УДК 004.8:65.05:681.5 DOI: 10.31673/2786-8362.2024.010808

Шрам М.М., Руденко Н.В., к.т.н.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЛОГІСТИКИ У СВІТІ ВЕЛИКИХ ДАНИХ, ХМАРНИХ ОБЧИСЛЕНЬ ТА ІНТЕРНЕТУ РЕЧЕЙ

Shram M.M., Rudenko N.V. Ensuring logistics security in the world of Big Data, Cloud Computing and the Internet of Things. In this research paper, qualitative research methods were applied to determine how new technologies such as the Internet of Things, 5g, big data, and cloud computing can be used to support a well-functioning logistics system. Thus, a literature review was conducted using online databases such as Scopus, Elsevier, ScienceDirect, and Springer publications. Scientific articles, official EU reports and research by large companies in this area were also used. The industrial revolution led to a number of technical developments that radically changed the way organizations work, and as a result, significant changes have taken place in the logistics industry in recent years. While advanced data mining and machine learning (MN) technologies have made it possible to automate many important procedures, integration with the Internet of Things (IoT) has allowed logistics companies to track their assets in real time. But as the sector becomes increasingly dependent on technology, new cybersecurity challenges are emerging that compromise the integrity and security of mission-critical data. In addition, with the introduction of 5G networks, there were concerns about the possibility of new attack methods and vulnerabilities. Attacks over the Internet can have disastrous consequences, such as disruptions, loss of important data, and poor reputation. Because of the large amount of confidential information shared by many stakeholders, including customers, suppliers, and logistics companies, the logistics sector is particularly susceptible to cyberattacks. For example, the NotPetya malware caused damage to the company's IT systems. The international shipping giant Maersk was forced to temporarily suspend some of its operations in 2017. As a result, Maersk was forced to face serious financial losses, supply delays and supply chain disruptions for some customers. The hack also damaged the business's reputation and made customers worry about the security of their personal information and purchases. This example highlights the need for proactive measures to reduce the risk of such attacks, showing how cyberattacks can have serious and far-reaching consequences for organizations operating in the logistics sector.

Keywords: logistics, security, supply chain, Internet of Things (IoT), 5G, big data, cloud computing

Шрам М.М., Руденко Н.В. Забезпечення безпеки логістики у світі великих даних, хмарних обчислень та Інтернету речей. В умовах використання технологій, таких як Інтернет речей (IoT), 5g, великі дані та хмарні обчислення, в даній дослідницькій роботі передбачається проаналізувати проблеми кібербезпеки, з якими стикається логістична галузь. У цій статті ми розглянемо основні проблеми кібербезпеки, що впливають на логістичну галузь, і пояснимо реальні способи зниження цих ризиків на основі ретельного вивчення останніх досліджень. Інтернет речей (IoT) дозволив використовувати розумні пристрої, які можуть збирати та аналізувати величезні обсяги даних у режимі реального часу, надаючи логістичним операціям цінну інформацію. Але в міру розвитку пристроїв IoT збільшується і площа атак, що робить логістичні системи відкритими для цифрових атак. З впровадженням мереж 5G підключення стало більш швидким і надійним, що дозволяє здійснювати зв'язок між пристроями Інтернету речей в режимі реального часу і спрощує впровадження передових логістичних систем. Аналіз даних у режимі реального часу стає можливим завдяки масштабованій та безпечній інфраструктурі, що надається хмарними обчисленнями, що також підвищує безпеку логістичних систем. Заходи безпеки логістичних систем будуть все більше залежати від кібербезпеки, Інтернету речей, 5g, великих обсягів даних і хмарних обчислень, оскільки логістичні організації продовжують впроваджувати цифрові технології.

Ключові слова: логістика, безпека, ланцюжок поставок, Інтернет речей (IoT), 5G, великі дані, хмарні обчислення

Вступ

У цій дослідницькій роботі були застосовані якісні методи дослідження, щоб визначити, яким чином нові технології, такі як Інтернет речей, 5g, великі дані і хмарні обчислення, можуть бути використані для підтримки добре функціонуючої логістичної системи. Таким чином, було проведено огляд літератури з використанням онлайн-баз даних, таких як Scopus, Elsevier, ScienceDirect та Springer publications. Також використовувалися наукові статті, офіційні звіти ЄС та дослідження великих компаній у цій галузі.

Промислова революція призвела до ряду технічних розробок, які докорінно змінили спосіб роботи організацій, і в результаті в останні роки в галузі логістики відбулися суттєві зміни. Хоча передові технології видобутку даних та машинного навчання (МН) дозволили автоматизувати багато важливих процедур, інтеграція з Інтернетом речей (IoT) дозволила логістичним компаніям відстежувати свої активи в режимі реального часу. Але в міру того, як сектор стає все більш залежним від технологій, виникають нові проблеми в області кібербезпеки, які ставлять під загрозу цілісність і збереження критично важливих даних. Крім того, з впровадженням мереж 5G виникли побоювання з приводу можливості появи нових методів атаки і вразливостей.

Постановка завдання. Атаки через Інтернет можуть мати катастрофічні наслідки, такі як збої в роботі, втрата важливих даних і погіршення репутації. Через велику кількість конфіденційної інформації, якою обмінюються багато зацікавлених сторін, включаючи клієнтів, постачальників та логістичних компаній, сектор логістики особливо схильний до кібератак.

Наприклад, шкідливе програмне забезпечення NotPetya завдало шкоди IT-системам компанії міжнародний судноплавний гігант Maersk в 2017 році був змушений тимчасово призупинити деякі зі своїх операцій. В результаті Maersk був змушений зіткнутися з серйозними фінансовими втратами, затримками поставок і збоями в ланцюжку поставок для деяких клієнтів. Злом також завдав шкоди репутації бізнесу та змусив клієнтів турбуватися про безпеку своєї особистої інформації та покупок. Цей приклад підкреслює необхідність вжиття попереджувальних заходів для зменшення небезпеки подібних атак, показуючи, як кібератаки можуть мати серйозні та далекосяжні наслідки для організацій, що працюють у секторі логістики.

Аналіз останніх досліджень. Останні дослідження в галузі безпеки логістики в умовах великих даних, хмарних обчислень та Інтернету речей відображають зростаючу увагу до цієї проблематики через швидкий технологічний прогрес і збільшення обсягу даних, що обробляються та передаються у логістичних системах. Дослідники акцентують на ризиках, пов'язаних з цифровими атаками, витоком даних та недостатньою захищеністю інформації.

Аналіз показує, що однією з ключових проблем є нестача адекватних методів та інструментів для виявлення та вирішення кіберзагроз у логістичних системах. Дослідники також відзначають необхідність розвитку інтелектуальних систем моніторингу та аналізу, які здатні вчасно реагувати на загрози та ідентифікувати вразливі місця.

Загалом, останні дослідження підкреслюють необхідність поєднання інноваційних технологій з ефективними стратегіями кібербезпеки для забезпечення безпеки та стійкості логістичних систем у світі великих даних, хмарних обчислень та Інтернету речей.

Наукові публікації останніх років в галузі безпеки логістики у світі великих даних, хмарних обчислень та Інтернету речей виявляють кілька ключових тенденцій та напрямків досліджень:

1. Застосування штучного інтелекту та машинного навчання [4]: Багато публікацій акцентують на використанні методів штучного інтелекту та машинного навчання для виявлення та протидії кіберзагрозам у логістичних системах. Це включає в себе розробку алгоритмів для виявлення аномальних подій та прогнозування ризиків у реальному часі.

2. Блокчейн технології для забезпечення безпеки даних: Деякі дослідження досліджують потенціал блокчейн технологій для створення безпечних та надійних логістичних систем, де дані зберігаються децентралізовано та захищено від змін [1].

3. Використання аналітики великих даних для підвищення безпеки: Деякі публікації досліджують роль аналітики великих даних у виявленні та аналізі потенційних загроз для логістичних систем. Це включає в себе аналіз даних з різних джерел для ідентифікації вразливих місць та прогнозування майбутніх загроз [2].

4. Стандартизація та регулювання: Деякі дослідження розглядають важливість розробки стандартів та регуляцій для забезпечення безпеки логістичних систем у цифровому середовищі. Це може включати в себе рекомендації щодо застосування кібербезпеки та захисту даних у логістичних процесах.

Метою роботи є дослідження сучасних можливостей, пов'язаних з безпекою логістики в контексті швидко зростаючих технологій великих даних, хмарних обчислень та Інтернету речей. Висвітлення важливості впровадження заходів для забезпечення ефективності, надійності та стійкості логістичних процесів у цифровій ері.

Виклад основного матеріалу дослідження.

Кожна інформаційно-комунікаційна технологія породжує нове рішення, пов'язане з логістикою. Концепція логістики включає два елементи: Технічні інструменти та технології, які допомагають здійснювати внутрішню діяльність у ланцюжку поставок, а також процесуальні аспекти.

Використання передових технологій, таких як IoT, 5g, big data та хмарні обчислення, може підвищити безпеку логістичних систем. Ці технології можуть покращити комунікацію та обмін даними, забезпечити моніторинг та відстеження в режимі реального часу, виявити потенційні загрози безпеці, а також забезпечити безпечне зберігання даних та системи контролю доступу. Можливі недоліки та обмеження використання цих технологій, а також їх вплив на загальну ефективність логістичних систем все ще потребують подальшого вивчення.

За даними Infosys, хоча автоматизація та цифрова трансформація в транспортній та логістичній галузі приносять користь, це також означає, що ця галузь є головною мішенню для кіберзлочинців. Коли різні ланки ланцюга поставок швидше підключаються до хмари, ризики кібербезпеки зростають.

За допомогою рішень IOT підприємства у виробництві, роздрібній торгівлі та транспорті можуть відстежувати свої товари в режимі реального часу, щоб переконатися, що вони доставляються до пунктів призначення вчасно та в хорошому стані. Рішення IOT також дозволяють компаніям використовувати дані з минулого, щоб визначити, коли поповнювати запаси та скільки замовляти.

Дослідження під назвою "Кібербезпека та загроза логістиці" показує нам, що логістичні компанії стикаються з проблемою зміни своїх процедур кібербезпеки відповідно до нової реальності, пов'язаної з гіперзв'язком, оскільки вони отримують вигоду від зростаючої цифровізації та підключення до інтернету.

Атаки зловмисного програмного забезпечення та інші порушення безпеки з кожним днем стають все частішими та серйознішими, і очікується, що ця тенденція збережеться до тих пір, поки зловмисники матимуть доступ до нових технологій, таких як штучний інтелект. Логістичні організації особливо вразливі через свої зв'язки з кількома сторонніми постачальниками та використання ними як нових, недостатньо захищених пристроїв Інтернету речей, так і старих, недостатньо обслуговуваних систем управління.

Компанії можуть зменшити ризик кібератак, ретельно проаналізувавши свої процедури та розробивши модель видимості та активного моніторингу всіх своїх систем. Жодна система захисту не може забезпечити повну безпеку від потенційного зловмисника. Але компанії можуть випередити конкурентів і забезпечити свою довгострокову стійкість до кіберзагроз, найнявши фахівців з безпеки для регулярного моніторингу та тестування своїх систем безпеки.

Сучасні системи доставки адаптуються до вимог логістики, яка описується як мережа взаємозв'язків незалежних логістичних систем, що використовують великий обсяг даних для визначення автоматизації, організації та ходу процесів, а також підтримки індустрії. Вона включає цифровізацію, хмарні обчислення та обмін даними. З точки зору окремих підсистем, цифровізація та автоматизація ланцюга поставок складають логістику, що підвищує якість та ефективність виробництва у зв'язку з:

- підвищення ефективності виробництва при одночасній подальшій автоматизації та оптимізації потоку даних (обмін інформацією здійснюється між підприємствами і всіма сторонами на верхньому і нижньому рівнях ланцюжка поставок);
- пропонує внести зміни в роботу складів, де все частіше використовуються інтелектуальні датчики, що дозволяють здійснювати віртуальне планування навантаження і розвантаження на основі спеціалізованих мережевих модулів і передавати дані про завантаженість приміщень;
- "відстеження" (моніторинг) відправлень і транзиту (автоматичне формування повідомлень для клієнтів, що повідомляють їх про вагу вантажу і передбачуваний час прибуття);
- спільне планування логістики в режимі реального часу в області виробництва, дистрибуції та закупівель;
- автоматизація процесів і оцифровка;
- швидкі індивідуальні поставки;
- цифровізація поставок по суші, морю і повітрю;
- широке використання хмарних обчислень для доступу до онлайн-баз даних у веб-середовищі без необхідності покупки (установки) додаткових додатків;
- логістична діяльність є цифровою копією реальності.

Кібербезпека логістики. Проблеми кібербезпеки логістики необхідно розглядати в контексті мегатенденцій і технологій, які змінюють цей сектор. Промислова революція характеризується злиттям передових технологій, включаючи Інтернет речей (IoT), аналітику великих даних, передові обчислення та штучний інтелект (ШІ). Ці технології дозволили автоматизувати і оптимізувати ряд найважливіших логістичних процедур, допомагаючи фірмам підвищити продуктивність і знизити витрати. Логістичний сектор стикається з новими викликами кібербезпеки внаслідок зростаючої залежності від технологій.

Наприклад, Інтернет речей дозволив логістичним організаціям відстежувати свої активи в режимі реального часу, але використання пристроїв IoT також створює нові прогалини в безпеці, якими можуть скористатися хакери. Подібно до того, як передові технології та штучний інтелект сприяли розгортанню все більш інтелектуальних та автономних логістичних систем, ці системи також створюють та обмінюються значними обсягами конфіденційних даних, які необхідно захищати від кіберзагроз.

Технологія 5G також перетворює сектор логістики. Очікується, що впровадження мереж 5G забезпечить швидший і надійніший зв'язок, що дозволить логістичним компаніям оптимізувати свої процеси і підвищити задоволеність клієнтів.

Логістичні компанії повинні бути добре обізнані про мегатенденції та технології, які змінюють галузь, щоб належним чином вирішувати проблеми кібербезпеки. Підприємства можуть розробляти успішні плани захисту своїх операцій та активів від кіберзагроз, дотримуючись найновіших інновацій у галузі кібербезпеки та логістичних технологій.

Надання рішень, адаптованих до конкретних вимог логістичного бізнесу, вимагає співпраці та партнерства між логістичними організаціями, постачальниками технологій та експертами з кібербезпеки. Зрештою, створення безпечної та надійної логістичної екосистеми, яка може процвітати в цифрову епоху, вимагає загального розуміння мегатенденцій та логістичних технологій.

Інтернет речей (IoT). Використання Інтернету речей (IoT) в ланцюгах поставок можна визначити як мережу, яка з'єднує провідні або безпроводові пристрої і характеризується автономною (без участі людини) роботою в області збору даних, обміну ними, обробки даних або взаємодії з навколишнім середовищем. Це стратегія створення комунікаційних мереж та інформаційних систем з високим ступенем розсіювання, яка може бути застосована, серед

іншого, для розробки інтелектуальних систем контролю та вимірювань, аналітичних систем або систем управління практично в будь-якій галузі [3].

Ідея IT-архітектури, яка підтримує багато польових додатків, забезпечуючи взаємодію різних систем, базується на наступних аспектах:

- обладнання-пристрої (або предмети, оснащені такими пристроями), зокрема датчики, виконавчі механізми, а також контролери, смартфони, планшети, ноутбуки або комп'ютери, які можуть передавати і обробляти дані без допомоги людей або з мінімальним втручанням людини;
- зв'язок-мережа (провідних або безпроводових) телекомунікацій, що працює на будь-якому діапазоні і будь-яких стандартах передачі даних, в даному випадку, інтернет;
- програмне забезпечення, включаючи IT-системи для пристроїв Інтернету речей (IoT) та програмне забезпечення для обробки даних, системного адміністрування та забезпечення безпеки;
- інтеграція певних наборів IT-сервісів, що гарантують сумісність програмного забезпечення на всіх архітектурних рівнях.

Поєднання продуктів та послуг Інтернету речей дозволяє краще зрозуміти споживача, навколишнє середовище, продукти та процеси, включаючи логістичні процеси. Це також дозволяє виявляти значущі події та негайно оптимізувати або більш точно персоналізувати відповідні дії. Найбільш широко використовувані логістичні рішення Інтернету речей (IoT) включають:

- інструменти управління запасами, які допомагають менеджерам з логістики планувати розподіл та поповнення запасів. Власники бізнесу зможуть виключити людські помилки, забезпечити безпечне зберігання товарів і заощадити час, швидко знаходячи необхідний товар за допомогою підключених датчиків. Впевненість в тому, що кожен етап ланцюжка поставок проходить успішно, підвищується завдяки можливості відстеження товару від складу до дверей клієнта;
- інструменти прогнозної аналітики, які допомагають менеджерам приймати обґрунтовані рішення щодо ланцюга поставок та управління складом. Вони використовуються для пошуку найшвидших маршрутів доставки, виявлення проблем з обладнанням до того, як вони стануть серйозними, і попередження працівників про необхідність ремонту обладнання. Системи прогнозного аналізу підвищують продуктивність складу при одночасному скороченні витрат на доставку;
- технології управління місцезнаходженням, які дозволяють в режимі реального часу відстежувати місцезнаходження кожного транспортного засобу, статус поставок і передбачувану тривалість процесу. Це також інструмент для пошуку складських інструментів для технічного обслуговування та ремонту, що підвищує ефективність управління складом. До таких інструментів відносяться стелажі, візки, крани, пристрої вентиляції та кондиціонування повітря, протипожежні пристрої і т. д.;
- автоматизовані транспортні засоби стануть основною інновацією в ланцюжку поставок і логістиці. Серед першопроходьців у використанні автономних транспортних засобів і тих, хто зможе отримати максимальну вигоду з цього нововведення, швидше за все, будуть логістичні організації. Транспортні засоби вибирають найбільш зручний маршрут, змінюють температуру в салоні та інші характеристики, щоб забезпечити сприятливі умови для зберігання товарів, а також використовують безліч додаткових додатків, які найкращим чином підходять для кожної доставки;

– автоматизована обробка замовлень і оновлення статусу, які допомагають компаніям наймати меншу кількість співробітників з доставки, тим самим знижуючи загальні витрати на логістику по всьому ланцюжку поставок. При доставці на завершальному етапі використання мережевих роботів може значно скоротити витрати і при цьому значно підвищити задоволеність клієнтів.

Підвищення безпеки логістики за допомогою інтернету речей. Можливість підключення до Інтернету безлічі об'єктів, від невеликих об'єктів до транспортних контейнерів і транспортних засобів, робить Інтернет речей (IoT) все більш значущим для сектора логістики. Завдяки новим можливостям, які відкрило це з'єднання для відстеження та моніторингу логістичної діяльності в режимі реального часу, тепер можливі більша наочність і контроль над ланцюжком поставок.

Можливість відстежувати окремі товари та поставки від початку до кінця – одна з головних переваг логістики в місті. Виявляючи та усуваючи вузькі місця та неефективність ланцюга поставок, логістичні організації оптимізують свою діяльність, знижують витрати та підвищують ефективність. Надаючи точну та своєчасну інформацію про стан вантажу та графіки доставки, логістичні компанії можуть використовувати технологію IOT для покращення обслуговування своїх клієнтів.

Моніторинг стану товарів в дорозі – ще одна перевага Інтернету речей в логістиці. Логістичні компанії можуть відстежувати температуру, вологість та інші умови навколишнього середовища, які можуть вплинути на якість та безпеку товарів, оснащуючи піддони, контейнери та транспортні засоби датчиками. Використовуючи цю інформацію, можна забезпечити належне транспортування предметів за належних обставин, що зменшує ймовірність їх пошкодження.

Відстежуючи переміщення та розташування вантажів та вантажних автомобілів у режимі реального часу, IT-система також дозволяє логістичним організаціям підвищити безпеку. Виявляючи потенційні ризики та вживаючи попереджувальних заходів для їх зменшення, це може сприяти підвищенню безпеки.

Інтернет речей застосовується до логістичного сектору, оскільки він може пов'язувати логістичні організації з інтернетом. Технологія IOT може допомогти логістичним підприємствам працювати ефективніше, економити гроші, забезпечувати краще обслуговування клієнтів та підвищувати надійність ланцюга поставок. Інтернет речей відіграватиме все більш важливу роль у визначенні майбутнього логістичного бізнесу, оскільки він продовжує розробляти та впроваджувати нові технології.

Edge intelligence – це обчислювальні рішення, що використовують унікальні обчислювальні механізми за межами хмари або центру обробки даних і засновані на IOT. Традиційні обчислювальні рішення є централізованими і обробляють дані з багатьох джерел (включаючи об'єкти з підтримкою Інтернету речей) в рамках бізнес-процесів або аналітичних систем, розміщених в хмарі або центрі обробки даних. Інтелектуальні периферійні рішення дозволяють використовувати додатковий комп'ютер на кордоні, а не "переміщати" обчислення туди. Edge intelligence вирішує цю задачу, роблячи об'єкти і середовища "розумними", тобто досить інтелектуальними, щоб брати активну участь в автоматизації бізнес-процесів.

Можливість надавати похідні знання або дозволяти "розумним" пристроям приймати рішення – це лише два приклади того, якими "розумними" можуть бути пристрої. Далі про користь Інтернету речей з точки зору оснащення шин вантажних автомобілів інтелектуальними датчиками, які можуть передавати дані в режимі реального часу:

– Ви можете періодично отримувати дані про тиск у шинах, вказавши інтернет-адресу датчика тиску в шинах. Такі показання підвищують безпеку, економію палива і надають інформацію про термін служби шин, режимах руху і т.д. централізованим аналітичним системам.

- Тиск у шинах можна вимірювати періодично (наприклад, кожні кілька секунд), щоб отримати середнє значення та стандартне відхилення, вказавши інтернет-адресу датчика тиску в шинах та виконавши локальну обробку. Середнє значення дає більш якісний результат, ніж періодичні знімки, і в міру зносу і стоншування шини стандартне відхилення показань тиску буде збільшуватися. Це відкриває нові аналітичні можливості, такі як прогнозування терміну служби шин для підвищення безпеки та більш ефективного планування заміни шин.
- Здатність шини безперервно регулювати власний тиск для подальшого підвищення безпеки, паливної економічності та терміну служби шин може бути забезпечена за рахунок підвищення інтелектуальності датчика тиску в шинах.

Застосування технології RFID (радіочастотної ідентифікації) для відстеження та моніторингу товарів у міру їх переміщення по ланцюжку поставок є одним з конкретних прикладів того, як Інтернет речей сприяє підвищенню безпеки ланцюжка поставок.

Теги RFID можуть бути нанесені на конкретні товари або упаковку, а зчитувачі RFID можуть читати ці мітки в різних місцях по всьому ланцюжку поставок, включаючи склади, розподільчі центри та роздрібні торговці. Це дозволяє відстежувати переміщення товарів у режимі реального часу, що може допомогти запобігти крадіжці, втраті або пошкодженню, а також виявити будь-які потенційні вузькі місця або затримки в ланцюжку поставок.

Наприклад, організація, яка виробляє та продає гаджети високого класу, може відстежувати переміщення своїх товарів від виробництва до продавця за допомогою технології RFID. Компанія може використовувати інформацію з RFID-міток для виявлення потенційної проблеми та вжиття необхідних заходів у разі втрати або затримки відвантаження товарів. Покращуючи планування та прогнозування, це може зменшити ризик крадіжки або підробки та підвищити ефективність ланцюга поставок.

Walmart, один з найбільших роздрібних торговців у світі, є прикладом бізнесу, який використовує технологію RFID. За допомогою технології RFID вони можуть відстежувати переміщення товарів у режимі реального часу, що підвищує ефективність відстеження запасів та поповнення запасів. RFID-мітки можна використовувати для відстеження того, коли речі переміщуються з певних місць або коли вони виносяться з магазину без покупки, що може допомогти зменшити усадку і крадіжки. Walmart закликав своїх постачальників використовувати технологію RFID на додаток до впровадження її у власних магазинах, щоб підвищити ефективність ланцюга поставок.

Безпроводовий зв'язок п'ятого покоління (5G). П'яте покоління мобільних технологій, або 5G, є визначальним фактором функціонування ланцюгів поставок. 5G – це стандарт передачі даних в стільникових мережах з поліпшеними критеріями продуктивності. Нижче наведено основні переваги технології 5G для управління ланцюгами поставок:

- Потенціал для широкого впровадження таких технологій, як Інтернет речей, хмарні обчислення, дистанційно керовані транспортні засоби, рішення для відстеження активів і визначення місця розташування, електрифікація інструментів, блокчейн, штучний інтелект, автоматизація процесів, автономні транспортні засоби та інтелектуальний транспорт, роботи і дрони, 3D-друк і доповнена реальність в майбутньому. моніторинг та вдосконалення логістичних процесів.
- Підвищена обізнаність про потоки поставок. Концепція видимості ланцюга поставок виходить далеко за рамки простого відстеження поставок. Найважливішою перевагою технології 5G є можливість швидкого та точного розуміння дій у ланцюзі поставок, включаючи інформацію про закупівлі, запаси, Виробництво та відвантаження в рамках всього операційного середовища, завдяки активному управлінню подіями в режимі реального часу. Щоб реагувати на збої в ланцюжку поставок, логістичні організації зможуть відстежувати потік операцій і послуг і керувати ним, приймаючи рішення в режимі реального часу.

– Нові можливості для управління автопарком. Датчики, що відстежують роботу кожного комерційного транспортного засобу, допомагають підтримувати готовність автопарку і запобігати збої. Автопарки комерційного транспорту стануть частиною транспортної мережі, яка завжди доступна, оскільки мережі 5G зможуть функціонувати за межами міських районів. Весь ланцюжок поставок виграє від контролю використання транспортних засобів у режимі реального часу, що стане можливим завдяки системам управління транспортом (TMS).

Використання Безпроводового зв'язку п'ятого покоління (5G) для підвищення безпеки логістики. Логістичний Сектор має важливе значення для світової економіки, оскільки полегшує доставку товарів від виробників до споживачів. Однак через сильну залежність від технологій цей сектор особливо схильний до кібератак. Кібератаки можуть негативно позначитися на фінансах і репутації компанії, а також на клієнтах. Очікується, що безпроводові технології п'ятого покоління, або 5G, змінять сектор логістики, забезпечуючи більш швидку і надійну зв'язок.

Покращене шифрування даних, що передаються по мережі, є одним з головних переваг 5G. завдяки 5G дані можуть бути зашифровані більш ретельно, ніж при використанні бнзпроводових технологій попередніх поколінь, що ускладнює їх перехоплення і розшифровку хакерами. Це може допомогти захистити конфіденційні дані від кібератак, включаючи інформацію про клієнтів, фінансову інформацію та специфікації продукту.

Крім того, 5G покращує видимість мережі в секторі логістики, полегшуючи виявлення загроз безпеці. За допомогою 5G компанії можуть відстежувати рух товарів по своїх ланцюгах поставок у режимі реального часу за допомогою датчиків та іншого підключеного обладнання. Це може допомогти компаніям визначити можливі проблеми до їх виникнення та швидко впровадити рішення.

Big data. Великі дані, найважливіший компонент логістики – це еволюційний спосіб збору даних із законних джерел, їх аналізу (за допомогою бізнес-аналітики) та застосування результатів для досягнення цілей, встановлених відповідно до вимог ланцюга поставок. Великі дані дають компаніям шанс отримати конкурентну перевагу на сучасному цифровому ринку завдяки поєднанню обсягу, різноманітності, швидкості та надійності.

Використання великих даних передбачає ретельне об'єднання багатьох видів даних, включаючи внутрішні та зовнішні, архівні, поточні та майбутні дані, з метою отримання додаткової інформації про стан верхнього та нижнього сегментів ланцюга поставок. Концепція великих даних визначається як:

– накопичення, обробка та аналіз великої кількості даних для вивчення нових речей;
– великі обсяги, висока швидкість і/або велика різноманітність інформаційних ресурсів, які вимагають творчих і економічно ефективних методів обробки інформації для поліпшення розуміння, прийняття рішень і автоматизації процесів;
– набори даних, які повинні оброблятися з використанням передових технологій, інструментів та інформаційних прийомів, які одночасно характеризуються великим обсягом, різноманітністю, потоковою передачею в режимі реального часу, мінливістю і складністю.

Великі дані підвищують ефективність ланцюга поставок, серед іншого, за рахунок:

– підвищення рівня інтеграції ланцюжка поставок і координації діяльності окремих її ланок на трьох рівнях: прийняття основоположних принципів управління ланцюжком поставок, співпраця і координація діяльності, цілей і заходів щодо їх реалізації, а також використання IT-систем для підвищення якості і швидкості обміну інформацією;

- використовуючи інструменти для моніторингу реєструються в електронному вигляді проявів рішень і дій споживачів, ланцюжок поставок підбирається (конфігурується) відповідно до їх вимог відповідно до їх потреб (персоналізація);
- оперативне виявлення та усунення недоліків (відходів) в переміщенні матеріалів і пов'язаної з ними інформації по ланцюжку поставок;
- зниження цінності для цільових клієнтів або збільшення витрат на логістику в результаті ефективного видалення непотрібних запасів або погіршення логістичних процесів;
- ефективний і швидкий пошук нових середовищ, технологій або методів для реалізації конкретних логістичних операцій, пов'язаних з потоками, процесами, учасниками і зв'язками.

Підвищення безпеки логістичних систем за допомогою аналітики великих даних. Аналізуючи дані з різних джерел, таких як пристрої IoT, GPS-трекери та камери безпеки, аналітика великих даних може надати корисну інформацію про безпеку логістичних систем. Наприклад, в даних GPS-навігатора вантажного автомобіля можна виявити відхилення від заданих маршрутів, що може вказувати на крадіжку або витік товару.

Аналіз великих даних також може бути використаний для виявлення та запобігання подій, пов'язаних з безпекою. Аналітичні технології, наприклад, можуть бути використані для виявлення схем шахрайської діяльності в логістичних мережах, шляхом вивчення минулих даних з метою виявлення закономірностей і тенденцій, які можуть вказувати на можливі загрози безпеці.

Аналіз великих обсягів даних також може допомогти логістичним організаціям більш ефективно реагувати на інциденти безпеки, коли вони дійсно виникають. При виникненні проблем з безпекою аналіз даних в режимі реального часу дозволяє негайно відправляти повідомлення співробітникам служби безпеки, що дозволяє їм оперативно реагувати. Наприклад, співробітники служби безпеки можуть бути попереджені про підозрілу активність, використовуючи аналіз даних камер спостереження в режимі реального часу, щоб виявити її.

Хмарні обчислення. Хмарні обчислення стосуються обчислювальних послуг (підтримки), що надаються іншими компаніями, які доступні за запитом у будь-який час і регулюються за потребою. Модель обробки даних, відома як "хмарні обчислення", заснована на використанні обчислювальних послуг, пропонованих постачальником послуг у вигляді масштабованих серверів, баз даних, мереж з найкращою пропускною здатністю і безпекою, програмного забезпечення, аналітики і т.д. хмарні провайдери – це компанії, що надають ці послуги. Згідно з раніше узгодженим контрактом, клієнт платить тільки за право користування певною послугою, наприклад, за можливість використання IT-інфраструктури, і як наслідок, не несе ніяких інвестиційних витрат. Для класифікації хмарних обчислень можна використовувати кілька критеріїв [5]. Перша класифікація стосується методів, що використовуються для планування, створення та подальшого управління хмарами. На основі цих критеріїв можна виділити наступні типи хмар:

- публічні Хмари, призначені для великих одержувачів і мають ту перевагу, що доступні кожному, хто має доступ до інтернету; безкоштовні послуги електронної пошти є прикладом звичайної публічної Хмари;
- приватні хмари, або спеціалізовані IT-ресурси (визначаються як новітні IT-технології), являють собою готові рішення, розроблені для однієї економічної одиниці;
- гібридна хмара, що включає компоненти обох моделей;
- хмара спільноти, в якій ресурси надаються групі організацій із спільними цілями, які виконують певні завдання (хмара може належати всім організаціям-учасникам, лише одній з них або навіть третій стороні);

- виділена хмара, де постачальник послуг надає Клієнту ексклюзивний доступ до певної області Хмари;
- віртуальна приватна хмара, де набір ресурсів надається відповідно до потреб користувача як частина сервісу "публічної хмари", при цьому враховується певний рівень ізоляції цих ресурсів.

Хмарні обчислення сьогодні підтримують розширені можливості зростання, такі як обчислення в реальному часі, прогнозування, штучний інтелект, безперервне навчання та машинне самонавчання, а також зберігання даних та масштабованість. Хмарні технології – це найважливіший компонент, який дозволяє компаніям у всіх секторах впроваджувати нові технології, включаючи штучний інтелект.

Підвищення безпеки логістичних систем за допомогою хмарних обчислень. Користувачі можуть отримувати доступ до обчислювальних ресурсів, включаючи сервери, сховища та програми, в інтернеті завдяки хмарним обчислювальним системам. Хмарні обчислення мають ряд переваг для забезпечення безпеки логістичних систем, включаючи:

- Масштабованість: обчислювальна потужність та масштабована інфраструктура, пропоновані хмарними обчисленнями, дозволяють обробляти великі обсяги даних та трафіку. Для логістичних систем, попит на які може істотно змінюватися, така масштабованість має вирішальне значення.
- Гнучкість: Хмарні обчислення забезпечують адаптивні послуги та інфраструктуру, які можуть бути адаптовані до унікальних вимог логістичних систем. Завдяки своїй адаптивності логістичні компанії можуть швидко реагувати на зміни стандартів безпеки та нові загрози.
- Безпека: Хмарні обчислення забезпечують передові можливості безпеки, включаючи шифрування, брандмауери та системи виявлення вторгнень, які можуть захистити логістичні системи від різних загроз безпеці.
- Економічна ефективність: оскільки підприємства просто платять за ресурси та послуги, якими вони користуються, без необхідності робити значні початкові інвестиції, Хмарні обчислення пропонують економічне рішення для забезпечення безпеки логістичних систем.

Висновки

З появою таких технологій, як Інтернет речей (IoT), 5G, великі дані та хмарні обчислення, логістичний сектор зазнав величезних цифрових змін. Ці інновації можуть підвищити продуктивність, зменшити витрати та покращити загальний досвід клієнтів. Однак для захисту логістичних систем вони також створюють нові проблеми безпеки, які необхідно вирішити. Покращена видимість і контроль над логістичними операціями стали можливі завдяки IoT і 5G, які надають нові можливості для моніторингу в режимі реального часу і обміну даними між обладнанням. Логістичні фірми можуть покращити свою роботу, використовуючи дані з пристроїв Інтернету речей про місцезнаходження, статус та стан товарів.

Покращена видимість і контроль над логістичними операціями стають можливими завдяки IoT і 5G, які надають раніше нечувані можливості для моніторингу та зв'язку між обладнанням в режимі реального часу. Логістичні компанії можуть приймати обґрунтовані рішення та вдосконалювати операції, використовуючи дані пристроїв Інтернету речей про місцезнаходження, статус та стан товарів. Використання мереж 5G також може полегшити впровадження складних логістичних систем, які потребують більшої пропускної здатності та низької затримки.

Аналітика великих даних може надати цінну інформацію про логістичні процеси, але для цього потрібна масштабована та безпечна інфраструктура для зберігання та обробки. Хмарні обчислення пропонують безпечну та гнучку платформу для обробки великих обсягів даних,

що дозволяє аналізувати дані в режимі реального часу та підвищує безпеку логістичних систем. Використовуючи хмару, логістичні компанії можуть отримувати доступ до даних з різних джерел, оцінювати їх у режимі реального часу та використовувати отримані знання для прийняття рішень.

Однак використання цих технологій також створює нові проблеми безпеки, які необхідно вирішити. Ланцюги поставок можуть бути порушені, гроші можуть бути втрачені, а конфіденційні дані можуть бути скомпрометовані кіберзагрозами, такими як злом, порушення даних та атаки програм-вимагачів. Як результат, важливо забезпечити ефективні заходи кібербезпеки для захисту логістичних систем від потенційних небезпек в Інтернеті.

Таким чином, існує великий потенціал для підвищення безпеки логістичних систем та підвищення ефективності та надійності логістичних операцій шляхом інтеграції таких технологій, як IoT, 5G, big data та хмарні обчислення. Для захисту від потенційних кіберзагроз вкрай важливо враховувати вплив цих технологій на безпеку та впроваджувати практичні запобіжні заходи. Логістичні організації можуть скористатися перевагами цих технологій, одночасно забезпечуючи безпеку своєї діяльності.

Список використаної літератури:

1. Дзюндзюк Б. В. Особливості використання великих даних, штучного інтелекту та технології блокчейн у публічному управлінні. Derzhavne upravlinnya udoskonalennya ta rozvytok. 2023. № 5. URL: https://doi.org/10.32702/2307-2156.2023.5.11
2. Quotes C. Cybersecurity Engineer I'm Not Arguing I'm Just Explaining Why I'm Right. Independently Published, 2020.
3. Дранчук С. М., Зарицька О. І., Кочетков О. В. Моніторинг процесів та штучний інтелект. Од. нац. мор. ун-т, 2023. URL: https://doi.org/10.47049/onmu-2023-np8
4. Sharrock, J., (2018). Cybersecurity and the threat to logistics. Cybercitadel. URL: https://www.cybercitadel.com/docs/Cyber-Security-and-the-Threat-to-Logistics-A.pdf
5. Хмарні технології в освіті. URL: https://lib.iitta.gov.ua/840/1/cloud.pdf.

Автори статті

Шрам Максим - аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Руденко Наталія - кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Authors of the article

Shram Maksym - postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

Rudenko Natalia - Candidate of Science (technic), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.