УДК 621.317
DOI: https://doi.org/10.26642/tn-2018-2(82)-208-214

Ю.О. Подчашинський, д.т.н., проф.
О.О. Лугових, ст. викладач
О.Р. Немчак, магістрант, гр. АТ-21-2м
Житомирський державний технологічний університет

Дослідження методів ідентифікації та визначення параметрів руху транспортних засобів в системі доступу на закритий об'єкт

Безпека в нашій країні та за її межами вимагає знайдення нових інформаційних технологій захисту та охорони об'єктів від несанкціонованого доступу. Особливо нагальною є потреба у захисті об'єктів державного значення. Охорона периметру територій неможлива без використання комп'ютеризованих систем контролю та вимірювання параметрів руху об'єктів. З розвитком інформаційних технологій і зростає оснащеність зловмисників, які знаходять все нові шляхи подолання перешкод на своєму шляху.

Тому актуальною задачею є удосконалення комп'ютеризованих систем доступу на закритих об'єктів з метою підвищення їх стійкості до нападів та надійності функціонування.

У роботі проведено аналіз сучасних методів, засобів та технологій ідентифікації та визначення параметрів руху транспортних засобів. Виявленні переваг та недоліки для розробки нових інформаційних технологій ідентифікації об'єктів в системах контролю доступу на об'єкт.

Сучасні моделі та методи побудови комп'ютеризованої системи ідентифікації транспортних засобів ґрунтуються на комплексному рішенні. Запропоновано метод побудови блоку прийняття рішень з ідентифікації об'єктів. Здійснене проектування продукційної моделі бази знань із врахуванням вагових коефіцієнтів для зниження показників помилок першого та другого роду.

Ключові слова: *ідентифікація транспортних засобів; параметри руху; система контролю і управління доступом (СКУД); радіочастотна ідентифікація (RFID); розпізнавання номерних знаків; смарт-карти.*

Постановка проблеми. Напруженість ситуації на сході нашої країни та й у світі в цілому вимагає знайдення нових інформаційних технологій захисту та охорони об'єктів від несанкціонованого доступу. Особливо нагальною є потреба у захисті об'єктів критичної інфраструктури.

Охорона периметру територій неможлива без використання комп'ютеризованих систем управління та автоматики. Однак з розвитком інформаційних технологій і зростає оснащеність зловмисників, які знаходять все нові шляхи подолання перешкод на своєму шляху. Тому достатньо актуальним є удосконалення комп'ютеризованих систем доступу на закритих об'єктів з метою підвищення їх стійкості та надійності функціонування.

Досягти належного рівня захисту периметру закритих об'єктів неможливо без використання сукупності методів ідентифікації транспортних засобів та осіб, які інтегровані в комп'ютеризовані системи контролю доступу на об'єкт.

Аналіз останніх досліджень і публікацій. Вагомий внесок у створення подібних систем та розвиток методів і засобів їх побудови внесли роботи таких вітчизняних та закордонних авторів: Т.К. Вінцюка, М.І. Шлезінгера, Ю.А. Оленіна, О.О. Кузнєцова, О.К. Юдіна, О.Г. Корченка, Г.Ф. Конаховича, О.М. Новікова, М.В. Гайворонського, О.О. Шелупанова, О.О. Афанасьева, Л.Шапиро, Ф.Уоссермена, Дж. Стокмана та інші.

Метою проведення досліджень є підвищення рівня захисту периметру закритих об'єктів від несанкціонованого доступу, головною задачею якого є дослідження та оптимізації методів ідентифікації транспортних засобів для інтеграції в комп'ютеризовані системи контролю доступу на об'єкт.

Викладення основного матеріалу. Аналіз робіт вказаних авторів показав, що вони направлені, в основному, на розробку моделей та методів побудови інтелектуальних інформаційних систем виявлення порушника; технічних засобів захисту інформації; систем однофакторної та багатофакторної ідентифікації особи; методів автоматизації обробки зорової інформації; створення засобів фізичного захисту.

В результаті проведеного аналізу виявлено, що в сучасних комп'ютеризованих системах доступу на об'єкт необхідно використовувати багатофакторну ідентифікацію як транспортних засобів так і осіб для захисту від підробок. Однак наявність великої кількості методів ідентифікації вимагає їх ретельного аналізу та вибору для сукупного використання шляхом інтеграції в єдину комп'ютеризовану систему контролю доступу на закритий об'єкт.

Система контролю і управління доступом (СКУД) – це комплекс об'єднаних електронних, механічних, електротехнічних, апаратно-програмних та інших засобів, що забезпечують можливість

доступу певних осіб в окремі зони або до певної апаратури, технічних засобів і предметів. І що обмежують доступ особам, які не мають такого права [1, 2].

Захист будь-якого об'єкта включає кілька рубежів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках важливим рубежем буде система контролю та управління доступом (СКУД) на об'єкт.

Добре організована з використанням сучасних технічних засобів СКУД дозволить вирішувати цілий ряд завдань. До числа найбільш важливим можна віднести наступні: протидія промислового шпигунства; протидія розкраданню; протидія саботажу; протидія навмисного пошкодження матеріальних цінностей; облік робочого часу; контроль своєчасності прибуття і відбуття співробітників; захист конфіденційності інформації; регулювання потоку відвідувачів; контроль в'їзду та виїзду транспорту.

В якості найбільш часто використовуваних СКУД можна назвати такі: турнікети звичайні і настінні; турнікети для проходу в коридорах; шлюзові кабіни; автоматичні заслінки; роторні турнікети; обертові двері; дорожні блокіратори; шлагбауми; паркувальні системи; круглі розсувні двері; триштангові турнікети; повнозростові турнікети; розсувні турнікети.

В нашому випадку розглядається ідентифікація транспортних засобів для доступу на закритий об'єкт. Для організації в'їзду/виїзду транспорту створюються транспортні контрольно-пропускні пункти КПП. До складу транспортного КПП входить оглядовий майданчик і службові приміщення.

Контрольно-пропускні пункти для пропуску автотранспорту обладнуються:

– розсувними або зсувними воротами і шлагбаумами з механічним, електромеханічним і гідравлічним приводами, а також пристроями для аварійної зупинки воріт і відкривання їх вручну,
– майданчиками для контролю з помостами для огляду автомобілів;
– світлофорами, попереджувальними знаками і світловими табло типу «Бережись автомобіля»;
– телефонним та тривожним зв'язком і освітленням для огляду транспорту.[3]

Системи контролю та управління доступу (СКУД) є найдавнішою складовою системи безпеки. На сьогоднішній день існує дуже багато різновидів СКУД різних виробників, а також її компонентів.

Незважаючи на унікальність кожної конкретної системи контролю доступу, вона містить 4 основних елемента: ідентифікатор користувача (карта-пропуск, ключ), пристрій ідентифікації, керуючий мікроконтролер і виконавчі пристрої. Загальна схема СКУД показана на рисунку 1.

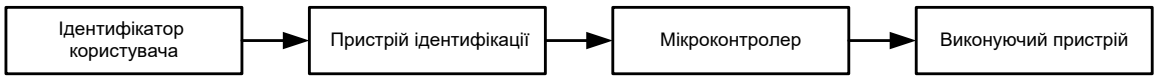

Рис. 1. Загальна схема СКУД

Роботу системи контролю та управління доступом можна описати наступним чином. Кожен співробітник або постійний відвідувач організації отримує ідентифікатор (електронний ключ) – пластикову картку або таблетку ibutton з індивідуальним кодом. Електронні ключі видаються в результаті реєстрації перерахованих осіб за допомогою засобів системи. Паспортні дані, фото (відеозображення) та інші відомості про власника електронного ключа заносяться в персональну електронну картку. Персональна електронна картка власника і код його електронного ключа зв'язуються один з одним і заносяться в спеціально організовані комп'ютерні бази даних.

Залежно від способу перевірки прийнято розрізняти кілька видів СКУД:

– ручні (визначення автентичності особистості здійснюється контролером на основі пред'явленого пропуску з фотографією власника);
– механізовані (фактично та ж ручна перевірка з елементами автоматизації зберігання і пред'явлення пропусків);
– автоматизовані (ідентифікація користувача і перевірка особистісних атрибутів здійснюється електронним автоматом, а аутентифікація і прийняття рішення про надання доступу проводиться оператором КПП;
– автоматичні (вся процедура перевірки і прийняття рішення здійснюється комп'ютером).[4].

Розглянемо автоматизовану систему управління транспортним пунктом «CarGo Enterprise» та мережеву систему контролю і управління проїздом автомобілів «ISBS RFID», зокрема їх технічні та програмні засоби.

АСУ КТП призначена для роботи самостійно або при взаємодії з інтегрованим комплексом безпеки.

Доступ автомобілів через контрольні точки (контрольно-транспортні пункти, проміжні пункти реєстрації, вагові та т.п.) здійснюється на основі даних, одержуваних від відеокамер системи розпізнавання державних номерних знаків автомобілів. Система приймає рішення про допуск автомобіля на контрольовану територію згідно правил, співставлення номерному знаку автомобіля (рис. 2).

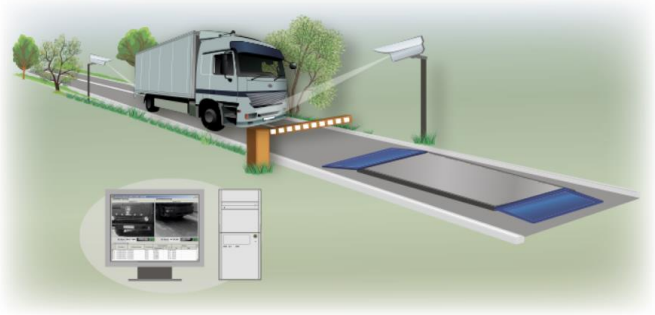

Рис. 2. Зона контролю транспортним пунктом

Вона має всі необхідні засоби для опису структури проїздів підприємства, яка може мати складну, в тому числі і ієрархічну, організацію з безліччю майданчиків, в'їздів і виїздів і т.п. Дозволяє організувати гнучку систему доступу автомобілів на майданчики підприємства шляхом створення відповідних груп доступу, і опису дозволених інтервалів часу доступу. Дозволяє вести каталог транспортних засобів (автомобілів) із завданням відповідних атрибутів в разі необхідності (для постійних автомобілів).

Всі ПК системи за допомогою відповідних засобів підключаються до локальної мережі або об'єднуються в окремий її сегмент. Мінімальний комплект програмного забезпечення системи складається з одного модуля «CarGo. Сервер ТД» і одного модуля «CarGo. Адміністратор». Мінімальний комплект може забезпечити роботу тільки в режимі «Реєстрація». В якості системи управління базами даних використовується СУБД «FireBird» версії 2.5 [5].

Мережева система контролю і управління проїздом автомобілів «ISBS RFID» являє собою апаратно-програмний комплекс, за допомогою якого вирішується завдання організації автоматичного або автоматизованого проїзду на підконтрольну територію і обліку переміщення транспорту. До складу входить апаратна RFID-платформа (зчитувач, мітки) і web-сервіс, реалізований на «хмарних» технологій. Ідентифікація автомобілів здійснюється за принципом «свій/чужий». Ідентифікаторами є безконтактні мітки радіочастотної ідентифікації (RFID), які однозначно визначають конкретний автомобіль або людини, керуючого автомобілем. Мітка не має ні батарейки, ні акумулятора, термін її експлуатації практично не обмежений. На підставі аналізу даних RFID-мітки відбувається управління шлагбаумами, воротами або іншими бар'єрами (рис. 3). Дальність виявлення мітки налаштовується програмно і може залишати від 0.5 до 10 метрів, що для більшості завдань з організації проїзду більш ніж достатньо. У деяких випадках, за запитом замовника, можна досягти дальності до 20 метрів.

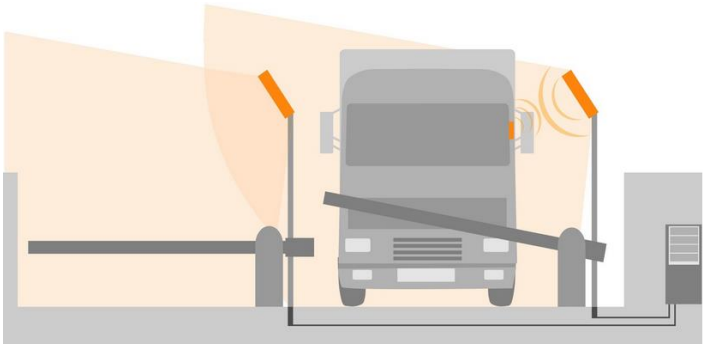

Рис. 3. Загальний вигляд КТП, на якому застосовується RFID-ідентифікація

Додатковою функцією мережевої системи контролю може бути фіксація та аналіз параметрів руху транспортних засобів. При цьому фіксується час проходження цих засобів повз контрольні точки, оснащені зчитувачами радіочастотної ідентифікації. Далі ці дані аналізуються з метою оптимізації траєкторій переміщень транспортних засобів на закритому об'єкті, визначення потрібних часових інтервалів та швидкостей руху, виявлення порушень правил доступу.

Зчитувач радіочастотної ідентифікації розміщується поблизу шлагбаума (воріт або інших бар'єрів), яким він керує. До RFID зчитувача підключаються від 1 до 4 антен, які здійснюють постійний моніторинг міток. Як тільки RFID-мітка потрапляє в поле дії антени, відбувається її ідентифікація та визначення прав доступу. Якщо автомобілю з даної міткою проїзд дозволений – RFID-зчитувач відкриває шлагбаум. Управління шлагбаумом проводиться за допомогою внутрішнього реле пристрою, внутрішніх оптронів або за допомогою реле зовнішнього Ethernet-модуля промислової автоматизації Laurent. Всі дії можуть бути записані в журнал подій мережевого програмного забезпечення.

Програмне забезпечення складається з декількох модулів. Всі модулі є «мережевими», тобто розгортаються на будь-якому ПК локальної мережі Ethernet, доступ до WEB-інтерфейсу здійснюється через браузер (можливий доступ і через глобальну мережу Інтернет). WEB-інтерфейс адаптивний, зручний для роботи на будь-якому пристрої (ПК, планшет, смартфон, iPhone та ін.) [6].

Згідно з проведеного аналізу сучасних СКУД для транспортних засобів запропонованих на ринку, можна визначити основні особливості роботи, матеріально-технічний склад, методи та засоби ідентифікації, що застосовуються в цих системах. Отже можна зробити висновок, що всі системи доступні на ринку використовують однофакторну систему ідентифікації.

Отже, перейдемо до аналіз методів ідентифікації транспортних засобів, а саме, до аналізу методу та технології ідентифікації транспортних засобів по номерному знаку.

В даний час існує не так багато систем визначення номерних знаків, не всі з яких є по-справжньому якісною продукцією. Однак, паралельно з написанням алгоритмів, розробляються апаратні засоби саме для цих цілей. Системи, що володіють високою швидкодією і точністю розпізнавання, як правило, дуже дорогі. Висока вартість існуючих продуктів не дозволяє здійснити їх масове впровадження.

Задачу ідентифікації автомобіля можна умовно розділити на дві частини: локалізація номерної пластини і розпізнавання символів.

Алгоритм розпізнавання номерного знака складається з наступних етапів:

1. Початок.
2. Вхідне зображення.
3. Запис в конвеєр обробки.
4. Еквалізація (вирівнювання гістограми).
5. Фільтрація.
6. Пошук ліній.
7. Бінарізація.
8. Відфільтрування надлишковості.
9. Пошук області інтересу.
10. Пошук цифр та літер (9 символів з літерами).
11. Порівняння з тесовим зображенням (кореляція).
12. Вивід значень номерного знаку.
13. Вивід розпізнаного зображення.
14. Кінець.

Рис. 4. Приклади роботи алгоритмів нормалізації і сегментації символів

Ці цифри згенеровані заздалегідь. Далі вибираємо найкраще збіг, і, якщо воно більше деякого порога – приймаємо це за хороший результат. Області перебираються зліва направо, так що потрібні цифри вийдуть в потрібному порядку.

В даному випадку реалізований найпростіший алгоритм виведення цифри за параметрами – порівняння з шаблоном. Є кілька варіантів, у кожного є свої плюси і мінуси. Даний метод, який реалізований – цілком простий, має прийнятну надійність, прийнятну стійкість.[7, 8, 9].

Розглянуті вище методи ідентифікації транспортних засобів мають ряд недоліків.

RFID СКУД має вразливості в системи. Зі збільшенням популярності дана технологія викликає більший і більший інтерес у зловмисників, які прагнуть отримати неправомірну вигоду, обходячи, зламуючи RFID системи ідентифікації. Всебічне поширення технології зумовило виникнення цілої низки різноманітних атак, які спрямовані виключно на перешкоджання штатній роботі систем.

Але при всьому найбільш вразливим є канал передачі даних при штатному використанні є смарт-карти. Зафіксовано такі різновиди атак на канал: блокування доступу для рідера; часовий аналіз;простий аналіз споживаної потужності; атаки на відмову. Також можлива фізична атака на чіп, яка є дуже простою й може забезпечити доступ до його найбільш захищених частин.

Ідентифікації транспортного засобу по номерному знаку також виявлено певні недоліки:

- відсутність можливості розпізнавання забруднених державних реєстраційних номерних знаків;
- низька швидкодія розпізнавання, зумовлена складністю алгоритму розпізнавання зображень;
- можливість використання зловмисниками викраденого, підробленого номерного знаку або його імітації.

Отже, в результаті проведеного аналізу методів та технологій транспортних засобів встановлено, що для удосконалення методів ідентифікації транспортних засобів необхідним є використання комбінування методів розпізнавання та засобів безконтактної ідентифікації в інтегрованій комп’ютеризованій системі доступу на закритий об’єкт.

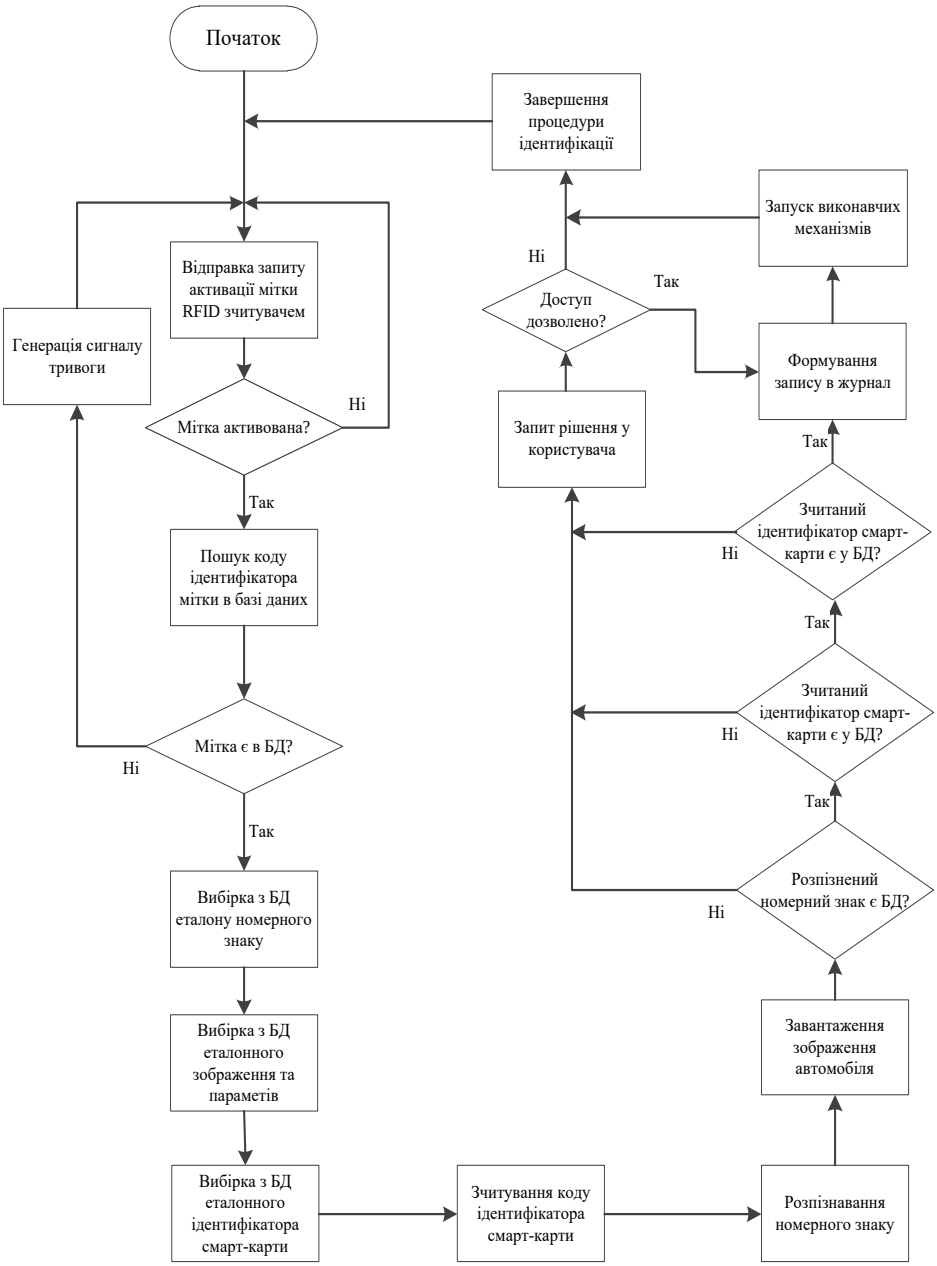

Рис. 5. Блок-схема алгоритму роботи блоку ідентифікації та контролю доступу

Проведений аналіз відомих методів ідентифікації транспортних засобів показав, що найбільш ефективними, на наш погляд, є:

- метод ідентифікації по номерному знаку автомобіля;
- метод ідентифікації транспортних засобів по їх зображенню;
- RFID-технологія ідентифікації;
- ідентифікація водія за допомогою смарт-карти.

Запропонуємо скласти систему ідентифікації з відповідних чотирьох модулів.

Модуль 1 являє собою комп'ютеризовану підсистему ідентифікації транспортних засобів по номерному знаку.

Модуль 2 являє собою комп'ютеризовану підсистему ідентифікації транспортних засобів по їх зображенню. Підсистема складається з двох блоків, а саме: блоку попередньої обробки; блоку ідентифікації по зображенню.

Модуль 3 – метод побудови комп'ютеризованої підсистеми ідентифікації транспортних засобів з використанням RFID-технологій та Модуль 4 смарт-карти.

В системі багатофакторної ідентифікації програма є модулем прийняття рішень, програма дозволяє здійснювати адміністрування баз даних ідентифікаторів. Для даної системи була розроблена блок-схема алгоритму програми, що представлена на рисунку 5 [10].

Висновки. Для оцінки ефективності роботи запропонованої комп'ютеризованої системи багатофакторної ідентифікації транспортних засобів скористаємося методами теорії ймовірності. Результат приведено на рисунку 6.

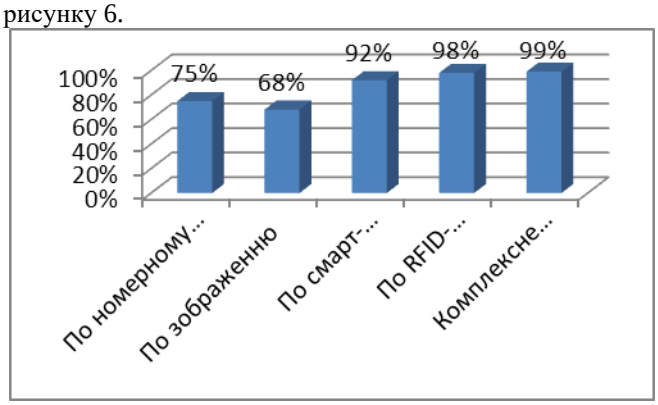

Рис. 6. Діаграма відображення ймовірності спрацьовування системи

Таким чином, здійснена оцінка ефективності роботи запропонованої комп'ютеризованої системи багатофакторної ідентифікації транспортних засобів, яка побудована за допомогою системного підходу, підтвердила ефективність такого підходу та підвищила ймовірність спрацьовування кожної із систем до 99 %.

Список використаної літератури:

1. *Корченко А.Г.* Анализ и оценивание рисков информационной безопасности : монография / *А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук.* – К. : ООО «Лазурит- Полиграф», 2013. – 275 с.
2. *Оленин Ю.А.* Проблемы комплексного обеспечения охранно-территориальной безопасности и физической защиты особо важных объектов / *Ю.А. Оленин* // Охранные системы. – 2002. – № 3 (27). – С. 7–26.
3. *Оленин Ю.А.* Специфика построения периметровых систем охраны / *Ю.А. Оленин, Н.П. Петровский* // Системы безопасности, связи и телекоммуникаций. – 1999. – № 29. – С. 85.
4. *Оленин Ю.А.* К вопросу о категорировании объектов с позиции охранной безопасности / *Ю.А. Оленин, С.Ф. Алаухов* // Системы безопасности, связи и телекоммуникаций. – 1999. – № 30. – С. 26.
5. Автоматизированная система управленияконтрольно транспортным пунктом / CarGo Enterprise [Електронный режим]. – Режим доступу : http://intteks.com.ua/images/materials/doc/enterprise2.pdf.
6. ISBS RFID – Мережева системи контролпю і уравління проїздом автомобілів [Електронний ресурс]. – Режим доступу : http://www.isbc-rfid.ru/_solutions/id_12/.
7. *Мурыгин К.В.* Нормализация изображения автомобильного номера и сегментация символов для последующего распознавания / *К.В. Мурыгин* // Искусственный интеллект. – 2010. – № 3. — С. 367–369.
8. *Лугових О.О.* Дослідження методів ідентифікації для доступу транспортних засобів на закритий об'єкт / *О.О. Лугових, О.Р. Немчак* : IX Міжнародна науково-технічна конференція «Інформаційно-комп'ютерні технології 2018», м. Житомир, 20–21 квітня 2018р. – С. 182–183 [Електронний ресурс]. – Режим доступу : https://conf.ztu.edu.ua/wp-content/uploads/2018/05/182-1.pdf.
9. *Nemchak O.* Study of identification methods for access of vehicles to closed object / *O.Luhovykh, S.Kobzar* // V All Ukrainian Scientific and Practical Conference «Current trends in young scientists' researches», April 12, 2018. – Zhytomyr : ZHDTU, 2018. – С. 92–95.
10. *Ворона В.А.* Системы контроля и управления доступом / *В.А. Ворона, В.А. Тихонов.* – М. : Горячая линия Телеком, 2010. – 272 с. : ил.

References:

1. Korchenko, A.G., Arkhipov, A.E. and Kazmirchuk, S.V. (2013), *Analiz i otsenivanie riskov informatsionnoy bezopasnosti*, monografiya, OOO «Lazurit- Poligraf», 275 p.
2. Olenin, Yu.A. (2002), «Problemy kompleksnogo obespecheniya okhranno-territorial'noy bezopasnosti i fizicheskoy zashchity osobo vazhnykh ob"ektov», *Okhrannye sistemy*, No. 3 (27), Pp. 7–26.
3. Olenin, Yu.A. and Petrovskiy, N.P. (1999), «Spetsifika postroeniya perimetrovykh sistem okhrany», *Sistemy bezopasnosti, svyazi i telekommunikatsiy*, No. 29, 85 p.
4. Olenin, Yu.A. and Alaukhov, S.F. (1999), «K voprosu o kategorirovanii ob"ektov s pozitsii okhrannoy bezopasnosti bezopasnosti», *Svyazi i telekommunikatsiy*, No. 30, 26 p.
5. CarGo Enterprise (2012) «Avtomatizirovannaya sistema upravleniya kontrol'no transportnym punktom», available at: http://intteks.com.ua/images/materials/doc/enterprise2.pdf

6. ISBS RFID (2018), «Merezheva sistemi kontrolpyu i uravlinnya proïzdom avtomobiliv», avialable at: http://www.isbc-rfid.ru/_solutions/id_12/
7. Murygin, K.V. (2010), «Normalizatsiya izobrazheniya avtomobil'nogo nomera i segmentatsiya simvolov dlya posleduyushchego raspoznavaniya», *Iskusstvennyy intellect*, No. 3, Pp. 367–369.
8. Lugovykh, O.O. and Nemchak, O.R. (2018), «Doslidzhennja metodiv identyfikacii' dlja dostupu transportnyh zasobiv na zakrytyj ob'jekt», *IX Mizhnarodna naukovo-tehnichna konferencija «Informacijno-komp'juterni tehnologii' 2018*, 20–21 kvitnja, Zhytomyr, Pp. 182–183.
9. Nemchak, O., Luhovykh, O. and Kobzar, S. (2018), «Study of identification methods for access of vehicles to closed object», *V All Ukrainian Scientific and Practical Conference «Current trends in young scientists' researches»*, April 12, Zhytomyr, ZHDTU, Pp. 92–95.
10. Vorona, V.A. and Tikhonov, V.A. (2010), *Sistemy kontrolya i upravleniya dostupom*, Goryachaya liniya Telekom, M., 272 p.

Подчашинський Юрій Олександрович – доктор технічних наук, професор кафедри метрології та інформаційно-вимірювальної техніки Житомирського державного технологічного університету.

Наукові інтереси:
- методи вимірювання механічних величин;
- цифрова обробка відеозображень;
- комп'ютеризовані системи управління.

E-mail: ju.podchashinskiy@gmail.com.

Лугових Оксана Олександрівна – старший викладач кафедри метрології та інформаційно-вимірювальної техніки Житомирського державного технологічного університету.

Наукові інтереси:
- методи вимірювання механічних величин;
- цифрова обробка відеозображень;
- комп'ютеризовані системи управління.

E-mail: auts_ksy@ztu.edu.ua.

Немчак Ольга Русланівна – магістрант групи АТ-21-2м Житомирського державного технологічного університету.

Наукові інтереси:
- безпека середовищ та об'єктів ;
- комп'ютеризовані системи управління.

E-mail: olga.nemchak@gmail.com.

Стаття надійшла до редакції 08.10.2018.