

ОСОБЛИВОСТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. Розглянуті особливості побудови та використання корпоративних інформаційних систем для оптимізації функціонування організації, покращення процесів виробництва та керування персоналом, а також внутрішньої взаємодії між різними її підрозділами. Визначені основні можливості, що надаються системами даного типу для забезпечення інформаційної безпеки. Описані основні типи підсистем, що можуть створюватися при реалізації систем даного типу та їх функції. Визначені основні переваги таких систем та можливі вразливості, що можуть бути притаманні таким системам через недостатність впроваджених заходів безпеки.

Ключові слова: корпоративна інформаційна система, управління ресурсами, аналіз даних, управління взаємовідносинами з клієнтами, електронний документообіг, керування безпекою.

Вступ

Постановка проблеми. Корпоративна інформаційна система - це вид інформаційної системи, який покращує функції процесів підприємства чи організації шляхом інтеграції. Це, як правило, означає високу якість обслуговування, роботу з великими обсягами даних і здатність підтримувати якусь велику організацію. КІС може використовуватися всіма підрозділами компанії та на всіх її рівнях.

Корпоративні інформаційні системи (КІС) забезпечують технологічну платформу, яка дозволяє організаціям інтегрувати та координувати свої процеси на надійній основі. На сьогодні КІС використовується в поєднанні з системами управління взаємовідносинами з клієнтами і ланцюгами поставок для автоматизації бізнес-процесів. КІС забезпечує єдину систему, яка є центральною для організації, яка забезпечує обмін інформацією на всіх функціональних рівнях та ієрархіях управління.

КІС може бути використана для підвищення продуктивності та скорочення циклів обслуговування, циклів розробки продукту та життєвих циклів. Його можна використовувати для об'єднання існуючих програм задля забезпечення вищого рівня надійності та покращення інформаційної безпеки [1]. В сучасних умовах також слід зазначити необхідність забезпечення безпеки як при організації взаємодії між різними рівнями системи, так і при зберіганні, обробці та передачі інформації [2].

Аналіз останніх досліджень і публікацій. В рамках сучасних наукових публікацій дослідники частіше за все розглядаються заходи по забезпеченню безпеки корпоративних інформаційних систем, а також їх використання для оптимізації та автоматизації процесів функціонування організацій в різних сферах діяльності.

Частіше за все дослідники розглядаються корпоративні інформаційні системи для використання їх в оптимізації бізнес-процесів великих корпорацій, а також малого та середнього бізнесу. При аналізі даної сфери діяльності були розглянуті роботи за авторством Ali Sunyaev, "The Future of Enterprise Information

Systems" [1], William MacKinnon "Enterprise Information Systems and Strategic Flexibility" [3], David L. Olson, "Enterprise Information System Trends" [4] та Maria Manuela Cruz-Cunha, "Enterprise information systems design, implementation and management: Organizational applications" [5] та їх співавторів.

В роботі "The Future of Enterprise Information Systems" автори розкривають основні особливості систем даного типу та підіймають питання доцільності впровадження децентралізованого підходу до побудови систем даного типу. Також автори визначають основні переваги та можливі ризики від його впровадження.

В роботі "Enterprise Information Systems and Strategic Flexibility" автори визначають можливості, що надаються корпоративними інформаційними системами при забезпеченні стратегічною гнучкістю керуванні процесами організації.

В роботі "Enterprise Information System Trends" автори розглядають сучасні тенденції при створенні корпоративних інформаційних систем, визначають основні напрямки наукових досліджень в даній сфері, а також описують процес управління ризиками з урахуванням особливостей систем даного типу.

В совою чергу робота "Enterprise information systems design, implementation and management: Organizational applications" розглядає загальне використання корпоративних інформаційних систем для оптимізації процесів в організаціях.

Окремо розглядають використання корпоративних інформаційних систем в банківській сфері через підвищені вимоги до безпеки даних та особливостей організації роботи подібних установ. При аналізі даної сфери діяльності були розглянуті роботи за авторством Peggy E. Chaudhry "Enterprise Information Systems Security: A Case Study in the Banking Sector" [6], Mircea Georgescu "The Particularity of the Banking Information System" [7], а також Karolina Pilarezyk "Importance of Management Information System in Banking Sector" [8].

В роботах "Enterprise Information Systems Security: A Case Study in the Banking Sector" та "The Particularity of the Banking Information System" автори

формулюють особливості використання корпоративних інформаційних систем в банківському секторі та пропонують свій підхід до побудови інформаційної безпеки з урахуванням його особливостей.

В свою чергу в роботі “Importance of Management Information System in Banking Sector” автори фокусуються саме на використанні інформаційних систем для організації та оптимізації процесу менеджменту компаній.

Також важливим питанням в даній сфері є забезпечення інформаційної безпеки корпоративних інформаційних систем. Дана тематика розглядається як в розрізі окремих підсистем так і для всієї системи загалом.

При аналізі даної сфери діяльності були розглянуті роботи за авторством Johansson E. “Assessment of Enterprise Information Security; The Importance of Information Search Cost” [9], Merrill Warkentin “Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues” [10], Anirban Sengupta “A Formal Methodology for Detecting Managerial Vulnerabilities and Threats in an Enterprise Information System” [11], Wei She “Security for Enterprise Resource Planning Systems” [12], Olesia Fedoruk “Security and protection of information in electronic document management systems: improving the level of cyber defense” [13], Peggy E. Chaudhry “Enterprise Information Systems Security: A Conceptual Framework” [14], Radoslav Nikolov Hrishev “ERP systems and data security” [15], Jeffry Ventje “Customer Relationship Management and Information Security in the Development of Small and Medium Enterprises in the Era of Digitalization as Strengthening Human Resources” [16], а також Stefan Brands “Secure Access Management: Trends, Drivers and Solutions” [17] та їх співавторів.

В роботі “Assessment of Enterprise Information Security; The Importance of Information Search Cost” автори описують підходи до проведення загального аналізу інформаційної безпеки в корпоративних інформаційних системах, та визначають міжнародну нормативно-правову базу для цього.

В роботі “Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues” автори описують технічні та організаційні виклики, що виникають перед розробниками корпоративних інформаційних систем в результаті розвитку технологій та зміни потреб організацій.

В роботі “A Formal Methodology for Detecting Managerial Vulnerabilities and Threats in an Enterprise Information System” автори фокусуються на виявленні вразливостей в КІС в результаті управлінських недоліків. Також формується структурований підхід для проведення комплексного аналізу управлінської структури організації та виявлення в ній потенційних вразливостей.

Усі інші роботи, що зазначені висше розглядають особливості забезпечення безпеки в окремих підсистемах КІС.

Також важливою темою для дослідження в даній сфері є вивчення потенційних підсистем в рамках корпоративних інформаційних систем. Досліджуючи дане питання були вивчені наукові публікації за

авторством Adnan Mustafa AlBar “Enterprise Resource Planning (ERP) Systems: Emergence, Importance and Challenges” [18], Ellen Monk “Concepts in Enterprise Resource Planning” [19], Essam Shehab “Enterprise resource planning: An integrative review” [20], Adam Idzikowski “Customer Relationship Management (CRM) - Philosophy and its Significance for the Enterprise” [21], Ioan Alexandru Rîpa “Customer relationship management in the international context – theoretical and practical considerations” [22], Andrea Disanferdinand “Human Resource Management” [23], Lee Khuay Guan Lionel “Human Resource Management And Organizational Performance” [24], Mustafa Kamal “Enterprise IT Asset Management” [25], Khaled El-Akruti “A framework for the engineering asset management system” [26], Ikuomola Aderonke Justina “A Secured Cloud-Based Electronic Document Management System” [27].

Основними задачами робіт даної групи є аналіз особливостей конкретних підсистем корпоративних інформаційних систем, визначення принципів їх функціонування та побудови, а також визначення принципів їх застосування для забезпечення функціонування організації.

Мета. Дослідити можливості що задаються корпоративними інформаційними системами для оптимізації процесів, менеджменту та забезпечення безпеки. Визначити основний набір підсистем для систем даного типу та їх загальний вплив на її функціонування. Визначити переваги, що надаються такими системами та потенційні вразливості, що пов'язані з їх використанням.

Виклад основного матеріалу

Корпоративні інформаційні системи поділяються на кілька категорій, кожна з них займає певну нішу в життєвому циклі організації. Вони можуть бути використані як окремо, так і в комплексі, для забезпечення більш широких можливостей. Основні категорії систем описані нижче.

ERP (Enterprise Resource Planning) - Система планування (управління) ресурсами. ERP-системи розробляються навколо спільної, визначеної структури даних (схеми), яка зазвичай має загальну базу даних. ERP-системи надають доступ до корпоративних даних з кількох видів діяльності, використовуючи загальні конструкції та визначення, а також загальний користувацький досвід.

Ключовим принципом ERP є централізований збір даних для широкого розповсюдження. Замість кількох автономних баз даних з нескінченним списком розрізнених електронних таблиць, ERP-системи вносять порядок у хаос, щоб усі користувачі з різними правами доступу та робочими функціями створювали, зберігали та використовували одні й ті самі дані, отримані за допомогою загальних процесів. Завдяки безпечному та централізованому сховищу даних кожен співробітник організації може бути впевнений, що дані є правильними, актуальними та повними. Цілісність даних гарантується для кожного завдання, що виконується в усій організації [18].

Схематичне представлення функціональних областей подано на рис. 1.



Рис. 1. Функціональні області ERP-систем

ERP-система охоплює наступні загальні функціональні області. У багатьох системах даного типу вони називаються і групуються разом як модулі ERP[19, 20]:

- фінансовий облік;
- управлінський облік;
- виробництво;
- обробка замовлень;
- управління ланцюгом поставок;
- управління проектами;
- управління взаємовідносинами з клієнтами;
- сервіси даних.

Під фінансовим обліком розуміємо платежі, включаючи, вимоги до оплати, виконання платежів та стягнення, управління грошима, фінансова консолідація. Під управлінським обліком розуміємо бюджетування, обчислення собівартості та управління витратами. Під обробкою замовлень розуміємо Замовлення на готівку, введення замовлення, перевірка кредитоспроможності, ціноутворення, доступне для обіцяння, запаси, доставка, аналіз і звітність продажів, а також комісійні продажі. Під виробництвом розуміється специфікація матеріалів, планування, управління робочими процесами, контроль якості, виробничий процес, виробничі проекти, виробничий потік, управління життєвим циклом продукції. Під управлінням ланцюгом поставок розуміємо планування ланцюга поставок, планування постачальників, конфігуратор продуктів, закупівля, інвентаризація, обробка претензій, зберігання. Під управлінням проектами розуміємо Планування проекту, планування ресурсів, обчислення вартості проекту, структурна декомпозиція робіт, виставлення рахунків, управління діяльністю. Під управлінням взаємовідносинами з клієнтами розуміємо продажі та маркетинг, комісійні, обслуговування, контакти з клієнтами.

Під сервісами даних розуміємо різноманітні інтерфейси самообслуговування для клієнтів, постачальників та/або співробітників.

Системи управління взаємовідносинами з клієнтами(CRM) використовують для управління та аналізу взаємодії з клієнтами та даних протягом усього життєвого циклу клієнта з метою покращення ділових відносин, сприяння їх утриманню.

Системи CRM збирають дані з різних каналів комунікації, включаючи веб-сайт компанії, телефон (до якого часто входить програмне забезпечення для

IP-телефонії), електронну пошту, чат в реальному часі, маркетингові матеріали, а також з соціальних мереж. Вони дозволяють підприємствам дізнатися більше про свою цільову аудиторію та як краще відповісти їхнім потребам, тим самим зберігаючи клієнтів та забезпечуючи зростання продажів. CRM може використовуватися з минулими, поточними або потенційними клієнтами. Ця повна взаємодія охоплює безпосередній контакт з клієнтами, такі як операції з продажу та обслуговування, прогнозування, аналіз споживчих патернів та поведінки з точки зору компанії. Загальна схема взаємодії з клієнтами в рамках CRM подана на рис. 2 [21, 22].

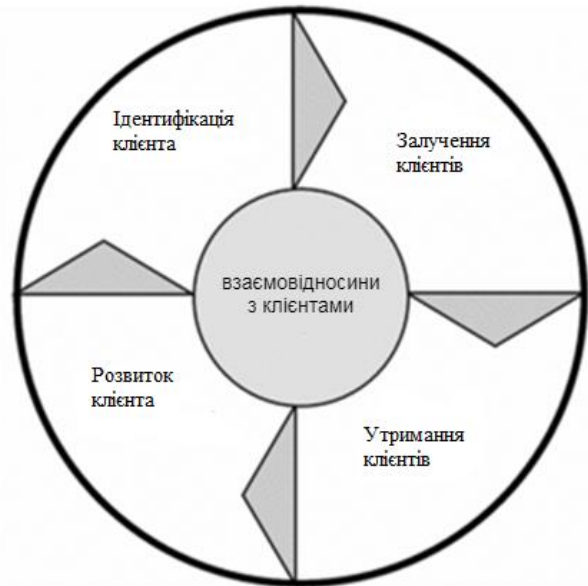


Рис. 2. Схема взаємодії з клієнтами в рамках CRM

Система управління людськими ресурсами(HRM) - це форма програмного забезпечення, яка поєднує в собі ряд систем і процесів для забезпечення легкого управління людськими ресурсами, процесами і даними. Програмне забезпечення для управління персоналом використовується підприємствами для об'єднання ряду необхідних функцій, таких як зберігання даних співробітників, управління нарахуванням заробітної плати, підбір персоналу, адміністрування пільг, обліку робочого часу та відвідуваності, управління ефективністю співробітників, а також відстеження записів про компетенції та навчання [23]. Система HRM є найуразливішою з погляду захисту персональних даних

Система управління людськими ресурсами забезпечують [24]:

- ведення кадрового обліку;
- звітність і аналіз даних про працівників;
- робочий графік та облік відвідування;
- оцінка продуктивності праці;
- виплату пільг та компенсацій;
- рекрутинг та адаптацію персоналу;
- планування управління кадрами;
- формування кадрових резервів;
- відстежування претендентів та їх резюме.

Схематичне представлення системи управління людськими ресурсами подано на рис. 3 [24].



Рис. 3. Система управління людськими ресурсами

Система управління активами організації (EAM) – система управління життєвим циклом фізичних активів організації. Вона охоплює такі теми, як проектування, будівництво, введення в експлуатацію, експлуатація, технічне обслуговування та виведення з експлуатації або заміна установок, обладнання та споруд. Активами можуть бути або нерухомість, така як будівлі, заводи, виробниче обладнання, або рухомі активи, такі як транспортні засоби, кораблі, рухоме обладнання тощо. Управління життєвим циклом цінних фізичних активів вимагає регресивного планування та виконання роботи [25, 26]. Схематичне представлення задач системи управління активами підприємства подано на рис. 4 [27].

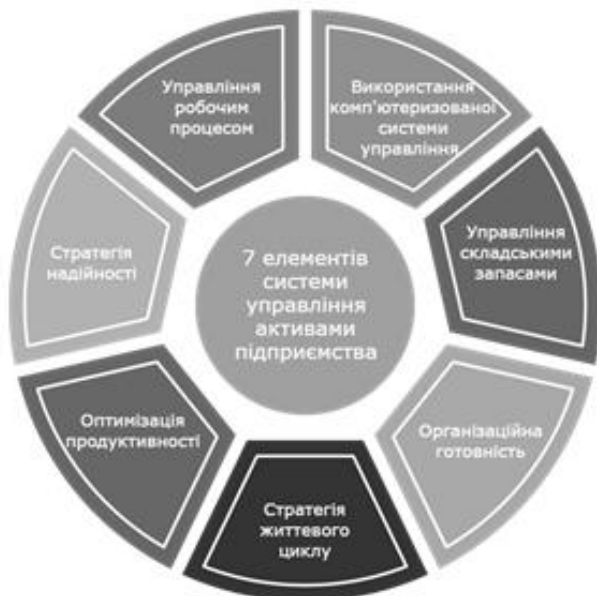


Рис. 4. Задачі системи управління активами підприємства

Головною метою EAM-систем є забезпечення такого режиму експлуатації основних виробничих фондів, який забезпечував би максимальну пропускну здатність виробництва за рахунок підтримки необхідного коефіцієнта технічної готовності при допустимому рівні витрат на обслуговування і ремонт основних фондів підприємства.

Система електронного документообігу (EDMS) – це програмне рішення, яке забезпечує централізовану платформу для управління, організації та зберігання електронних документів і файлів. EDMS дозволяє організаціям оптимізувати процеси керування документами, покращити співпрацю та підвищити безпеку та доступність своїх цифрових документів. EDMS зазвичай включає такі функції, як сканування документів, індексування, контроль версій, контроль доступу та функція пошуку. Ці функції дозволяють організаціям цифровізувати робочі процеси з документами та автоматизувати багато ручних завдань для керування паперовими документами[28].

Одна з переваг використання EDMS полягає в тому, що вона може підвищити безпеку та доступність цифрових документів. EDMS надає функції контролю доступу, які дозволяють організаціям контролювати, хто може отримувати доступ до своїх цифрових документів і змінювати їх. EDMS також надає функції контролю версій, які дозволяють організаціям відстежувати зміни документів у часі, забезпечуючи контрольний журнал змін і переглядів документів[29,30]. Схематичне представлення даної системи подано на рис. 5 [30].



Рис. 5. Задачі системи електронного документообігу

Також в певних наукових роботах окремо виділяють систему забезпечення інформаційної безпеки. Дана підсистема включає в себе процеси збору та обробки інформації про інциденти безпеки, що виникають в інших підсистемах КІС, можливості по автоматизованому або керованому адміністратором системи реагуванню на ці інциденти, тощо. Також під функціонал даної підсистеми підпадає керування доступом до ресурсів КІС, визначення та керування політикою паролів, забезпечення заходів безпеки, що визначені політикою безпеки компанії, в процесі передачі, обробки на зберігання інформації. Схема забезпечення безпеки КІС подана на рис. 6.

Важливим фактором при організації підсистеми даного типу є питання централізації або децентралізації керування безпекою.

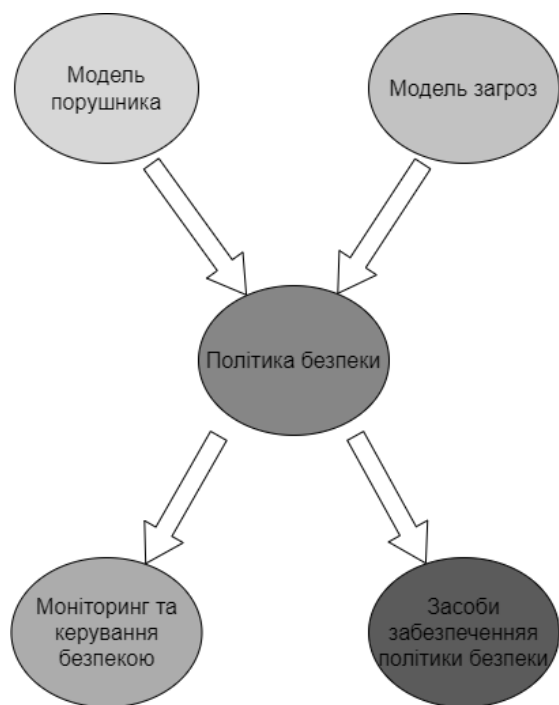


Рис. 6. Схема забезпечення безпеки КІС

Децентралізоване керування безпекою полягає в створенні окремих безпекових заходів в рамках кожної з підсистем КІС. До переваг подібного принципу побудови слід віднести [2, 9–13]:

- політики та рішення узгоджуються з конкретною моделлю та потребами в рамках кожної з підсистем;
- більша швидкість прийняття рішень та автономізація операцій безпеки;
- ширші можливості по налаштуванню політик безпеки.

В свою ж чергу централізований підхід до керування безпекою полягає в створенні загальної системи безпеки, що буде здирати, та оброблювати дані з різних підсистем та встановлювати загальні заходи безпеки, що будуть діяти в рамках всієї організації.

Також слід зазначити, що деякі великі корпорації використовують комбінацію централізованої та децентралізованої моделі. Вона полягає в тому, що

створюються централізовані системи керування безпекою для кожного з регіонів (області, країни тощо) які забезпечують заходи безпеки в межах даного регіону та передають звіти в центральний офіс для аналізу інцидентів безпеки та створення регіональних або загальних рекомендацій по забезпеченню безпеки [31, 32].

Висновки

Виходячи з досліджених наукових публікацій в рамках корпоративних інформаційних систем рекомендується використовувати саме централізовану модель побудови системи забезпечення безпеки через її потенційно більший рівень захищеності, порівняно з децентралізованою, зменшення ризиків неузгодженості політик безпеки в різних підрозділах організації.

Всі описані висше системи дозволяють розподілити задачі в рамках підприємства, розробити та впровадити відповідні програмні, апаратні та організаційні заходи безпеки для кожної з областей діяльності. Системи управління активами та документацією дозволяють оптимізувати облік інцидентів безпеки. На основі звітів про інциденти буде можливо провести аналіз та виявити недоліки системи.

Слід також зазначити, що у разі того, якщо заходи безпеки, що реалізовані в рамках корпоративної інформаційної системи будуть недостатніми, то це може призвести до витоку персональних даних користувачів, працівників компанії, корпоративної інформації, порушення функціонування системи або її підсистем, пошкодження або відмови засобів виробництва та іншим інцидентам безпеки.

КІС надають широкий спектр можливостей по оптимізації процесу виробництва, управління персоналом та активами та впровадженням заходів безпеки. Але через збільшення об'єму даних що зберігаються та кількості обслуговуючого персоналу, який може отримати доступ до даних в рамках системи підвищується ризик витоку інформації. Через це такий тип систем також потребує комплексної системи безпеки що буде охоплювати всі сфері діяльності підприємства, системи виявлення інцидентів та заходи з її запобігання.

СПИСОК ЛІТЕРАТУРИ

1. Sunyaev F., Dehling T., Strahinger S. & al. The Future of Enterprise Information Systems. *Business & Information Systems Engineering*. 65, 2023. Pp. 731–751. DOI: 10.1007/s12599-023-00839-2
2. Pevnev, V., Tsuranov, M., Zemlianko, H., Amelina, O. Conceptual Model of Information Security. *Lecture Notes in Networks and Systems*. Springer, Cham. 2021. Vol 188. P. 158–168. DOI: 10.1007/978-3-030-66717-7_14
3. W. MacKinnon, G. Grant and D. Cray, Enterprise Information Systems and Strategic Flexibility, Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, USA, 2008, pp. 402–402, DOI: 10.1109/HICSS.2008.149
4. David L. Olson, Subodh Kesharwani. Enterprise Information System Trends. *Enterprise Information Systems*. Berlin, Heidelberg, 2011. Pp 3–14. DOI: 10.1007/978-3-642-19802-1_1
5. Cruz-Cunha M. M. Enterprise information systems design, implementation and management: Organizational applications. Maria Manuela Cruz-Cunha. – Hershey, PA : Business Science Reference, 2011. 586 p.
6. Peggy E. Chaudhry & al. Enterprise Information Systems Security: A Case Study in the Banking Sector. *Lecture Notes in Business Information Processing*. Berlin, Heidelberg, 2013. Pp. 206–214. DOI: 10.1007/978-3-642-36611-6_18
7. Georgescu M., Jeflea V. The Particularity of the Banking Information System. *Procedia Economics and Finance* 20. 2015 Pp. 268–276. DOI: 10.1016/s2212-5671(15)00074-x
8. Pilarczyk K. Importance of Management Information System in Banking Sector. *Annales Universitatis Mariae Curie-Skłodowska, sectio H, Oeconomia* 50. 2016, № 2. Pp. 69. DOI: 10.17951/h.2016.50.2.69

9. E. Johansson, M. Ekstedt, P. Assessment of Enterprise Information Security. The Importance of Information Search Cost. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), Kauia, HI, USA, 4–7 січ. 2006 p. 2006. DOI: 10.1109/hicss.2006.67
10. Warkentin M. Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues: IGI Global, 2006. – 406 с.
11. Anirban Sengupta, Chandan Mazumdar, Aditya Bagchi. A Formal Methodology for Detecting Managerial Vulnerabilities and Threats in an Enterprise Information System. *Journal of Network and Systems Management* 19, № 3, 2010. Pp. 319–342. DOI: 10.1007/s10922-010-9180-y
12. Wei She, Bhavani Thuraisingham. Security for Enterprise Resource Planning Systems. *Information Systems Security* 16, № 3, 2007. Pp.152–163. DOI: doi.org/10.1080/10658980701401959
13. Fedoruk O. Security and protection of information in electronic document management systems: improving the level of cyber defense. *Вісник Книжкової палати* № 4, 2024. Pp. 39–44. DOI: doi.org/10.36273/2076-9555.2024.4(333).39-44
14. Peggy E. Chaudhry & al. Enterprise Information Systems Security: A Conceptual Framework. Re-conceptualizing Enterprise Information Systems. Berlin, Heidelberg, 2012. Pp. 118–128. DOI: 10.1007/978-3-642-28827-2_9
15. Hrishev R. ERP systems and data security. *IOP Conference Series: Materials Science and Engineering* 878, 2020. Pp. – 012009. DOI: 1088/1757-899x/878/1/012009
16. Ventje Jeffry Kuhuparuw, Elyta ., Syarif Redha Fachmi Al Qadrie. Customer Relationship Management And Information Security In The Development Of Small And Medium Enterprises In The Era Of Digitalization As Strengthening Human Resources. *International Journal of Multidisciplinary Research & Reviews* 3, № 1, 2024. Pp. 39–58 DOI: 10.56815/ijmrr.v3.i1.2024/39-58
17. Secure Access Management: Trends, Drivers and Solutions Information Security Technical Report 7, № 3, 2002. Pp. 81–94. DOI: doi.org/10.1016/s1363-4127(02)00309-6
18. Adnan Mustafa AlBar, Mashaal A. Hddas, Md Rakibul Hoque. Enterprise Resource Planning (ERP) Systems: Emergence, Importance and Challenges. *The International Technology Management Review* 4, № 4, 2014. Pp. 170. DOI: 10.2991/itmtr.2014.4.4.1
19. Ellen Monk, Bret Wagner. *Concepts in Enterprise Resource Planning Technology*, 2012. 272 p.
20. E. M. Shehab & al. Enterprise resource planning. *Business Process Management Journal* 10, № 4, 2004. Pp. 359–386. DOI: 1108/14637150410548056
21. Adam Idzikowski & al. Customer Relationship Management (CRM) - Philosophy and its Significance for the Enterprise. *System Safety: Human - Technical Facility – Environment* 1, № 1, 2019. Pp. 1004–1011. DOI: 10.2478/czoto-2019-0127
22. Rîpa I. A. Customer relationship management in the international context – theoretical and practical considerations. Proceedings of the International Conference on Business Excellence 16, № 1, 2022. Pp. 1060–1072. DOI: 10.2478/picbe-2022-0098
23. Disanferdinand A. Human Resource Management. *International Journal of Scientific and Research Publications (IJSRP)* 8, № 9, 2018. DOI: 10.29322/ijsrp.8.9.2018.p8126
24. Lee Khuay Guan Lionel, Sukhumpong Channuwong, Kulpornpath Wongmajarapinya. Human resource management and organizational performance. *Int. Journal of Advanced Research* 11, № 05, 2023. Pp. 872–881. DOI: 10.21474/ijar01/16940
25. HRM functions slide template with circle diagram - Dreamstime [Електронний ресурс] // Dreamstime. – Режим доступу: <https://www.dreamstime.com/vector-slide-template-circle-diagram-human-resources-management-hrm-functions-diagram-scheme-planning-recruitment-image132671587>
26. Mustafa Kamal, Russell Petree. Enterprise IT Asset Management. *Review of Business Information Systems (RBIS)* 10, № 3, 2006. Pp. 47–52. DOI: 10.19030/rbis.v10i3.5337
27. Khaled El-Akruti, Richard Dwight. A framework for the engineering asset management system. *Journal of Quality in Maintenance Engineering* 19, № 4, 2013. Pp. 398–412. DOI: 10.1108/jqme-01-2012-0002
28. Enterprise Asset Management [Електронний ресурс] // ABS Group. – Режим доступу: <https://www.abs-group.com/Solutions/Asset-Management/Enterprise-Asset-Management/>
29. Ikuomola Aderonke Justina, Oyekan, Ezekiel Abiodun, Orogbemi, Olutomisin M. Secured Cloud-Based Electronic Document Management System. *International Journal of Innovative Research and Development*, 2022. DOI: 10.24940/ijird/2022/v11/i12/dec22010;
30. Document Management System [Електронний ресурс] // indiamart.com. – Режим доступу: <https://www.indiamart.com/proddetail/document-management-system-15507440897.html>
31. Pevnev, V., Frolov, A., Tsuranov, M., & Zemlianko, H. Ensuring the Data Integrity in Infocommunication Systems. *International Journal of Computing*. 2022. Vol. 21(2), P. 228-233. DOI: 10.47839/ijc.21.2.2591;
32. Serkov, A., Kasilov, O., Lazurenko, B., Pevnev, V., Trubchaninova, K. *Strategy of Building a Wireless Mobile Communication System in the Conditions of Electronic Counteraction*. *Radioelectronic and Computer Systems*, no. 2, pp. 160–170, 2023 DOI: 10.32620/reks.2023.2.13.

Received (Надійшла) 19.06.2024

(Accepted for publication) Прийнята до друку 30.10.2024

Features of enterprise information systems

S. Butenko

Abstract. The features of constructing and using corporate information systems for optimizing the functioning of an organization, improving production processes, and managing personnel, as well as internal interaction between its various departments, are considered. The main capabilities provided by such systems to ensure information security are identified. The main types of subsystems that can be created when implementing such systems and their functions are described. The main advantages of such systems and possible vulnerabilities that may be inherent in such systems due to insufficiently implemented security measures are identified.

Keywords: enterprise information system, resource management, data analysis, customer relationship management, electronic document management, security management.