https://www.sworldjournal.com/index.php/swj/article/view/swj06-01-077
DOI: 10.30888/2663-5712.2020-06-01-077

УДК 004.056.523

CYBERSECURITY OF AUTOMATED WORKING TIME ACCOUNTING SYSTEM USING BIOMETRICS OF FACE

КІБЕРБЕЗПЕКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ОБЛІКУ РОБОЧОГО ЧАСУ З ВИКОРИСТАННЯМ БІОМЕТРІЇ ОБЛИЧЧЯ

Ostapets D.O. / Остапець Д.О.
c.t.s., as. prof. / к.т.н., доц.
ORCID: 0000-0003-1778-7770
Dzuba V.V. / Дзюба В.В.
senior lecturer / ст. викл.
ORCID: 0000-0003-3008-5669
Kapshuchenko D.O. / Капшученко Д.О.
student / студент
Hodun E.D. / Годун Є.Д.
student / студент
Dnipro National University of Railway Transport named after Academician V.Lazaryan,
Dnipro, Lazaryana St., 2, 49010
Дніпровський національний університет залізничного транспорту
імені академіка В.Лазаряна, Дніпро, вул. Лазаряна, 2, 49010

Анотація. *В роботі розглядаються принципи побудови захищеної системи обліку робочого часу (на прикладі системи обліку відвідування занять студентами університету) з використанням ідентифікації за біометрією обличчя. Впровадження таких систем допомагає мінімізувати втрати підприємства. Використання біометрії обличчя дозволяє мінімізувати витрати на обладнання, оскільки передбачається використовувати відеокамери у складі існуючої системи відеоспостереження підприємства. Основною метою є розвиток принципів та методик побудови захищених систем обліку робочого часу. Вирішувані задачі: визначення раціональної біометричної методики (конкретного механізму) для використання в системі обліку робочого часу; розробка принципів побудови захищеної системи обліку робочого часу з використанням механізму ідентифікації / аутентифікації за біометрією обличчя. Пропонується клієнт-серверна організація системи. Отримані структурні схеми системи, структура захищеної БД, схеми роботи захищених протоколів взаємодії програмного забезпечення клієнтської та серверної частин. Система забезпечує конфіденційність інформації завдяки використанню відповідних криптографічних засобів та безпечних мережених протоколів.*

Ключові слова: *система, контроль доступу, облік робочого часу, ідентифікація, аутентифікація, біометрія обличчя, біометрична методика, клієнт, сервер, протокол, SSL, HTTPS, IP-камера.*

Вступ.

На сьогоднішній день механізми ідентифікації / аутентифікації застосовуються в усіх галузях та сферах діяльності. Одним з таких прикладів є використання ідентифікації / аутентифікації в системах обліку робочого часу. Впровадження таких систем допомагає мінімізувати втрати, що пов’язані з затримками або відсутністю персоналу на робочому місці. Біометричні методики засновані на унікальних характеристиках особи, які важко підробити. При цьому, біометрія обличчя дозволяє уникнути використання вартісного обладнання, оскільки головне додаткове обладнання – це відеокамера, яка, як правило, вже інтегрована та використовується у системі відеоспостереження

підприємства. В рамках роботи пропонуються принципи побудови захищеної системи обліку робочого часу з використанням біометрії обличчя.

Основний текст.

Основною метою роботи є розвиток принципів та методик побудови захищених систем обліку робочого часу. Для досягнення мети поставлені наступні задачі:

- визначення раціональної біометричної методики (конкретного механізму) для використання в системі обліку робочого часу;
- розробка принципів побудови захищеної системи обліку робочого часу з використанням механізму ідентифікації / аутентифікації за біометрією обличчя.

Система контролю і управління доступом (СКУД) являє собою сукупність апаратних та програмних засобів, які забезпечують обмеження або реєстрацію входу чи виходу людей (та/або інших об'єктів) за межі периметру контрольованої зони. Однією з найголовніших додаткових функцій СКУД є облік робочого часу персоналу, ведення журналу відвідувачів, тощо. Подібні функції можуть бути реалізовані також окремими системами обліку робочого часу [1, 2].

Реєстрація входу чи виходу за межі периметру в системах обліку робочого часу реалізується на основі ідентифікації / аутентифікації персоналу. Відомі три фактори ідентифікації / аутентифікації: парольний, майновий та біометричний [3]. Всі вони можуть бути використані в системах такого класу, але, в останній час, перевага віддається біометрії.

Кожна біометрична методика використовує певний біометричний параметр. Слід зазначити, що для біометричних параметрів зазвичай висуваються критерії, комбінація яких визначає ефективність біометрії [4]: загальність, унікальність, сталість, вимірність, прийнятність.

Крім того, для порівняння біометричних методик при виборі доцільно використовувати такі характеристики:

- необхідність у спеціалізованому обладнанні;
- відносна вартість обладнання;
- відносна вартість реалізації СКУД на базі методики (дана характеристика також передбачає оцінку вартості підтримання системи у працездатному стані);
- відносна точність розпізнавання (під цією характеристикою слід розуміти низький показник помилкових спрацьовувань);
- відносна зручність використання (враховує чи потрібно користувачу робити додаткові дії, щоб пройти ідентифікацію, та їх складність).

За сукупністю вказаних вище критеріїв та характеристик одним з найкращих варіантів є використання біометрії обличчя.

В даній роботі описано автоматизовану систему обліку робочого часу на прикладі розроблюваної системи обліку відвідування занять студентами університету [1, 2, 5].

Основними функціями та можливостями системи є:

- реєстрація у системі нової особи для розпізнавання;
- реєстрація у системі нового користувача (викладача);
- авторизація зареєстрованих користувачів;
- розпізнавання осіб на відео;
- формування журналу відвідувань (відвідувань занять студентами);
- редагування таблиць БД;
- підтримування з'єднання між серверною та клієнтськими частинами.

Для реалізації комплексу обрано дворівневу клієнт-серверну архітектуру.

Головною задачею серверу у комплексі контролю доступу за біометрією обличчя є розпізнання людей на відео, ідентифікація їх за унікальними біометричними характеристиками та оновлення бази даних, що містить інформацію про відвідування студентами занять.

Відео для аналізу потрапляє на сервер від розгалуженої системи відеоспостереження, що представлена IP-камерами, розташованими на території університету. Сучасні IP-камери можуть працювати за протоколом HTTPS, що підвищує їх стійкість до атак зловмисників, а також мають достатню роздільну здатність для проведення аналізу кадрів з відео на наявність людей та їх ідентифікацію.

Клієнтські станції, в свою чергу, дозволяють користувачам комплексу отримувати інформацію про відвідування занять студентами у зручний для них спосіб.

Оскільки програма-сервер може виконувати запити від багатьох програм-клієнтів, планується розмістити її на спеціально виділеній захищеній машині. Також через необхідність роботи з відео потоками ця машина повинна мати підвищені вимоги до об'ємів оперативної пам'яті та графічного процесору.

Для захисту передачі даних між сервером та клієнтами використовується криптографічний протокол SSL, що забезпечує шифрування, аутентифікацію та цілісність.

Загальний вигляд комплексу контролю доступу (системи обліку робочого часу) за біометрією обличчя представлений на рис. 1.

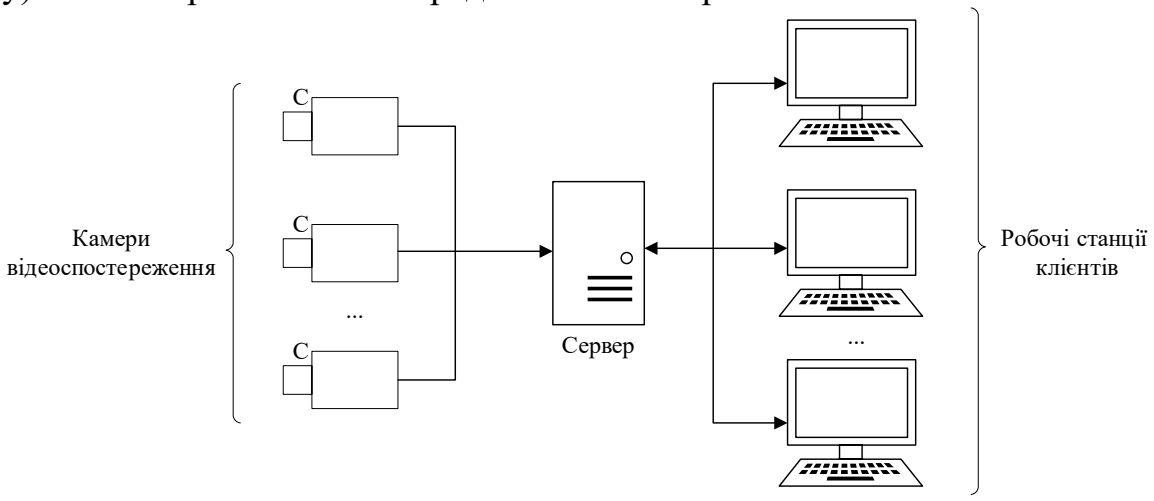

Рис. 1. Загальний вигляд системи

Авторська розробка

Інформаційна структура комплексу контролю доступу за геометрією обличчя показана на рис. 2. До елементів структури належать:

- Відеопотік з камер відеоспостереження;
- Набір фотознімків, що використовується комплексом при реєстрації нової особи;
- Зразки біометричних характеристик осіб, отримані у процесі розпізнавання;
- База даних;
- Протокол взаємодії серверної та клієнтської частин.

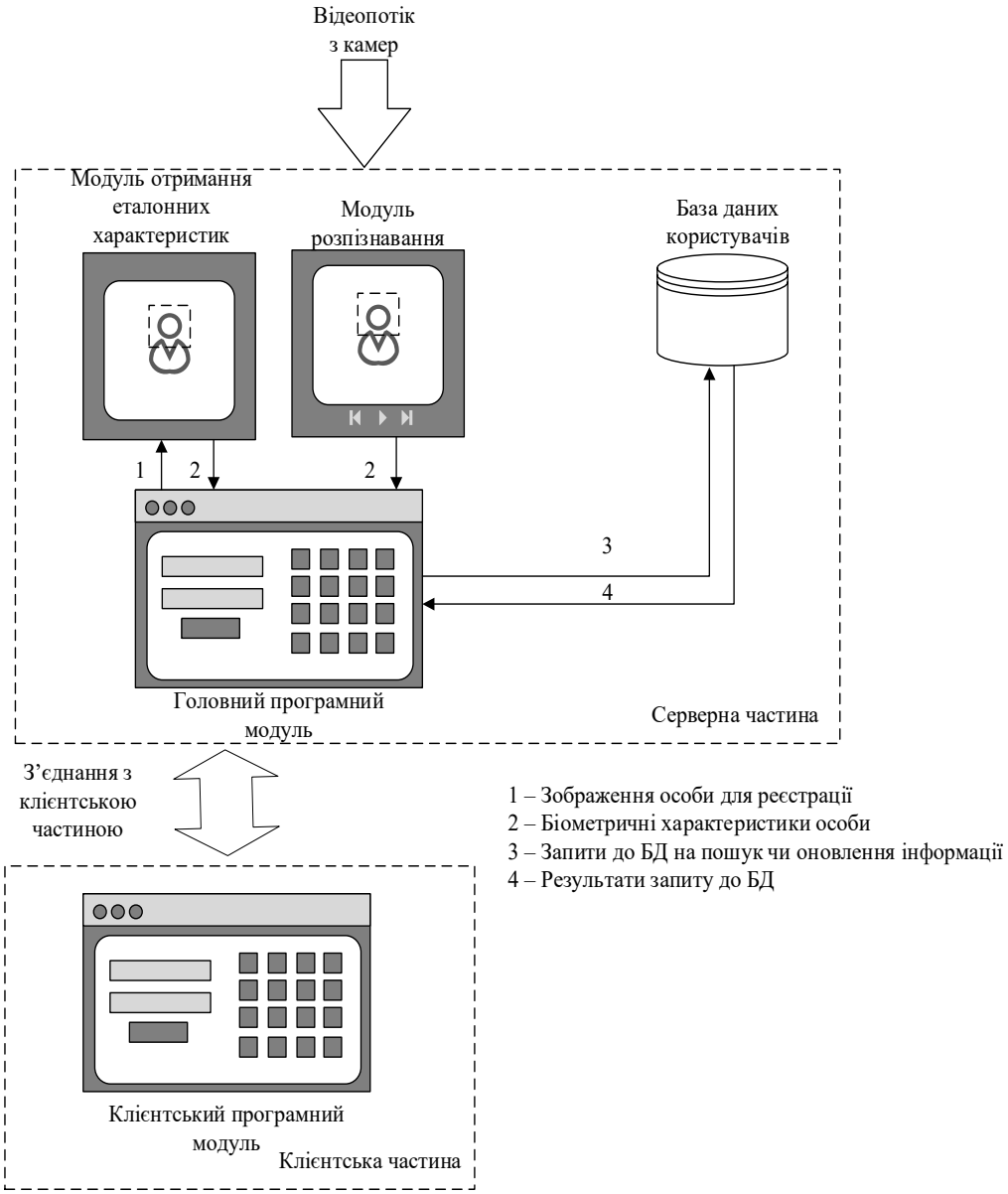

Рис. 2. Інформаційна структура системи

Авторська розробка

Відеопотік, що надходить з камери, одразу перехоплюється модулем розпізнавання та кадрується.

Набори фотознімків для реєстрації нової особи мають бути у форматі *.jpeg, зроблені з різних ракурсів за різним освітленням.

Модуль розпізнавання витягає з відео біометричні характеристики осіб та повертає їх головному модулю у форматі JSON. Кількість записів у структурі файлу відповідає кількості розрахованих біометричних характеристик, що використовуються для розпізнавання. Також JSON-формат використовується при отриманні еталонних біометричних характеристик під час реєстрації нової особи.

У якості БД для обліку користувачів комплексу та студентів університету, а також контролю їх відвідування, використовується вбудована СУБД SQLite. БД складається з таблиць «STUDENTSTAB» (облік студентів), «GROUPSTAB» (облік академічних груп), «BIOMETRICSTAB» (облік біометричних характеристик студентів), «VISITSTAB» (облік відвідування занять студентами) та «USERSTAB» (облік користувачів системи). Передбачається, що при розгортанні комплексу, таблиці «STUDENTSTAB» та «GROUPSTAB» будуть імпортовані з бази даних університету. Через це створено окрему таблицю «BIOMETRICSTAB», що пов'язує ідентифікатори студентів з їх еталонними біометричними характеристиками. В цій таблиці ведеться облік певної кількості біометричних характеристик для кожної особи. Кожна біометрична характеристика представлена співвідношенням двох відстаней між деякими ключовими точками на обличчі особи. Наприклад, характеристика R1 являє собою відношення відстані між зіницями очей до відстані між переніссям і крайньою точкою підборіддя.

Взаємодія між серверною та клієнтською частиною відбувається за спеціально розробленим протоколом (рис. 3):

1) Для отримання даних від серверу користувач має пройти процес автентифікації на сервері. Для цього користувач надсилає на сервер ідентифікатор запиту, свій логін та хеш паролю.

2) Сервер перевіряє логін та хеш у базі даних користувачів і, якщо користувач зареєстрований у системі, посилає користувачу у відповідь «0». Якщо користувач не зареєстрований у системі, клієнтська сторона отримує у відповіді від сервера код помилки «100».

3) Для отримання даних про відвідування студентами університету клієнт має сформувати запит до сервера, що містить такі дані, як: ідентифікатор запиту та дату. Додатковими, але необов'язковими, даними у запиті можуть виступати: номер групи, факультет, спеціальність, прізвище, ім'я та по батькові студента.

4) У разі наявності у базі даних інформації, що запитується, сервер повертає клієнту у відповідь кількість присутніх студентів та масив рядків, кожен з яких містить прізвище, ім'я та по батькові студента, що був присутній в університеті у запитувану дату. Якщо у БД немає запитуваних даних, сервер повертає код помилки «102».

Програмне забезпечення комплексу розроблене на мові програмування C++ за допомогою кросплатформного фреймворку Qt. Для створення сертифікатів, що потрібні для налагодження SSL-каналу, була використана бібліотека OpenSSL. Крім того, для проведення досліджень та налагодження системи була використана відкрита база даних LFW Face [6].

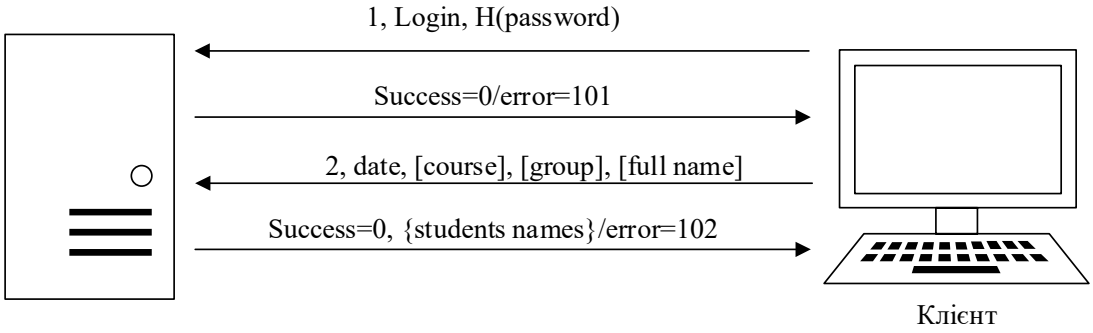

Рис. 3. Схема комунікації між клієнтом і сервером

Авторська розробка

Для розпізнавання облич в розроблюваній системі використовується раціональний набір біометричних ознак, який сформовано за результатами окремої роботи.

Висновки.

В роботі розглянуті принципи побудови системи обліку робочого часу (як складової частини СКУД або самостійної системи) на основі використання біометрії обличчя. Вибір біометричної методики засновано на базі аналізу набору можливих критеріїв та характеристик. Система забезпечує конфіденційність інформації завдяки використанню відповідних криптографічних засобів та безпечних мережених протоколів. В роботі отримані структурні схеми системи, структура захищеної БД, схеми роботи захищених протоколів взаємодії підсистем.

Література:

1. Годун Е.Д., Капшученко Д.О., Остапец Д.А. Биометрия лица в системах учета рабочего времени // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 05-06 квітня 2018 року р.; Київський національний університет імені Тараса Шевченка / Редкол.: Оксіюк О.Г. (голова) та ін. – К.: ВПЦ «Київський університет», 2018. – С. 14–18.

2. Godun E. D., Kapshuchenko D.O., Ostapets D.O., Pererva K.M. Biometry Of Faces In Identification Systems // Матеріали Міжнародної науково-практичної конференції «Технічні науки та інформаційні технології: актуальні проблеми і перспективи розвитку» / Харківськ. нац. тех. ун-т сільськ. госп-ва ім. П. Василенка. – Харків, 2018. – С.98–100.

3. Смит Р.Э. Аутентификация: от паролей до открытых ключей // М.: Издательский дом «Вильямс» – 2002 – 432 с.

4. Болл Р.М., Коннел Дж. Х., Панканти Ш., Ратха Н.К., Сеньор Э.У. Руководство по биометрии // М.: Техносфера – 2007. — 368с.

5. Годун Є.Д., Капшученко Д.О., Остапець Д.О. Комплекс контролю доступу на базі біометричних методик // Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості і освіті: Тези XIII Міжнародної науково-практичної конференції (Дніпро, 11-12 грудня 2019 р.). – Д.: ДІІТ, 2019. – С.63

6. LFW Face Database [Electronic resource] – Режим доступу: http://vis-www.cs.umass.edu/lfw/

References:

1. Godun E.D., Kapshuchenko D.O., Ostapets D.A. Facial biometrics in working time accounting systems // Problems of cybersecurity of information and telecommunication systems: Collection of materials for additional information and thesis; Kiev, 05-06 April 2018, Kiev National University of Taras Shevchenko / Editorial Board: Oksiyuk O.G. (head) - K.: VPC "Kiev University", 2018. - P. 14-18.

2. Godun E. D., Kapshuchenko D.O., Ostapets D.O., Pererva K.M. Biometry Of Faces In Identification Systems // Materials of the International scientific-practical conference "Technical sciences and information technologies: current issues and prospects for development" / Kharkiv Technical University of Agriculture named after P. Vasilenko. - Kharkiv, 2018. - P.98–100.

3. Smith R.E. Authentication: from passwords to public keys // M.: Williams Publishing House - 2002 - 432 p.

4. Ball R.M., Connel J.H., Pankanti S., Ratha N.K., Senor E.W. Guide to biometrics // M.: Technosphere - 2007 .- 368p.

5. Godun E.D., Kapshuchenko D.O., Ostapets D.O. Complex of access control on the basis of biometric methods // Modern information and communication technologies in transport, industry and education: Abstracts of the XIII International scientific-practical confere

nce (Dnipro, December 11-12, 2019). - D.: DIIT, 2019. - P.63

6. LFW Face Database [Electronic resource] – Access mode: http://vis-www.cs.umass.edu/lfw/

Abstract. *The paper considers the principles of building a secure system of accounting of working time (for example, the system of accounting of attendance by university students) using identification by facial biometrics. The introduction of such systems helps to minimize enterprise losses. The use of facial biometrics minimizes the cost of equipment, as it is expected to use video cameras as part of the existing video surveillance system of the enterprise. The main goal is to develop principles and methods of building of secure working time accounting systems. Solved problems: determination of rational biometric methods (specific mechanism) for use in the system of working time accounting; development of principles of construction of the secured system of the account of working time with use of the mechanism of identification / authentication on face biometrics. The client-server organization of the system is offered. The structural schemes of the system, the structure of the protected database, the schemes of operation of the protected protocols of interaction of the software of the client and server parts are received. The system ensures the confidentiality of information through the use of appropriate cryptographic tools and secure network protocols.*

Key words: *system, access control, working time accounting, identification, authentication, facial biometrics, biometric methodology, client, server, protocol, SSL, HTTPS, IP-camera.*