http://doi.org/10.51707/2618-0529-2020-17-02

УДК 004.94(063)

В. В. Коленко,
М. С. Сафонов,
О. Є. Яковенко

МОДЕЛЮВАННЯ СИСТЕМ АВТОМАТИЗОВАНОГО КОНТРОЛЮ РОБОЧОГО ЧАСУ В ОСВІТНІХ ЗАКЛАДАХ

Анотація. *У статті проведено моделювання автоматизованої системи обліку робочого часу персоналу з подальшим розробленням і впровадженням його в освітньому закладі. Практика свідчить, що завдяки використанню автоматизованого обліку робочого часу стає ефективнішим управління персоналом, підвищується дисципліна співробітників, на 5–15% економиться фонд оплати праці. Було визначено методи персоніфікованої ідентифікації персоналу, обґрунтовано вибір технічного обладнання та програмного забезпечення для збору даних, розроблено модель обліку робочого часу; розроблено та впроваджено програмне забезпечення для ідентифікації співробітників, фіксування та обліку робочого часу. Для цього на прохідній було встановлено спеціальне устаткування для керування доступом. Співробітники мають при собі спеціальні картки, які дають їм змогу безперешкодно пройти через ці пристрої. Якщо на території декілька пунктів пропуску, то доцільно використовувати комп'ютерну мережу для передачі даних на сервер, де зберігаються всі дані про співробітників. На основі таких даних можуть бути сформовані точні звіти про порушення дисципліни, а також отриманий табель робочого часу. Ідентифікація користувачів є невід'ємним і дуже важливим елементом для будь-якої інформаційної системи. Система ідентифікації і аутентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу. Завданням систем ідентифікації і авторизації є визначення і верифікація набору повноважень суб'єкта при доступі до інформаційної системи. Однозначним ідентифікатором персони може також виступати штрихкод. Кожному співробітнику видається картка з унікальним штрихкодом, цей код фіксується за особою в базі даних. На кожній контрольній точці пропуску встановлюється сканер штрихкодів. Цю модель з розробленим алгоритмом ідентифікації персони та фіксування проходження контролю було впроваджено в Херсонському політехнічному фаховому коледжі Державного університету «Одеська політехніка».*

Ключові слова: *облік робочого часу, персоніфікована ідентифікація, сканер штрихкодів, ідентифікація користувачів, біометрія, база даних.*

Постановка проблеми. З розвитком інформаційних технологій щораз частіше постає необхідність перекласти рутинну роботу обліку робочого часу персоналу на сучасні комп'ютеризовані прилади. У нинішній час проблема контролю над персоналом вельми актуальна на багатьох підприємствах.

Регулярне порушення трудової дисципліни призводить до фінансових втрат. Важливим моментом підвищення продуктивності є облік робочого часу кожного співробітника [1].

Аналіз останніх досліджень. Автоматизовані системи обліку робочого часу дають змогу за певними параметрами надійно і швидко ідентифікувати персонал. Завдяки таким терміналам відходять у минуле недосконалі

елементи контролю: картки, перепустки, підписи в журналі.

Системи обліку робочого часу за відбитками пальців повністю унеможливлюють запис одного співробітника замість іншого, спізнення або раннє залишення робочого місця.

Майже всі підприємства бажають скоротити витрати на процес обліку часу роботи співробітників, використовують високоякісні термінали, які допомагають з максимальною точністю виробляти контроль обліку робочого часу [2].

Автоматизовані системи обліку робочого часу дають змогу:

- зменшити кількість прогулів і запізнень на підприємстві;
- підвищити дисциплінованість колективу;
- коректно нараховувати зарплату людям, беручи до уваги лише фактично відпрацьований ними час;
- скласти графік робочого часу і доступу;
- здійснювати прогнозування діяльності та планування трудомісткості компанії;
- вести чітку базу даних співробітників і відділів;
- визначити реальний внесок конкретного співробітника в діяльність організації, означити його корисність [3].

Автоматизовані системи обліку робочого часу припускають використання спеціального обладнання, за допомогою якого здійснюється реєстрація співробітників. Практика свідчить, що у разі використання автоматизованого обліку робочого часу управління персоналом стає ефективнішим, підвищується дисципліна співробітників, на 5–15% економиться фонд оплати праці [4].

Реєстрація присутності на робочому місці всіх співробітників підприємства при автоматизованому обліку відбувається за допомогою спеціальних систем контролю. Для цього на прохідній встановлюються різні шлагбауми, контролери, турнікети та інше устаткування для керування доступом. Співробітники мають при собі спеціальні пропуски, картки, брелоки, які дають змогу їм безперешкодно пройти через ці пристрої, в деяких випадках робити це доводиться за допомогою відбитків пальця. У цей час система зчитує інформацію про кожного співробітника, відзначаючи точний час його входу і виходу. Уся інформація передається в програмне забезпечення і зберігається в пам'яті підключеного комп'ютера. На основі таких даних можуть бути сформовані точні звіти про порушення дисципліни, а також отриманий табель робочого часу [5].

Системи контролю доступу та обліку робочого часу мають зрозумілий і доступний інтерфейс, тому в процесі експлуатації терміналу кожен користувач протягом декількох секунд проходить ідентифікацію.

Програми обліку персоналу розроблені в такий спосіб, що термінали можуть і отримувати дані, і передавати інформацію про реєстрацію для складання платіжних відомостей.

Мета статті — створення моделі обліку робочого часу персоналу з подальшим розробленням та впровадженням його в освітньому закладі.

Для досягнення мети поставлені такі **завдання**:

- визначити методи персоніфікованої ідентифікації персоналу;
- обґрунтувати вибір технічного обладнання та програмного забезпечення для збору даних;
- розробити модель обліку робочого часу;
- розробити і впровадити програмне забезпечення для ідентифікації співробітників, фіксування та обліку робочого часу.

Виклад основного матеріалу. У контексті нашого дослідження важливим є забезпечення захисту інформації в автоматизованій системі обліку робочого часу.

Питання захисту інформації в комп'ютерних системах вирішується для того, щоб ізолювати інформаційну систему, яка нормально функціонує, від несанкціонованих керівних дій і доступу сторонніх осіб або програм до комп'ютерних даних, що захищаються. Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури [6].

Управління доступом — метод захисту інформації, що регулює використання ресурсів інформаційної системи, для якої розроблялася концепція інформаційної безпеки [7].

Методи і системи захисту інформації, що спираються на управління доступом, охоплюють такі функції захисту інформації в інформаційних системах, як-от:

- ідентифікація користувачів, ресурсів і персоналу системи інформаційної безпеки;
- впізнання і встановлення достовірності користувача за обліковими даними, що вводяться;
- допуск до певних умов роботи згідно з регламентом;
- протоколювання звернень користувачів до ресурсів, інформаційна безпека яких захищає ресурси

ISSN 2786-4510 (Online)

від несанкціонованого доступу і відстежує некоректну поведінку користувачів системи.

Ідентифікація користувачів є невід'ємним та важливим елементом для будь-якої інформаційної системи. Система ідентифікації і аутентифікації — один з ключових елементів інфраструктури захисту від несанкціонованого доступу. Завданням систем ідентифікації і авторизації є визначення й верифікація набору повноважень суб'єкта при доступі до інформаційної системи. [8].

Ідентифікація дає змогу суб'єкту (користувачеві, процесу, що діє від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я).

Ідентифікація — це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). За допомогою ідентифікації контролювальна сторона переконується, що суб'єкт справді той, за кого він себе видає, і перевіряє, чи має користувач із пред'явленим ідентифікатором право на доступ до ресурсу.

Існує три найпоширеніших види ідентифікації:

- парольна ідентифікація; ще не дуже давно парольна ідентифікація була ледве не єдиним способом визначення особистості користувача, вона найбільш проста як у реалізації, так і у використанні;
- апаратна (або електронна) ідентифікація — цей принцип ідентифікації ґрунтується на визначенні особистості користувача за якимось предметом, ключем, що перебуває в його користуванні; на сьогодні найбільше поширення одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти, картки зі штрихкодом і т. д.) і т. зв. токени (token), які підключаються безпосередньо до одного з портів комп'ютера;
- біометрична ідентифікація. Біометрія — це ідентифікація людини за унікальними, властивими тільки їй біологічними ознаками. Біометричні технології споконвічно розроблялися для точного встановлення особистості людини. Причому для найпоширеніших із них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів.

Останнім часом набуває поширення комплексна або багатофакторна ідентифікація, яку не можна виділити в окремий вид. У системах комплексної ідентифікації для визначення особи користувача комп'ютерної інформаційної системи застосовується відразу кілька параметрів [9].

Ідентифікатор користувача — певна унікальна кількість інформації, що дає змогу розрізняти індивідуальних користувачів парольної системи (проводити їх ідентифікацію).

Ідентифікація особи за персональним штрихкодом — на зворотному боці документа розміщується QR-код або штрихкод [10].

База даних респондентів містить облікові записи всіх користувачів цієї системи. Основними компонентами системи є:

- інтерфейс користувача;
- інтерфейс адміністратора;
- модуль сполучення з іншими підсистемами безпеки;
- база даних облікових записів.

Ідентифікація призначена для розпізнання користувачів і процесів за допомогою присвоєного індивідуального імені або особистого коду. Підсистема перевіряє, чи зареєстрований він у базі даних. Вона дає змогу спростити процедуру виокремлення конкретного користувача або процес із безлічі однотипних. Підсистема ідентифікації забезпечує виконання функцій, як-от:

- встановлення автентичності і визначення повноважень користувача або процесу при його допуску в систему;
- контролювання визначених повноважень у процесі сеансу роботи, реєстрація дій користувача.

Підсистема ідентифікації призначена для підтвердження достовірності ідентифікації як користувача, так і процесу або об'єкта системи.

Якщо в процесі ідентифікації справжність користувача або процесу встановлена, то система захисту інформації має визначити його повноваження. Це необхідно для подальшого контролю і розмежування доступу до інформаційних ресурсів системи. У цій підсистемі можуть використовуватися методи ідентифікації, засновані на: використанні паролів, використанні жетонів, електронних карток тощо, вимірі біометричних параметрів людини [11].

Поняття «робочий час» означає період, протягом якого співробітник виконує трудові обов'язки. Тривалість періоду залежить від умов трудового контракту, розпорядку робочого дня і внутрішніх правил організації.

Для оптимізації робочого процесу, підвищення ефективності праці й дотримання строків виконання завдань не обійтися без чіткого планування й контролю використання робочого часу.

Чітка організація робочого часу рівною мірою необхідна й керівнику, і підлеглим. Контроль

з боку керівника підтримує робочу дисципліну в колективі й гарантує справедливу оплату праці. Керівники організацій з великим штатом співробітників не встигають особисто допильнувати за кожним підлеглим. Крім функції контролю менеджер, начальник відділу або керівник виконує й інші обов'язки.

Під час роботи виникають непередбачені труднощі або обставини, не передбачені планом, і робочий процес повністю вгадати й розпланувати не вдається навіть лідерам тайм-менеджменту. Одночасно зі збільшенням штату множаться й завдання, так що особистий контроль робочого часу стає неможливим. Один з варіантів розв'язання проблеми — автоматизований облік робочого часу. Автоматизований моніторинг робочого часу не обмежується встановленням спеціалізованого програмного забезпечення і передбачає також встановлення контрольного обладнання при вході/виході з будівлі, обладнання пунктів пропуску, використання системи особистих ідентифікаторів для кожного працівника, фіксацію пересування персоналу під час роботи з території. Комплексний підхід до обліку робочого часу передбачає аналіз роботи фахівців з контрольних точок: штатного розкладу, плану робіт, термінів виконання завдань, території виконання обов'язків, графіка робіт.

На сьогодні усе більше систем контролю доступу оснащуються функцією обліку робочого часу, а фіксація часу входу-виходу персоналу береться до уваги при контролі дисципліни, нарахуванні заробітної плати, премій або штрафів. Утім, експлуатація цього обладнання в організації має чимало «підводних каменів», тому далеко не завжди приносить очікуваний ефект [12].

Ба більше, навіть сучасні інноваційні системи керування доступом не можуть контролювати продуктивність персоналу. Вони тільки фіксують, хто і коли приходить на роботу, а коли йде з неї. Робітник може демонструвати ідеальний 8-годинний робочий день без найменших запізнень або зайвих перерв, але при цьому буде постійно спілкуватися в соціальних мережах і влаштовувати перерви замість виконання своїх обов'язків. А інший співробітник може щодня трохи спізнюватися, але працювати з максимальною ефективністю — однак у ньому система обліку робочого часу буде розпізнавати злісного порушника дисципліни. Система такого типу потребує професійного обслуговування, без якого вона не зможе грамотно й точно обробляти отримані дані.

У будь-якій організації є різні категорії персоналу, кожна з них має свій особливий графік роботи й посадові обов'язки. Наприклад, багато співробітників (особливо на керівних посадах) регулярно відвідують інші відділи, офіси компаній-підрядників, виїжджають на ділові переговори — тому часто вони будуть відсутні на робочому місці. Навіть новітні моделі систем обліку робочого часу не зможуть ураховувати подібні нюанси самостійно, тому треба буде доручити ці завдання оператору [13].

Грамотний облік робочого часу містить у собі безліч деталей і варіантів, від дотримання яких напряму залежить правильність його результатів. Наприклад, система має враховувати не тільки загальний час перебування на робочому місці протягом дня з моменту першого входу до моменту останнього виходу. Також необхідно брати до уваги інтервали присутності, як сумарно, так і окремо. Правильна фіксація всієї цієї інформації (особливо для великого колективу) вимагає чимало часу й відповідальності.

Однозначним ідентифікатором особи може також виступати штрихкод. Кожному співробітникові видається картка з унікальним кодом, цей код фіксується за ним у базі даних (БД). На кожній контрольній точці пропуску встановлюється сканер штрихкодів, наприклад *SUNMI BLINK* 2*D* (*рис. 1*).

Sunmi Blink має інтерфейс *USB*. Сканер штрихкоду адаптований для операційної системи *Windows, Android, Linux* або іншого системного устаткування. Швидкість сканування *QR*-коду як один із критеріїв оцінки якості зчитувача штрихкоду в *Sunmi Scanning Box* становить менш ніж 0,1 секунди, що дає змогу сканувати без втрати часу.

Навіть більше, ідеальна комбінація сенсорного світіння і звукового підтвердження про стан зчитування штрихкоду підвищує ефективність роботи.

Після підключення цього сканера до комп'ютера потрібно організувати передачу даних до БД. Код, зчитаний сканером, перевіряється на присутність у БД. Якщо він присутній, то відбувається ідентифікація співробітника і запис часу проходження контролю.

Якщо такий код відсутній, то виводиться відповідне повідомлення про помилку. Алгоритм

ISSN 2786-4510 (Online)

Рис. 1. Сканер штрихкодів SUNMI BLINK 2D

ідентифікації особи і фіксування проходження контролю представлено на рис. 2.

Якщо на території декілька пунктів пропуску, то доцільно використовувати комп'ютерну мережу для передачі даних на сервер, де зберігаються всі дані про співробітників.

Передачу потрібно організувати через протокол TCP/IP. Для фіксування проходження контролю

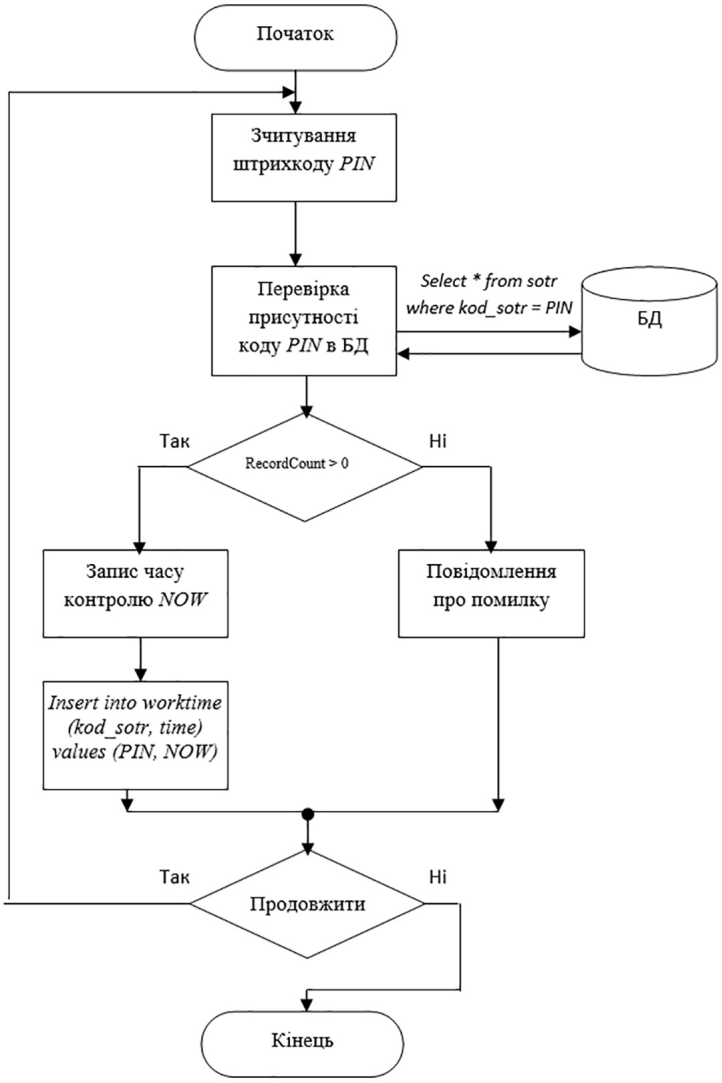


Рис. 2. Алгоритм ідентифікації особи і фіксування проходження контролю

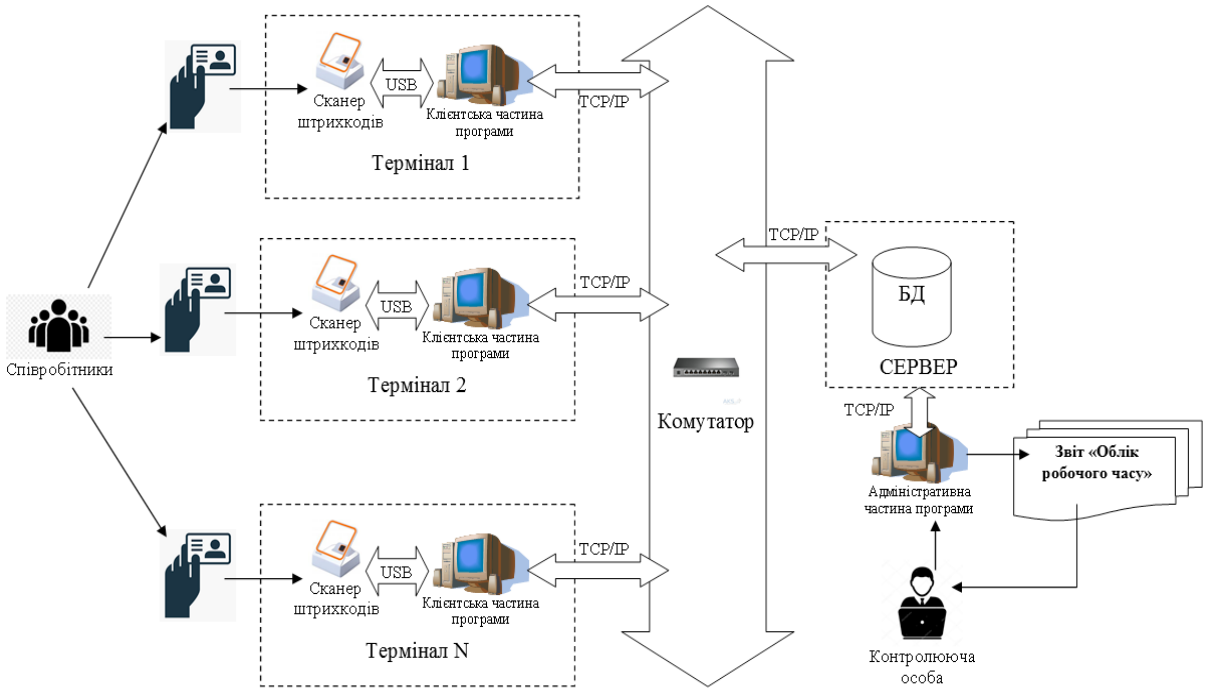


Рис. 3. Модель системи обліку робочого часу

використовується клієнтська частина програми, яка зв'язується з головною БД, проводить ідентифікацію співробітника і відправляє дані.

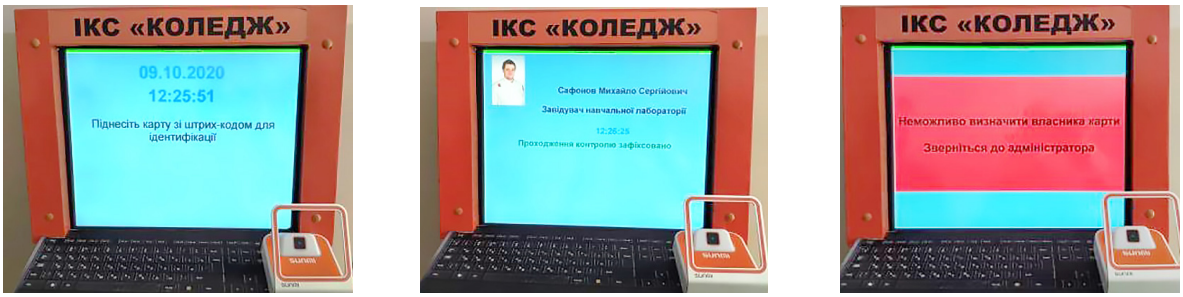
Для формування звітності, редагування переліку співробітників та відділів використовується адміністративна частина програми. Модель системи обліку робочого часу представлено на рис. 3.

Цю модель з розробленим алгоритмом ідентифікації особи і фіксування проходження контролю було впроваджено в Херсонському політехнічному фаховому коледжі Державного університету «Одеська політехніка».

Усім співробітникам коледжу видали персональні картки з унікальним штрихкодом, зареєстрованим в БД. Встановили п'ять точок проходження контролю (*рис. 4*).

У результаті впровадження алгоритму ідентифікації особи і фіксування проходження контролю з розробленою моделлю системи обліку робочого часу можна стверджувати про створення методу обліку робочого часу, що пройшов перевірку в реальних умовах [14].

Висновки. У дослідженні визначено методи персоніфікованої ідентифікації співробітників, обґрунтовано вибір технічного обладнання



а) режим очікування б) ідентифікація особи в) повідомлення про помилку

Рис. 4. Встановлена точка контролю робочого часу

ISSN 2786-4510 (Online)

та програмного забезпечення для збору даних, розроблено модель обліку робочого часу і впроваджено програмне забезпечення для ідентифікації співробітників, фіксування та обліку робочого часу.

Це дало змогу створити власний метод обліку робочого часу та впровадити систему в реальний освітній процес.

Список використаних джерел

1. Сардак С. Е., Третьяк О. О. Управління персоналом: теоретичні аспекти та практичні здобутки : монографія. Дніпропетровськ : Інновація, 2009. 157 с.
2. Краснокутська Н. С., Нащекіна О. М., Замула О. В. Менеджмент : навч. посіб. Харків : Друкарня «Мадрид», 2019. 231 с.
3. Докучаєв О. А. Методи дослідження механізму мотивації персоналу підприємства. *Економіка та держава*. 2006. № 8. С. 79–82.
4. Колісник-Гуменюк Ю. І. Сучасні тенденції розвитку освіти й науки: проблеми та перспективи : зб. наук. пр. Київ – Львів – Бережани – Гомель, 2019. Вип. 4: в 2-х томах. Т. 2. 335 с.
5. Скібіцька Л. І. Організація праці менеджера : навч. посіб. Київ : Центр учбової літератури, 2010. 360 с.
6. Бобало Ю. Я., Горбатий І. В., Яковенко Є. І. Інформаційна безпека. Львів : Львівська політехніка, 2019. 580 с.
7. Галатенко В. А. Основы информационной безопасности : учеб. пособ. Москва : Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. 205 с.
8. Воронова В. А., Тихонов В. А. Системы контроля и управления доступом. Москва : Горячая линия — Телеком, 2010. 272 с.
9. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. СПб. : Наука и техника, 2004. 384 с.
10. Шрамко В. Н. Комбинированные системы идентификации и аутентификации. *PCWeek/RE*. 2004. № 45.
11. Соловйова Т. Електронна ідентифікація захистить персональні дані українців. URL: https://uz.ligazakon.ua/ua/magazine_article/EA011004 (дата звернення 09.02.2020).
12. Контроль доступу. URL: https://uk.wikipedia.org/wiki/Контроль доступу (дата звернення: 09.02.2020).
13. Системи контролю доступу. URL: https:// smartvision.ua /category/ kontrol-dostupa/ (дата звернення: 09.02.2020).
14. Учет рабочего времени сотрудников: понятие, виды и методы. URL: https://www.kickidler.com/ru/for-it/methods-of-working/time-tracking-employees-methods.html (дата звернення: 09.02.2020).

References

1. Sardak, S. E., Tretiak, O. O. (2009). *Personnel management: theoretical aspects and practical achievements: monograph*. Dnipro : Innovatsiia [in Ukrainian].
2. Krasnokutska, N. S., Nashchekina, O. M., Zamula, O. V. (2019). *Management*. Kharkiv : Drukarnia "Madryd" [in Ukrainian].
3. Dokuchaiev, O. A. (2006). Methods of research of the mechanism of motivation of the personnel of the enterprise. *Ekonomika ta derzhava: Mizhnarodnyi naukovopraktychnyi zhurnal*, 8, 79–82 [in Ukrainian].
4. Kolisnyk-Humeniuk, Yu. I. (2019). *Current trends in education and science: problems and prospects* : zb. nauk. prats. Kyiv – Lviv – Berezhany – Homel, Vol. 4. T. 2. [in Ukrainian].
5. Skibitska, L. I. (2010). *Organization of the manager's work*. Kyiv : Tsentr uchbovoi literatury [in Ukrainian].
6. Bobalo, Yu. Ya., Horbatyi, I. V., Yakovenko, Ye. I. (2019). *Information security*. Lviv : Lvivska politekhnika [in Ukrainian].
7. Galatenko, V. A. (2008). *Fundamentals of information security.* Moscow : Internet-Universitet Informatsionnykh tekhnologiy; BINOM. Laboratoriya znaniy [in Russian].
8. Voronova, V. A., Tikhonov, V. A. (2010). *Access control and management systems*. Moscow : Goryachaya liniya — Telekom [in Russian].
9. Shcheglov, A. Yu. (2010). *Protection of computer information from unauthorized access*. St. Petersburg : Nauka i tekhnika [in Russian].
10. Shramko, V. N. (2004). *Combined identification and authentication systems*. *PCWeek/RE*. Vol. 45. Retrieved from : https://www.itweek.ru/infrastructure/article/detail.php?ID=69114 [in Russian].
11. Soloviova, T. (2018). *Electronic identification will protect the personal data of Ukrainians*. Retrieved from : https://uz.ligazakon.ua/ua/magazine_article/EA011004 [in Ukrainian].
12. *Access control* (2020). Retrieved from : https://uk.wikipedia.org/wiki/ [in Ukrainian].
13. *Access control systems* (2017). Retrieved from : https://smartvision.ua/category/kontrol-dostupa/ [in Ukrainian].
14. *Employee time tracking: concept, types and methods* (2018). Retrieved from : https://www.kickidler.com/ru/for-it/methods-of-working/time-tracking-employees-methods.html [in Russian].

V. V. Kolenko,
M. S. Safonov,
O. Ye. Iakovenko

MODELLING OF AUTOMATED WORKING TIME CONTROL SYSTEMS IN EDUCATIONAL INSTITUTIONS

Abstract. *The article includes modeling of the automated system of personnel time recording with further development and implementation of it in the educational institution. Practice shows that when using automated time recording, more effective personnel management occurs, employee discipline is increased, and the wage fund is saved on 5–15%. Personalized personnel identification methods have been identified; the selection of technical equipment and software for data collection is justified; A work time model has been developed; Software for employee identification, recording and recording of working hours has been developed and introduced. To do this, special access control equipment was installed on the passageway. Employees have special cards that allow them to easily overcome these devices. If there are several checkpoints in the territory, it is advisable to use a computer network to transfer data to the server, where all data about employees are stored. Based on such data, accurate reports of misconduct can be generated, as well as a time sheet. User identification is an integral and important element for any information system. The identification system is one of the key elements of the infrastructure for protection against unauthorized access. The task of identification and authorization systems is to determine and verify the set of authority of the subject when accessing the information system. A barcode can also act as a unique person identifier. Each employee is issued a card with a unique bar code, this code is fixed to the person in the database. A barcode scanner is installed on each pass point. This model with a developed algorithm for identifying a person and fixing the passage of control was introduced at the Kherson Polytechnic Vocational College of Odessa Polytechnic State University.*

Keywords: *time accounting, personalized identification, barcode scanner, user identification, biometrics, database.*

В. В. Коленко,
М. С. Сафонов,
А. Е. Яковенко

МОДЕЛИРОВАНИЕ СИСТЕМ АВТОМАТИЗИРОВАННОГО КОНТРОЛЯ РАБОЧЕГО ВРЕМЕНИ В УЧЕБНЫХ ЗАВЕДЕНИЯХ

Аннотация*. В статье выполнено моделирование автоматизированной системы учета рабочего времени персонала с дальнейшей разработкой и внедрением ее в учебном заведении. Практика показывает, что при использовании автоматизированного учета рабочего времени происходит более эффективное управление персоналом, повышается дисциплина сотрудников, на 5–15% экономится фонд оплаты труда. Были определены методы персонифицированной идентификации персонала; обоснован выбор технического оборудования и программного обеспечения для сбора данных; разработана модель учета рабочего времени; разработано и внедрено программное обеспечение для идентификации сотрудников, фиксирования и учета рабочего времени. Для этого на проходной было установлено специальное оборудование для управления доступом. Сотрудники имеют при себе специальные карточки, которые позволяют им беспрепятственно преодолеть эти устройства. Если на территории несколько пунктов пропуска, то целесообразно использовать компьютерную сеть для передачи данных на сервер, где хранятся все данные о сотрудниках. На основе таких данных могут быть сформированы точные отчеты о нарушении дисциплины, а также табель рабочего времени. Идентификация пользователей является неотъемлемым и важным элементом для любой информационной системы. Система идентификации есть одним из ключевых элементов инфраструктуры защиты от несанкционированного доступа. Задача систем идентификации и авторизации — определение и верификация набора полномочий субъекта при доступе к информационной системе. Однозначным идентификатором персоны может также выступать штрихкод. Каждому сотруднику выдается карточка с уникальным штрихкодом, который фиксируется за персоной в базе данных. На каждой контрольной точке пропуска устанавливается сканер штрихкодов. Данная модель с разработанным алгоритмом идентификации персоны и фиксирования прохождения контроля была введена в Херсонском политехническом профессиональном колледже Государственного университета «Одесская политехника».*

Ключевые слова: *учет рабочего времени, персонифицированная идентификация, сканер штрихкодов, идентификация пользователей, биометрия, база данных.*

ІНФОРМАЦІЯ ПРО АВТОРІВ

Коленко Віолетта Володимирівна — заступниця директора з навчально-виробничої роботи, спеціалістка І категорії, Херсонський політехнічний коледж Одеського національного політехнічного університету, м. Херсон, Україна, violka1986@ukr.net; ORCID ID: https://orcid.org/0000-0001-6376-1278

Сафонов Михайло Сергійович — канд. техн. наук, завідувач кафедри, Херсонський політехнічний коледж Одеського національного політехнічного університету, м. Херсон, Україна, nemko85@gmail.com; ORCID ID: https://orcid.org/0000-0001-9742-8270

Яковенко Олександр Євгенович — канд. техн. наук, доцент, директор, Херсонський політехнічний коледж Одеського національного політехнічного університету, м. Херсон, Україна, 00237191@ukr.net; ORCID ID: https://orcid.org/0000-0001-7647-6425

INFORMATION ABOUT THE AUTHORS

Kolenko V. V. — Deputy Director for Training and Production, Category I specialist, Kherson Polytechnic College of Odessa National Polytechnic University, Kherson, Ukraine, violka1986@ukr.net; ORCID ID: https://orcid.org/0000-0001-6376-1278

Safonov M. S. — PhD in Engineering, Head of Sub-Department, Kherson Polytechnic College of Odessa National Polytechnic University, Kherson, Ukraine, nemko85@gmail.com; ORCID ID: https://orcid.org/0000-0001-9742-8270

Iakovenko O. Ye. — PhD in Engineering, Associate Professor, Director, Kherson Polytechnic College of Odessa National Polytechnic University, Kherson, Ukraine, 00237191@ukr.net; ORCID ID: https://orcid.org/0000-0001-7647-6425

ИНФОРМАЦИЯ ОБ АВТОРАХ

Коленко В. В. — заместитель директора по учебно-производственной работе, специалист I категории, Херсонский политехнический колледж Одесского национального политехнического университета, г. Херсон, Украина, violka1986@ukr.net; ORCID ID: https://orcid.org/0000-0001-6376-1278

Сафонов М. С. — канд. техн. наук, заведующий кафедры, Херсонский политехнический колледж Одесского национального политехнического университета, г. Херсон, Украина, nemko85@gmail.com; ORCID ID: https://orcid.org/0000-0001-9742-8270

Яковенко А. Е. — канд. техн. наук, доцент, директор, Херсонский политехнический колледж Одесского национального политехнического университета, г. Херсон, Украина, 00237191@ukr.net; ORCID ID: https://orcid.org/0000-0001-7647-6425

Стаття надійшла до редакції / Received 28.02.2020