УДК 004.056

ОРГАНІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ЛОГІСТИЧНИХ ЦЕНТРАХ

Євгеній Василенко
Національний авіаційній університет, Київ

Науковий керівник – Суворова Ірина Миколаївна

Ключові слова: кібербезпека, міжнародний стандарт, мікросегментація.

В сучасному логістичному середовищі забезпечення кібербезпеки відіграє ключову роль у підтримці конкурентоспроможності та відповіді на потреби клієнтів. Клієнти більше не обмежуються лише вимогами щодо якості послуг, а також ставлять важливість на захист їхніх даних та конфіденційності під час логістичних операцій.

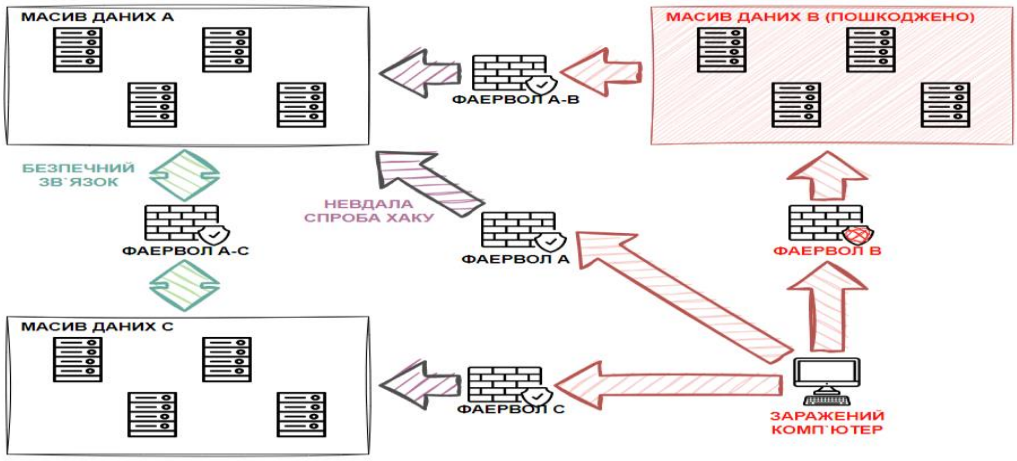
Для наукового обґрунтування важливості належної організації системи кібербезпеки в логістичних центрах було використано теоретичний метод дослідження.

Логістичні центри виконують важливу функцію в ланцюгу постачання, забезпечуючи перехід товарів від виробників до кінцевих споживачів. Безпека функції логістичного постачання на даному перехідному етапі не була б можлива без використання систем кібербезпеки. Керування кібербезпекою забезпечується завдяки міжнародному стандарту ISO 27001 (Інформаційна безпека, кібербезпека та захист конфіденційності). Це включає в себе оцінку ризиків, управління доступом, фізичну та цифрову безпеку, управління інцидентами та свідомість про безпеку серед персоналу. Аналогом даного стандарту в Україні є ISO/IEC 27001:2023, який встановлює принципи та вимоги для створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ), яка, в свою чергу, допомагає захищати важливі дані, з якими працюють логістичні компанії, від несанкціонованого доступу та забезпечує безперебійну роботу логістичних центрів у динамічному світі цифрових технологій.

Метод Zero Trust (нульового довір’я) частково вирішує цю проблему. Він відкидає традиційну модель захисту периметра та передбачає, що жоден користувач або пристрій не може бути повністю довіреним всередині мережі [1]. Замість цього, він базується на ідеї перевірки та аутентифікації кожного запиту на доступ до ресурсів, незалежно від того, з якого пристрою чи мережі він надходить. Це означає, що доступ до ресурсів надається тільки після перевірки автентичності користувача, стану пристрою, безпекових політик та інших контекстуальних факторів. Такий підхід дозволяє зменшити ризики порушення безпеки та захистити ресурси від внутрішніх та зовнішніх загроз. Використання програмного забезпечення та API від третіх сторін може бути надзвичайно зручним, проте одночасно воно створює додаткові шляхи для потенційних кібератак. За даними Всесвітнього економічного форуму, зростає загальна частка непрямих кібератак (тобто тих, що відбуваються через треті сторони), з 44% до 61% за останні

роки. Аналітики Gartner попереджають, що використання вразливостей API стає одним з головних векторів кібератак на ланцюжки постачання [2]. Аби запобігти цьому, співзасновник Menlo Security Мартін МакГрю винаходить мікросегментацію - стратегію захисту мережі, яка передбачає розділення мережевого трафіку на дрібні, відокремлені сегменти для забезпечення більшої безпеки і контролю.

Суть мікросегментації полягає в тому, щоб створити віртуальні сегменти в мережі, які відокремлюються один від одного за допомогою внутрішніх мережевих бар'єрів. Кожен сегмент може мати власні правила безпеки і політики доступу, які дозволяють контролювати трафік між різними частинами мережі. Мікросегментація дозволяє зменшити поверхню атаки, оскільки навіть якщо один сегмент мережі буде скомпрометований, це не дозволить зловмисникові безпосередньо отримати доступ до інших частин мережі. Крім того, цей підхід полегшує впровадження Zero Trust, оскільки правила безпеки можуть бути налаштовані більш детально для кожного окремого сегмента мережі[3].



Принцип роботи мікросегментації.

Висновок

Кібербезпека стала невід'ємною частиною логістичного середовища, адже від неї залежить не лише конкурентоспроможність, але й довіра клієнтів. Логістичні центри, як ключові ланки ланцюгів постачання, потребують комплексного підходу до кібербезпеки, і можуть досягти бажаного використовуючи новітні методи боротьби з кібератаками.

Список використаних джерел:

1. Edo, O., Emakhu, J. (2022). Zero Trust Architecture: Trend and Impact on Information Security. International Journal of Emerging Technology and Advanced Engineering, 144 (45-50).

2. D'Hoinne, J., Gill, S., Pillai, S. (2021). APIs Demand Improved Security and Management. Gartner`s research, 14 (17-21).

3. McGrue, M., Misaki, N., Satoru, G. (2021). Microsegmentation: the next frontier of cyber security, TechCrunch journal 2, 15.