УДК 658.5.012.7

ИНФОРМАЦИОННЫЕ ПОТОКИ ПРЕДПРИЯТИЯ СКЛАДСКОГО ХОЗЯЙСТВА ТОВАРОВ НАРОДНОГО ПОТРЕБЛЕНИЯ КАК ОБЪЕКТ ЗАЩИТЫ ИНФОРМАЦИИ

Пономарева Ольга Алексеевна, доцент, кандидат технических наук, Учебно-научный центр «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Грибов Михаил Андреевич, магистрант, Учебно-научный центр «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Чистяков Максим Владимирович, магистрант, Учебно-научный центр «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Барыбин Дмитрий Александрович, магистрант, Учебно-научный центр «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Аннотация

Целью исследования является оценка угроз информационной безопасности на предприятиях складского хранения и разработка мероприятий по их устранению. В работе проведен анализ нормативных документов, публикаций в специализированных журналах и мнений экспертов в сферах логистики и информационной безопасности, а также рассмотрены инциденты, связанные с утечкой данных в логистических компаниях. Исследование также охватило специфику информационных потоков на складах и уязвимости, возникающие при внедрении новых технологических решений. В статье предложена модель системы обмена и обработки информации на складе, основанная на стандарте функционального моделирования IDEF0. Были идентифицированы ключевые угрозы информационной безопасности, такие как вредоносное программное обеспечение, фишинг, DDoS-атаки, уязвимости веб-приложений и социальная инженерия. Для каждой угрозы предложены контрмеры, включающие использование современных протоколов шифрования, двухфакторную аутентификацию, регулярное обновление программного обеспечения и обучение сотрудников. Даны рекомендации по минимизации рисков, связанных с использованием RFID-меток, штрихкодов и QR-кодов, а также по обеспечению безопасности беспроводных каналов передачи данных. В исследовании подчеркивается необходимость комплексного подхода к обеспечению информационной безопасности на складах, включающего технические, организационные и обучающие мероприятия. Результаты исследования могут быть использованы для разработки методических рекомендаций по защите данных на предприятиях складского хранения.

КЛЮЧЕВЫЕ СЛОВА: защита информации, предприятия складского хранения, уязвимости, системы управления складом, социальная инженерия.

INFORMATION FLOWS OF A CONSUMER GOODS WAREHOUSE ENTERPRISE AS AN OBJECT OF INFORMATION PROTECTION

Ponomareva Olga Alexeevna, Associate Professor, Candidate of Sciences (Engineering), Educational and Research Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Gribov Mikhail Andreevich, Master's Student, Educational and Research Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Chistyakov Maxim Vladimirovich, Master's Student, Educational and Research Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Barybin Dmitry Alexandrovich, Master's Student, Educational and Research Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Abstract

The aim of the study is to assess information security threats at warehouse storage enterprises and develop measures to address them. The work involved an analysis of regulatory documents, publications in specialized journals, and expert opinions in the fields of logistics and information security, as well as an examination of incidents related to data leaks in logistics companies. The study also explored the specifics of information flow in warehouses and vulnerabilities arising from the implementation of new technological solutions. The article proposes a model of the information exchange and processing system in a warehouse, based on the IDEF0 functional modeling standard. Key information security threats, such as malware, phishing, DDoS attacks, web application vulnerabilities, and social engineering, were identified. For each threat, countermeasures were proposed, including the use of modern encryption protocols, two-factor authentication, regular software updates, and employee training. Recommendations were provided to minimize risks associated with the use of RFID tags, barcodes, and QR codes, as well as to ensure the security of wireless data transmission channels. The study emphasizes the need for a comprehensive approach to ensuring information security in warehouses, encompassing technical, organizational, and educational measures. The results of the research can be used to develop methodological recommendations for data protection at warehouse storage enterprises.

KEYWORDS: information protection, warehouse storage enterprises, vulnerabilities, warehouse management systems, social engineering.

Введение

В условиях цифровизации и глобализации бизнеса предприятия складского хранения сталкиваются с новыми вызовами в сфере кибербезопасности, а количество выявляемых угроз постоянно растет. По данным за январь–октябрь 2024 года, количество кибератак на ИТ-инфраструктуру транспортно-логистических компаний возросло на 30% по сравнению с 2023 годом. Каждая из атак представляет собой новую задачу для подразделений информационной безопасности, поскольку злоумышленники разрабатывают новые схемы взлома защищенной инфраструктуры [1].

Увеличение объемов данных и автоматизация процессов требуют разработки эффективных методов обеспечения информационной безопасности. В данной статье рассматриваются основные угрозы, с которыми сталкиваются логистические компании, а также предлагаются решения по повышению уровня защиты данных.

Проанализировав данные о построении информационно-технической структуры складского предприятия с учетом применения современных методов организации хранения, на основе необходимости обеспечения сохранности информации, циркулирующей в складской системе, требуется выявить элементы, подверженные атакам, и разработать меры по их защите.

Для анализа уязвимостей и угроз на предприятиях складского хранения была проведена оценка существующих методов обеспечения информационной безопасности. Применялись методы качественного анализа, включая изучение интервью с экспертами в области кибербезопасности и исследование случаев утечек данных. Также был проведен анализ литературы, посвященной современным информационным технологиям и их уязвимостям.

Результаты

Складское предприятие представляет собой организацию, предназначенную для

хранения, обработки и управления товарными запасами в рамках логистической цепи.

Можно выделить несколько основных функциональных операций, выполняемых персоналом в процессе складской деятельности:

1. Приёмка товаров и материалов.
2. Непосредственно хранение.
3. Контроль за состоянием единиц складского учета.
4. Обеспечение сохранности имущества, принятого на склад.
5. Взаимодействие с контрагентами.
6. Комплектация и упаковка заказов.
7. Отгрузка товара.
8. Документооборот.

Складские операции представляют собой один из важнейших этапов бизнес-процесса любого предприятия, занятого в производстве или торговле. Это задача, напрямую связанная с эффективностью и рентабельностью предприятия в целом, поэтому использование современных технологий в складской деятельности в наши дни является необходимостью [2].

В условиях современных высококонкурентных рынков эффективная организация складского хозяйства имеет критически важное значение, поскольку она составляет значительную часть логистических затрат [3]. Таким образом, цифровизация представляет собой неизбежный процесс развития логистических и складских предприятий. В результате использования высокотехнологичных устройств и современных систем обработки информации повышаются точность и скорость выполнения заказов, предоставляются дополнительные возможности пользователю, однако одновременно с этим возрастают и риски, связанные с утечкой критически важной информации и сбоями в системах информационного обмена [4].

«Мозговым центром» современного цифрового логистического предприятия является WMS (Warehouse Management System) — система управления складом, обладающая широким набором учетных и регулирующих функций, позволяющая полностью автоматизировать управление складским хозяйством [5].

Целью ее внедрения является повышение прозрачности складских операций и снижение затрат ресурсов на управление типовыми задачами, а именно:

1. своевременное информирование об операциях, осуществляемых на складе;
2. управление структурой складского пространства;
3. автоматизация управления процедурами приёмки и хранения товаров;

4. автоматизированный контроль корректности учетных данных о количестве и номенклатуре единиц хранения;
5. управление складскими операциями с применением программно-аппаратных решений [5].

Складские системы подвержены многочисленным угрозам различного характера, обусловленным повсеместным использованием высокотехнологичных ИТ-систем, задействованных в WMS. Эти угрозы можно обобщенно классифицировать на несколько групп: управление данными, программные системы, аппаратные средства автоматизации, цифровая сетевая инфраструктура, физическая инфраструктура и взаимодействие «человек-машина» [6].

Согласно исследованиям экспертов, наиболее распространенными угрозами для WMS являются вредоносное программное обеспечение (38%), фишинг (30%) и DDoS-атаки (20%) [7]. Количество фишинговых атак растет, при этом следует отметить возросшую «компетентность» злоумышленников. Рассылаемые ими письма зачастую идентичны запросам официальных учреждений, содержат актуальные названия должностей и фамилии сотрудников. Также для реализации своих планов преступники активно используют ранее полученную незаконным путем конфиденциальную информацию о деятельности компании – номера договоров, внутреннюю переписку, должности и фамилии сотрудников.

Анализ киберинцидентов показывает, что около трети (26%) уязвимостей в логистике связаны с недостатками алгоритмов защиты при использовании SMS для регистрации, авторизации или восстановления пароля. Киберпреступники используют скрипт для подбора чужих номеров телефонов, в результате система рассылает тысячи текстовых сообщений, расходуя средства компании [1].

WMS функционирует в рамках системного окружения предприятия и взаимодействует со смежными системами через интерфейсы (рис. 1). На схеме показано взаимодействие WMS с другими информационными системами предприятия [8, стр. 3-4, 9].

Проанализировав направления информационного обмена, характерные для предприятий складского хранения, на основе выполнения основных функций от поступления товарно-материальных ценностей до их отгрузки контрагентам [2, 3, 10] и рассмотрев возможные угрозы информационной безопасности [7, 9], была разработана функциональная модель информационного обмена складского предприятия в разрезе воздействия угроз информационной безопасности в соответствии со стандартом функционального моделирования IDEF0, представленная на рис. 2.

Рис. 1. Схема взаимодействия WMS с информационными системами предприятия

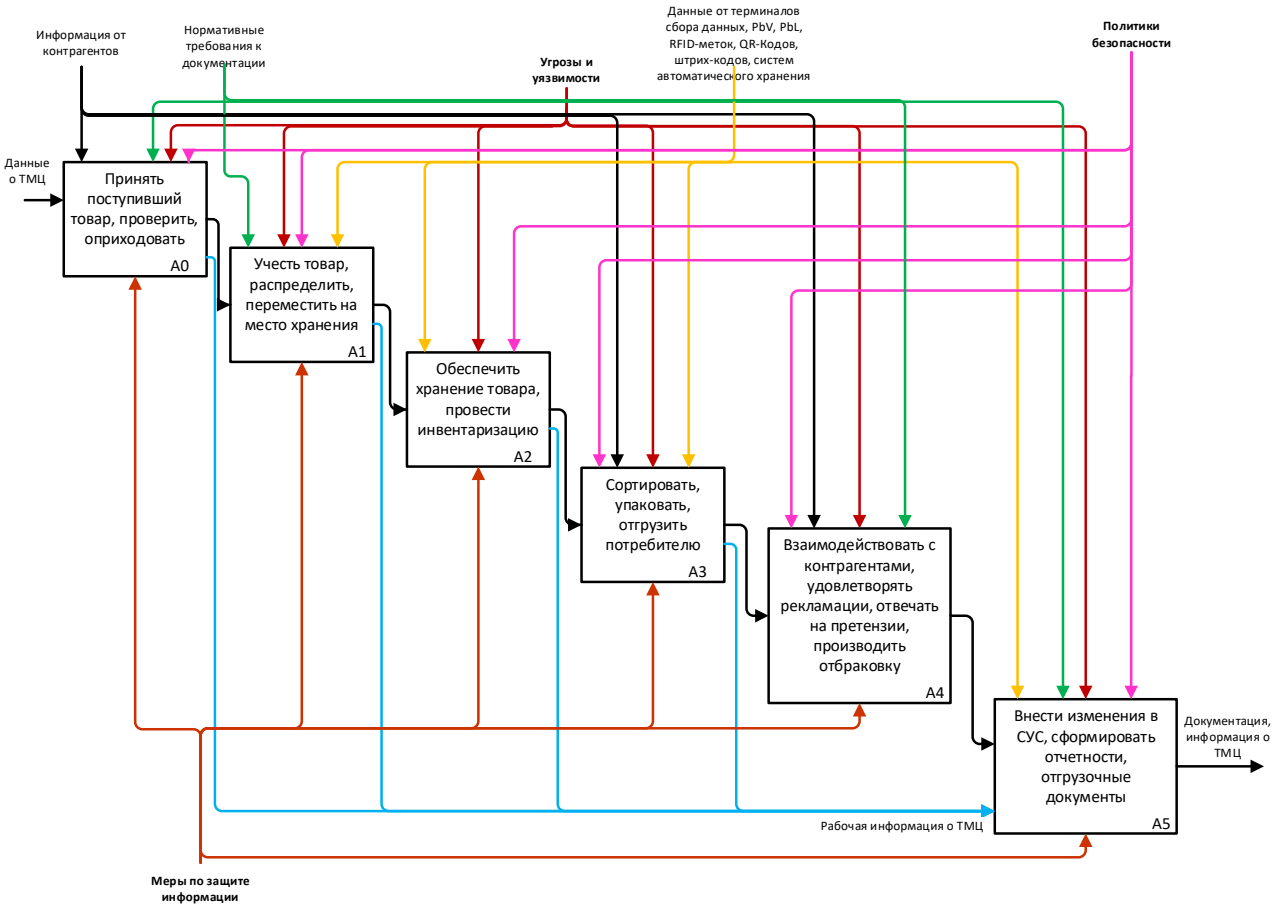

Рис. 2. Модель информационного обмена складского предприятия с точки зрения воздействия угроз информационной безопасности.

Основные угрозы информационной безопасности и меры борьбы с ними представлены в таблице 1.

Таблица 1. Уязвимости и меры борьбы с ними

№ п/п	Уровень	Уязвимость	Меры борьбы
	A0	1. Разглашение чувствительной информации на стороне контрагентов.	1. Заключение соглашения о защите информации.
		2. Уязвимости в веб-приложениях: SQL-инъекции, XSS, Data-bombs.	2. Параметризованные запросы, использование ORM-библиотек (Object-Relational Mapping); экранирование данных, ограничение привилегий; экранирование вывода, внедрение CSP (Content Security Policy) для предотвращения выполнение неавторизованных скриптов; фильтрация ввода, лимиты на размер данных, фильтрация, мониторинг.
		3. Атаки на отказ в обслуживании сетевого оборудования: DDoS-атаки, направленные на перегрузку сетевых ресурсов.	3. Использование брандмауэров, систем обнаружения и предотвращения вторжений (IDS/IPS), облачных хранилищ.
		4. Вредоносное программное обеспечение (Malware): вирусы, черви, трояны и шпионские программы.	4. Антивирусное ПО, обучение пользователей, мониторинг и анализ систем.
		5. Атаки на протоколы передачи данных: ARP spoofing, DNS spoofing и Man-in-the-Middle (MitM).	5. Статические ARP-записи; использование DNSSEC и мониторинг DNS-трафика; HTTPS, TLS и многофакторная аутентификация.
		6. Устаревшее ПО.	6. Регулярное обновление ПО.
		7. Не используются современные протоколы защиты при передаче и хранении информации, незащищенное хранение информации на серверах.	7. Использование протоколов TSL актуальных версий, IPsec, SSH, PGP/GPG, AES, S/MIME.
		8. Отсутствие или неправильно реализованная политика по разграничению прав доступа.	8. Разработка и внедрение политики доступа с минимально необходимыми правами, занятия с сотрудниками, регулярные аудиты.

№ п/п	Уровень	Уязвимость	Меры борьбы
		9. Использование паролей недостаточной степени сложности, отсутствие их периодической замены, недостатки аутентификации в системе.	9. Адекватная парольная политика, аудит, занятия с сотрудниками, двухфакторная аутентификация с защитой от многократного ввода.
		10. Социальная инженерия, фишинг	10. Занятия с сотрудниками, тренинги по ИБ.
	A1, A2, A3	1. Недостаточная защита программного интерфейса приложений (API).	1. Аутентификация (OAuth 2.0), шифрование (TLS), контроль доступа (RBAC/ABAC), API Gateway, валидация данных, ограничение скорости, мониторинг, обновления, тестирование безопасности.
		2. Отсутствие шифрования данных.	2. Использование протоколов TSL актуальных версий, IPsec, SSH, PGP/GPG, AES, S/MIME.
		3. Использование средств беспроводной передачи данных с недостаточным уровнем защищенности каналов связи.	3. Шифрование WPA3, сегментация сети, VPN, многофакторная аутентификация, обновления, мониторинг, скрытие SSID, фильтрация MAC-адресов, ограничение мощности сигнала.
		4. Уязвимости радиочастотнаых меток (Radio Frequency Identification - RFID), штрих-кодов, QR-кодов.	4. Внедрение защиты в RFID-метки, двухфакторная аутентификация, защиты радиоканала, использование специализированного ПО, физическая защита кодов, мониторинг и аудит.
		5. Отсутствие или неправильно реализованная политика по разграничению прав доступа.	5. Разработка и внедрение политики доступа с минимально необходимыми правами, занятия с сотрудниками, регулярные аудиты.
		6. Использование паролей недостаточной степени сложности, отсутствие их периодической замены.	6. Адекватная парольная политика, аудит, занятия с сотрудниками.
		7. Социальная инженерия.	7. Проведение учений по кибербезопасности на предприятиях,тренинги для сотрудников по вопросам выполнения требований информационной безопасности.
	A4	1. Разглашение чувствительной информации на стороне контрагентов.	1. Заключение соглашения о защите информации.

№ п/п	Уровень	Уязвимость	Меры борьбы
		2. Уязвимости в веб-приложениях: SQL-инъекции, XSS, Data-bombs.	2. Параметризованные запросы, использование ORM-библиотек (Object-Relational Mapping); экранирование данных, ограничение привилегий; экранирование вывода, внедрение CSP (Content Security Policy) для предотвращения выполнение неавторизованных скриптов; фильтрация ввода, лимиты на размер данных, фильтрация, мониторинг.
		3. Атаки на отказ в обслуживании сетевого оборудования: DDoS-атаки, направленные на перегрузку сетевых ресурсов.	3. Использование брандмауэров, систем обнаружения и предотвращения вторжений (IDS/IPS), облачных хранилищ.
		4. Вредоносное программное обеспечение (Malware): вирусы, черви, трояны и шпионские программы.	4. Антивирусное ПО, обучение пользователей, мониторинг и анализ систем.
		5. Атаки на протоколы передачи данных: ARP spoofing, DNS spoofing и Man-in-the-Middle (MitM).	5. Статические ARP-записи; использование DNSSEC и мониторинг DNS-трафика; HTTPS, TLS и многофакторная аутентификация.
		6. Устаревшее ПО.	6. Регулярное обновление ПО.
		7. Не используются современные протоколы защиты при передаче и хранении информации, незащищенное хранение информации на серверах.	7. Использование протоколов TSL актуальных версий, IPsec, SSH, PGP/GPG, AES, S/MIME.
		8. Отсутствие или неправильно реализованная политика по разграничению прав доступа.	8. Разработка и внедрение политики доступа с минимально необходимыми правами, занятия с сотрудниками, регулярные аудиты.
		9. Использование паролей недостаточной степени сложности, отсутствие их периодической замены, недостатки аутентификации в системе.	9. Адекватная парольная политика, аудит, занятия с сотрудниками, двухфакторная аутентификация с защитой от многократного ввода.
		10. Социальная инженерия, фишинг	10. Занятия с сотрудниками, тренинги по ИБ.
	A5	1. Разглашение чувствительной информации на стороне контрагентов.	1. Заключение соглашения о защите информации.
		2. Уязвимости в веб-приложениях: SQL-инъекции, XSS, Data-bombs.	2. Параметризованные запросы, использование ORM-библиотек (Object-Relational Mapping);

№ п/п	Уровень	Уязвимость	Меры борьбы
			экранирование данных, ограничение привилегий; экранирование вывода, внедрение CSP (Content Security Policy) для предотвращения выполнение неавторизованных скриптов; фильтрация ввода, лимиты на размер данных, фильтрация, мониторинг.
		3. Атаки на отказ в обслуживании сетевого оборудования: DDoS-атаки, направленные на перегрузку сетевых ресурсов.	3. Использование брандмауэров, систем обнаружения и предотвращения вторжений (IDS/IPS), облачных хранилищ.
		4. Вредоносное программное обеспечение (Malware): вирусы, черви, трояны и шпионские программы.	4. Антивирусное ПО, обучение пользователей, мониторинг и анализ систем.
		5. Атаки на протоколы передачи данных: ARP spoofing, DNS spoofing и Man-in-the-Middle (MitM).	5. Статические ARP-записи; использование DNSSEC и мониторинг DNS-трафика; HTTPS, TLS и многофакторная аутентификация.
		6. Устаревшее ПО.	6. Регулярное обновление ПО.
		7. Не используются современные протоколы защиты при передаче и хранении информации, незащищенное хранение информации на серверах.	7. Использование протоколов TSL актуальных версий, IPsec, SSH, PGP/GPG, AES, S/MIME.
		8. Отсутствие или неправильно реализованная политика по разграничению прав доступа.	8. Разработка и внедрение политики доступа с минимально необходимыми правами, занятия с сотрудниками, регулярные аудиты.
		9. Использование паролей недостаточной степени сложности, отсутствие их периодической замены, недостатки аутентификации в системе.	9. Адекватная парольная политика, аудит, занятия с сотрудниками, двухфакторная аутентификация с защитой от многократного ввода.
		10. Социальная инженерия, фишинг	10. Занятия с сотрудниками, тренинги по ИБ.
		11. Недостаточная защита программного интерфейса приложений (API).	11. Аутентификация (OAuth 2.0), шифрование (TLS), контроль доступа (RBAC/ABAC), API Gateway, валидация данных, ограничение скорости, мониторинг, обновления, тестирование безопасности.

№ п/п	Уровень	Уязвимость	Меры борьбы
		12. Отсутствие шифрования данных.	12. Использование протоколов TSL актуальных версий, IPsec, SSH, PGP/GPG, AES, S/MIME.
		13. Использование средств беспроводной передачи данных с недостаточным уровнем защищенности каналов связи.	13. Шифрование WPA3, сегментация сети, VPN, многофакторная аутентификация, обновления, мониторинг, скрытие SSID, фильтрация MAC-адресов, ограничение мощности сигнала.
		14. Уязвимости радиочастотнаых меток (Radio Frequency Identification - RFID), штрих-кодов, QR-кодов.	14. Внедрение защиты в RFID-метки, двухфакторная аутентификация, защиты радиоканала, использование специализированного ПО, физическая защита кодов, мониторинг и аудит.

Заключение

Разработка эффективной методики обеспечения информационной безопасности на складских предприятиях требует комплексного подхода, учитывающего специфику процессов и технологий. Для эффективной защиты от угроз информационной безопасности на складах необходимо комплексно оценивать угрозы и каналы утечки конфиденциальной информации, разрабатывать системные решения, внедрять их на предприятиях и требовать от сотрудников строгого соблюдения положений политики информационной безопасности. На основе рассмотренных условий в дальнейшем необходимо продолжить исследования для разработки методических рекомендаций по обеспечению информационной безопасности на складских предприятиях.

Литература

1. Мишина, В. Штурма, Я. Направить в ссылку: компании по кибербезопасности назвали топ уязвимостей логистов. — Текст: электронный // Известия: [сайт]. — 2024. — URL: https://iz.ru/1798721/valeria-misina-ana-sturma/napravit-v-ssylku-kompanii-po-kiberbezopasnosti-nazvali-top-uazvimostei-logistov?roistat_visit=345503 (дата обращения: 02.03.2025).
2. Белан, Л. С. Сущность и методы рационализации системы складской логистики предприятия. — Текст: электронный // Экон. Финанс. Общ.: [сайт]. — 2023. — № 3(7). — URL: https://cyberleninka.ru/article/n/suschnost-i-metody-ratsionalizatsii-sistemy-skladskoy-logistiki-predpriyatiya (дата обращения: 02.03.2025).
3. Дыбская, В. В., Сергеев, В. И., Лычкина, Н. Н. и др. Цифровые технологии в логистике и управлении цепями поставок: аналитический обзор. — Текст: электронный // Изд.

дом Высшей школы экономики: [сайт]. — 2020. — URL: https://publications.hse.ru/pubs/share/direct/437257024.pdf (дата обращения: 02.03.2025).

4. Garcia, M. R., Betts, K., Ponce, E. Identifying the key vulnerabilities in the warehouses of the future. — MIT's Warehouse of the Future Initiative. — 2025.
5. Александрова, Л. Ю., Мунши, А. Ю. Актуальные проблемы логистики на складе и их решения. — Текст: электронный // Вестн. РУК: [сайт]. — 2020. — № 1(39). — URL: https://cyberleninka.ru/article/n/aktualnye-problemy-logistiki-na-sklade-i-ih-resheniya (дата обращения: 02.03.2025).
6. Enache, G. I. Security management in the context of supply chains technological upgrades. — International Conference on Business Excellence. — 2023. — Vol. 17. — No. 1. — P. 200-2012.
7. Токбай, А. Безопасность данных в WMS: методы защиты от киберугроз в управлении складом. — Текст: электронный // Актуал. Исслед.: [сайт]. — 2022. — № 30(109). — URL: https://apni.ru/article/4422-bezopasnost-dannyh-v-wms-metody-zashhity-ot-kiberugroz-v-upravlenii-skladom (дата обращения: 02.03.2025).
8. ГОСТ Р 59282-2020. Национальный стандарт Российской Федерации. Системы управления складом. Функциональные требования. — Москва: Стандартинформ, 2021.
9. Kim, J. Y., Park, D. J. Internet-of-things based approach for warehouse management system. — International journal of Multimedia and ubiquitous Engineering. — 2016. — No.11(10). — P. 159-166.
10. Boiko, A., Shendryk, V., Boiko, O. Information systems for supply chain management: uncertainties, risks and cyber security. — Procedia computer science. — 2018. — No. 149. — P. 65-70.