



ISSN 2091-5187

СЕРВИС

№4

ИЛМИЙ-АМАЛИЙ
ЖУРНАЛ

2025



СЕРВИС

ИЛМИЙ-АМАЛИЙ ЖУРНАЛ 2025 йил, 4-сони

Муассис: Самарқанд иқтисодиёт ва сервис институти

Ўзбекистон Матбуот ва ахборот агентлиги томонидан 2008 йил 31 декабрда
0561-рақам билан рўйхатга олинган.

ЎзР ОАК Риёсатининг 19.03.2017 й., 239/5-сонли қарори билан эътироф этилган

**Тахририят ижодий
жамоаси:**

Бош муҳаррир:

и.ф.д., проф. М.Э.Пўлатов

Бош муҳаррир

ўринбосари:

и.ф.н., проф. Д.Х.Асланова

Масъул котиб:

и.ф.д., проф. М.Қ.Пардаев

Муҳаррирлар:

и.ф.д., доцент Ф.А.Сафаров

PhD, доцент И.М.Пардаева

PhD, И.Ш.Эрназарова

Техник муҳаррир:

и.ф.н., проф. А.Н.Холиқулов

Корректор:

PhD, доц. С.А.Бабаназарова

Саҳифаловчи:

PhD Х.Н.Очилова

1 йилда 4 маротаба

чоп этилади.

Ўзбекистон худудида

тарқатилади.

Тахририят манзили:

140100, Самарқанд шаҳар,

Амир Темур кўчаси, 9-уй,

тел.: +998(66)233-28-38,

+998(97)913-74-40

факс: +998(366)231-12-53

эл.почта:

samisiservis@mail.ru

Тахририят кенгаши раиси:

М.Э.Пўлатов – Самарқанд иқтисодиёт ва сервис институти ректори, и.ф.д., профессор

Тахририят кенгаши раиси ўринбосари:

Д.Х.Асланова – СамИСИ илмий ишлар ва инновациялар бўйича проректори, и.ф.н., профессор

Тахрир кенгаши аъзолари:

Б.А.Бегалов – Ўзбекистон Республикаси Президенти ҳузуридаги Статистика агентлиги директори, и.ф.д., профессор

М.Қ.Пардаев – СамИСИ профессори, и.ф.д.

Б.К.Ғоибназаров – и.ф.д., профессор.

М.М.Мухаммедов – СамИСИ профессори, и.ф.д.

Д.Р.Зайналов – СамИСИ профессори, и.ф.д.

О.М.Муртазаев – ТДИУ СФ директори, и.ф.д., проф.

М.Р.Болтабаев – ТДИУ профессори, и.ф.д.

Р.Х.Эргашев – ҚарМИИ профессори, и.ф.д.

И.С.Тўхлиев – СамИСИ профессори, и.ф.д.

К.Б.Уразов – СамИСИ профессори, и.ф.д.

Қ.Ж.Мирзаев – СамИСИ профессори, и.ф.д.

Б.И.Исроилов – ТДИУ профессори, и.ф.д.

Г.М.Шодиева – СамИСИ профессори, и.ф.д.

Б.Абдукаримов – СамИСИ профессори, и.ф.н.

Р.Қобилов – Самарқанд вилояти ҳокими ўринбосари

С.Н.Тошназаров – СамИСИ профессори, и.ф.д.

Р.Н.Нормахматов – СамИСИ профессори, т.ф.д.

А.Бектемиров – СамИСИ профессори, и.ф.д.

О.М.Пардаев – СамИСИ профессори, и.ф.д.

М.Т.Алимова – СамИСИ профессори, и.ф.д.

З.Дж. Адилова – ТДИУ профессори, и.ф.д.

Ш.О.Қувондиқов – СамИСИ профессори в.б., иқтисод фанлари доктори

Л.Н.Халикова – СамИСИ профессори, DSc

Ф.А.Сафаров – СамИСИ доценти, DSc

А.М.Каримова – СамИСИ профессори в.б., DSc

И.Б.Маттиев – СамИСИ профессори, DSc

МУНДАРИЖА:

НАЗАРИЯ ВА МЕТОДОЛОГИЯ	
Саидахроп Саидахмедович Фуломов, Мамаюнус Қаршибоевич Пардаев, Мунаввархон Хаётовна Мухитдинова, Дилшод Субонкулович Пардаев Таълим сифати ва самарадорлигини оширишга қаратилган сунъий интеллектдан Янги Ўзбекистонни шакллантиришда фойдаланиш имкониятлари	5
Умар Худайбердиев Ўзаро манфаатли ҳамкорлик – иқтисодий ривожланишнинг муҳим омили	11
Соҳибназар Каримов “Авесто” жамият тараққиётининг иқтисодий мезонлари ҳақида	14
РАҚАМЛИ ВА ИННОВАЦИОН ИҚТИСОДИЁТ	
Abdumalik Bektemirov Яшил иқтисодиёт шароитида инсон капитални ривожлантириш: стратегик ёндашувлар ва барқарор ўсиш омиллари	19
Fazilat Esirgarpovna Jomonqulova, Nodir Rasulovich Zaynalov, Shohrux Djurabekovich Abdurasulov Korxonaning ERP axborot tizimini yaratishda xavfsizlik elementlari haqida	22
Мохигул Эркиновна Ахтамова Управление информационно-экономических систем цифровизации бизнеса и перспективы её развития в Республике Узбекистан	26
Abdumalik Bektemirov, Bekzod Muxiddin o‘g‘li Abduvaliyev Qurilishda investitsion va innovatsion faollikni oshirishning dolzarb masalalari	31
Қаюм Ҳамраевич Собиров Табиий қор-ёмғир суви ресурсидан оқилона фойдаланиш орқали мамлакатни сув танқислигидан сақлаб қолиш омиллари	34
Ashur Ali Rustam o‘g‘li Latipov, Abdulxofiz Jamshid o‘g‘li Hamrayev Sun‘iy intellekt yordamida xodimlarning mehnat samaradorligini monitoring qilish	42
Дилрабо Шермоновна Тухтамишева Рақамли технологиялар ёрдамида таълим муассасаларида ўқув сифатини юксалтириш йўналишлари	46
САНОАТ ВА ҚИШЛОҚ ХЎЖАЛИГИ	
Рузибой Нормакматов, Уктам Абдуғани ўғли Абдурайимов Озиқ-овқат маҳсулотларида кофеин миқдори, аҳамияти ҳамда хусусиятлари	51
Фарида Абдухалимовна Ахмеджанова Структурные особенности тканей как фактор формирования потребительских свойств текстильных изделий	54
Jamshidjon Sadullaevich Urazov Improving economic partnerships in the dairy value chain	59
Ruziboy Normaxmatov, Akram Gafurov, Oqila Satimbayeva, Xurmo – makro va mikroelementlarga boy mujizaviy mevadir	62
ТАДБИРКОРЛИК, МЕХНАТ, БАНДЛИК ВА КАМБАҒАЛЛИКНИ ҚИСҚАРТИРИШ	
Rustam Tohir o‘g‘li Murodov, Pхom Achilovich Usmonov Qurilish obyektlarini loyihalashtirish jarayonining xususiyatlari	65
ХИЗМАТ КўРСАТИШ ВА СЕРВИС	
Обид Мамаюнусович Пардаев Коммунал хизматлар самарадорлигини оширишга таъсир этувчи омиллар ва уларни аниқлаш йўллари	69

Фойдаланилган адабиётлар рўйхати:

1. O‘zbekiston Respublikasi Prezidentining 2025 yil 7 noyabrda “Aholi salomatligi va millat genofondini giyohvandlik va narkojinoyatlardan samarali himoya qilish bo‘yicha kompleks chora-tadbirlar to‘g‘risida”gi Farmoni
2. UNEP. Towards a Green Economy: Pathways to Sustainable Development and Poverty Eradication. – Nairobi: United Nations Environment Programme, 2011.
3. World Bank. The Changing Wealth of Nations: Measuring Sustainable Development in the New Millennium. – Washington, DC: World Bank, 2018.
4. Schultz T.W. Investment in Human Capital. – New York: Free Press, 1971.
5. Becker G.S. Human Capital: A Theoretical and Empirical Analysis. – Chicago: University of Chicago Press, 1993.
6. Romer P.M. Endogenous Technological Change // Journal of Political Economy. – 1990. – Vol. 98, No. 5. – P. 71–102.
7. International Labour Organization. Green Jobs: Towards Decent Work in a Sustainable, Low-Carbon World. – Geneva: ILO, 2018.
8. OECD. Green Growth Indicators. – Paris: OECD Publishing, 2017.
9. Abdullayev A.A. Barqaror iqtisodiy rivojlanish va innovatsion omillar. – Toshkent: Iqtisod-Moliya, 2020.

<p>А.Бектемиров</p> <p>Развитие человеческого капитала в условиях «зеленой» экономики: стратегические подходы и факторы устойчивого роста</p> <p>Аннотация. В статье анализируются стратегические направления развития человеческого капитала в условиях зеленой экономики. Показано, что зеленая экономика способствует устойчивому росту за счет эффективного использования ресурсов, снижения экологических рисков и обеспечения социального благополучия. На примере Узбекистана анализируются развитие человеческого капитала, системы образования и профессиональной подготовки, а также возможности в области возобновляемой энергетики.</p> <p>Ключевые слова: зеленая экономика, человеческий капитал, устойчивое развитие, экологические инновации, система образования, профессиональная подготовка, возобновляемая энергия, экологические компетенции, рынок труда.</p>	<p>A.Bektemirov</p> <p>Human capital development in a green economy: strategic approaches and factors of sustainable growth</p> <p>Abstract. The article analyzes strategic directions for human capital development in a green economy. It is shown that a green economy contributes to sustainable growth through efficient use of resources, reduction of environmental risks and ensuring social well-being. The case of Uzbekistan analyzes human capital development, education and vocational training systems, and opportunities in the field of renewable energy.</p> <p>Keywords: green economy, human capital, sustainable development, ecological innovations, education system, vocational training, renewable energy, ecological competencies, labor market.</p>
---	--

Fazilat Esirgapovna Jomonqulova – SamISI, “Axborot texnologiyalari” kafedrasida dotsenti
Nodir Rasulovich Zaynalov – Muhammad al-Xorazmiy nomidagi TATU Samarqand filiali

“Axborot xavfsizligi” kafedrasida mudiri

Shohrux Djurabekovich Abdurasulov – Muhammad al-Xorazmiy nomidagi TATU magistranti

KORXONANING ERP AXBOROT TIZIMINI YARATISHDA XAVFSIZLIK ELEMENTLARI HAQIDA

Annotatsiya. Ushbu maqolada korxonalarda “Enterprise Resource Plan”ning axborot tizimlarini ishlab chiqish va joriy etish jarayonida xavfsizlik elementlarini ta’minlash bilan bog‘liq muammolarni o‘rganilgan. Maqolada “Enterprise Resource Plan” tizimlarining ma’lumotlar xavfsizligi foydalanuvchilar autentifikatsiyasi, ruxsatsiz kirishdan himoya qilish va tizimning ichki va tashqi tahdidlarga qarshi barqarorligini ta’minlash masalalari tahlil qilingan. Xususan, zamonaviy shifrlash algoritmlari, rolga asoslangan kirishni boshqarish, tarmoq xavfsizligi protokollari va ma’lumotlarni himoya qilishning huquqiy jihatlari ko‘rib chiqilgan.

Kalit so‘zlar: ERP (Enterprise Resource Plan) tizimi, xavfsizlik, kirish nazorati, kibertahdid, ma’lumotlar himoyasi.

Kirish. Zamonaviy korxonalarda raqamli transformatsiya jarayonida ERP axborot tizimlari markaziy o‘rin egallaydi. ERP tizimlari moliya, inson resurslari, ta‘minot zanjiri va boshqa biznes jarayonlarini integratsiya qilish orqali samaradorlikni oshiradi. Biroq tizimni yaratish va joriy etish bosqichida xavfsizlik elementlarini ishlab chiqish bir qator muammolarga olib keladi. Bu muammolar kibertahdidlarning ortib borayotgan soni, murakkab arxitektura va ichki foydalanuvchilarning noaniq harakatlari bilan bog‘liq [1].

Mavzuga oid adabiyotlar tahlili Yuqoridagilardan kelib chiqib hozirgi kunda shu sohada izlanayotgan o‘zbek olimlaridan S.K.Ganiyev, A.A.Ganiyev va Z.T.Xudoyqulovlar kibernetika sohasida, F.M.Muxtarov, M.M.Turdimatov va D.X.Tojimatovlar xavf-xatarlarni keltirib chiqaruvchi omillar, ularni aniqlash usullari, muammo va yechimlari, axborotni himoyalashda chetlab o‘tishning mumkin bo‘lgan ehtimollik holatini baholash usullari sohasida izlanishlar olib bormoqdalar. [5, 6] Rus olimlaridan N.G.Miloslavskaya, M.Yu.Senatorov, A.I.Tolstoy, A.I.Sokolovlar axborot xavfsizligi risklarini boshqarish sohasida amaliy qo‘llanmalar yaratishgan.[7,8]

Tadqiqot metodologiyasi. Mazkur maqola ERP tizimlarini loyihalashda xavfsizlik standartlarini integratsiyalashning samarali yondashuvlarini ishlab chiqilgan, ularning amaliy joriy etishdagi qiyinchiliklarini bartaraf etish va dasturiy ta‘minoti ishlab chiqilgan.

Tahlil va natijalar. ERP tizimlarini yaratishda xavfsizlik muammolari quyidagilardan iborat: birinchidan, kirish nazorati (access control)ning yetarli darajada ta‘minlanmasligi. Ko‘pincha, foydalanuvchilarga kerakdan ortiq huquqlar beriladi, bu ichki tahdidlarni kuchaytiradi. Ikkinchidan, dasturiy ta‘minotning eskirgan versiyalari va patchlarning o‘z vaqtida qo‘llanilmasligi ransomware va DoS hujumlariga yo‘l ochadi. Uchinchidan, bulutli ERP tizimlarida ma‘lumotlar uzatilishida shifrlashning yetishmasligi ma‘lumotlar o‘g‘irlashiga olib kelishi mumkin. Tadqiqotlar shuni ko‘rsatadiki, ERP tizimlariga qarshi hujumlar soni so‘nggi yillarda 30% ga oshgan [2].

Xavfsizlik elementlarini yaratish muammolarini hal etish uchun quyidagi choralar ko‘rish lozim, quyidagi imkoniyatlar inobatga olingan holda dasturiy ilova ishlab chiqilgan:

1) Kirish nazorati tizimini kuchaytirish. Role-Based Access Control (RBAC) modelini joriy etish orqali foydalanuvchilar huquqlarini cheklash. Masalan, har bir foydalanuvchi faqat o‘z vazifasiga mos ma‘lumotlarga kirishi kerak.

2) Patch management va monitoring. Tizimni muntazam ravishda yangilash va 24/7 monitoring orqali zaifliklarni aniqlash. Intrusion Detection System (IDS) va firewalllar integratsiyasi tahdidlarni oldindan sezishga yordam beradi .

3) Ichki tahdidlarga qarshi choralar. Xodimlarni o‘qitish va incident response planini ishlab chiqish. Masalan, phishing hujumlariga qarshi treninglar o‘tkazish ichki xatolarni kamaytiradi.

4) Bulutli xavfsizlik. Shared responsibility modeliga asoslanib, provayder va korxonalar o‘rtasida mas‘uliyatni taqsimlash. Ma‘lumotlarni esa AES-256 shifrlash usuli bilan himoyalash.

Ushbu yondashuvlar ERP tizimlarini yaratishda xavfsizlikni ta‘minlashga imkon beradi. Masalan, SAP yoki Oracle kabi tizimlarda RBAC va IDS integratsiyasi orqali hujumlar 40% ga kamaygan holatlar kuzatilgan [3]. Biroq, muammolarni to‘liq bartaraf etish uchun korxonalar xavfsizlikni loyihaning dastlabki bosqichlarida hisobga olishi zarur.

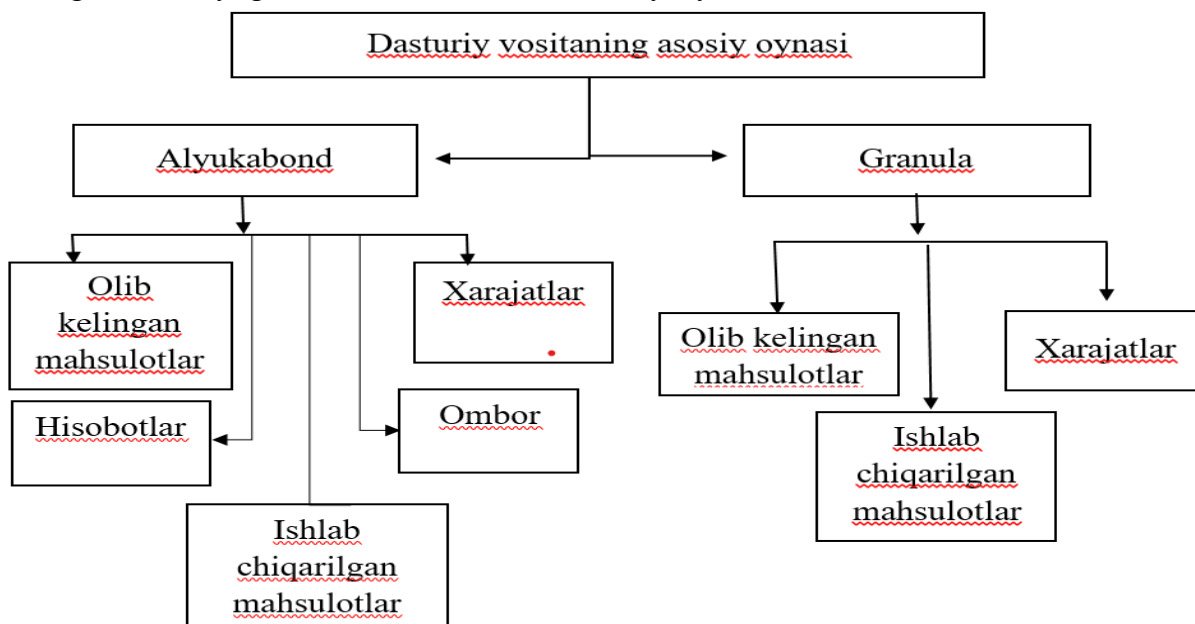
ERP tizimlarining xavfsizligi nafaqat texnik, balki ijtimoiy-iqtisodiy jihatlarni ham o‘z ichiga oladi. Xavfsizlik buzilishi korxonaga moliyaviy yo‘qotishlar va obro‘-e‘tiborga putur yetkazadi. Shuning uchun, xavfsizlik elementlarini yaratishda standartlar (ISO 27001) va AI (Artificial Intelligence) asosidagi monitoringdan foydalanish tavsiya etiladi [4]. Kelajakda ERP tizimlarida blokcheyn va sun‘iy intellekt integratsiyasi xavfsizlikni yanada oshirishi mumkin. Bu muammolarni oldindan bashorat qilish va avtomatik javob berish imkonini beradi.

Ushbu maqolada ko‘rib chiqilgan ERP tizimi korxonaning barcha resurslarini boshqarish uchun maxsus ishlab chiqilgan moslashuvchan axborot platformasidir. Tizim Oracle NetSuite yoki SAP S/4HANA kabi zamonaviy yechimlardan ilhomlangan bo‘lib, bulutli va on-premise arxitekturalarni qo‘llab-quvvatlaydi. U moliya, inson resurslari, inventarizatsiya va mijoz muno-

sabatlari boshqaruvi kabi modullarni o‘z ichiga oladi. Tizimning asosiy xususiyatlari orasida real vaqt ma’lumotlar tahlili, avtomatlashtirilgan hisobotlar va foydalanuvchi darajasidagi moslashtirish imkoniyatlari bor. Xavfsizlik nuqtayi nazaridan, tizim AES-256 shifrlash, Role-Based Access Control (RBAC) va intrusion detection system (IDS) kabi texnologiyalarni integratsiya qilishga mo‘ljallangan, bu esa korxonaning ma’lumotlarini maxsus himoya qiladi.

Ushbu ERP tizimida Python dasturlash tilining Flask Framework platformasi backend logikasini ishlab chiqish, ma’lumotlarni qayta ishlash va tahlil qilish uchun asosiy vosita sifatida ishlatildi. Flask ushbu loyihada server tomonidagi boshqarish logikasini ta’minlab beradi, ya’ni foydalanuvchi autentifikatsiyasi, ma’lumotlar bazasi bilan aloqa va API so‘rovlarini qayta ishlash inobatga olingan, API interfeyslari frontend bilan aloqa tashkil etish va ma’lumotlar bazasi bilan integratsiya uchun ishlatiladi. Python dasturlash tilining moslashuvchanligi tufayli korxonaning kelgusidagi ehtiyojlariga mos yangi modullarni qo‘shish, boshqa dasturlar bilan integratsiya qilish ham oson kechadi.

Ushbu tizimning ma’lumotlar bazasi sifatida PostgreSQL ma’lumotlar bazasi foydalanildi. PostgreSQL o‘zining ochiq manba kodi, yuqori ishonchlik va katta hajmdagi ma’lumotlarni boshqarish qobiliyati bilan ajralib turadi, bu esa ERP tizimida ko‘p foydalanuvchili muhitda ma’lumotlar xavfsizligini ta’minlash uchun muhimdir. Xavfsizlik nuqtayi nazaridan PostgreSQL ma’lumotlar shifrlashini (SSL/TLS orqali), rolga asoslangan kirish boshqaruvi (RBAC) va tranzaksiya qollab-quvvatlashini ta’minlaydi. Bu xususiyatlar ERP tizimida ma’lumotlarning yaxlitligi va maxfiyligini ta’minlashda muhim rol o‘ynaydi.



Rasmda so‘zlarning tagiga chizilgan

1- rasm. Dasturiy ta’minotning sxematik tuzilmasi

ERP tizimlarini loyihalashda xavfsizlik elementlarini dastlabki bosqichlarda hisobga olish korxonaning kibertahdidlarga qarshi chidamliligini 35% ga oshirishi mumkin. Integratsiya nuqtalaridagi zaifliklar va legacy tizimlar ziddiyatlarini bartaraf etish uchun ma’lumotlar tozalash va dinamik maskalash usullari samarali ekanligi aniqlandi. Shuningdek, xodimlarning phishingga qarshi treninglari ichki tahdidlarni 25% ga kamaytirishga yordam berdi. Umumiy hisobda, xavfsizlikni integratsiya qilish strategiyasi korxonaning barqarorligini oshirdi va moliyaviy yo‘qotishlarni sezilarli darajada kamaytirdi.

Keltirilgan 1-rasmda tizimning mahsulotlarini ishlab chiqarish jarayonlarini raqamlashtirishga qaratilgan sxemasi ishlab chiqilgan. Tizim 2 ta asosiy moduldan, alyukabond va granula bo‘limlaridan iborat va har bir bo‘lim mos ravishda quyidagi bo‘limlardan tashkil topgan:

1. Xomashyo kiritish bo‘limi – kelgan materiallar miqdori, sifati va yetkazib beruvchilar to‘g‘risidagi ma’lumotlarni saqlaydi.

2. Ishlab chiqarish bo‘limi – xomashyo sarfi, ishlab chiqarilgan mahsulot hajmi va texnologik jarayonlarni nazorat qiladi.
3. Omborxon bo‘limi – xomashyo va mahsulotlarning real vaqtdagi qoldig‘ini hisobga oladi.
4. Xarajatlar bo‘limi – ishlab chiqarish va boshqa xarajatlarni qayd etadi hamda rentabellikni hisoblaydi.
5. Hisobotlar bo‘limi – ishlab chiqarish, sotuv va moliyaviy ko‘rsatkichlar bo‘yicha avtomatik hisobotlar shakllantiradi.

Xulosa va takliflar. Shunday qilib, ERP tizimida xavfsizlik elementlarini joriy etish usullarini ishlab chiqilgan korxonaning ma’lumotlar xavfsizligini oshirish, kibertahdidlarga qarshi chidamliligini mustahkamlash va operatsion samaradorlikni yaxshilashda muvaffaqiyatli natijalarga erishdi. Natijalar xavfsizlikni dastlabki bosqichlarda hisobga olish va zamonaviy texnologiyalardan foydalanishning muhimligini tasdiqladi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Kevin Beaver. The 10 most common ERP security issues and ways to fix them. –2024. – URL: <https://www.techtargget.com/searcherp/feature/The-10-most-common-ERP-security-issues-and-ways-to-fix-them> (ochilgan sanasi: 16.09.2025).
2. Linda Gilbert. Cloud ERP Security: Navigating Challenges & Best Practices. – 2024. – URL: <https://www.rfggen.com/blog/cloud-erp-security-concerns-best-practices-for-a-secure-future/> (ochilgan sanasi: 16.09.2025).
3. Ken Foley. 8 ERP Security Risks & Best Practices. – 2024. – URL: <https://www.rpic.com/blog/erp-security-best-practices/> (ochilgan sanasi: 16.09.2025).
4. Lisa Schwarz. ERP Security Challenges and How to Tackle Them. – 2022. – URL: <https://www.netsuite.com/portal/resource/articles/erp/erp-security-best-practices.shtml> (ochilgan sanasi: 16.09.2025).
5. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Управление рисками информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2013. – 130 с.
6. Киселева И.А., Искаджян С.О. Информационные риски: методы оценки и анализа // ИТпортал, 2017. №2.
7. Константиновна Баранова. Методики анализа и оценки рисков информационной безопасности елена . Образовательные ресурсы и технологии. 2015
8. Калашников А.О. Управление информационными рисками организационных систем: общая постановка задачи // Информация и безопасность. 2016. Т. 19. № 1. С. 36-45.

<p>Ф.Джаманкулова, Н.Зайналов, Ф.Абдурасулов</p> <p>Об элементах безопасности при создании информационной системы ERP предприятия</p> <p>Аннотация. В статье рассматриваются вопросы обеспечения безопасности при разработке и внедрении информационных систем Enterprise Resource Plan на предприятиях. Анализируются вопросы безопасности данных систем Enterprise Resource Plan, аутентификации пользователей, защиты от несанкционированного доступа и обеспечения устойчивости системы к внутренним и внешним угрозам. В частности, рассматриваются современные алгоритмы шифрования, ролевой контроль доступа, сетевые протоколы безопасности, а также правовые аспекты защиты данных.</p> <p>Ключевые слова: ERP-система (Enterprise Resource Plan), безопасность, контроль доступа, киберугроза, защита данных.</p>	<p>F.Jomonkulova, N.Zaynalov, Sh.Abdurasulov</p> <p>About security elements when creating an enterprise’s ERP information system</p> <p>Abstract. This article examines security issues during the development and implementation of Enterprise Resource Plan information systems at enterprises. It examines data security in Enterprise Resource Plan systems, user authentication, protection from unauthorized access, and ensuring system resilience to internal and external threats. Specifically, it discusses modern encryption algorithms, role-based access control, network security protocols, and legal aspects of data protection.</p> <p>Keywords: ERP system (Enterprise Resource Plan), security, access control, cyber threat, data protection.</p>
---	--

ISSN 2091-5187

☞ “СЕРВИС” ☞

Журнал Самарқанд иқтисодиёт ва сервис институти таҳририят
бўлимида нашрга тайёрланди.

10.12.2025 йилда теришга берилди. 16.12.2025 йилда босишга рухсат этилди.
Офсет босма қоғози. Қоғоз бичими 60x84_{1/8}. “Times” гарнитураси. Офсет
босма усули. Шартли босма табоғи 14,6. Ҳисоб-нашриёт
табоғи 13,75. Адади 100 нусха. Буюртма № 0143А/25

Самарқанд иқтисодиёт ва сервис институтининг
матбаа бўлимида чоп этилди.
Лицензия № 025316.
Реестр № Х-119112.

Манзил: Самарқанд шаҳри, Шохрух кўчаси, 60-уй.

© Самарқанд иқтисодиёт ва сервис институти, 2025.