісності і доступності даних, що загрожує підприємству фінансовими збитками.

Стандартні засоби захисту СУБД

Основні методи захисту, що реалізовані у більшості СУБД, полягають у наступному [4]: використання паролю; розподілення прав доступу до складових чи інформації сховища або бази даних між користувачами; шифрування й криптографія даних та програмних модулів.

Захист від несанкціонованого доступу через використання паролю є одним з найпоширеніших та ефективних способів. Паролі встановлюються користувачами або адміністраторами, а їх облік і зберігання забезпечується СУБД у зашифрованому вигляді в певних

системних файлах. Незручність полягає у тому, що всі користувачі мають один пароль і за недбалого відношення він може стати надбанням третьої особи.

Розподілення прав доступу до складових чи інформації сховища або бази даних полягає у поєднанні користувачів у певні групи, які мають визначені набори правил та обмежень. Такий підхід, залежно від СУБД, забезпечує багатошаровий доступ. Кожна СУБД використовує свої методи для шифрування та криптографії даних та програмних модулів. При цьому відкритий текст перетворюється на шифрограму, яку можна прочитати, тільки виконавши зворотний процес дешифрування.

Фізичні засоби захисту призначені для зовнішнього захисту обчислювальної техніки, території та об'єктів. Вони реалізуються на базі ЕОМ, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до компонентів інформаційних систем, що захищаються.

Програмні засоби захисту – це електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передавання даних для внутрішнього захисту терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку тощо.

Використання фізичних засобів захисту основане на створенні фізичних перешкод для зловмисника, що перегороджують йому шлях до інформації (сувора система пропуску на територію і в приміщення з апаратурою або з носіями інформації). Ці засоби дають захист тільки від "зовнішніх" зловмисників і не захищають інформацію від тих осіб, які володіють правом входу до приміщення.

До законодавчих засобів захисту належать законодавчі акти, які регламентують правила використання й обробки інформації обмеженого доступу і встановлюють кримінальну відповідальність за порушення цих правил. Під організаційним розуміють захист інформації регулюванням доступу до всіх ресурсів системи (технічних засобів, системи безпеки телекомунікацій та зв'язку, програмних елементів тощо). В автоматизованих системах інформаційного забезпечення повинні бути регламентовані порядок роботи користувачів і персоналу, право доступу до інформації, окремих файлів та баз даних.

Програмні засоби захисту, які вмонтовані до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

З програмних засобів найефективніші криптографічні засоби захисту інформації. Якщо фізичні засоби захисту можна подолати, наприклад, дистанційним наглядом, підключенням до мережі або підкупом персоналу, а організаційні не гарантують від проникнення зловмисників, то програмно-технічні, і насамперед, криптографічні методи, якщо вони задовольняють відповідні вимоги, є "найміцніші".

Криптографічний захист, тобто кодування тексту за допомогою складних математичних алгоритмів, завойовує все більшу популярність.

Шифрування – це процес перетворення відкритого тексту на шифрограму, яку можливо прочитати, тільки виконавши зворотний процес дешифрування.

Звичайно, жоден з шифрувальних алгоритмів не дає цілковитої гарантії захисту від зловмисників, але деякі методи шифрування настільки складні, що ознайомитись зі змістом зашифрованих повідомлень практично неможливо.

Види систем шифрування:

– симетричні алгоритми шифрування – алгоритми, які застосовують для шифрування інформації, особливість яких полягає у тому, що ключ шифрування та розшифрування однаковий, тобто за його допомогою можна як зашифрувати, так і розшифрувати (відновити) повідомлення;

– асиметричні алгоритми шифрування – алгоритми шифрування, які використовують різні ключі для шифрування та дешифрування даних.

Основні криптографічні методи шифрування:

– шифрування за допомогою датчика псевдовипадкових чисел, яке полягає у тому, що генерується гама шифру за допомогою датчика псевдовипадкових чисел і накладається на відкриті дані з урахуванням зворотності процесу;

– шифрування за допомогою криптографічних стандартів шифрування даних (за симетричною схемою шифрування), в основу якого покладено перевірені і випробувані алгоритми шифрування даних з великою криптостійкістю;

– шифрування за допомогою пари ключів (з асиметричною системою шифрування), в яких один ключ є відкритим і використовується для шифрування інформації, другий ключ – закритий і використовується для розшифрування інформації.

Отже, зрозуміло, що на етапі розроблення інформаційної системи важливу роль у захисті даних відіграє правильний вибір СУБД, але разом з цим виникає запитання: як підсилити захист та завадостійкість даних завдяки додатковим програмним засобам, якщо на підприємстві вже використовують певну СУБД.

Аналіз програмних продуктів для додаткового захисту

Автори дослідили засоби, наявні на сучасному ринку програмних продуктів для захисту сховищ та баз даних. Усі засоби відрізняються за призначенням, принципом дії та іншими показниками. Маємо вузькоспеціалізовані продукти для шифрування даних: “BestCrypt Container Encryption”, “PGPdisk”, а також продукти, які являють собою системи, що організовують всебічний захист даних: “Крипто БД”, “Oracle Audit Vault and Database Firewall”, “McAfee Data Center Security Suite for Databases”, “Елвіс Плюс”, “Гарда БД”.

На думку авторів, доцільно виділити чотири програмні продукти, що мають, на відмінну від інших, більший спектр дії та функціонал.

“Oracle Audit Vault and Database Firewall” об’єднує ключові можливості продуктів Oracle Audit Vault і Oracle Database Firewall і при цьому розширює можливості захисту інформації на СУБД Microsoft SQL Server, SAP Sybase, IBM DB2, MySQL завдяки підтримці аудиту каталогів операційних систем і призначених для користувача джерел даних аудиту. Він надає уніфіковану платформу моніторингу та контролю, можливості якої виходять за межі захисту СУБД. Містить такі компоненти: Database Activity Monitoring and Firewal; Expanded Enterprise Auditing; Consolidated Reporting and Alerting. Компоненти Database Activity Monitoring and Firewall забезпечують моніторинг трафіку SQL-запитів для всіх сертифікованих версій сучасних СУБД. Методика граматичного аналізу SQL-запитів дає змогу скоротити кількість даних для аналізу завдяки представленню всіх запитів у вигляді кластерів, що дає змогу досягти високої точності і масштабованості, а також спростити створення списків винятків, білих і чорних списків для більш ефективного виявлення несанкціонованого доступу до баз даних, включаючи атаки типу SQL-ін’єкцій (SQL-injections) [8].

“Oracle Audit Vault and Database Firewall” забезпечує повний і гнучкий контроль за рахунок консолідації даних аудиту Oracle та інших баз даних, операційних систем, каталогу файлових систем, моніторингу SQL трафіку. Водночас “Oracle Database Firewall” може набувати в якості першої лінії оборони в мережі, допомагаючи запобігати порушенням, які виникають внаслідок SQL-ін’єкцій, несанкціонованих SQL-запитів, а також іншої шкідливої діяльності відносно баз даних.

“Oracle Audit Vault and Database Firewall” підтримує СУБД Oracle, Microsoft SQL Server, IBM DB2 для LUW, SAP Sybase ASE, бази даних Oracle MySQL і Oracle Big Data Appliance.

Продукт “McAfee Data Center Security Suite for Databases” дає фахівцям можливість отримувати повну інформацію про стан баз даних і рівні захищеності, що дозволяє уніфікувати процеси управління їх безпекою, а також ефективно забезпечувати нормативно-правову відповідність.

Рішення “McAfee Data Center Security Suite for Databases” у режимі реального часу забезпечує надійний захист критично важливих для комерційної діяльності баз даних від усіх видів зовнішніх і внутрішніх загроз.

Комплект містить провідні продукти McAfee: Database Activity Monitoring, McAfee Vulnerability Manager for Databases і McAfee Virtual Patching for Databases, що здійснюють централізоване управління безпекою баз даних паралельно з іншими захисними рішеннями [9]. Завдяки модульному характеру рішення McAfee можуть бути індивідуально налаштовані та забезпечуватимуть автоматизацію процесів захисту, моніторингу та інші аспекти безпеки баз даних. Система захисту "Елвіс Плюс" дає змогу ефективно вирішити проблему несанкціонованого доступу до інформації, що обробляється в СУБД. Система ґрунтується на програмних рішеннях Imperva SecureSphere Database Security і IBM InfoSphere Guardium, що скеровані на забезпечення аудиту та захисту баз даних у реальному часі для великих корпоративних інформаційних систем. Основними функціями системи є: контроль доступу до облікових записів; оперативне виявлення та реагування на спроби несанкціонованого доступу до інформації в базі даних; можливість оперативного контролю стану захищеності баз даних [10].

Ключові можливості:

– управління доступом до БД, що являє собою міжмережеве екранування за допомогою аналізу SQL-запитів користувачів;

– моніторинг активності користувачів БД, інформація про яку надходить з мережевого обладнання, а також з агентів моніторингу, розгорнутих безпосередньо на серверах БД;

– блокування доступу, що забезпечує перехоплення, аналіз і відповідне реагування (зокрема блокування) SQL-запитів користувачів;

– централізоване управління системою;

– забезпечення доступу засобами служби Application Defense Center (ADC) до актуальних оновлень конфігураційних даних, включаючи сигнатури атак, політики тощо.

Продукт "Гарда БД" забезпечує захист з єдиного інтерфейсу різних бізнес-додатків та СУБД, таких як: Oracle, Microsoft SQL, MySQL, PostgreSQL, Teradata, Sybase ASE, IBM Netezza, IBM DB2, Линтер, Apache Cassandra.

Перевагами програмного продукту є [11]:

– функціонування в пасивному режимі з копією трафіку (SPAN) не впливає на роботу баз даних;

– здійснення контролю локальних звернень до серверу СУБД за допомогою агентського програмного забезпечення;

– не перевищує пікового навантаження у 5% при локальних клієнтських запитах;

– блокування небажаних дій користувачів баз даних здійснюється в активному режимі за рахунок мережевого екрана;

– здійснюється сканування та тестування на вразливість для виявлення незаблокованих облікових записів, невстановлених патчів, облікових записів з простими паролями, активності системних облікових записів інших додатків, атак з підбору облікових записів або назв таблиць.

Реалізовано та застосовуються такі інтелектуальні алгоритми пошуку:

– контентний: за запитами, відповідями і змінними;

– атрибутивний: за IP-адресами, обліковим записом, текстами помилок тощо;

– пошук неконтрольованих баз даних у мережі підприємства;

– класифікація баз даних за типом вмісту.

До переваг також належать високоефективне зберігання усього трафіку обсягом до 100 Тб, а також швидкісний критеріальний та повнотекстовий пошук інформації, що дають змогу аналізувати дані за будь-який період часу незалежно від того, враховані вони в політиках чи ні. Дані зберігаються в знеособленому вигляді завдяки технології маскування. Моніторинг баз даних відбувається в режимі реального часу. Система адаптована для обробки вхідного трафіку на високих швидкостях.

Розглянуті програмні продукти відрізняються за призначенням, принципом дії та іншими показниками, тому вибирати додатковий засіб захисту корпоративної інформації необхідно залежно від завдань, які продукт має вирішувати.

Розглянуті рішення мають великий спектр специфічних функцій, а також забезпечують пасивний захист через моніторинг баз даних у реальному часі.

У цьому плані позитивно вирізняється рішення “Гарда БД”, яке працює із копією вхідного трафіку, що дає змогу досягти високих показників швидкості під час його обробки без сповільнення роботи БД.

З іншого боку, відмінність рішення “Елвіс-плюс” полягає у моніторингу активності користувачів БД завдяки інформації з активного мережевого обладнання, а також з агентів моніторингу, розгорнутих безпосередньо на серверах БД. Це рішення дає змогу аналізувати дії користувачів та відслідковувати порушників.

На відміну від решти, рішення “McAfee Data Center Security Suite for Databases” та “Oracle Audit Vault and Database Firewall” мають окремі модулі “McAfee Database Activity Monitoring” та “Database Activity Monitoring and Firewall” які забезпечують моніторинг загроз в реальному часі.

Унікальність рішення “McAfee Data Center Security Suite for Databases” полягає в тому, що використовуються датчики, які розташовані в оперативній пам’яті, для встановлення усіх типів загроз.

А особливістю рішення “Database Activity Monitoring and Firewall” є те, що ефективність моніторингу усіх запитів забезпечується за рахунок їх представлення у вигляді кластерів, що дає змогу досягти високої точності і масштабованості, а також спростити створення списків винятків, білих і чорних списків для ефективнішого виявлення несанкціонованого доступу до баз даних, зокрема атак типу SQL-ін’єкцій.

Висновок

Дослідження показали, що в захисті сховищ та баз даних велику роль відіграють СУБД, але не всі вони задовольняють вимоги захисту відповідного рівня.

Використання додаткових засобів захисту посилять захист та завадостійкість сховищ та баз даних будь-якої організації, навіть у разі їх рефакторингу чи модернізації елементів корпоративних інформаційних систем. Вибір додаткового засобу захисту повністю залежить від використовуваної СУБД, а також від пріоритетів та можливостей керівництва кожної фірми. Також необхідно зазначити, що використання більше ніж одного додаткового засобу захисту може призвести до виникнення конфліктів пріоритетності та перешкоджання один одному.

Для підвищення ефективності безпеки баз та сховищ даних компаніям достатньо дотримуватися таких правил: використовувати підготовлені запити; захищати порти серверів, на яких встановлена СУБД; використовувати шифровані з’єднання; постійно на корпоративному рівні забезпечувати оновлення паролів та забезпечувати їх складність; використовувати розподілені права доступу з їх мінімізацією для кожного окремого користувача; забезпечувати мінімальний доступ до вузлів корпоративної мережі.

1. Козаченко І. П., Голубєв В. О. Загальні принципи захисту інформації в банківських автоматизованих системах [Електронный ресурс]. – Режим доступа : http://www.bezpeka. com/ru/lib/ spec/infsys/ art92.html, 2005. 2. Височенко А. А., Петренко А. Б. Методи захисту баз даних [Електронный ресурс] – режим доступа : http://www.bezpeka.com/ru/lib/spec/infsys/art92.html. 3. Исследование утечек информации за первое полугодие 2015 года [Електронный ресурс] – режим доступа : https://www.infowatch.ru/analytics/reports/16340. 4. Top 5 Database Security Threats [Електронный ресурс] – режим доступа : https://www.imperva.com/docs/gated/WP_ Top_5_Database_Security_Threats.pdf, 2016. 5. Кононова В. О., Грибков С. В., Харкянен О. В. Оцінка засобів захисту інформаційних ресурсів / В. О. Кононова, С. В. Грибков, О. В. Харкянен // Вісник Нац. ун-ту “Львівська політехніка”. – 2014. – № 806. – С. 99–105. 6. Using Secure Connections [Електронный ресурс] – режим доступа : https://dev.mysql.com/doc/refman/5.6/en/secure-connections.html. 7. Douglas Crawford OpenVPN over TCP vs. UDP: what is the difference, and which should I choose? [Електронный ресурс] – режим доступа : https://www.bestvpn.com/openvpn-tcp-vs-udp-difference-choose/ , 2013. 8. Короткова Т. Oracle представила новый продукт для защиты баз данных [Електронний ресурс] / Т. Короткова // CNews. – 2012. – Режим доступу до ресурсу :

http://www.cnews.ru/news/line/oracle_predstavila_novyj_produkt_dlya. 9. Надежная защита критически важных баз данных в реальном времени [Електронний ресурс]. Режим доступу до ресурсу : https://www.mcafee.com/ru/products/data-center-securi. 10. Система защиты баз данных [Електронний ресурс]. Режим доступу до ресурсу : http://elvis.ru/services/application/database/. 11. Безопасность баз данных под контролем [Електронний ресурс]. Режим доступу до ресурсу : http://www.mfisoft.ru/direction/ib/garda-bd/.

УДК 519.7

В. Хома[1,2], Ю. Хома[1], В. Герасименко[1], Д. Сабодашко[1]
[1]Національний університет "Львівська політехніка",
кафедра захисту інформації,
кафедра інформаційно-вимірювальних технологій,
[2]Політехніка Опольська (Польща)

ЕКГ-ІДЕНТИФІКАЦІЯ З ВИКОРИСТАННЯМ ГЛИБИННИХ НЕЙРОННИХ МЕРЕЖ

Описано розроблення нової біометричної системи на основі електрокардіограми людини (ЕКГ) як альтернативного джерела біометричної інформації. Для здійснення ідентифікації запропоновано використати передові алгоритми машинного навчання (глибинні нейроні мережі) у поєднанні з техніками цифрового опрацювання сигналів. Всі експерименти проводились на самостійно зібраному наборі даних з використанням вбудованої електроніки з мінімізованою аналоговою частиною.

Ключові слова: біометрія, нейронні мережі, ідентифікація, електрокардіограма.

This paper is focus on developing novel biometric system based on humans' electrocardiogram (ECG) as alternative type of biometric information. To perform identification advanced machine learning algorithms (deep neural networks) combined with digital signal processing techniques. All experiments were done on self-collected data set using the embedded electronics with a minimized analog front end.

Keywords: biometrics, neural networks, identification, electrocardiogram.

Вступ

Багато аспектів нашого повсякденного життя потребують автоматичного і точного підтвердження ідентичності особистості. Широке впровадження механізмів розпізнавання, побудованих на основі сутностей (USB-брелок, ID-картка) або на основі знань (PIN-код, пароль), викликає побоювання щодо безпеки через ризик крадіжки ідентифікаторів.

Процес розпізнавання ідентифікатора користувача називається ідентифікацією. Автентифікація являє собою процес підтвердження достовірності заявленого користувачем ідентифікатора. Рівень безпеки визначається рівнем прийняття системи.

За високого рівня безпеки (наприклад, на військовому об'єкті) не має бути жодних помилкових валідацій невідомих персон, навіть якщо це збільшує кількість помилок під час перевірки акредитованих користувачів.

Найкращим способом перевірити ідентичність суб'єкта є використання його біометричних даних. Використання цих даних (характеристик або ознак) у методах ідентифікації та/або автентифікації