УДК 004.934:681.391
DOI: 10.18372/2310-5461.38.12830

О. К. Юдін, д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0001-5098-7796
e-mail: kszi@ukr.net;

О. М. Весельська
Національний авіаційний університет
orcid.org/0000-0002-4914-2187
e-mail: olga_veselskaya@ukr.net

АНАЛІЗ ТА КЛАСИФІКАЦІЯ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА ПІДПРИЄМСТВІ

Вступ

Підприємство — це складна система, яка складається з однієї або декількох виробничих, адміністративних будівель і споруд та володіє власною інфраструктурою, включаючи системи гідро-, енерго- і транспортних комунікацій. Всі вони вимагають особливого підходу в оснащенні автоматизованими системами для забезпечення безперебійної роботи.

Однією з найголовніших таких систем є система управління контролю доступу на підприємстві (СУКД).

Установка системи контролю та управління доступом є однією з найбільш важливих і необхідних систем в структурі будь-якого підприємства. Функціонал системи автоматизує виробничі процеси, контролює доступ на територію підприємства і до його споруд, ідентифікує і управляє користувачами, запобігає несанкціонованому доступу, дозволяє зонувати приміщення з різними правилами організації доступу. Все це стало можливим завдяки використанню інформаційних технологій, які стрімко розвиваються, і цим самим надають нові можливості для посилення контролю і безпеки не тільки до об'єктів, а і до інформації підприємства. На сьогодні існує безліч варіантів використання СУКД залежно від режиму таємності підприємства та від його потреб та можливостей [1–3].

Для оптимального вибору СУКД для кожного підприємства необхідно проаналізувати та класифікувати існуючі СУКД. З огляду на остатні проаналізовані дослідження у цієї області [1–10], з'ясовано, що в сучасних системах управління контролю доступом велику увагу приділено таким новітнім інформаційним технологіям як ідентифікація, біометрична аутенфікація особистості, що надає нові можливості для розвитку цих систем.

Мета статті — проаналізувати існуючі сучасні системи контролю та управління доступом. На базі проведеного аналізу здійснити класифікацію сучасних систем контролю та управління доступом на підприємстві. Виявити подальші шляхи дослідження з використанням інформаційних технологій, з метою посилення рівня безпеки на підприємстві, а також можливості отримання інформації різного рівня таємності.

Основна частина

Системою контролю та управління доступу називають сукупність програмно-апаратних технічних засобів безпеки, що мають на меті: обмеження і реєстрацію входу-виходу об'єктів (людей, транспорту) на заданій території через «точки проходу»: двері, ворота, контрольно-пропускні пункти [3]. Також, СКУД використовують для збору різноманітної інформації про працівників, їх пересування територією підприємства, термінів і часу знаходження в підрозділах та ін.

Сучасні СКУД складаються з таких елементів:

1. *Ідентифікатор* — пристрій, який дозволяє системі розпізнати людину. На цій посаді часто використовуються популярні зараз безконтактні карти, контактні карти (з чорної магнітної смужкою), електронні брелоки. Ще в ролі ідентифікатора може виступати спеціальний код, який вводить людина під час входу в зону, що охороняється або біометричні дані — відбитки пальців або долоні, відбиток сітківки очей, розпізнавання голосу і т. д.

2. *Зчитувач* — пристрій для розпізнавання і передачі даних на керуючий блок.

3. *Керуючий блок*— «мозок» системи. Виконує функцію прийняття рішень щодо можливості визначити, чи потрібен доступ до приміщення для власника конкретного ідентифікатора. Якщо доступ дозволяється — надсилається сигнал на

відкриття електронного замка (турнікета, шлагбаума, двері). У мережевих СКУД додатково до керуючого блоку підключається комп'ютер.[3]

Основним завданням СКУД є управління доступом на задану територію, включаючи також обмеження доступу на задану територію, ідентифікація особи, яка має доступ на задану територію, а також облік робочого часу; розрахунок заробітної плати (при інтеграції з системами бухгалтерського обліку); ведення бази персоналу/відвідувачів; інтеграція зі всіма системами безпеки:

- з системою відеоспостереження для суміщення архівів подій систем, передачі системі відеоспостереження повідомлень про необхідність стартувати запис, повернути камеру для запису наслідків зафіксованого підозрілого події;
- з системою охоронної сигналізації (СОС) для обмеження доступу в приміщення, або для автоматичного зняття і постановки приміщень на охорону;
- з системою пожежної сигналізації (СПС) для отримання інформації про стан пожежних сповіщувачів, автоматичного розблокування евакуаційних виходів і закривання протипожежних дверей в разі пожежної тривоги [4].

На особливо відповідальних об'єктах мережа пристроїв СКУД виконується фізично незв'язаної з іншими інформаційними мережами.

У точках доступу на об'єкт монтуються зчитувачі, які зчитують код електронних карт доступу і передають його в контролери СКУД.

Далі контролер приймає рішення на підставі внутрішньої бази даних користувачів або отриманої з комп'ютерної бази даних, і відповідно до запрограмованих алгоритмам контролю, управляє виконавчими пристроями СКУД.

Кожен користувач СКУД, будь то працівник підприємства або відвідувач, отримує електронну пластикову карту доступу, яка видається після реєстрації на пункті контролю.

Кожній електронній карті доступу відповідає конкретний користувач системи зі своїми правами доступу на контрольований об'єкт.

Уся необхідна інформація про користувача також заноситься на комп'ютер диспетчера системи в базу даних СКУД.

При побудові мережевих СКУД використовуються чотири рівні мережевої взаємодії [5]:

1. Перший (вищий) рівень являє собою комп'ютерну мережу типу клієнт/сервер на основі мережі ETHERNET, з протоколом обміну TCP/IP і з використанням мережевих операційних систем Windows NT або Unix. Цей рівень забезпечує зв'язок між сервером і робочими комп'ютерами підсистем.

2. Другий рівень — зв'язок між контролерами і комп'ютерами підсистем. На цьому рівні використовується інтерфейс RS 232.

3. Третій рівень — зв'язок між контролерами і зчитувачами пристроями. Тут застосовується інтерфейс RS 485 або, що стали вже стандартом, інтерфейси зчитувачів або магнітних карт.

4. Четвертий рівень — рівень сповіщувачів пожежної сигналізації і ланцюгів управління — збалансовані і незбалансовані радіальні і адресні шлейфи, релейні вихідні ланцюга управління. Тут застосовуються нестандартні спеціалізовані інтерфейси і протоколи обміну інформацією.

Системи автоматизованого контролю доступу можна поділити на два типа: *автономні і мережеві системи* [6].

До *автономних* СКУД належать системи, що розташовані у одному приміщені. Їх головна функція — обмеження доступу до об'єктів, що контролюються.

Такі СКУД використовують для невеликих підприємств з декількома пунктами пропуску на об'єкт.

До таких СКУД можливо підключити різні пристрої: шлагбауми, турнікети, електромагнітні замки та зчитувачі RFID. RFID (Radio Frequency Identification) — метод, що автоматично ідентифікує об'єкти за допомогою запису даних, що зберігаються в так званих RFID-мітках і зчитує ці данні за допомогою радіопристроїв.

Структурно-логічну схему автономної системи контролю управління доступу представлено на рис. 1.

До *мережевих* СКУД відносять системи, що дають можливість контролювати присутність працівників на робочих місцях, отримувати різноманітні звіти про присутність за різні відрізки часу по кожному працівнику і по підрозділу в цілому, обмежувати доступ до контрольованих об'єктів за часом доби, розподіляти зони доступу по кабінетах, поверхах, корпусах і т.п., розробити програмне забезпечення для складання особистої карточки для кожного працівника з фотографією, особистими даними, маркою автомобілю та ін.

Структурно-логічну схему мережевої системи контролю управління доступу представлено на рис. 2.

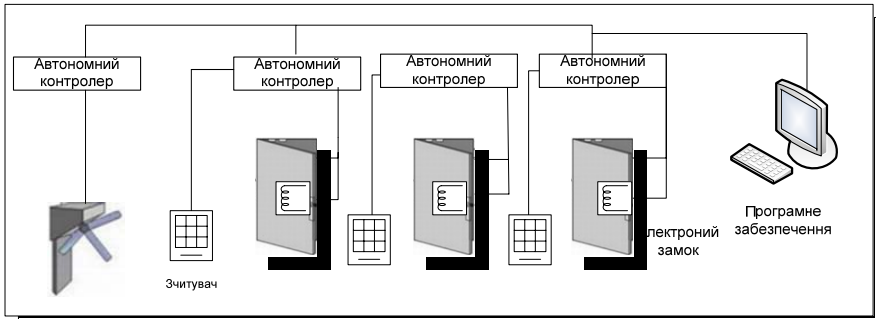

Рис. 1. Структурно-логічна схема автономної СКУД

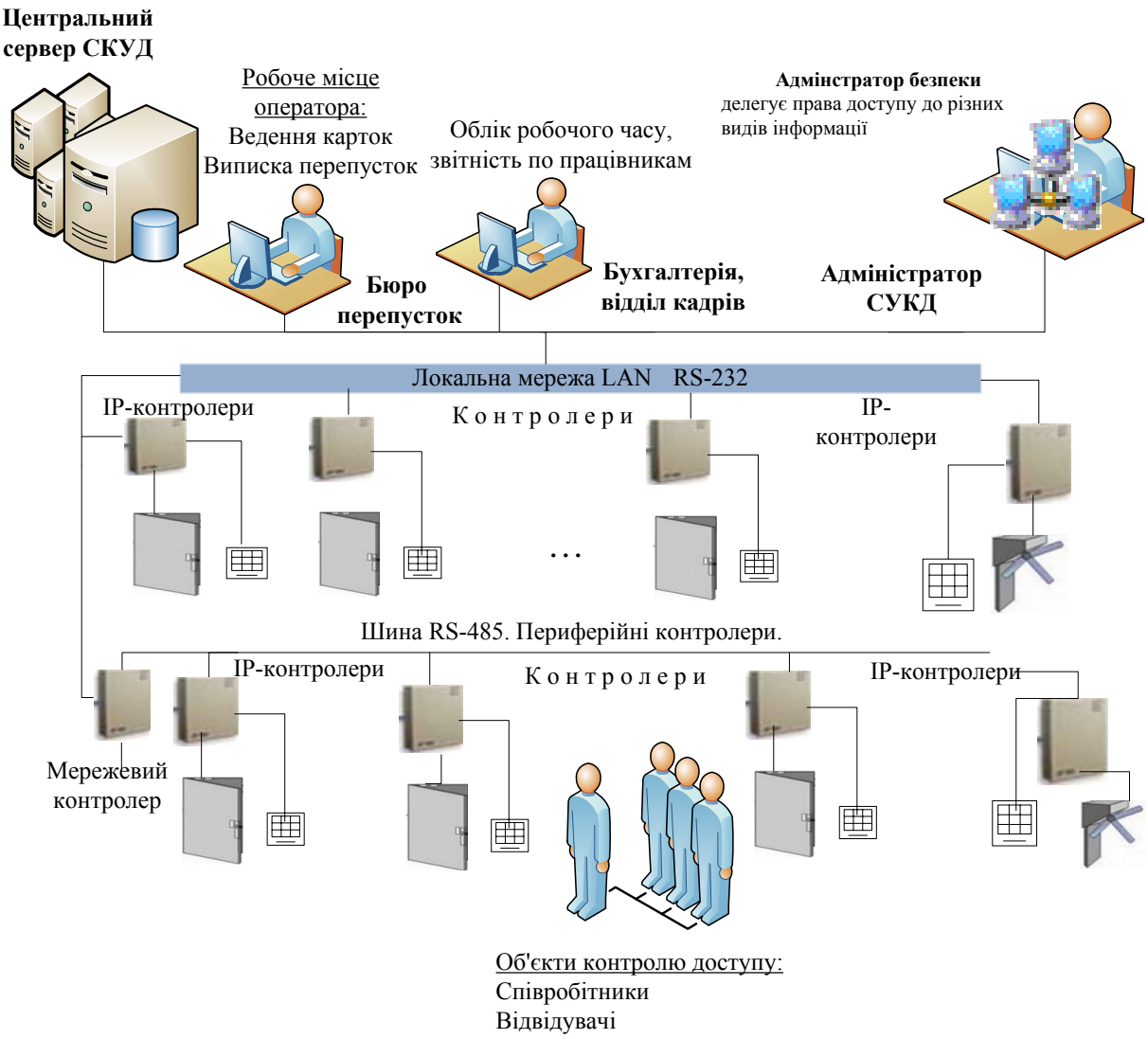

Рис. 2. Структурно-логічна схема мережевої СКУД

Контролери, що працюють в *автономному* режимі, повинні забезпечувати прийом інформації від зчитувачів, обробку інформації та вироблення сигналів управління для пристроїв виконавчих [7]. Контролери, що працюють в *мережевому* режимі, повинні забезпечувати:

- обмін інформацією по лінії зв'язку між контролерами і керуючим комп'ютером або провідним контролером;
- збереження пам'яті, установок, кодів ідентифікаторів у разі обриву зв'язку з керуючим комп'ютером, відключення живлення і при переході на резервне живлення;
- контроль ліній зв'язку між окремими контролерами і між контролерами і керуючим комп'ютером.

Для гарантованої роботи СКУД відстань між окремими компонентами не повинна перевищувати величин, зазначених в паспортах.

Протоколи обміну інформацією і інтерфейси повинні бути стандартних типів.

Види і параметри інтерфейсів повинні бути встановлені в паспортах та/або інших нормативних документах на конкретні засоби.

Рекомендовані типи інтерфейсів:

- між контролерами — RS 485;
- між контролерами і керуючим комп'ютером — RS 232.

Програмне забезпечення має забезпечувати:

- ініціалізацію ідентифікаторів (занесення кодів ідентифікаторів у пам'ять системи);
- завдання характеристик контрольованих точок;
- установку тимчасових інтервалів доступу (вікон часу);
- установку рівнів доступу для користувачів;
- протоколювання поточних подій;
- ведення баз даних;
- збереження даних і установок при аваріях і збоях у системі між контролерами і комп'ютерами підсистем. На цьому рівні використовують інтерфейс RS 232.

Класифікація систем контролю та управління доступом

Наведемо класифікацію сучасних систем автоматизованого контролю доступу за різними критеріями (див. таблицю).

Класифікація сучасних систем автоматизованого контролю доступу

Класифікація СКУД	
За технічними характеристиками і функціональними можливостями	• рівень ідентифікації; • кількість контрольованих місць; • пропускна здатність; • кількість користувачів; • умови експлуатації
За рівнем ідентифікації доступу	• однорівневі (ідентифікація здійснюється за однією ознакою, наприклад, з зчитування коду картки); • багаторівневі (ідентифікація здійснюється за кількома ознаками, наприклад, з зчитування коду картки і біометричних даних)
За кількістю контрольованих місць	• малої місткості (до 16 місць); • середньої місткості (від 16 до 64 місць); • великої місткості (понад 64 місць)
За умовами експлуатації	• у закритих приміщеннях; • у закритих неопалюваних приміщеннях; • під навісом на вулиці в умовах помірно-холодного клімату; • на вулиці в умовах помірно-холодного клімату; • в особливих умовах (підвищена вологість, запиленість, вібрації і т. п.)
За основними функціональними можливостями	• можливість оперативного перепрограмування; • схемно-технічний та програмний захист від вандалізму і саботажу; • високий рівень секретності; • автоматична ідентифікація; • розмежування повноважень співробітників і відвідувачів з доступу в приміщення і на об'єкт у цілому; • надійне механічне замикання контрольованих місць з можливістю аварійного ручного відкриття; • автоматичний збір і аналіз даних; • вибіркова роздруківка даних

Важливою характеристикою СКУД є ступінь доступу: недостатній, середній, високий і дуже високий. СКУД умовно поділяють на чотири класи з різним рівнем доступу. Залежно від особливостей об'єкта, конфігурації СКУД, фірми виробника набір функцій у кожному класі може змінюватися і доповнюватися функціями з інших класів [8].

До СКУД 1-го класу відносять малофункціональні системи малої місткості, що працюють в автономному режимі і забезпечують:

- допуск до зони, яка знаходиться під охороною всіх осіб, які мають відповідний ідентифікатор;
- вбудовану світлову/звукову індикацію режимів роботи;
- управління (автоматичне або ручне) відкриттям/закриттям пристроїв загородження (наприклад, двері).

Такі системи застосовують тоді, коли замовнику необхідно забезпечити контрольований доступ працівників і відвідувачів, що мають від-

повідний ідентифікатор. При цьому не ставиться завдання контролю часу доступу і виходу з приміщення, реєстрація проходів, передавання даних на центральний комп'ютер. Робота СКУД не контролюється. Зазвичай адміністратор (або особа відповідальна за пропускний режим) має майстер-карту (міні-комп'ютер), за допомогою якої він може вносити до списку системи коди ідентифікаторів працівників і відвідувачів або виключати їх зі списку, а також зчитувати інформацію з буфера системи. Використовують на об'єктах, де потрібно обмеження доступу тільки сторонніх осіб.

До СКУД 2-го класу відносять однорівневі і багаторівневі СКУД малої і середньої місткості, що працюють в автономному або мережевому режимах і забезпечують:

- обмеження допуску в зону, що охороняється, конкретної особи, групи осіб за датою і тимчасовими інтервалами відповідно до наявного ідентифікатора;
- автоматичну реєстрацію подій у власному буфері пам'яті,
- видачу тривожних сповіщень (за несанкціонованого проникнення, неправильного набору коду або зломі перешкоджаючого пристрою або його елементів) на зовнішні оповіщувачі або внутрішній пост охорони; автоматичне керування відкриттям/закриттям пристроїв загородження.

Використовуються, як і СКУД 1-го класу, на об'єктах, де потрібний облік і контроль присутності працівників у дозволеній зоні, як доповнення до наявних на об'єкті систем охорони і захисту.

До СКУД 3-го класу відносять однорівневі та багаторівневі СКУД середньої місткості, що працюють у мережевому режимі і забезпечують:

- функції СКУД 2 класу;
- контроль переміщень осіб і майна по охоронним зонам підприємства;
- ведення табельного обліку і баз даних по кожному працівнику, безперервний автоматичний контроль справності складових частин системи;
- інтеграцію з системами і засобами пожежної сигналізації і телевізійних систем відеоконтролю на релейному рівні.

Використовуються як і СКУД 2-го класу, на об'єктах, де потрібно табельний облік і контроль переміщень працівників по об'єкту, для спільної роботи з системами охорони та пожежної сигналізації і телевізійних систем відеоконтролю.

До СКУД 4-го класу відносять багаторівневі СКУД середньої та великої місткості, що працюють у мережевому режимі і забезпечують:

- функції СКУД 3 класу;
- охоронну та пожежну безпеку, телевізійних систем відеоконтролю і інших систем безпеки та управління на програмному рівні;
- автоматичне керування пристроями загородження в разі пожежі та інших надзвичайних ситуаціях.

Використовуються як і СКУД 2-го класу на об'єктах, де потрібно табельний облік і контроль переміщень працівників по об'єкту, для спільної роботи з системами охорони та пожежної сигналізації і телевізійних систем відеоконтролю.

В Україні на сьогодні існує близько 35 компаній, які виробляють як технічні засоби, так і програмне забезпечення і надають послуги для формування СКУД під конкретні потреби підприємства. Серед них — CYPHRAX, U-Pro, Orion, SmartSecurity, Tescom, Elko, ВТП Трансэкспо Бренд-Енерго Тов., ООО Энерго Инжиниринг, ООО «Эксимтек ПЛЮС», Vel-Trade та ін.

Висновки

Проведено аналіз існуючих систем контролю управління доступом, наведено типи та рівні мережевої взаємодії між її блоками.

Наведено класифікацію систем автоматизованого контролю доступу за різними критеріями.

Наведені чотири класи СКУД залежно від ступеню розмежування та захищеності доступу, яке потребує підприємство.

Наведені рекомендації до використання різних типів інтерфейсів.

Проведений аналіз дозволяє зробити такий висновок — завдяки розвитку інформаційних технологій, системи управління контролю і доступу можуть ефективно використовуватись не тільки як контроль доступу для підприємства, а і як засіб для накопичування інформації, важливої для прийняття рішень.

ЛІТЕРАТУРА

1. **Юдін О. К**. Інформаційна безпека держави / О. К. Юдін. — К. : Консум. — 2005. — 576 с.

2. **Гинце А. А.** Особенности СКУД систем доступа крупных распределенных объектов / А. А. Гинце. ААМ Систем, 2005.

3. **Юдін О.** Критеріальний аналіз сучасних операційних систем у задачах захисту інформаційних ресурсів / О. Юдін, О. Весельська // Наукоємні технології. — 2012. — Т. 14. — №. 2. — С. 74–79.

4. **Волхонский В. В**. Системы контроля и управления доступом / В. В. Волхонский. — СПб. : Университет ИТМО. — 2015.

5. **Юдін О. К.** Класифікація загроз державним інформаційним ресурсам інженерно-технічного спрямування. Методологія побудови класифікатора / О. К. Юдін, С. С. Бучик // Наукоємні технології. — 2015. — Т. 25. — №. 1. — С. 188–195.

6. **Ворона В. А**. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. — М. : Горячая линия–Телеком. — 2010. — Т. 272.

7. **Даутов А. Л**. Внедрение и развитие систем контроля и управления доступом на предприятии / А. Л. Даутов, А. С. Пуряев // Инновационная наука. — 2016. — №. 5–1 (17).

8. Системы контроля и управления доступом. URL: http://infoteclab.ru/skud.html (дата обращения: 11.03.2018).

9. Вісник України. Про доктрину інформаційної безпеки України. — 2009. — Т. 514. — С. 1783.

10. **Шаньгин В**. Информационная безопасность. — Litres, 2017. —702 с.

Юдін О. К., Весельська О. М.

АНАЛІЗ ТА КЛАСИФІКАЦІЯ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА ПІДПРИЄМСТВІ

Проведено аналіз існуючих систем контролю управління доступом, наведені типи та рівні мережевої взаємодіє між її блоками. Наведено класифікацію систем автоматизованого контролю доступу за різними критеріями. Наведені чотири класи СКУД залежно від ступеню розмежування та захищеності доступу, яке потребує підприємство. Наведені рекомендації до використання різних типів інтерфейсів. З'ясовано, що системи управління контролю і доступу можуть ефективно використовуватись не тільки як контроль доступу для підприємства, а і як засіб для накопичування інформації, важливої для прийняття рішень.

Ключові слова: інформаційна технологія, системи управління та контролю доступом, інформація, дані.

Judin O. K., Veselska O. M.

ANALYSIS AND CLASSIFICATION OF CONTROL AND ACCESS CONTROL SYSTEMS AT THE ENTERPRISE

The analysis of existing systems of control of access control is conducted, types and levels of network interaction between its blocks are given. Classification of automated access control systems according to different criteria is given. The four classes of ACS are given depending on the degree of delimitation and access security required by the company. The recommendations for using different types of interfaces are given. It has been discovered that control and access control systems can be effectively used not only as access control for the enterprise, but also as a means for the accumulation of information important for decision-making.

Keywords: information technology, systems of control and access control, information, data.

Юдин А. К., Весельская О. М.

АНАЛИЗ И КЛАССИФИКАЦИЯ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ПРЕДПРИЯТИИ

Проведен анализ существующих систем контроля управления доступом, приведены типы и уровни сетевого взаимодействия между ее блоками. Приведена классификация систем автоматизированного контроля доступа по различным критериям. Приведенные четыре класса СКУД, в зависимости от степени разграничения и защищенности доступа предприятия. Приведены рекомендации к использованию различных типов интерфейсов. Выяснено, что системы управления контроля и доступа могут эффективно использоваться не только в качестве доступа для предприятия, но и как средство для накопления информации, важной для принятия решений.

Ключевые слова: информационная технология, системы управления и контроля доступом, информация, данные.

Стаття надійшла до редакції 19.03.2018 р.
Прийнято до друку 04.06.2018 р.
Рецензент — д-р техн. наук, доц. Бучик С. С.