UDC 004
Hrechuk D.V. student of group 125м-24-1
Research supervisor: Shevtsova O.S. associate professor of department of software of computer systems
(Dnipro University of technology, Dnipro, Ukraine)

ACCESS MANAGEMENT OF SAP ARIBA PURCHASING MANAGEMENT SYSTEM

SAP Ariba is an intelligent cloud-based software for supply and procurement management. It allows companies to improve efficiency and control costs by optimizing the procurement-to-payment (P2P) process.

SAP Ariba covers the end-to-end source-to-pay process, including strategic sourcing, supplier management, procurement, working capital optimization, account management, and cost transparency. The SAP solution enables buyers and suppliers to conduct business on a single platform, organizing and unifying their supply chain strategy[1-3].

SAP Ariba is used to optimize procurement processes and supply chain management. This platform reduces costs and facilitates cooperation between suppliers and buyers. SAP Ariba offers effective tools for supplier management, providing transparency and control at all stages of the procurement process. Thanks to this, companies can achieve a higher quality of resource management and optimize their costs[4].

SAP Ariba uses an attribute-based access control (ABAC) model, which provides a dynamic and flexible approach to access control. ABAC is fully suited for use in environments with multiple attributes such as department, location, time of day. This allows you to increase the level of security and optimize access control processes. The use of ABAC in SAP Ariba allows for more detailed configuration of access rights for each user, which is important for large companies with a complex structure.

Figure 1 - Functional diagram of access control in SAP Ariba

SAP S/4HANA, in turn, is the main ERP solution for many companies, which provides effective management of finance, production, logistics and other business processes. SAP S/4HANA is based on the role-based access control (RBAC) model, which provides a simple assignment of rights to actions in the system. This approach simplifies the access management process, especially for large companies. Attribute-based access control (ABAC) is also used to increase flexibility and security. By combining RBAC and ABAC, companies can create flexible and secure access control solutions that take into account both general roles and specific user attributes.

An integration test between SAP Ariba and other SAP systems showed that differences in access control models and structure can lead to problems when merging systems. These issues include inconsistent user IDs and data conversion issues across systems. In particular, during integration, difficulties may arise with the unification of authorization processes, since different models of access control have their own characteristics. For example, ABAC allows you to consider additional user

attributes such as location or working hours, while RBAC is based on roles, which may not be flexible enough in certain scenarios.

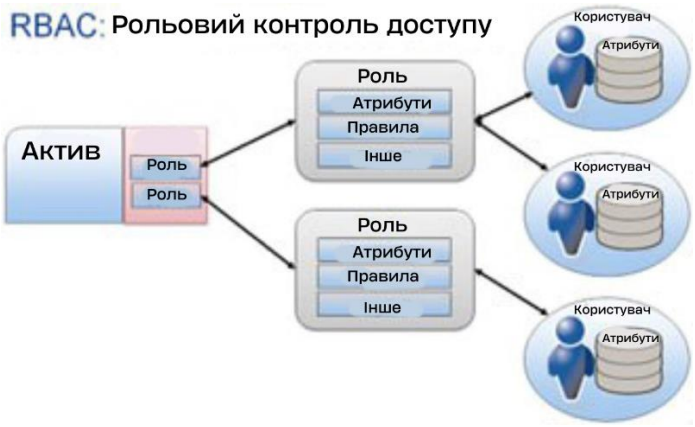

Figure 2 - Diagram of access control model in SAP S/4HANA

Integrating SAP Ariba with other SAP modules, such as SAP S/4HANA, requires careful planning and implementation of a joint security strategy. This includes creating common access policies that ensure compatibility between different access control models and take into account the needs of each system. For this, it is important to take into account not only technical aspects, but also organizational ones — for example, how to structure the interaction between different divisions of the company to ensure maximum efficiency and security.

CONCLUSION

Comparing access control concepts in SAP Ariba and SAP S/4HANA allows you to choose an approach to security management depending on the needs of the company. The joint integration of these systems requires a coordinated strategy to improve security and improve the efficiency of processes. The implementation of both systems makes it possible to optimize business processes and ensure effective access management at different levels of the organization. An important component of success is the correct configuration of access control and interaction between systems, which will avoid potential security problems and ensure transparency of all operations. This study highlights the importance of careful integration planning and the selection of access control models that meet business needs in order to achieve maximum results and improve the company's competitiveness in the market.

REFERENCE

1. Riabchinska V. Methods of providing cyber protection at enterprises / Riabchinska V. Olishevskyi I.H. // МОЛОДЬ: НАУКА ТА ІННОВАЦІЇ: матеріали X Міжнародної науково-технічної конференції студентів, аспірантів та молодих вчених, Дніпро, 23–25 листопада 2022 року / Національний технічний університет «Дніпровська політехніка» – Дніпро : НТУ «ДП», 2022 – С. 179–180. http://ir.nmu.org.ua/handle/123456789/167094

2. Svietkina, O., Bas, K., Haddad, J., Ziborov, K., & Olishevska, V. (2020). Mechanochemical Activation of Polymetallic Ore and Further Selective Floatation. Key Engineering Materials, 844, 65–76. https://doi.org/10.4028/www.scientific.net/kem.844.65

3. Гречук Д.В. AUTOPILOT TECHNOLOGY IN VEHICLES/ І.Г. Олішевський, Д.В. Гречук // МОЛОДЬ: НАУКА ТА ІННОВАЦІЇ: матеріали X Міжнародної науково-технічної конференції студентів, аспірантів та молодих вчених, Дніпро, 23–25 листопада 2022 року / Національний технічний університет «Дніпровська політехніка» – Дніпро : НТУ «ДП», 2022 – С. 339–340. http://ir.nmu.org.ua/handle/123456789/162724

4. Khabarlak, K. S. (2022). FASTER OPTIMIZATION-BASED META-LEARNING ADAPTATION PHASE. Radio Electronics, Computer Science, Control, (1), 82. https://doi.org/10.15588/1607-3274-2022-1-10