https://orcid.org/0000-0002-5080-1856
https://orcid.org/0000-0003-3370-4584

УДК 004.056.5

Ю.М. ЛИСЕЦЬКИЙ[*], Д.Й. КАЛБАЗОВ[**]

ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

[*]ДП «ЕС ЕНД ТІ УКРАЇНА», м. Київ, Україна
[**]ТОВ «Інформаційні спеціалізовані системи», м. Київ, Україна

Анотація. *У статті проаналізовано підходи до забезпечення інформаційної безпеки, що склалися на сьогоднішній день серед підприємств вітчизняного ринку: ситуаційний, інтеграційний та інтеграційно-інноваційний. Визначено їх відмінності: ситуаційний – це точкове впровадження систем інформаційної безпеки, децентралізація управління, відсутність єдиного підходу до проєктування системи захисту, інертність впровадження систем; інтеграційний – наявність служб планування і забезпечення інформаційної безпеки, формування єдиних вимог для інформаційної безпеки, аналіз критичності інформаційних активів, управління ризиками та загрозами, проєктування інформаційної безпеки від бізнес-процесів підприємства; інтеграційно-інноваційний – наявність операційних центрів безпеки, центрів оперативного реагування, централізованих систем моніторингу інформаційної безпеки, планування безперервності бізнесу та створення планів аварійного відновлення, формування відмовостійких систем захисту. Наведено існуючі проблеми вибору методів і технологій захисту інформації. Розглянуто способи та засоби ефективного забезпечення інформаційної безпеки підприємства: міжмережеві екрани нового покоління, SIEM-системи, DLP-системи, а також брокер безпеки хмарного доступу – CASB. Його використання для забезпечення інформаційної безпеки у хмари дозволяє вирішувати такі завдання: контроль доступу; захист даних; виявлення та реагування на загрози; відповідність регуляторним вимогам; моніторинг та аудит; управління політиками безпеки. Проаналізувавши підходи до забезпечення інформаційної безпеки вітчизняних підприємств, можна зробити висновок, що воно має ґрунтуватися на комплексному підході та ефективній інтеграції всіх елементів IT-інфраструктури на різних рівнях їх взаємодії.*

Ключові слова: *інформаційна безпека, кібербезпека, підходи, методи, технології, системи, захист інформації, моніторинг, хмари, IT-інфраструктура, підприємство.*

Abstract. *The article analyzes situational, integration, and integration and innovation approaches that have emerged among domestic enterprises in today's market to ensure information security. The following differences between them have been identified: the situational approach involves the point implementation of information security systems, decentralized management, the lack of a unified approach to system design, and inertia in system implementation; the integration approach involves the presence of planning and information security provisioning services, the formulation of unified requirements for information security, analysis of the criticality of information assets, risk and threat management, and the design of information security from business processes of the enterprise; the integration and innovation approach includes the presence of security operation centers, operational response centers, centralized information security monitoring systems, the creation of Business Continuity Plans and Disaster Recovery Plans, and the formation of fault-tolerant protection systems. Some existing problems in choosing methods and information protection technologies are presented in the paper. The ways and means for ensuring effective information security in an enterprise are discussed. These are next-generation network firewalls, SIEM systems, DLP systems, as well as a cloud access security broker – CASB. Using CASB to ensure information security in the cloud allows for addressing the following tasks: access control; data protection; detection and response to threats; compliance with regulatory requirements; monitoring and auditing; and security policy management. Analyzing the approaches to ensuring information security in domestic*

enterprises, we can conclude that it should be based on a comprehensive approach and effective integration of all elements of IT infrastructure at different levels of their interaction.
Keywords: *information security, cybersecurity, approaches, methods, technologies, systems, information protection, monitoring, clouds, IT infrastructure, enterprise.*

DOI: 10.34121/1028-9763-2023-4-26-32

1. Вступ

Незважаючи на зростання рівня кіберзагроз і актуальність підвищення рівня забезпечення інформаційної безпеки (ІБ) для українських підприємств, цій проблемі приділяється недостатньо уваги. Одна з основних причин такої ситуації – відсутність на вітчизняному ринку компаній, які змогли б оцінити і гарантувати зниження ризику кіберзагроз після впровадження технологічного рішення, що формує систему ІБ підприємства. Тому найбільш простим і зрозумілим рішенням для підприємств є придбання антивірусного ПЗ і міжмережевих екранів. Саме з цієї причини вони є найпоширенішими інструментами у сфері ІБ.

З огляду на те, що ризики від недостатнього рівня забезпечення ІБ не є очевидними, а впровадження систем ІБ є досить витратним, підприємства не можуть коректно оцінити співвідношення вартості потенційних втрат до вартості впровадження систем ІБ. У сукупності з фінансовими труднощами вітчизняних підприємств, а також відсутністю чіткого розуміння ризиків для ІБ і методів їхнього зниження, все це призводить до низького рівня розвитку ІБ загалом по країні.

2. Підходи до забезпечення ІБ підприємства

На сьогоднішній день серед підприємств вітчизняного ринку можна виділити такі підходи до забезпечення ІБ: ситуаційний, інтеграційний та інтеграційно-інноваційний.

Ситуаційний підхід характерний для підприємств, у яких збереження інформації не впливає безпосередньо на ведення їхнього бізнесу. Відмінними рисами ситуаційного підходу є точкове впровадження систем безпеки і відсутність централізації управління ІБ. Наприклад, під час розгортання нової CRM-системи (Customer Relationship Management) фахівці із впровадження самі визначають механізми захисту нової системи. IT-фахівці на свій розсуд обирають методи захисту, наприклад, PAM (Privileged Access Management), DLP (Data Loss Prevention), 2FA (Dual Factor Authentication), а після впровадження приймають увесь комплекс в експлуатацію. Таким чином, фахівці з баз даних (БД) відповідають за безпеку БД, фахівці з систем зберігання даних (СЗД) відповідають за захист СЗД, фахівці із програмного забезпечення (ПЗ) – за безпеку свого ПЗ. У таких умовах кожен структурний підрозділ підприємства формує свої правила безпеки, власну політику надання доступу співробітникам, роботи з паролями, відстеження параметрів роботи обладнання, регулярного резервного копіювання тощо. При цьому завдання з регулярного сканування IT-інфраструктури, відстеження актуальності версій використовуваного ПЗ, контролю вірусної активності на підприємстві, як правило, залишаються без належної уваги фахівців або віддаються «на відкуп» локальним адміністраторам.

Отже, ситуаційний підхід вирізняється інертністю і незлагодженістю систем захисту та забезпечення ІБ-підприємства, відсутністю системного планування розвитку IT-інфраструктури, що негативно впливає на планування розвитку систем ІБ на підприємстві загалом. Тому ситуаційний підхід може бути застосований тільки для малих підприємств (100 - 200 співробітників) з єдиною IT-службою, яка обслуговує всю IT-інфраструктуру. У разі збільшення масштабів підприємства або поділу IT-служби за напрямами (мережа, сервери, БД, ПЗ, оптична мережа, системи автоматизації тощо) підприємству необхідно переглянути свій підхід до забезпечення ІБ і трансформувати його в інтеграційний.

Інтеграційний підхід – це наступний рівень забезпечення ІБ. Він характеризується наявністю виділених служб планування і забезпечення роботи систем ІБ, формуванням

єдиних вимог до систем ІБ, аналізом критичності інформаційних активів і потенційних загроз, їх залежністю від бізнес-процесів підприємства.

Інтеграційний підхід має на увазі насамперед розробку вимог до забезпечення безпеки ІТ-інфраструктури та даних з урахуванням архітектури філіальної мережі, особливостей хмарних сервісів, унікальних потреб персоналу і клієнтів. При цьому першим важливим кроком розроблення таких вимог є визначення та розуміння ландшафту кіберзагроз, можливих напрямків атак і потенційних проблем під час роботи із критичною інформацією.

Застосування інтеграційного підходу до забезпечення ІБ-підприємства дає змогу передбачити потенційні загрози та вектори атак, знизити ризик витоку та пошкодження даних, зменшити час простою сервісу під час відновлення. Середні та великі підприємства мають велику і комплексну ІТ-інфраструктури, що, у свою чергу, значно збільшує периметр ІБ. Великі масштаби вимагають також нових механізмів забезпечення ІБ.

Інтеграційно-інноваційний підхід до забезпечення ІБ застосовують підприємства корпоративного рівня, які будують Security Operation Centers (SOC), Центри оперативного реагування (ЦОР) або системи забезпечення кібербезпеки [1–3]. Такі централізовані системи моніторингу ІБ в автоматичному режимі відстежують показники роботи різних елементів ІТ-інфраструктури, а застосування штучного інтелекту підвищує ефективність забезпечення ІБ-підприємства в цілому [4]. Окремим напрямом у рамках інтеграційно-інноваційного підходу є розробка процедур забезпечення безперервності бізнесу (Business Continuity Plan) і плану відновлення після збою (Disaster Recovery Plan) [5, 6]. Підприємства, які розробили такі процедури, забезпечують завчасну підготовку до негативних сценаріїв порушення роботи ІТ-інфраструктури.

Отже, основні відмінності розглянутих підходів до забезпечення ІБ представлені на рис. 1.

Ситуаційний підхід:

- точкове впровадження;
- децентралізація управління;
- відсутність єдиного підходу до проєктування системи захисту;
- інертність впровадження систем.

Інтеграційний підхід:

- наявність служб планування і забезпечення ІБ;
- формування єдиних вимог ІБ;
- аналіз критичності інформаційних активів;
- управління ризиками та загрозами;
- проєктування ІБ від бізнес-процесів підприємства.

Інтеграційно-інноваційний:

- наявність Security Operation Centers (центрів оперативного реагування);
- централізовані системи моніторингу ІБ;
- створення Business Continuity Plan (планів безперервності бізнесу), Disaster Recovery Plan (планів аварійного відновлення);
- формування відмовостійких систем захисту.

Рисунок 1 – Підходи до забезпечення ІБ-підприємства

3. Проблеми вибору методів і технологій захисту інформації

Нині, незалежно від підходу до забезпечення ІБ, підприємства стикаються з аналогічними проблемами під час вибору методів і технологій захисту інформації.

По-перше, це нестача фахівців у галузі кібербезпеки, що створює додаткові ризики піддатися кібератакам із порушенням роботи сервісів або витоком даних. Дуже важливою складовою системи ІБ є персонал.

Основними вимогами до персоналу, що відповідає за ІБ, є знання інструментів безпеки хмарних і серверних платформ, симптомів атак і загроз ІБ, критичних бізнес-процесів для підприємства.

На тлі постійного зростання і ускладнення ІТ-інфраструктури ефективність процесів оновлення прошивок операційних систем і версій ПЗ, що використовується, знижується внаслідок недостатньої систематизації та автоматизації цих завдань, що, зі свого боку, не дає змоги забезпечувати необхідний рівень ІБ-підприємства.

По-друге, периметр корпоративної мережі «розмився» в результаті впровадження віддалених/мобільних робочих місць і технологій BYOD (Bring Your Own Device) [7]. Поступова міграція у хмарні технології, з появою некерованих користувацьких мобільних пристроїв, ускладнює захист активів підприємства, вимагає впровадження відповідних політик управління та обліку мобільних пристроїв, а операційне середовище підприємства – багатофакторної аутентифікації й шифрування даних.

По-третє, недостатня увага до тонкого налаштування міжмережевих екранів, які забезпечують доступ користувачів до ІТ-інфраструктури та захист від неавторизованого доступу. Завдання ускладнюється, оскільки частина сервісів, користувачів і даних перебуває за міжмережевим екраном у хмарі, що збільшує ризик витоку інформації та безпеки використання особистих пристроїв і ПЗ.

Проблему тонкого налаштування частково вирішують міжмережеві екрани нового покоління NGFW (Next-Generation Firewall) і SIEM (Security Information and Event Management) системи [8, 9]. NGFW, об’єднуючи в собі антивірусний захист, перевірку шифрованого трафіка і трафіка на різних рівнях OSI-моделі (Open Systems Interconnection model), веб-фільтр, контроль доступу на основі DNS (Domain Name System), запобігання вторгненням і антиспам, спрощує завдання контролю ключових точок периметра ІБ [10, 11]. А інтеграція NGFW з технологіями і пристроями програмно-керованих мереж SD-WAN (Software Defined Wide Area Network) являє собою ще більш ефективний інструмент для застосування в розподілених мережах [12].

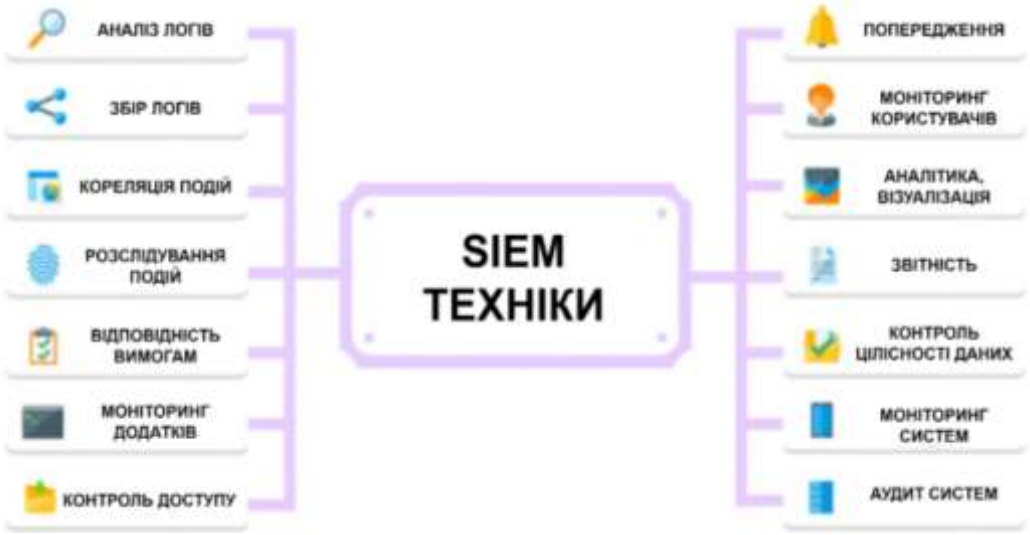

Рисунок 2 – Функціонал SIEM-системи

SIEM-системи з поширенням хмарних технологій стали доступнішими та дешевшими. Відповідно більшість підприємств із розвиненою IT-інфраструктурою вже знайомі з роботою SIEM на практиці. Проте ефективність SIEM-системи, в першу чергу, залежить від розуміння IT-службою вимог до ІБ від бізнесу і правильного налаштування кореляційних правил для ефективного виявлення релевантних загроз. Функціонал SIEM-системи представлено на рис. 2.

Широке застосування хмарних технологій призвело до появи нових векторів атак і, відповідно, нових викликів для наявних систем ІБ. Поширення набули публічні та гібридні моделі розгортання хмар. Однак, крім традиційних загроз (втрата та витік даних; несанкціонований доступ; неналежний контроль за правами доступу), додаються нові загрози: небезпечні інтерфейси та API (Application Programming Interface); неправильне налаштування хмарної платформи. Що стосується інструментів і платформ забезпечення ІБ у хмарі, то наявність віртуалізації та різноманітних сервісних моделей хмарних обчислень призвела до появи нових, специфічних, але водночас більш продуктивних і масштабованих інструментів захисту.

При цьому основними специфічними функціями забезпечення ІБ у хмарі є перевірка достовірності та авторизація; захист даних і запобігання їхньому витоку; забезпечення всебічної видимості бізнес-сервісів і блокування роботи несанкціонованого ПЗ. Цією функціональністю володіє сервіс CASB (Cloud Access Security Broker) – брокер безпеки хмарного доступу, який об’єднує в собі функції IAM-системи (Identity and Access Management) перевірки автентичності, хмарного брандмауера, безпечного веб-шлюзу – WAF (Web Application Firewall)) і DLP-системи запобігання втрати даних [13–15]. Використання CASB у галузі інформаційної безпеки дозволяє вирішувати такі завдання (рис. 3):

• *Контроль доступу:* CASB забезпечує контроль над доступом до хмарних сервісів, додатків та даних. Він дозволяє визначати й управляти політиками доступу, аутентифікацією, авторизацією та аудитом, щоб запобігти несанкціонованому доступу та керувати привілеями користувачів.

• *Захист даних*: CASB забезпечує механізми захисту даних у хмарі. Він може застосовувати шифрування даних, контролювати та запобігати витоку інформації, виявляти й запобігати шкідливим атакам, забезпечувати безпечне зберігання та передачу даних.

• *Виявлення та реагування на загрози:* CASB надає можливості виявлення та моніторингу аномальної активності й потенційних загроз безпеці у хмарних сервісах. Він може попереджувати про підозрілі дії, пропонувати алгоритми реагування та вживати заходів для пом'якшення загроз.

• *Відповідність регуляторним вимогам*: CASB допомагає організаціям дотримуватися регуляторних вимог та стандартів у галузі інформаційної безпеки. Він надає інструменти для контролю та звітності, а також допомагає встановлювати відповідні політики та процедури.

• *Моніторинг та аудит:* CASB надає можливість моніторингу та аудиту дій користувачів, доступу до даних та подій у хмарних сервісах. Він реєструє та аналізує активність, дозволяючи організаціям відстежувати та ідентифікувати потенційні проблеми безпеки.

• *Управління політиками безпеки*: CASB дозволяє визначати та застосовувати політики безпеки у хмарних середовищах. Він надає засоби для встановлення й управління політиками, правилами та обмеженнями, щоб забезпечити відповідність внутрішнім вимогам організації і встановити узгоджену безпеку у хмарі.

Основні тенденції розвитку IT-інфраструктури сьогодні сфокусовані в напрямку хмарних технологій. Відповідно, вже сьогодні та в найближчому майбутньому будуть актуальними завдання забезпечення безпечної взаємодії «наземної» частини IT-

інфраструктури із хмарною, інтеграції систем авторизації хмарних і наземних інфраструктур, витоку інформації із хмарних СЗД.

Рисунок 3 – Завдання, які вирішує CASB

4. Висновки

Розглянувши підходи до забезпечення ІБ вітчизняних підприємств, можна дійти висновку, що ІБ має ґрунтуватися на комплексному підході та ефективній інтеграції всіх елементів ІТ-інфраструктури на різних рівнях взаємодії. Це зумовлено впровадженням нових методів організації роботи на сучасних підприємствах, передових ІТ-технологій, повсюдної автоматизації та цифровізації, розповсюдженням хмарних технологій, BYOD, SD-WAN, IoT. Додаткові вимоги до забезпечення ІБ також диктуються регуляторною політикою держави та галузевими стандартами. Водночас виникає необхідність розроблення стратегій захисту та впровадження систем управління кібербезпекою, що дають змогу оперативно реагувати на загрози ІБ, контролювати інформаційний периметр підприємства та керувати потоками даних (traffic flow) в ІТ-інфраструктурі.

СПИСОК ДЖЕРЕЛ

1. What is a Security Operations Center (SOC)? URL: https://www.ibm.com/topics/security-operations-center (дата звернення: 10.03.2023).
2. Лисецький Ю.М. Центр реагування на інциденти інформаційної безпеки. *Сектор безпеки і оборони України: технології асиметричного протиборства*: матеріали наук.-практ. конф. (Київ, 04.12.2020). 2020. № 42. С. 22.
3. Бобров С.І., Лисецький Ю.М. Security Operation Systems. *Математичні машини і системи.* 2020. № 2. С. 51–59.
4. Тернавский В.О., Калбазов Д.Й., Лисецький Ю.М. Система моніторингу та автоматизації обробки інцидентів. *Математичні машини і системи.* 2020. № 3. С. 80–86.
5. Business Continuity Plan | Kyndryl. URL: https://www.kyndryl.com/nz/en/learn/plan (дата звернення: 10.03.2023).
6. IT Disaster Recovery Plan – Ready.gov. URL: https://www.ready.gov/it-disaster-recovery-plan (дата звернення: 12.03.2023).
7. BYOD-стратегии, ориентированные на сотрудников. URL: http://allta.com.ua/about-byod (дата звернення: 12.03.2023).
8. Next Generation Firewall (NGFW) проти кібератак. URL: https://hub.kyivstar.ua/news/next-generation-firewall-nadijnyj-shhyt-vid-novyh-kiberatak-na-biznes/ (дата звернення: 16.03. 2023).

9. SIEM (Security information and event management). URL: https://it-guild.com/info/glossary/siem/ (дата звернення: 18.03.2023).
10. Рівні моделі OSI. URL: http://smartandyoung.com.ua/rivni-modeli-osi (дата звернення: 20.03.2023).
11. DNS – что это и как работает. URL: https://hostiq.ua/blog/ukr/how-does-dns-work/ (дата звернення: 24.03.2023).
12. Что такое SD-WAN – сложная технология простыми словами. URL: https://gigatrans.ua/ru/news/chto-takoe-sd-wan-slozhnaya-tehnologiya-prostumi-slovami (дата звернення: 24.03.2023).
13. What is a Cloud Access Security Broker (CASB)? URL: https://www.wiz.io/academy/what-is-a-cloud-access-security-broker-casb (дата звернення: 28.03.2023).
14. AWS Identity and Access Management (IAM) – Explained With. URL: https://www.freecodecamp.org/news/aws-iam-explained/ (дата звернення: 10.03.2023).
15. WAF (Web Application Firewall) – межсетевой экран для веб-приложений. URL: https://itglobal.com/ru-ru/company/glossary/waf/ (дата звернення: 28.03.2023).

Стаття надійшла до редакції 30.05.2023