УДК 65.012.8.004.9

Ганна Іващенко
кандидат економічних наук, доцент кафедри міжнародних економічних відносин та безпеки бізнесу Харківського національного економічного університету імені Семена Кузнеця, Україна, a502330109@gmail.com
Салюк Олександр
здобувач другого магістерського рівня вищої освіти 2М курсу освітньої програми 292 «Міжнародні економічні відносини» Харківського національного економічного університету імені Семена Кузнеця, Україна

ФОРМУВАННЯ БЕЗПЕКООРІЄНТОВАНОГО РОЗВИТКУ ІМПОРТНОЇ ДІЯЛЬНОСТІ ІТ-КОМПАНІЇ
FORMATION OF SECURITY-ORIENTED DEVELOPMENT OF IT COMPANY'S IMPORT ACTIVITIES

Анотація. Визначено основні аспекти формування безпекоорієнтованого розвитку імпортної діяльності ІТ-компанії. Розроблено основні рекомендації щодо вдосконалення безпекоорієнтованого розвитку імпортної діяльності ІТ-компанії.

Annotation. The main aspects of the formation of the security-oriented development of the import activity of the IT company have been determined. The main recommendations for improving the security-oriented development of the import activity of the IT company have been developed.

Ключові слова: безпекоорієнтований розвиток; імпортна діяльність; високотехнологічна компанія; міжнародний бізнес; ризики; загрози.

Keywords: security-oriented development; import activity; high-tech company; international business; risks; threats

У сучасному глобалізованому світі імпортна діяльність ІТ-компаній стає дедалі важливішою для забезпечення їхнього зростання та конкурентоспроможності. Однак, зростання обсягів імпорту приносить не лише нові можливості, а й значні ризики, пов'язані з безпекою даних, кібератаками та дотриманням міжнародних стандартів. Формування безпекоорієнтованого розвитку в цій сфері є ключовим завданням для забезпечення стабільності бізнес-процесів і захисту інформаційних активів.

Безпекоорієнтований підхід до імпортної діяльності передбачає інтеграцію принципів безпеки на всіх етапах – від вибору постачальників до обробки та зберігання даних. Це дозволяє не лише зменшити ризики, але й підвищити довіру клієнтів і партнерів, а також покращити імідж компанії на міжнародному рівні.

У цьому контексті важливо врахувати сучасні виклики, з якими стикаються ІТ-компанії, такі як швидкий розвиток технологій, зміни в законодавстві та зростаюча конкуренція. Розробка та впровадження ефективних стратегій безпеки стане основою для успішної імпортної діяльності, що відповідає вимогам часу та забезпечує стабільний розвиток бізнесу.

У даному дослідженні буде проаналізовано ключові аспекти безпекоорієнтованого розвитку імпортної діяльності ІТ-компаній, а також запропоновано рекомендації для їх впровадження.

Метою дослідження є розроблення теоретико-методичних основ формування безпекоорієнтованого розвитку імпортної діяльності ІТ-компанії.

ІТ-індустрія в Україні є відносно молодою галуззю, але вона швидко набула значення для формування іміджу країни. В останні роки українські ІТ-компанії, зокрема аутсорсингові, зайняли провідні позиції у численних впливових міжнародних рейтингах.

Безпекоорієнтований розвиток – це підхід, що враховує безпеку на всіх етапах планування, реалізації та управління проектами чи бізнес-процесами. Основна мета цього підходу – забезпечення стабільності, зменшення ризиків та захисту активів, ресурсів і людей.

Ключові аспекти безпекоорієнтованого розвитку: оцінка ризиків; інтеграція безпеки; сталий розвиток; технологічні рішення; перенавчання; регуляторні вимоги.

Систематичний аналіз потенційних загроз і вразливостей, що можуть вплинути на організацію. Включення безпекових аспектів у всі процеси – від проєктування до реалізації та моніторингу.

Підходи, які забезпечують баланс між економічними, соціальними та екологічними факторами без шкоди для безпеки. Використання сучасних технологій для моніторингу, управління ризиками та забезпечення безпеки даних. Підвищення рівня обізнаності співробітників та зацікавлених сторін про важливість безпеки. Дотримання всіх необхідних норм і стандартів, які стосуються безпеки.

Безпекоорієнтований розвиток є важливим елементом сучасного управління, що допомагає організаціям адаптуватися до змінюваних умов і знижувати ризики, забезпечуючи при цьому стабільність і довіру серед усіх учасників процесу [5].

Формування безпекоорієнтованого розвитку імпортної діяльності IT-компанії є важливим аспектом, який дозволяє зменшити ризики та забезпечити стабільність бізнес-процесів. Основні аспекти, які можуть бути враховані в при формуванні безпекоорієнтованого розвитку імпортної діяльності IT-компанії: аналіз ризиків; оцінка загроз; політика безпеки; технологічні рішення; захист даних; вибір бізнес-партнерів.

Ідентифікація потенційних загроз, які можуть виникнути під час імпортних операцій, таких як кібератаки, шахрайство та нестабільність ринку.

Визначення вразливостей внутрішніх систем і процесів, які можуть бути експлуатовані зловмисниками може активно впливати на формування безпекоорієнтованого розвитку IT-компанії. Встановлення чітких політик і процедур для управління імпортом, включаючи обробку даних, контроль доступу та інші аспекти безпеки.

Регулярні навчання з безпеки для працівників є важливим аспектом для того, щоб вони були ознайомлені з ризиками і знали, як їх уникати [3].

Використання сучасних технологій для захисту інформації, таких як шифрування, брандмауери та системи виявлення вторгнень. Впровадження систем моніторингу для виявлення аномалій і проведення регулярних аудитів безпеки системи.

Оцінка постачальників виконується на основі проведення оцінки надійності постачальників і партнерів, з якими планується співпраця, включаючи їхню політику безпеки. Контракти важливо виконувати на базі включення безпекових умов у контракти з постачальниками, що визначають їхні зобов’язання щодо захисту даних та інформації.

Відповідність законам є важливим аспектом для забезпечення дотримання всіх регуляторних вимог, що стосуються імпорту та безпеки даних, включаючи GDPR, CCPA та інші [4].

Довгострокове планування виконується на базі визначення стратегій розвитку імпортної діяльності, які включають елементи безпеки на всіх етапах – від постачання до доставки.

Формування безпекоорієнтованого підходу до імпортної діяльності IT-компанії допомагає не лише знизити ризики, а й підвищити довіру клієнтів і партнерів. Це може стати важливою конкурентною перевагою на ринку.

Брандмауери – це системи безпеки, які контролюють вхідний та вихідний трафік мережі на основі визначених правил безпеки. Вони служать захистом комп’ютерних мереж від несанкціонованого доступу, атак та інших загроз.

Основні функції брандмауерів: контроль трафіку; фільтрація; захист від кібератак; VPN-підключення.

Контроль трафіку виконується таким чином, що брандмауери перевіряють дані, які проходять через мережу, та приймають рішення про їхню пропуску або блокування. Фільтрація проводиться так, що брандмауери можуть блокувати або дозволяти трафік на основі IP-адрес, портів, протоколів та інших параметрів.

Захист від кібератак виконується таким чином, що брандмауери допомагають захищати мережі від зовнішніх загроз, таких як DDoS-атаки та зловмисні програми.

Моніторинг проводиться таким чином, що ведуться журнали активності, що дозволяє відстежувати підозрілі дії та забезпечувати аудит безпеки.

VPN-підключення здійснюються таким чином, що деякі брандмауери підтримують віртуальні приватні мережі (VPN), що забезпечує безпечний доступ до мережі з віддалених точок [7].

Брандмауери можуть бути апаратними (окремі пристрої) або програмними (встановлюються на комп'ютерах або серверах) і є важливим елементом в системах кібербезпеки.

GDPR (General Data Protection Regulation) і CCPA (California Consumer Privacy Act) – це два важливих законодавчі акти, що регулюють захист даних та приватність споживачів.

GDPR встановлює суворі штрафи за порушення – до 4% річного глобального доходу компанії. CCPA вводить штрафи за недотримання правил, зокрема у разі крадіжки даних..

Формування безпекоорієнтованого розвитку імпортної діяльності ІТ-компанії потребує комплексного підходу, що включає оцінку ризиків, розробку відповідних політик та процедур, а також впровадження сучасних технологічних рішень. Основними рекомендаціями щодо вдосконалення цього процесу є такі: оцінка ризиків та аналіз загроз; розробка політики безпеки імпортної діяльності; захист даних; моніторинг безпеки; вдосконалення процесів управління ІТ-компанією; забезпечення інформаційної прозорості; удосконалення зовнішньоекономічного співробітництва. В подальших дослідженнях доцільно розвивати кожний з розроблених напрямів удосконалення.

Література

1. Балан, О.С., 2018. Сценарне управління інформаційною діяльністю підприємства. Економіка: реалії часу, 4(38), с.31-35.

Бойко В. С. Тенденції розвитку ІТ-ринку в Україні. Вісник економічних наук, 2018. № 6. С. 64-70.

3. Вінник, О. М., 2018. Правове забезпечення цифрової економіки та електронного бізнесу: монографія. Київ: НДІ приватного права і підприємництва ім. акад. Ф. Г. Бурчака.

4. Гафіяк, А.М., 2018. ІТ-технології та бізнес-аналітика, Економіка та суспільство, 15, с.933-937.

5. Карчева, Г. Т., Огородня, Д. В., & Опенько, В. А. (2017). Цифрова економіка та її вплив на розвиток національної та міжнародної економіки. Фінансовий простір, (3), 13-23.

6. Комса, К., Гребеник, К., 2017. Світовий ринок ІТ: місце України на ньому. [Електронний ресурс]. – Режим доступу: https://mind.ua/publications/20178608-svitovij-rinok-it-misce-ukrayini-na-nomu

7. Соловей П. І. Інноваційний розвиток ІТ-галузі України. Інноваційна діяльність та інвестиції, 2021. № 2. С. 18-26.