МЕНЕДЖМЕНТ ТА УПРАВЛІННЯ

https://doi.org/10.5281/zenodo.16409682

ЗЕЙНАЛОВ Р. Е.

Захист даних як стратегічна функція управління розвитком software –компаній

Предметом дослідження *є стратегічні підходи до забезпечення безпеки даних у процесі розвитку software–компаній. У роботі проаналізовано вплив рівня захисту даних на ефективність управління на різних етапах життєвого циклу компанії, визначено ключові ризики та обґрунтовано необхідність інтеграції практик data security у загальну стратегію управління розвитком. Розкрито залежність між інвестиціями у захист даних та стійкістю бізнес–моделі в умовах цифрової трансформації.*

Метою дослідження *є визначення ролі та значення захисту даних як стратегічної функції управління розвитком software–компаній в умовах зростання кіберзагроз і технологічної еволюції.*

Методи дослідження. *У дослідженні застосовано системний і порівняльний аналіз, методи узагальнення, логічного та структурного підходів, а також візуалізацію аналітичних даних. Це дозволило комплексно дослідити еволюцію підходів до захисту даних на різних етапах розвитку software–компаній.*

Результати роботи. *У статті обґрунтовано необхідність стратегічного підходу до захисту даних як одного з ключових факторів сталого розвитку software–компаній. Визначено особливості організації data security на стадіях стартапу, масштабування та зрілого бізнесу. Показано, що інвестиції в системі захисту даних прямо впливають на довіру клієнтів, зниження ризиків та конкурентоспроможність компаній. Запропоновано базову модель інтеграції безпеки даних у загальну систему управління.*

Галузь застосування результатів. *Результати дослідження можуть бути використані в управлінні software–компаніями, у консалтингу з цифрової безпеки, у сфері стартап–менеджменту та в освітніх програмах, що стосуються управління інноваційним бізнесом.*

Висновки. *Захист даних є не лише технічним аспектом, а й стратегічною управлінською функцією, що впливає на динаміку розвитку software–компаній. Для досягнення стабільного зростання в умовах цифрової турбулентності необхідно інтегрувати політики безпеки у всі бізнес–процеси з урахуванням стадії розвитку підприємства. Ефективне управління data security сприяє зниженню ризиків, підвищенню інвестиційної привабливості та зміцненню довіри з боку клієнтів і партнерів.*

Ключові слова: *захист даних, software–компанії, стратегічне управління, інформаційна безпека, ризики, розвиток бізнесу, цифрова трансформація.*

RAUF ZEINALOV

Data protection as a strategic function in the management of software company development

The subject of the study *is strategic approaches to ensuring data security in the process of software company development. The paper analyzes the impact of data protection levels on management efficiency across various stages of the company life cycle, identifies key risks, and substantiates the need to integrate data security practices into the overall development management strategy. It highlights the correlation between investments in data protection and the resilience of the business model under conditions of digital transformation.*

The purpose of the study *is to determine the role and significance of data protection as a strategic management function in the development of software companies amid increasing cyber threats and technological evolution.*

Research methods. *The study substantiates the necessity of a strategic approach to data protection as a key factor for the sustainable development of software companies. It identifies the specifics of organizing data security during the startup, scaling, and mature business stages. The study demonstrates that investments in data protection systems directly impact customer trust, risk reduction, and companies' competitiveness. A basic model for integrating data security into the overall management system is proposed.*

Results of work. *The article justifies the necessity of a strategic approach to data protection as one of the key factors for the sustainable development of software companies. It outlines the specific features of organizing data security at the startup, scaling, and mature business stages. The study demonstrates that investments in data protection systems directly influence customer trust, risk reduction, and company competitiveness. A foundational model for integrating data security into the overall management system is proposed.*

Field of application of results. *The research results can be applied in the management of software companies, digital security consulting, startup management, and educational programs related to innovative business management.*

Conclusions. *Data protection is not only a technical issue but also a strategic management function that influences the development dynamics of software companies. To achieve stable growth amid digital turbulence, it is essential to integrate security policies into all business processes, taking into account the company's stage of development. Effective management of data security helps reduce risks, increase investment attractiveness, and strengthen trust among clients and partners.*

Key words: *data protection, software companies, strategic management, information security, risks, business development, digital transformation.*

Постановка проблеми. У сучасних умовах цифрової трансформації та зростаючої кількості кіберзагроз захист даних стає одним із критичних чинників стабільного функціонування та стратегічного розвитку software–компаній. Активне впровадження хмарних рішень, зберігання великих масивів інформації, використання штучного інтелекту та інтеграція відкритих API суттєво підвищують вразливість цифрових активів компаній. У результаті втрати, витоки або несанкціонований доступ до даних можуть призводити не лише до фінансових збитків, а й до втрати довіри клієнтів, судових позовів, порушення регуляторних вимог та підриву репутації компанії. Особливо вразливими є малі та середні software–компанії, які часто ігнорують системний підхід до управління безпекою даних через обмежені ресурси.

Традиційно функції захисту інформації сприймалися як суто технічне завдання, проте у сучасних умовах вони потребують стратегічного осмислення та інтеграції в загальну систему управління розвитком підприємства. Це особливо важливо на різних етапах життєвого циклу software–компаній, де характер ризиків та підходи до захисту даних істотно відрізняються. Таким чином, актуальним постає завдання визначення ролі та практик забезпечення безпеки даних як управлінської функції, що впливає на довгостро–

кову стійкість, конкурентоспроможність та динаміку зростання компаній у сфері розробки програмного забезпечення.

Аналіз останніх досліджень і публікацій. Питання захисту даних активно досліджується як у міжнародному, так і в українському науковому та професійному середовищі. У працях провідних фахівців, зокрема О. Маковоз, С. Лисенка, М. Буряка, А. Швінбахера, P. Hagen та T. Scholz, розглядаються аспекти кібербезпеки, цифрової трансформації та впровадження інноваційних технологій у сфері управління. Зокрема, у роботах Лисенка та Маковоз акцентовано увагу на важливості адаптації компаній до цифрових загроз, що зростають у постпандемічний та післявоєнний період. Буряк і Швінбахер аналізують взаємозв'язок між безпекою даних та інвестиційною привабливістю IT–бізнесу, підкреслюючи роль стратегічного підходу до інформаційної безпеки.

У роботах міжнародних дослідників, зокрема представників Verizon, Gartner, IBM Security, Cisco та ENISA, представлено класифікацію загроз, оцінку ризиків та інвестиційні підходи до data security. Водночас більшість досліджень зосереджується на технічних аспектах безпеки, залишаючи поза увагою управлінський вимір — зокрема, інтеграцію захисту даних у систему стратегічного менеджменту та його залежність від етапу розвитку компанії.

В українському науковому дискурсі питання захисту даних у контексті розвитку software–компаній розглядаються фрагментарно, переважно з позиції технічної реалізації або правового регулювання. Водночас проблема формування стратегічної моделі управління data security як частини загальної системи розвитку software–компаній залишається недостатньо дослідженою, що актуалізує потребу у поглибленому аналізі цієї тематики.

Метою статті є обґрунтування ролі захисту даних як стратегічної управлінської функції в процесі розвитку software–компаній, визначення особливостей організації системи безпеки даних на різних етапах життєвого циклу компанії, аналіз впливу рівня data security на довгострокову стійкість, інвестиційну привабливість та конкурентоспроможність підприємства в умовах цифрової трансформації та зростання кіберзагроз.

Виклад основного матеріалу. Життєвий цикл software–компанії включає кілька послідовних етапів розвитку, які визначають зміни у структурі, стратегії та управлінні, зокрема в аспектах інформаційної безпеки. Від початкового стартапу до зрілої міжнародної компанії кожен етап характеризується специфічними викликами і пріоритетами, що накладають особливі вимоги до захисту даних та управлінських практик [1, 2].

Згідно з моделлю Adizes [3], організації проходять фази народження, зростання, зрілості та спаду, де кожна фаза має свої особливості в управлінні і ризиках. Для software–компаній це особливо важливо, оскільки швидкість змін технологій і високий рівень конкуренції змушують динамічно адаптуватися до зовнішніх і внутрішніх факторів.

Водночас, як підкреслюють Гуменна та Карпіщенко [1], ефективне управління інформаційною безпекою має бути системним і інтегрованим у стратегію підприємства.

Початковий етап — стартап — характеризується фокусом на швидкому запуску продукту з мінімальними ресурсами і часто без належної уваги до захисту даних. Часто в таких компаніях відсутні формалізовані політики безпеки, а керівники та розробники не завжди усвідомлюють потенційні ризики, пов'язані з витоком або втратою інформації. Як показує дослідження Метлешко, це призводить до високої вразливості до атак на ранніх стадіях і може загрожувати як репутації, так і можливості подальшого залучення інвестицій.

Фаза зростання супроводжується появою перших клієнтів, розширенням команди та початком формалізації внутрішніх процесів. Саме на цьому етапі компанії починають впроваджувати базові заходи безпеки, такі як контроль доступу, використання договорів про нерозголошення (NDA), регулярне резервне копіювання даних. При цьому важливо зазначити, що вимоги клієнтів і інвесторів до безпеки починають зростати, що стимулює інвестиції в інформаційну безпеку. За даними звіту ENISA (2024), середні software–компанії все більше орієнтуються на впровадження стандартів ISO/IEC 27001 та NIST, що забезпечує базовий рівень контролю ризиків [4].

Етап масштабування — це період, коли компанія виходить на нові ринки, зокрема міжнародні, і стикається з суворими регуляторними вимогами, наприклад GDPR в Європейському Союзі або SOC 2 у США. Це ставить перед компанією необхідність глибшого впровадження політик інформаційної безпеки, автоматизації процесів захисту даних і регулярних зовнішніх ауди–

тів. Водночас масштаби бізнесу ускладнюють управління ризиками, оскільки зростає кількість інтеграцій, API, партнерських зв'язків, що потенційно збільшують поверхню атаки [5, 6].

Для зрілої компанії інформаційна безпека стає невід'ємною частиною стратегії розвитку. Формуються спеціалізовані департаменти кібербезпеки, впроваджуються політики реагування на інциденти (Incident Response), регулярного аудиту та навчання персоналу. Важливу роль відіграє формування культури безпеки на всіх рівнях організації, що зменшує людський фактор як причину порушень [7]. Як показують дослідження Safa, Sookhak та von Solms (2016), у провідних компаніях світу зростання інвестицій у кібербезпеку прямо корелює з рівнем довіри клієнтів, зниженням ризику витоку даних та довгостроковою конкурентоспроможністю [8].

Таким чином, управління захистом даних на різних етапах розвитку software-компанії має свої особливості та потребує відповідного адаптованого підходу, який враховує як технологічні, так і організаційні фактори.

1. Стартап: мінімізація витрат та низька увага до безпеки

Стартапи у сфері software характеризуються високою динамікою змін, обмеженими ресурсами та фокусом на швидкому виході на ринок. Основною метою на цій фазі є створення мінімально життєздатного продукту (MVP) із мінімальними витратами, що часто призводить до зневаги питаннями інформаційної безпеки. Низька увага до безпеки у стартапах відображається у відсутності формалізованих політик, недостатньому контролі доступу, слабкому захисті даних клієнтів і відсутності процесів реагування на інциденти.

Згідно з даними OWASP Top 10 for Startups, основними уразливостями у цій фазі є відсутність належної автентифікації та авторизації, неправильне управління сесіями, а також недотримання принципу найменших привілеїв, що створює можливості для експлуатації вразливостей. Недооцінка цих аспектів може спричинити серйозні проблеми, включаючи витік конфіденційних даних, порушення цілісності та доступності систем.

Однією з ключових проблем є також недостатня обізнаність команди щодо актуальних кіберризиків. Часто засновники та розробники сконцентровані на функціональності продукту та залученні клієнтів, не враховуючи потенційні загрози і не формуючи культуру безпеки в команді. Згідно з дослідженням ENISA (2023), понад 60% стартапів не мають навіть базових політик інформаційної безпеки, що робить їх привабливою ціллю для кіберзлочинців.

Переважно стартапи використовують хмарні сервіси з базовими налаштуваннями безпеки, не впроваджуючи додаткових шарів захисту, таких як багатофакторна аутентифікація (MFA) або регулярні аудитні перевірки. Внаслідок цього зростає ймовірність компрометації ключових даних, що в подальшому може вплинути на репутацію і здатність залучати інвестиції.

Водночас, через обмеженість ресурсів, у стартапів немає можливості або часу для впровадження складних систем безпеки. Для них актуальними є прості, недорогі та ефективні рішення, які мінімізують ризики без суттєвого навантаження на розробку. Google for Startups рекомендує починати з найпростіших заходів: налаштування безпечних паролів, резервне копіювання даних, використання захищених протоколів зв'язку (HTTPS).

Крім технічних аспектів, важливу роль відіграє управлінський фактор — здатність засновників закласти безпекові практики у культуру компанії з перших днів її існування. Це дозволяє змен-

Таблиця 1. Основні кіберризики на стадії стартапу та рекомендовані заходи*

Кіберризик	Опис	Рекомендовані заходи
Недостатня автентифікація	Відсутність MFA, слабкі паролі	Впровадження багатофакторної автентифікації
Неправильне управління доступом	Надмірні права користувачів	Принцип найменших привілеїв
Відсутність резервного копіювання	Втрата даних через збої або атаки	Регулярне резервне копіювання даних
Вразливості в веб-застосунках	SQL-ін'єкції, XSS, CSRF	Використання OWASP рекомендацій
Відсутність інцидент-менеджменту	Нездатність швидко реагувати на кіберінциденти	Формування процесу реагування на інциденти

** Джерело: побудовано автором за [9]*

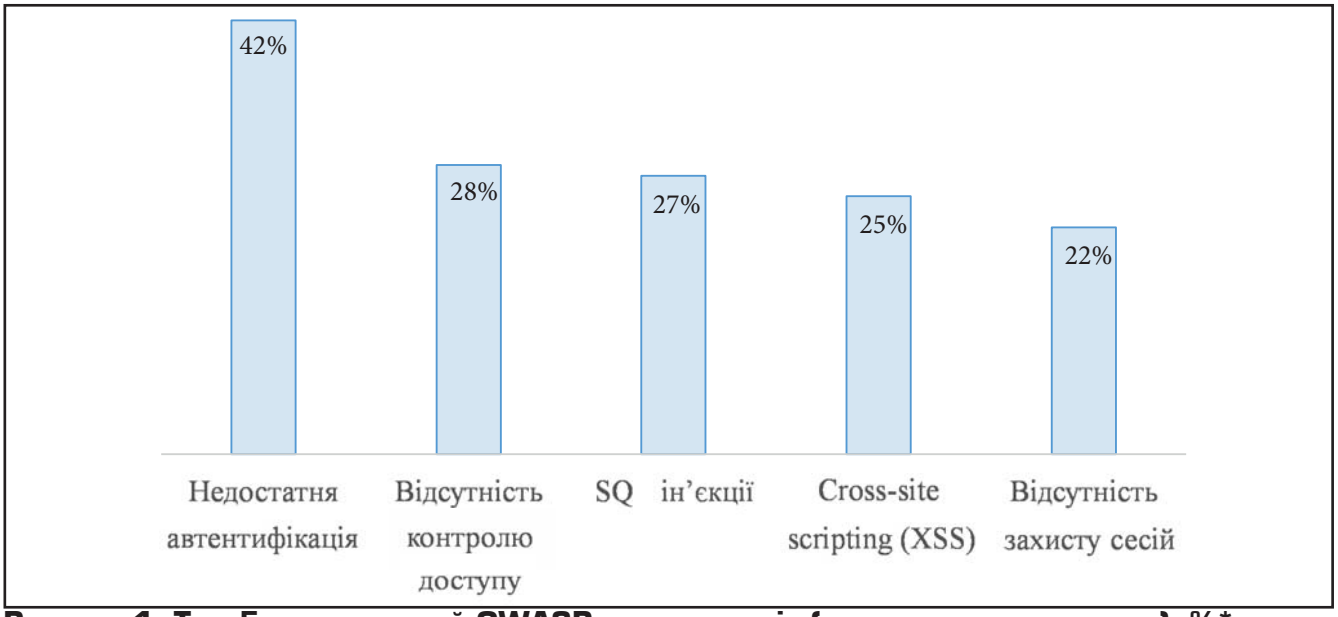

Рисунок 1. Топ–5 вразливостей OWASP для стартапів (за частотою виявлення), %*

**Джерело: побудовано автором за [10]*

шити ризики, підготувати базу для подальшого масштабування і знизити вразливість до кібер–загроз на наступних етапах розвитку.

Дані таблиці 1 і графіка 1 демонструють, що стартапи часто недооцінюють важливість кібер–безпеки, особливо у малих командах, де головна увага приділяється швидкому розвитку продукту. Основні вразливості, визначені OWASP, вказують на типові слабкі місця, які можуть бути ефективно усунені простими, недорогими методами безпеки.

2. Фаза зростання: перші клієнти, перші вимоги до безпеки

На цьому етапі компанії вже мають функціональний продукт, починають працювати з клієнтами, з'являється команда продажів і розширюється розробка. Зростає і обсяг зібраних даних — як користувацьких, так і бізнесових. У результаті керівництво вперше стикається з необхідністю формалізувати мінімальні заходи безпеки.

Поширеними стають базові практики: розмежування доступів до даних (role–based access control), підписання NDA з працівниками та підрядниками, резервне копіювання, впровадження двофакторної автентифікації. Компанії починають цікавитися стандартами типу ISO/IEC 27001 або рекомендаціями NIST для малого бізнесу, однак повного впровадження системи управління інформаційною безпекою (ISMS) зазвичай ще не відбувається.

Безпека на цій стадії носить фрагментарний характер і часто обмежується ініціативами технічної команди. Формалізована стратегія безпеки відсутня, однак з'являється її усвідомлення як одного з факторів інвесторської привабливості.

3. Масштабування: міжнародні ринки, регуляції, репутаційні ризики

Масштабування супроводжується збільшенням кількості клієнтів, виходом на міжнародні ринки та інтеграцією з іншими системами. Усе це робить компанію вразливою до юридичних, репутаційних і технологічних ризиків.

Відповідність вимогам регуляторів стає критичною: на перший план виходять GDPR, SOC 2, ISO/IEC 27001, California Consumer Privacy Act (CCPA). Часто вже запроваджуються практики audit logging, penetration testing, шифрування даних у transit і at rest, а також оцінка постачальників (vendor risk management) [11].

Оскільки компанія переходить від реактивного до проактивного підходу до безпеки, зростає роль зовнішнього аудиту та автоматизованих інструментів моніторингу. Починає формуватись політика безперервного покращення — регулярний перегляд політик безпеки, впровадження процедури реагування на інциденти (incident response).

4. Зріла компанія: системна безпека як частина стратегічного управління

У зрілих software–компаніях безпека інтегрована у всі бізнес–процеси. Формується окремий департамент або щонайменше посада CISO (Chief Information Security Officer), визначаються KPI з безпеки, проводяться тренінги для персоналу, реалізується Zero Trust модель.

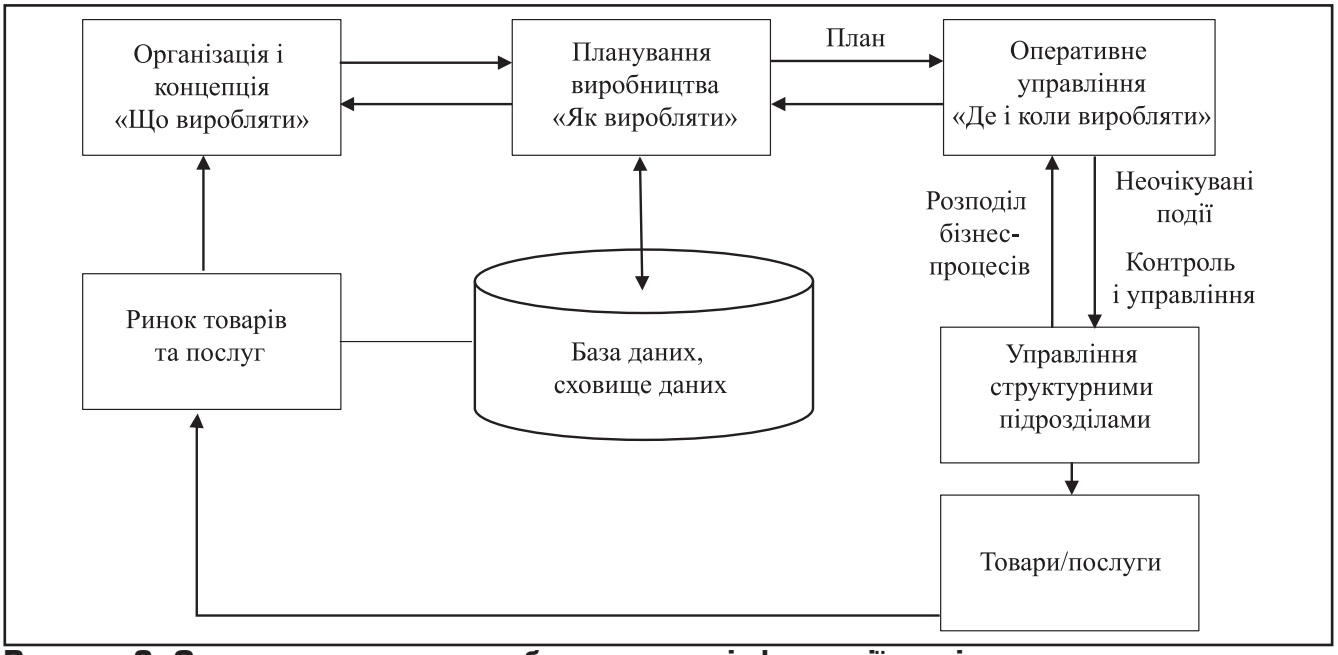

Рисунок 2. Структура основних проблем захисту інформації на підприємствах
Джерело: побудовано автором за [12]

Такі компанії, як правило, мають повністю сертифіковану систему інформаційної безпеки (наприклад, ISO 27001 або SOC 2 Type II) і регулярно проходять зовнішній аудит. Особливу увагу приділяють безпеці DevOps-процесів (DevSecOps), автоматизованому виявленню вразливостей та хмарній інфраструктурі (наприклад, контроль за використанням API та внутрішніми сервісами).

На стратегічному рівні безпека починає розглядатись не лише як обов'язок, а як конкурентна перевага. Наприклад, компанії можуть надавати клієнтам White Paper з описом власної інфраструктури захисту, аби підвищити рівень довіри.

5. Етапи трансформації: злиття, інтернаціоналізація, перехід до хмари

На етапах реструктуризації, злиття/поглинання (M&A) або міграції в хмарні середовища виникають нові виклики для захисту даних. Поєднання систем безпеки різних компаній вимагає інтеграції політик, синхронізації інфраструктур, адаптації до міжнародного законодавства.

У випадку переходу до хмари (наприклад, AWS або Azure) критичними стають питання розмежування відповідальності (shared responsibility model), шифрування, а також відповідності вимогам ISO/IEC 27018 щодо захисту персональних даних у хмарі.

Кіберризики в умовах трансформації часто недооцінюються. Дослідження Accenture вказують, що понад 50% компаній після злиття мають проблеми з безпечним об'єднанням інформаційних систем. Тому роль CISO в таких процесах має бути не технічною, а стратегічною — участь у due diligence, оцінка ризиків та підготовка plan B у разі інцидентів.

В умовах цифрової економіки, де інформація виступає не лише як ресурс, а й як актив компанії, питання захисту даних виходить за межі технічної компетенції IT-відділів. Ефективне управління software-компанією вимагає стратегічного підходу до кібербезпеки, що охоплює не лише технології, але й бізнес-процеси, фінансові ризики, управління персоналом і юридичну відповідність.

1. Принципи інтеграції.

Інтеграція безпеки даних у стратегічне управління передбачає:

- Включення оцінки ризиків кібербезпеки в загальний процес стратегічного планування;
- Формування KPI в сфері інформаційної безпеки, прив'язаних до цілей компанії (наприклад, відсоток інцидентів, виявлених протягом 24 годин; кількість навчальних сесій із безпеки на одного працівника) [13];
- Залучення керівництва C-рівня (особливо CEO, CTO, CISO) до процесів прийняття рішень у сфері захисту даних;
- Побудову системи моніторингу і регулярного аудиту інформаційної безпеки як інструменту контролю;
- Забезпечення внутрішньої культури безпеки, що поширюється на всі рівні персоналу.

Таблиця 2. Еволюція організаційного управління безпекою даних*

Тип компанії	Основний відповідальний	Органи контролю	Звітність
Стартап	CTO / Team Lead	Відсутні / Ad hoc	Нерегулярна
Компанія в зростанні	CISO / Security Officer	IT–менеджмент	Раз на квартал
Зріла компанія	CISO + департамент IS	Аудиторський комітет	Регулярна (місячна)

** Джерело: побудовано автором*

2. Організаційна структура управління безпекою.

Залежно від масштабу компанії і фази життєвого циклу, структура може варіюватися:

3. KPI та оцінка ефективності.

Ключові показники ефективності (KPI) повинні відповідати як технічним цілям, так і бізнес–результатам:

• MTTD (Mean Time to Detect) – середній час виявлення інциденту;

• MTTR (Mean Time to Respond) – час реагування на інцидент;

• % працівників, які пройшли навчання з безпеки;

• % критичних систем, що мають актуальні патчі;

• Кількість зовнішніх аудитів на рік.

Ці показники використовуються не лише для оперативного контролю, а й для звітності перед інвесторами та регуляторами.

4. Системне включення стандартів та комплаєнсу.

Стандарти (ISO/IEC 27001, NIST CSF) мають бути не просто сертифікатами, а вбудованими в бізнес–архітектуру компанії. Це дозволяє забезпечити:

• Безперервне вдосконалення безпекових практик (PDCA–цикл);

• Прозору структуру відповідальності та процедур;

• Узгодженість дій між підрозділами компанії.

5. Безпека як драйвер інновацій.

У сучасних умовах компанії, що системно інтегрують безпеку в управління, отримують конкурентну перевагу:

• Клієнти обирають постачальника з перевіреною історією безпечного оброблення даних;

• Інвестори охочіше інвестують у компанії з чіткою стратегією захисту;

• Компанія готова до нових ринків і регуляторних вимог (наприклад, DORA або AI Act).

Висновки

Інтеграція захисту даних у стратегічне управління software–компаніями є ключовим елементом забезпечення їх стабільного розвитку в умовах сучасної цифрової трансформації. Впровадження політик безпеки, регулярний аудит, визначення ключових показників ефективності (KPI) та активна участь керівництва забезпечують комплексний підхід до управління ризиками і підвищують рівень довіри клієнтів і партнерів.

Комплексний підхід до кібербезпеки дозволяє компаніям не лише захищати інформаційні ресурси, а й використовувати захист даних як фактор конкурентної переваги, що відкриває нові можливості для масштабування бізнесу та виходу на міжнародні ринки. Особливо важливою є адаптація стандартів безпеки та вимог комплаєнсу до особливостей різних етапів життєвого циклу компанії, що сприяє її стійкості у довгостроковій перспективі.

Отже, стратегічне управління безпекою даних у software–компаніях повинно бути невід'ємною частиною загальної бізнес–стратегії, що забезпечує не лише мінімізацію ризиків, а й сприяє сталому розвитку і технологічній еволюції підприємств.

Список використаних джерел:

1. Гуменна О. В., Карпіщенко О. О. Управління інформаційною безпекою підприємства в умовах цифровізації. Економіка та суспільство. 2023. № 50. С. 132–137. URL: https://economyandsociety.in.ua/index.php/journal/article/view/4329/4255

2. Метелешко О. В. Інформаційна безпека підприємства: бакалаврська дипломна робота. Тернопіль: ТНТУ, 2021. 60 с. URL: https://elartu.tntu.edu.ua/bitstream/lib/35367/1/Dyp_Meteleshko_2021.pdf

3. Adizes Institute. Methodology [Електронний ресурс]. – URL: https://www.ichakadizes.com/methodology.

4. ENISA. ENISA Threat Landscape 2024 [Електронний ресурс]. – URL: https://www.enisa.europa.eu/publications/enisa–threat–landscape–2024.

5. GDPR Portal. Summary of key provisions [Електронний ресурс]. – URL: https://gdpr–info.eu/.

6. ISO/IEC 27001:2022 – International Standard for ISMS [Електронний ресурс]. – URL: https://www.iso.org/standard/27001.html.

7. Pavlovic N. How can organizations develop situation awareness for incident response? A case study of management practice // ResearchGate. – 2020. – URL: https://www.researchgate.net/

publication/347396345_How_can_organizations_develop_situation_awareness_for_incident_response_A_case_study_of_management_practice.

8. Alkalbani A., Deng H., Kam B. Information security policy compliance model in organisations // ResearchGate. – 2016. – URL: https://www.researchgate.net/publication/309045498_Information_security_policy_compliance_model_in_organisations.

9. Han Y., Wang H. Cyber risk management: Theories, frameworks, models and practices // ResearchGate. – 2024. – URL: https://www.researchgate.net/publication/389874462_Cyber_risk_management_Theories_frameworks_models_and_practices.

10. OWASP. The OWASP Top Ten [Електронний ресурс]. – URL: https://owasp.org/www-project-top-ten/.

11. Malik A., Avram M. Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies // ResearchGate. – 2024. – URL: https://www.researchgate.net/publication/381844798_Third-party_vendor_risks_in_IT_security_A_comprehensive_audit_review_and_mitigation_strategies.

12. Проблеми захисту інформації на підприємствах // Підручники онлайн. – URL: https://pidru4niki.com/1427040647714/informatika/problemi_zahistu_informatsiyi_pidpriyemstvah.

13. Ivanov I. Using security metrics to determine security program effectiveness // ResearchGate. – 2023. – URL: https://www.researchgate.net/publication/371993658_Using_Security_Metrics_to_Determine_Security_Program_Effectiveness.

References:

1. Gumena, O. V., & Karpishchenko, O. O. (2023). Management of enterprise information security in the context of digitalization. Economy and Society, (50), 132–137. URL: https://economyandsociety.in.ua/index.php/journal/article/view/4329/4255

2. Meteleshko, O. V. (2021). Enterprise information security: Bachelor's thesis. Ternopil National Technical University. URL: https://elartu.tntu.edu.ua/bitstream/lib/35367/1/Dyp_Meteleshko_2021.pdf

3. Adizes Institute. (n.d.). Methodology. URL: https://www.ichakadizes.com/methodology

4. European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

5. GDPR Portal. (n.d.). Summary of key provisions. URL: https://gdpr-info.eu/

6. International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information Security Management Systems. URL: https://www.iso.org/standard/27001.html

7. Pavlovic, N. (2020). How can organizations develop situation awareness for incident response? A case study of management practice. ResearchGate. URL: https://www.researchgate.net/publication/347396345_How_can_organizations_develop_situation_awareness_for_incident_response_A_case_study_of_management_practice

8. Alkalbani, A., Deng, H., & Kam, B. (2016). Information security policy compliance model in organisations. ResearchGate. URL: https://www.researchgate.net/publication/309045498_Information_security_policy_compliance_model_in_organisations

9. Han, Y., & Wang, H. (2024). Cyber risk management: Theories, frameworks, models and practices. ResearchGate. URL: https://www.researchgate.net/publication/389874462_Cyber_risk_management_Theories_frameworks_models_and_practices

10. OWASP Foundation. (n.d.). The OWASP Top Ten. URL: https://owasp.org/www-project-top-ten/

11. Malik, A., & Avram, M. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. ResearchGate. URL: https://www.researchgate.net/publication/381844798_Third-party_vendor_risks_in_IT_security_A_comprehensive_audit_review_and_mitigation_strategies

12. Online Textbooks. (n.d.). Problems of information protection in enterprises. Pidruchnyky Online. URL: https://pidru4niki.com/1427040647714/informatika/problemi_zahistu_informatsiyi_pidpriyemstvah

13. Ivanov, I. (2023). Using security metrics to determine security program effectiveness. ResearchGate. URL: https://www.researchgate.net/publication/371993658_Using_Security_Metrics_to_Determine_Security_Program_Effectiveness

Дані про автора

Рауф Ельшан огли Зейналов,

аспірант, Державний університет економіки і технологій

e-mail: zeinalov_re_24700@kneu.dp.ua

https://orcid.org/0009-0003-2733-3294

Data about the author

Rauf Zeinalov,

Postgraduate student state University of Ekonomics and Technology

e-mail: zeinalov_re_24700@kneu.dp.ua