https://orcid.org/0000-0002-5080-1856
https://orcid.org/0000-0003-3370-4584

УДК 004.7

Ю.М. ЛИСЕЦЬКИЙ[*], Д.Й. КАЛБАЗОВ[**]

ОСОБЛИВОСТІ УПРАВЛІННЯ ПРАВАМИ КОРИСТУВАЧІВ У КОРПОРАТИВНИХ IT-СИСТЕМАХ

[*]ДП «ЕС ЕНД ТІ УКРАЇНА», м. Київ, Україна
[**]ТОВ «Інформаційні спеціалізовані системи», м. Київ, Україна

Анотація. *Сьогодні жодне робоче місце працівника будь-якого підприємства не обходиться без використання інформаційних технологій. Автоматизація, яку можуть забезпечити інформаційні технології, охоплює вже всі аспекти діяльності підприємства: документообіг, бухгалтерський облік, складський облік, фінансовий облік, аналітичний, управління підприємством. Для ефективної роботи працівнику потрібен доступ до систем, робота з якими передбачена його посадою. Управління й контроль облікових записів користувачів у корпоративних IT-системах – серйозне завдання для IT-підрозділу чи служби інформаційної безпеки. Оскільки системи слабо інтегровані одна з одною, кожна система потребує окремого налаштування облікових записів користувачів та відповідні права доступу. Основні напрями в управлінні доступом до корпоративних IT-систем – ідентифікація облікових записів, управління обліковими записами користувачів, відповідність вимогам авторизованих прав доступу. Сучасна концепція роботи з корпоративними системами полягає у формуванні сервісної моделі на базі використовуваних IT-систем. З точки зору сервісної моделі підприємство надає працівнику певний сервіс на базі наявних корпоративних систем. Організація ефективного управління правами користувачів у корпоративних IT-системах вимагає автоматизації цього процесу. Кроком уперед в автоматизації управління доступом є створення порталів самообслуговування, де працівник може ознайомитися з переліком корпоративних сервісів, доступних для нього, та запросити до них доступ в автоматизованому режимі. Автоматизація процесу видачі та зміни облікових записів користувачів на корпоративних IT-системах дозволяє скоротити час створення чи зміни прав доступу, створити передумови для контролю прав доступу до систем та підвищити ефективність роботи IT-підрозділу в цілому.*
Ключові слова: *інформаційні технології, корпоративні IT-системи, управління, облікові записи, права користувачів, сервісна модель, ідентифікація, автоматизація.*

Abstract. *Today, there is no workplace at any enterprise where employees don't use information technologies. Automation provided by information technologies has already covered all the aspects of company's activity: document flow, accounting, warehouse accounting, financial accounting, analytical accounting, and enterprise management. To work efficiently, employees need access to systems the use of which is required by their positions. The management and control of user accounts in corporate IT systems are serious tasks for the IT department or information security service. Since the systems are weakly integrated with each other, each of them requires a separate configuration of user accounts and corresponding access rights. The main directions in the management of access to corporate IT systems are the identification of accounts, the management of user accounts, and compliance with the requirements of authorized access rights. The modern concept of work with corporate systems consists in the formation of a service model based on the used IT systems. From the point of view of the service model, the company provides an employee with a certain service based on the existing corporate systems. The organization of the effective management of user rights in corporate IT systems requires automation. A step forward in access management automation is the creation of self-service portals, where employees can familiarize themselves with the list of corporate services available to them and request access to them in the automated mode. The automation of the process of giving and changing user accounts in the corporate IT systems allows*

you to reduce the time it takes to create or change access rights, create prerequisites for controlling access rights to systems, and increase the efficiency of the IT department as a whole.
Keywords: *information technologies, corporate IT systems, management, accounts, user rights, service model, identification, automation.*

DOI: 10.34121/1028-9763-2023-2-28-33

1. Вступ

Цифрова революція докорінно змінила вигляд робочого місця працівника будь-якого підприємства. Сьогодні жодне робоче місце не обходиться без використання інформаційних технологій. Більше того, інформаційні технології ще глибше інтегруються у наше життя і вимагають наявність комп'ютеризованої техніки навіть на низькокваліфікованих робочих місцях, починаючи з програми обліку продажів у «мобільній» кав'ярні і закінчуючи відеонаглядом чи телефонією на пункті охорони [1]. Робоче місце касира в магазині також не обходиться без комп'ютеризованого касового обладнання з доступом до централізованої бази обслуговування клієнтів. Робоче місце бухгалтера теж передбачає доступ до IT-сервісів, використання програмного забезпечення і регулярну звітність у режимі on-line [2].

Автоматизація, яку можуть забезпечити інформаційні технології, охоплює всі аспекти діяльності підприємства: документообіг, бухгалтерський облік, складський облік, фінансовий облік, аналітичний, управління підприємством [3–4]. Важко знайти сферу діяльності, яка б не передбачала використання автоматизованих інформаційних систем.

Сучасне українське підприємство середнього-великого розміру володіє до 10 систем критичного рівня та 20–30 систем локального обслуговування. Кожна з таких систем потребує адміністрування, в першу чергу обліку користувачів, які мають доступ до таких систем.

Метою статті є розгляд особливостей управління правами користувачів у корпоративних IT-системах для підвищення його ефективності.

2. Управління доступом до критичних корпоративних систем

Типовими прикладами таких систем критичного рівня є:

- Microsoft AD, LDAP – система облікових записів користувачів.
- SAP, 1C, MeDoc – бухгалтерський облік.
- SAP HR, Talent Management System – системи кадрового обліку.
- Megapolis Docnet, SharePoint – системи документообігу та файлового обміну.
- Jira, Confluence, MS Project – системи управління проєктами та завданнями.
- MS exchange – корпоративна пошта.
- CRM – системи обслуговування клієнтів.
- ServiceDesk – системи обслуговування звернень.
- Складський облік.
- Управління бізнесом та аналітика.

Корпоративні системи активно використовуються працівниками в щоденній роботі. Для забезпечення їх коректного функціонування використовується значна кількість програмно-апаратних комплексів, включаючи:

- Операційні системи Window, Linux, Unix та ін.
- Системи моніторингу IT-інфраструктури.
- Міжмережеві екрани для віддалених користувачів, підключень відділень, у тому числі хмарної інфраструктури.
- Засоби віртуалізації, гіпервізори та ін.

Для ефективної роботи працівнику потрібен доступ до систем, які передбачені його посадою. Різним працівникам передбачено доступ до різного набору систем із різними

правами доступу. Підрозділ із обслуговування клієнтів має доступ до CRM та SAP, у той час бухгалтерія – SPA і 1С (рис. 1). При цьому під «бухгалтерією» потрібно розуміти набір користувачів із різними рівнями доступу.

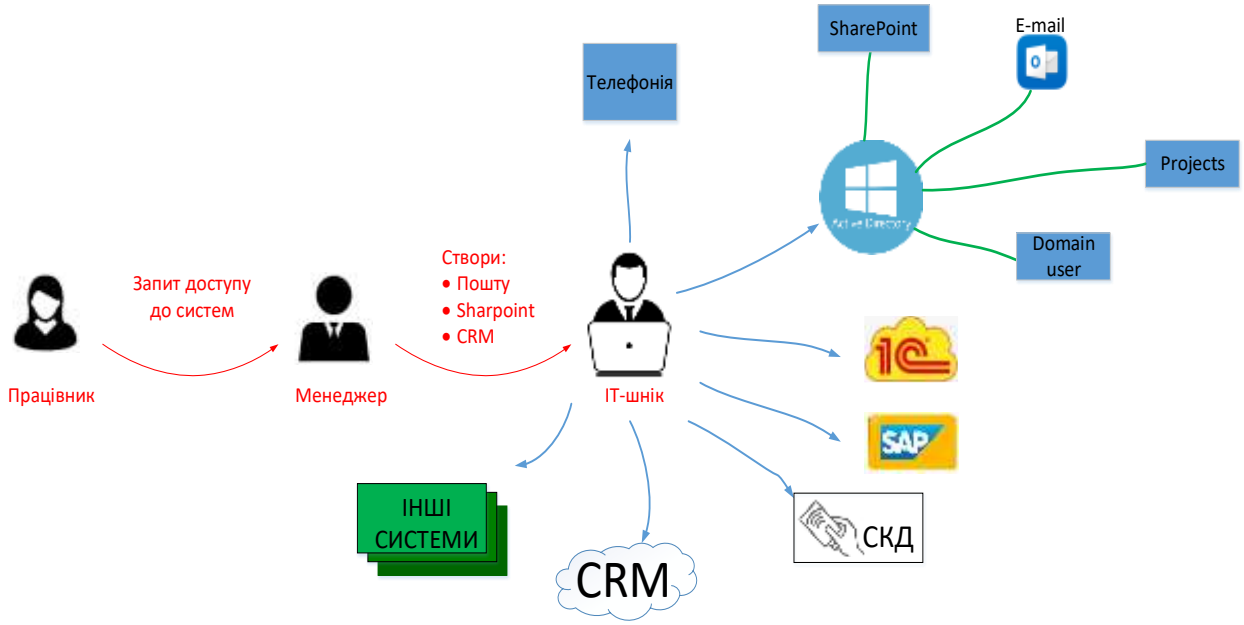

Рисунок 1 – Набір систем із різними правами доступу

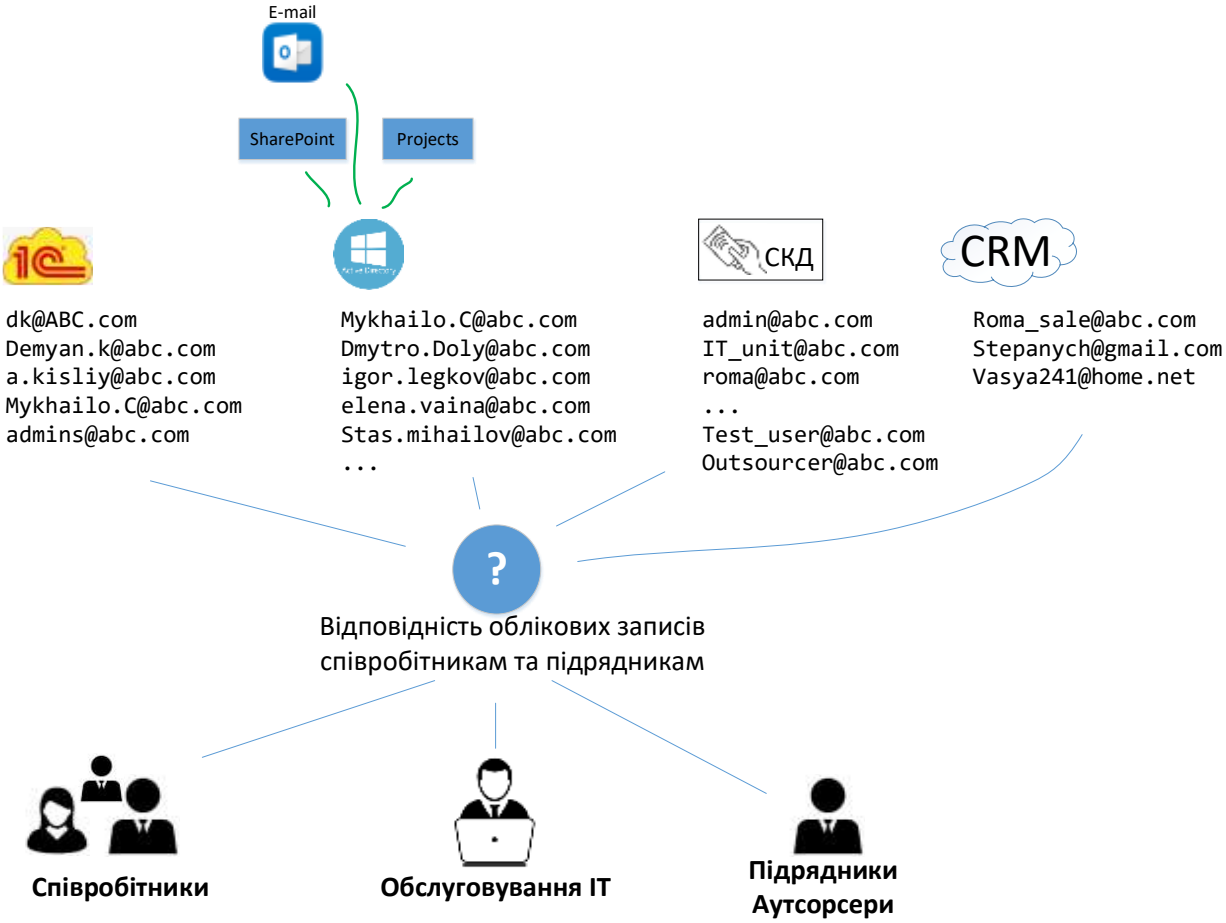

Рисунок 2 – Ідентифікація створених облікових записів на системах

Управління та контроль облікових записів користувачів у корпоративних системах – серйозне завдання для IT-підрозділу чи служби інформаційної безпеки (ІБ). Оскільки системи слабо інтегровані одна з одною, кожна система потребує окремого налаштування облікових записів користувачів та відповідних прав доступу. Створення, зміна та видалення прав доступу до кожної із цільових систем – це тривале та серйозне завдання для IT-підрозділу.

Ще складнішим завданням є ідентифікувати створені облікові записи на системах, визначити їх власників, класифікувати рівні прав доступу і тим більше виявити перевищення прав доступу до систем та подальша перевірка відповідності дозволеного та фактичного рівнів доступу до цільових систем (рис. 2).

3. Напрями діяльності в управлінні доступом

Можна виділити три основні напрями в управлінні доступом до критичних корпоративних систем:

• ідентифікація облікових записів систем – облікові записи важко однозначно «прив'язати» до працівника. Як «Login ID» використовуються скорочені імена чи прізвища, та їх неможливо зв'язати із працівником компанії;

• управління обліковими записами користувачів – робота IT-підрозділу щодо налаштування корпоративних систем, надання доступу, змін доступу при зміні посадових обов'язків чи звільненні працівника;

• відповідність вимогам (compliance) – робота служби інформаційної безпеки щодо виявлення порушень прав доступу, регулярних перевірок налаштованих прав доступу, забезпечення авторизованого процесу затвердження прав доступу.

Для невеликих підприємств, де роботодавець особисто знає свого працівника, чи для підприємств із невеликим і сталим колективом – актуальність управління обліковими записами користувачів не висока. Проте, для підприємств із кількістю користувачів 500 та більше налаштування доступів користувачів до кінцевих систем – це серйозне завдання, яке потребує окремого штату людей – IT-адміністраторів. У «просунутих» організаціях цей процес супроводжується оформленням заявок на обслуговування у системі service-desk [5].

Практичний досвід показує, що обслуговування облікових записів користувачів в організації з 4000 працівників потребує формування підрозділу з 5–15 працівників. Завдання аудиту та ідентифікації облікових записів по системах для такої організації настільки трудомістке, що потребує формування окремого проєкту обстеження для служби ІБ.

Не менш критичним завданням є проведення аудиту облікових записів користувачів, їх прав доступу до систем, визначення відповідальних осіб, які погоджували надання доступу.

На практиці це виглядає так: працівник або його керівник ініціює звернення в IT-підрозділ або у службу ІБ на надання доступу до тієї чи іншої системи. Протягом деякого часу працівнику створюють обліковий запис у системі та встановлюють одноразовий пароль. Завершальний крок при видачі доступу – заміна користувачем одноразового пароля на власний.

Складніша ситуація із працівниками, які ідуть із організації. Оскільки контроль неактивних користувачів ускладнений, як правило, облікові записи колишніх працівників залишаються активними ще тривалий термін. Такі ситуації створюють суттєву загрозу інформаційній безпеці, оскільки облікові записи «без власників» вразливі до зламів. Так як обліковий запис не заблокований і в нього немає власника, його компрометацію важко виявити стандартними інструментами – легітимний користувач отримує доступ до системи. Важко запідозрити компрометацію облікових записів у масштабах 1000 легітимних користувачів.

Тому для служби ІБ важливим є так звана сертифікація користувачів – оперативні та регулярні перевірки відповідності фактично наданих прав внутрішніми чи зовнішніми вимогами.

4. Автоматизація управління правами доступу

Як правило, процесс отримання доступу до корпоративних систем чітко регламентований. Керівник відділу ініціює запит до відповідних спеціалістів на надання доступу до певного корпоративного сервісу, який необхідний працівникам його відділу. Якщо система критична чи знаходиться під бізнес-управлінням сусіднього підрозділу, запускається процес погодження доступу до такої системи, зазвичай у форматі електронного листування.

Оскільки за роботу систем, наприклад, 1С та SAP на підприємстві відповідають різні підрозділи, для організації доступу до таких систем необхідно задіяти декількох спеціалістів, а часто декілька підрозділів [6]. З метою фіксації події щодо видачі нових прав користувачам усі дії по створенню чи зміні облікових записів фіксуються в електронному листуванні або у service-desk-системах. Оскільки відповідальні профільні спеціалісти, як правило, зайняті поточними завданнями, відпрацювання запитів триває від декількох годин до декількох тижнів. Весь процес роботи з обліковими записами створює значні затримки та додаткові завдання в повсякденній роботі працівників та IT-спеціалістів.

Сучасна концепція роботи з корпоративними системами полягає у формуванні сервісної моделі на базі використовуваних корпоративних систем. З точки зору сервісної моделі, організація надає працівнику певний сервіс на базі існуючих корпоративних систем. Прикладом корпоративного сервісу можуть бути доступи до:

- корпоративної пошти;
- мережі інтернет;
- системи CRM;
- системи SAP;
- тощо.

У більш розвинутій сервісній моделі можливе навіть таке розділення сервісів:

- необмежений доступ до мережі інтернет;
- доступ до мережі інтернет з обмеженням (Facebook, YouTube, ін.);
- доступ до мережі інтернет з 9:00 до 18:00.

Працівник чи його керівник знає, які сервіси йому необхідні для роботи. Тому, маючи можливість «замовити» відповідні сервіси, працівник автоматично запускає процедуру погодження доступу чи, якщо доступ надано, автоматично запускає механізм налаштування доступу до сервісу.

Кроком вперед у автоматизації управління доступом є створення порталів самообслуговування, де працівник може ознайомитись із переліком корпоративних сервісів, доступних для нього, та запросити до них доступ в автоматизованому режимі. При замовленні працівником доступних йому сервісів автоматично запускається процес погодження доступу до тих чи інших систем відповідальній особі. Відповідальна особа чи колектив осіб авторизує надання доступу. В такій системі можливо реалізувати процес багатовекторного погодження доступу, де декілька людей повинні погодити (не заперечувати проти) отримання доступу до системи.

Завдяки такій автоматизації, працівник служби ІБ має змогу втрутитись у процес, зупинити погодження сервісу, переглянути обґрунтування надання сервісу та ін. Результати погодження будуть зафіксовані та збережені для подальшого опрацювання.

Одне із ключових завдань служби ІБ – аудит доступних сервісів (контроль правильності виданих доступів по системах). Хто, до яких систем, який доступ має і хто йому цей доступ затвердив? Як перевірити рівні доступів усіх користувачів на всіх системах як на рівні додатків, так і на рівні операційних систем?

Зібрати та підсумувати таку інформацію видається складним завданням, оскільки кількість та різноманітність систем організації така, що потребує проєктної команди для виконання цього завдання в обмежений термін. А після збору та об'єднання інформації по користувачах та системах важливо зрозуміти, який обліковий запис і якому працівнику належить із подальшим визначенням правомірності виданого доступу.

5. Висновки

Організація ефективного управління правами користувачів у корпоративних ІТ-системах, безумовно, вимагає автоматизації цього процесу, тому що вона несе в собі нові можливості для бізнесу. Це створення бізнес-процесу замовлення та затвердження прав доступу користувачів, створення порталу самообслуговування, формування вимог до облікових записів та створення відповідних інструментів контролю, перевірка відповідності наданих прав внутрішнім чи зовнішнім регуляторам, аудит видачі та затвердження прав доступу.

Отже, автоматизація процесу видачі та зміни облікових записів користувачів на корпоративних ІТ-системах дозволяє скоротити час створення чи зміни прав доступу, створити передумови для контролю прав доступу до систем організації та підвищити ефективність роботи ІТ-підрозділу або служби ІБ у цілому.

СПИСОК ДЖЕРЕЛ

1. Лисецький Ю.М. Інформаційні технології в управлінні та обробці інформації: монографія. Київ: ЛАТ&К, 2018. 268 с.
2. Завгородний В.П. Автоматизация бухгалтерского учета, контроля, анализа и аудита. К.: А.С.К., 1998. 768 с.
3. Іванюта П.В. Управлінські інформаційні системи в аналізі та аудиті: навч. посіб. К.: ЦУЛ, 2007. 180 с.
4. Баронов В.В., Калянов Г.Н., Попов Ю.И. Автоматизация управления предприятием. М.: ИНФРА-М., 2000. 239 с.
5. Service Desk: что это и как помогает бизнесу. URL: https://it-guild.com/info/blog/service-desk-chto-eto-i-kak-pomogaet-biznesu/ (дата звернення: 07.01.2023).
6. Зеленская О.В., Голубева В.В., Шлегель О.А. Интегрированная автоматизированная система управления предприятием. *Вестник ТГУС. Экономика*. 2007. Вып. 2. С. 96–101.

Стаття надійшла до редакції 16.03.2023