МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «УПРАВЛІННЯ РЕПУТАЦІЙНИМИ РИЗИКАМИ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Данило ІВАНОВ
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Данило ІВАНОВ

Керівник:
к.е.н., доцент Тетяна КАПЕЛЮШНА

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ
_____Світлана ЛЕГОМІНОВА
“____”_____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Іванову Данилу Андрійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Управління репутаційними ризиками як складова забезпечення інформаційної безпеки компанії”

керівник кваліфікаційної роботи Тетяна КАПЕЛЮШНА, к.е.н, доцент
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “19“ жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи “18” грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: нормативно-правові акти, законодавство щодо інформаційної безпеки, аналітичні звіти компанії про репутаційні ризики та інформаційну безпеку підприємства, наукові статті та публікації українських та зарубіжних вчених, експертів щодо питань інформаційної безпеки та репутаційних ризиків, їх впливу на інформаційну безпеку, дані моніторингу соціальних мереж.

4. Перелік питань, які потрібно розробити:
   1. Уточнення понять "репутація" та "репутаційні ризики", визначення взаємозв'язку останніх з питаннями інформаційної безпеки компанії.
   2. Характеристика компанії, комплексний аналіз інформаційних та репутаційних ризиків.
   3. Виявлення прогалин у системі інформаційної безпеки та репутаційних ризиків, розробка комплексної технології управління репутаційними ризиками та забезпечення інформаційної безпеки підприємства, враховуючи класифікацію загроз.

5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання “02” жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	виконано
2.	Збір та аналіз літератури.	15.10.2023	виконано
3.	Розгляд аспектів основних рис репутації та ризиків для неї, а також їх взаємодії з аспектами інформаційної безпеки.	25.10.2023	виконано
4.	Дослідження та класифікація репутаційних ризиків компанії, зокрема ідентифікація потенційних загроз та визначення їхнього впливу на репутацію.	11.11.2023	виконано
5.	Розробка комплексної системи управління репутаційними ризиками компанії та включення її у процес оцінки конкретних ризиків.	15.11.2023	виконано
6.	Формулювання висновків на основі отриманих результатів дослідження.	22.11.2023	виконано
7.	Оформлення роботи.	04.12.2023	виконано
8.	Оформлення презентації.	14.12.2023	виконано
9.	Отримання рецензії на роботу.	18.12.2023	виконано
10.	Захист в ДЕК.	16.01.2024	виконано

Здобувач вищої освіти _____ Данило ІВАНОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Іванов Д.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "Управління репутаційними ризиками як складова забезпечення інформаційної безпеки компанії"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ІВАНОВ Данило** у кваліфікаційній роботі відповідно до обраної теми, визначив напрями та методи дослідження для опрацювання питань за темою та вирішення поставлених завдань. **ІВАНОВ Данило** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець.

Результати дослідження апробовані на конференції, що доводить практичну значимість отриманих результатів.

Вищевикладене дозволяє оцінити виконану кваліфікаційну роботу здобувачем **ІВАНОВИМ Данилом** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр з кібербезпеки" за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна Капелюшна
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"___"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Іванов Д.А. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Іванова Данила Андрійовича

на тему: “Управління репутаційними ризиками як складова забезпечення інформаційної безпеки компанії”

Актуальність. Сьогодення характеризується низкою невизначеностей та загроз, які впливають на роботу підприємств, організацій не залежно від організаційно-правових форм, їх розмірів. Останнім часом зростають атаки у інформаційному середовищі, що загрожують нормальному функціонуванню підприємств та негативно впливають на результати їх діяльності. Саме тому постає питання щодо захиту підприємств від інформаційних загроз, у тому числі репутаційних ризиків, задля убезпечення підприємства від матеріальних втрат. Тим самим, актуалізується проблемне питання, що поставлене для дослідження, оскільки нові виклики та загрози потребують вирішення даного питання у новому ключі розв’язання.

Позитивні сторони

1. У роботі досліджено основи забезпечення інформаційної безпеки підприємства; «репутаціні ризики» та визначено їх взаємовплив на інформаційну безпеку підприємства. Крім того, об’єктом дослідження обрано підприємство, на базі якого здобувач освіти проходив практику, що дозволило більш грунтовно, із розумінням вирішувати поставлені у роботі завдання. Досліджено репутаційні ризики компанії, виявлено прогалини у інформаційній безпеці компанії для подальшої розробки комплексної технології управління репутаційними ризиками.
2. Робота оформлена відповідно до вимог, що висуваються до написання кваліфікаційних магістерських робіт. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Основні положення роботи представлено у вигляді рисунків, таблиць. Опрацьовано достатню та актуальну інформацію із наукових джерел, статистичних звітів.
3. За результатами проведеного дослідження надано пропозиції щодо удосконалення управління репутаційними ризиками компанії, а ткож їх апробовано на Всеукраїнській науково-практичній конференції «Актуальні проблеми кібербезпеки».

Недоліки

1. Варто приділиту увагу питанням репутаційного протиборства компаніями, що являються конкурентами-лідерами, щоб врахувати їх досвід та розробки, однак зважаючи на складінсть отримання даної інформації, це не є вагомим недоліком та суттєво не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні, заслуговує позитивної оцінки, а здобувач Іванов Данило Андрійович заслуговує присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою “Управління інформаційною безпекою”

Рецензент: завідувач кафедри Інформаційної та кібернетичної безпеки, д.т.н, професор

підпис

Галина ГАЙДУР
(Ім’я ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра складається з 91 сторінки, включає 13 рисунків, 8 таблиць та базується на 61 джерелах.

Метою роботи є дослідження питань управління репутаційними ризиками як складової забезпечення інформаційної безпеки компанії.

Об'єктом дослідження є репутаційні ризики компанії

Предметом дослідження **-** особливості управління репутаційними ризиками підприємства.

Застосовані методи дослідження включають аналіз, синтез, дедукцію, SWOT-аналіз, прогнозування.

Метою дослідження є вивчення особливостей управління репутаційними ризиками підприємства з подальшою розробкою пропозицій щодо їх усунення та упередження.

Короткий зміст роботи. У роботі вивчено "репутацію" та "репутаційні ризики" компанії, їх вплив і взаємозв'язок з інформаційною безпекою. Проведено аналіз інформаційних та репутаційних ризиків, їх впливу на компанію. Розглянуто шляхи удосконалення управління репутаційними ризиками, включаючи виявлення прогалин, розробку технології та їх застосування до загроз. Висновки підкреслюють важливість управління репутаційними ризиками для інформаційної безпеки підприємства. Кінцеві висновки акцентують актуальність теми та її практичну значущість, додається перелік посилань та демонстраційні матеріали.

Галузь застосування. Запропоновані рекомендації до управління репутаційними ризиками можуть бути використані для систематизації та класифікації ризиків, а також для керування компанією під час кризових ситуацій, які виникають в інформаційному полі її діяльності

КЛЮЧОВІ СЛОВА: УПРАВЛІННЯ РЕПУТАЦІЙНИМИ РИЗИКАМИ, ІНФОРМАЦІЙНА БЕЗПЕКА, КОМПАНІЯ, АНАЛІЗ РИЗИКІВ, ІНФОРМАЦІЙНІ АКТИВИ, КРИЗА.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 93 pages, 10 figures, 7 tables, 61 sources.

The purpose of the work is to research the topic of reputational risk management as a component of ensuring the company's information security.

Object of research is reputational risks, and the subject is

Subject of research is the peculiarities of management of reputational risks of the enterprise. Applied research methods include analysis, evaluation and design.

Research methods. Methods are to study the features of reputation risk management of the enterprise.

Brief content of research. The work examines the "reputation" and "reputational risks" of the company, their influence and relationship with information security. An analysis of informational and reputational risks and their impact on the company was carried out. Ways to improve reputational risk management are considered, including identifying gaps, developing technology, and applying them to threats. The conclusions emphasize the importance of managing reputational risks for the information security of an enterprise. The final conclusions emphasize the topicality of the topic and its practical significance, a list of references and demonstration materials are attached.

Field of research. The developed approaches to reputation risk management can be used to systematize and classify risks, as well as to manage the company during crisis situations.

KEYWORDS: REPUTATION RISKS MANAGEMENT, INFORMATION SECURITY. COMPANY, RISK ANALYSIS, ASSETS. CRISIS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – Інформаційна безпека

ІТ – Інформаційні технології

КПК – Комуністична партія Китаю

ВСТУП

Актуальність теми. Актуальність обраної теми визначається необхідністю підприємств адаптуватися до швидкозмінюваного цифрового середовища. В умовах глобалізації та інтенсивного використання інтернет-технологій репутаційні ризики стають значущими факторами, які можуть серйозно вплинути на фінансові показники, стосунки з клієнтами та загальний імідж компанії.

Зростання важливості цифрової репутації визначає необхідність ретельного вивчення механізмів управління репутаційними ризиками в умовах інформаційного суспільства. Особливу актуальність ця тема отримує в контексті збільшення кількості кіберзагроз та несанкціонованого доступу до інформації, що вимагає від компаній надійних стратегій захисту не лише інформації, але й репутації як ключового актива в сучасному бізнесі. Таким чином, вивчення управління репутаційними ризиками стає пріоритетним завданням для підприємств у цифровій епохі.

Метою роботи є дослідження питань управління репутаційними ризиками як складової забезпечення інформаційної безпеки компанії.

Об'єктом дослідження є репутаційні ризики компанії

Предметом дослідження - особливості управління репутаційними ризиками підприємства.

Застосовані методи дослідження включають аналіз, синтез, дедукцію, SWOT-аналіз, прогнозування.

Метою дослідження є вивчення особливостей управління репутаційними ризиками підприємства з подальшою розробкою пропозицій щодо їх усунення та упередження.

Вивчення взаємозв'язку репутаційних ризиків та інформаційної безпеки. Це завдання передбачає ретельний аналіз і вивчення того, як репутаційні ризики взаємодіють із сферою інформаційної безпеки компанії.

Це охоплює аналіз можливих точок взаємодії, виявлення слабких місць та встановлення стратегій для їх врегулювання.

Аналіз функціонування компанії. В цьому завданні слід провести глибокий аналіз характеристик та особливостей функціонування підприємства. Це включає в себе розгляд структури компанії, її бізнес-процесів та взаємодії зі стейкхолдерами.

1. Розробка комплексної технології управління репутаційними ризиками. Це завдання вимагає розробки інтегрованої технології, яка охоплює всі аспекти управління репутаційними ризиками. Включає в себе визначення ефективних інструментів, процесів та стратегій, які сприятимуть зменшенню та контролю репутаційних ризиків.

2. Застосування технології до конкретних загроз. Це завдання передбачає практичне впровадження розробленої технології для управління репутаційними ризиками в конкретних ситуаціях. Це може включати імітацію кризових ситуацій, тестування ефективності стратегій та аналіз їх впливу на репутацію.

Методи дослідження включають аналіз існуючих підходів, емпіричні методи вивчення реальних випадків та розробку практичних рекомендацій.

Наукова новизна одержаних результатів у даній роботі виявляється у специфічному підході до розгляду і управління репутаційними ризиками підприємства, враховуючи їхній взаємозв'язок із загрозами інформаційної безпеки. Зокрема, робота розширює розуміння репутаційних ризиків, враховуючи їхню динаміку та вплив на інформаційну безпеку організації.

Першочерговим внеском є аналіз взаємозв'язку репутаційних ризиків із питаннями інформаційної безпеки, що враховує взаємодію цих двох аспектів в контексті сучасних викликів бізнесу. Робота детально розкриває механізми впливу репутаційних ризиків на інформаційну безпеку та визначає конкретні стратегії управління цією взаємодією.

Другим ключовим аспектом новизни є комплексний аналіз і оцінка репутаційних ризиків, що дозволяє враховувати їхній вплив на

функціонування компанії в різних аспектах. Такий глибокий розгляд покращує розуміння природи репутаційних ризиків та сприяє розробці більш ефективних стратегій управління ними.

Отже, наукова новизна роботи полягає у вдосконаленні теоретичного та прикладного підходів до управління репутаційними ризиками, враховуючи їхню взаємодію з інформаційною безпекою в умовах сучасного бізнес-середовища.

Практичне значення одержаних результатів. Практичне значення отриманих у роботі результатів виявляється у їхній конкретній застосовності для покращення стратегій управління репутаційними ризиками та інформаційною безпекою підприємства. Зокрема, розробка оптимальних стратегій управління репутаційними ризиками стає можливою завдяки глибокому аналізу функціонування компанії та її взаємодії зі стейкхолдерами.

Отримані дані сприяють визначенню ефективних підходів до взаємодії з громадськістю та розробки комунікаційних стратегій для управління репутацією. Також вони дозволяють підвищити рівень обізнаності персоналу щодо репутаційних ризиків та ефективно впроваджувати запропоновані технології управління ризиками в конкретних умовах підприємства.

Такий практичний підхід до отриманих результатів сприяє їх активному впровадженню в бізнес-процеси, підвищуючи загальний рівень інформаційної безпеки та доводячи до ефективного управління репутаційними ризиками на підприємстві.

Апробація результатів проводилася на ряді конференцій та форумів з питань кібербезпеки та управління ризиками.

РОЗДІЛ 1
УПРАВЛІННЯ РЕПУТАЦІЙНИМИ РИЗИКАМИ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

1.1 Поняття «інформаційні активи» та «репутація»

Підтримка інформаційної безпеки в умовах сучасного конкурентного ринку є необхідною умовою для ефективного функціонування більшості компаній. Для досягнення цього необхідно передбачати можливі ризики заздалегідь, щоб мінімізувати ймовірність виникнення проблем, пов'язаних з ними. Це означає, що важливо навчитися ефективно управляти цими ризиками.

Управління ризиками інформаційної безпеки - постійний процес, який не повинен перериватися або зупинятися, оскільки це може значно вплинути на функціонування корпоративної інформаційної системи. Основні завдання включають виявлення, оцінку та зменшення ризиків витоку особистих даних та комерційної інформації. Правильне управління IT-ризиками дозволяє отримувати реальну картину рівня захисту даних, виявляти найбільш критичні аспекти і раціонально визначати оптимальні витрати на інформаційну безпеку.

Ефективне управління ризиками інформаційної безпеки вирішує ряд важливих завдань. Зокрема, воно дозволяє створити модель взаємодії бізнес-процесів та IT-інфраструктури для ідентифікації ключових активів і оцінки пов'язаних з ними ризиків. Також, під час управління можна точно прогнозувати та виявляти потенційні загрози і порушення інформаційної безпеки. У процесі управління IT-ризиками можна розробити комплекс заходів для зменшення ймовірності виникнення ІБ-ризиків і розробити план з їх подальшого зниження. Крім того, правильне управління допомагає провести оцінку остаточних ризиків після впровадження заходів щодо їх попередження та мінімізації.

Визначення основних та допоміжних активів при управлінні ризиками

інформаційної безпеки є ключовим завданням. Ризик у бізнесі визначається як можливість виникнення збитків у випадку його реалізації. Зазначимо, що ці збитки можуть бути не лише матеріальними, а й непрямими, такими як втрачена вигода або невтрачені доходи, які могли б виникнути в ході господарської діяльності підприємства.

У випадку порушення інформаційної безпеки, компанії можуть зазнати настільки серйозних втрат, що це може призвести до значного погіршення їх позиції на ринку та навіть банкрутства. Тому контроль інформаційних ризиків важливий для всіх, хто прагне продовжувати успішну бізнес-діяльність. Кожна компанія має свої основні ресурси, які вважаються головними категоріями активів. Активом може бути все, що вкладається в ключові цінності фірми та сприяє отриманню прибутку і збереженню коштів.

Активи поділяються на фінансові, матеріальні, людські та інформаційні.

Поділ на фінансові, матеріальні, людські та інформаційні активи надає комплексне уявлення про різноманітні ресурси, які підтримують бізнес-процеси. Нижче наведено табл. 1.1 з розподілом активів підприємства.

Таблиця 1.1

Активи підприємства

Назва активу	**Склад активу**	**Опис**
Фінансові активи	Грошові кошти	Готівка та грошові еквіваленти, які належать підприємству
	Цінні папери	Акції, облігації та інші фінансові інструменти, які приносять дохід
Матеріальні активи	Нерухомість	Земля та будівлі, які володіє підприємство
	Обладнання та техніка	Машини, інструменти, комп'ютери та інші матеріальні засоби виробництва
Людські активи	Персонал	Кваліфіковані та навчені працівники, які приносять внесок у розвиток підприємства
	Навчальні та розвиваючі програми	Інвестиції в освіту та розвиток персоналу.
Інформаційні активи	Дані та інформація	Ключові бізнес-дані, клієнтська інформація, стратегічні плани
	Системи та програмне забезпечення	Інформаційні системи, програми та технології

Джерело: [5]

Міжнародні стандарти також визначають агреговані активи – це процеси, які оперують іншими активами, щоб досягти цілей компанії.

Агреговані активи в контексті міжнародних стандартів визначаються як процеси та системи, які використовують інші активи в організації для досягнення стратегічних цілей компанії. Цей підхід покликаний враховувати взаємодію та взаємозалежність різних активів у структурі підприємства, спрямованих на ефективне функціонування та забезпечення стійкого розвитку.

Агреговані активи включають в себе не лише фізичні ресурси, такі як обладнання чи техніка, але й процеси, які управляються та координуються з використанням інформаційних технологій та людського капіталу. Ці активи мають сприяти вдосконаленню операцій, зменшенню ризиків, а також підвищенню ефективності діяльності підприємства.

Ключові характеристики агрегованих активів:

Взаємозалежність: Агреговані активи взаємодіють та підтримують один одного, сприяючи цілеспрямованому використанню ресурсів.

Інтеграція процесів: Ці активи включають інтеграцію різноманітних бізнес-процесів для забезпечення оптимального функціонування підприємства.

Орієнтованість на стратегії: Агреговані активи орієнтовані на досягнення стратегічних цілей компанії та визначають, які ресурси та процеси важливі для успішного виконання стратегії.

Використання технологій: Залучення сучасних інформаційних технологій для управління та координації агрегованих активів для підвищення продуктивності та конкурентоспроможності.

Зорієнтованість на результат: Агреговані активи спрямовані на досягнення позитивних результатів, включаючи збільшення ефективності операцій, підвищення якості продукції та реагування на зміни на ринку.

Імідж компанії та її репутація стають все більш цінним активом для бізнесу. Їх називають інформаційними активами, оскільки образ та ділова репутація представляють собою важливу інформацію про організацію.

Імідж компанії – це візуальне та емоційне уявлення про неї, яке формується у

свідомості споживачів, партнерів та інших зацікавлених сторін. Цей імідж визначається рядом факторів, але основними серед них є інформація, яку компанія комунікує через свою діяльність та взаємодії з оточуючим середовищем.

Імідж компанії формується такою інформацією:

1. Бренд і логотип: Графічні елементи, які найчастіше асоціюються з компанією, створюючи визуальний образ.

2. Маркетингові комунікації: Реклама, просування, участь у подіях, які допомагають створювати позитивне враження.

3. Соціальні мережі та онлайн-присутність: Відгуки, рецензії, та активність у соціальних мережах формують публічну думку.

4. Продукція та послуги: Якість та властивості товарів і послуг компанії впливають на уявлення споживачів.

5. Корпоративна культура: Спосіб, яким працівники компанії взаємодіють між собою та з клієнтами, визначає її корпоративний образ.

Ділова репутація визначається сприйняттям громадськістю та стейкхолдерами діяльності компанії. Це надто важливий інформаційний актив, оскільки впливає на відносини з клієнтами, інвесторами, партнерами та іншими учасниками ринку. Якість ділової репутації визначається наступною інформацією:

Етика та корпоративна відповідальність: Споживачі та партнери оцінюють компанію за її дотримання етичних стандартів та соціальної відповідальності.

Фінансова стабільність: Інформація про фінансовий стан компанії та її здатність виконувати фінансові зобов’язання впливає на репутацію.

Якість обслуговування та взаємодія з клієнтами: Корпоративна репутація значно залежить від того, як компанія вирішує проблеми клієнтів та надає послуги.

Інновації та розвиток: Оцінка за інноваційність та здатність до постійного розвитку впливає на сприйняття компанії як лідера ринку.

Репутація є ключовим інформаційним активом, оскільки вона може визначати успіх або невдачі компанії на ринку. Вона створюється та утримується через об’єктивну та суб’єктивну інформацію, яка формується в процесі взаємодії компанії з її оточуючим середовищем. Ефективне управління інформацією, що впливає на

ділову репутацію, може сприяти підвищенню конкурентоспроможності та довіри до бренду компанії.

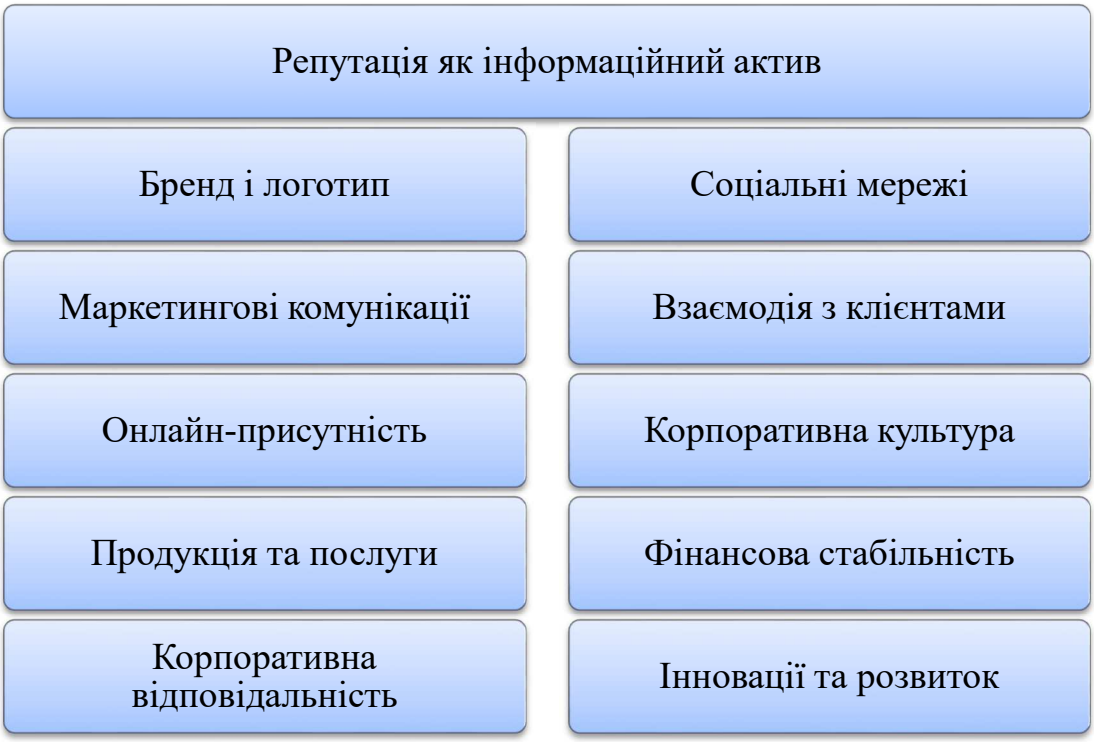

Рис. 1.1. Інформаційні активи підприємства

Джерело: узагальнено за даними [2]

Після аналізу інформаційних ризиків стає зрозуміло, що вони вимагають уваги, оскільки розголошення деякої інформації може негативно вплинути на бізнес.

Для успішного бізнесу важливо враховувати фактори, які можуть негативно впливати на будь-який цінний актив, що є своєрідними ризиками. Проблеми з доступом до Інтернету чи несправності комп'ютерної техніки можуть знизити ефективність захисту даних. Неправильна робота сервісів може негативно позначитися на відношенні клієнтів, псувати ділову репутацію та призводити до збитків. Враховуючи ці чинники, слід дуже серйозно підходити до обслуговування ІТ-інфраструктури та підтримки ІБ.

Для організацій важливі як первинні, так і допоміжні активи. Первинні – це ресурси, без яких фірма не може вести свою діяльність. Це матеріальні (наприклад, нерухомість, земля, обладнання) та фінансові (страхування, кредити, інвестиції) активи. Деякі види бізнесу напряму залежать від рівня компетентності персоналу

(навчання, консультування, аудит) та активів інформаційних технологій (створення програм, інтернет-магазини тощо).

Ризики для таких активів можуть призвести до значних збитків або навіть призвести до руйнування бізнесу. Щодо допоміжних активів, їх ризики відображають собою втрати, які можна відшкодувати в майбутньому. Такі ризики вважаються менш важливими при управлінні ризиками. Однак, що стосується ризиків, пов'язаних з первинними активами, до них слід підходити з великою увагою. Часто управління допоміжними активами довіряється компаніям-аутсорсерам, оскільки цей підхід сприяє підвищенню ефективності управління в цілому.

Експерти виділяють три основні методи управління інформаційною безпекою, які відрізняються рівнем глибини і формалізації. Вибір конкретного методу залежить від того, наскільки важлива для компанії інформаційна безпека. Якщо інформаційні активи є допоміжними для організації, то оцінка ризиків може не бути високою пріоритетом. Для таких компаній більш відповідним є збереження базового рівня інформаційної безпеки, який відповідає актуальним стандартам та враховує досвід, включаючи досвід конкурентів.

Підприємства, де інформаційні активи не є основними, але мають велику кількість інформаційних бізнес-процесів, обов'язково повинні проводити оцінку ризиків. У таких випадках можна використовувати менш формальний підхід, зосереджуючись на виявленні «вузьких місць» в безпеці.

Якщо інформаційні активи є основою бізнесу, то ризики в цьому випадку вважаються ключовими. Для оцінки таких ризиків застосовують формальний підхід і кількісні методи.

Часто компанії вважають різні види активів однаково цінними. Так, при створенні програмного забезпечення важливими є як інформаційні, так і трудові активи. Раціональний підхід з багаторівневою оцінкою ризиків ІБ може виявити найбільш вразливі компоненти корпоративної інфраструктури та найбільш критичні для бізнесу ризики [2].

Всі повинні мати розуміння того, що це не питання «чи», а «коли» підприємство буде скомпрометоване.

Тому для цього треба гтуватися, підхід до кіберзабезпечення передбачає розміщення захисту навколо ключових активів, оскільки це саме ті активи, які найважливіші для організації. Функції реагування та відновлення щодо загроз в Національному інституті стандартів і технологій у галузі кібербезпеки є двома областями низької зрілості для багатьох організацій. Однак важливо розуміти, що, коли вашу організацію атакують, планування та реагування буде вирішальним.

Нещодавні порушення також показали, що організаціям потрібно зосередитися на нематеріальних активах, а саме на репутації організації.

Що важливо відразу визначити, це те, що порушення даних миттєво створить ризики для репутації організації. Те, як організація реагує на це порушення, або, можливо, як зовнішні зацікавлені сторони сприймають реакцію організації, має вирішальне значення.

«Репутація – це загальна оцінка організації її зацікавленими сторонами. Це агреговані сприйняття зацікавленими сторонами здатності організації виконати їхні очікування, чи ці зацікавлені сторони зацікавлені у покупці продуктів компанії, працевлаштуванні в компанії чи інвестуванні в акції компанії».

Глобальне дослідження управління ризиками Aon за 2019 рік показало, що серед ключових ризиків і викликів, з якими зараз стикаються організації, «шкода репутації/бренду» була другою, а «кібератака» — шостою [5].

Огляд Deloitte 2014 року з ризиків репутацій повідомляв, що фізична безпека та кібербезпека, які ми знаємо, що взаємно пов’язані, були вказані як один із ключових чинників ризику репутації серед керівників, які брали участь у опитуванні. Хоча ці дані дещо застарілі, і підтверджені наслідками кількох порушень за останні кілька років, зрозуміло, що на тлі теперішніх подій та інформаційних війн, відповіді керівників в 2021 році були б такими ж [3].

Однак цей ризик, ймовірно, не обмежений лише короткостроковими впливами. Звіт Aon і Pentland Analytics «Ризик репутації в кібер-добу» вказує, що вплив на репутацію може бути довгостроковим. Звіт підкреслює, що кібератака має значний вплив на акції компаній, і деякі звітували про зниження їхньої вартості навіть через рік після кібератаки. Дані надають можливість впливати на управління, не лише

демонструючи репутаційний вплив кібератаки, але й фінансові наслідки [4].

Прогностичне управління кіберзахистом базується на постійному оцінюванні ризиків організації, яке визначає підхід та управління їхніми оборонами. Це правда для всіх організацій, незалежно від їхнього розміру, місця розташування, галузі або обороту.

Одна область, яка, можливо, не завжди явно включена, - це те, як організація реагуватиме на кібератаку. Якщо це виконано погано, це може мати реальні, негативні наслідки для репутації, а також подальших вторинних і третинних ефектів. Це вимагає, щоб організація розробила відповідний план реагування в разі кіберподії, оскільки одним з найважливіших факторів, які впливають на репутацію організації, є те, як вважається, що вона реагує на подію – створення сприйняття прозорості та чесності тут, ймовірно, ключове.

Безперечно, будь-яке повідомлення та інформація, що поширюються підприємством має бути сильно підкріплена справжністю подій. Важливо – вживати заходів для мінімізації впливу негативної інформації на роботу та імідж підприємства, уникати порушення позитивного сприйняття організації наскільки це можливо. Організація повинна повністю повідомити про кроки, які вона вживає для мінімізації впливу події на своїх зацікавлених сторін та, в кінцевому рахунку, для відновлення довіри та впевненості в організації. Якщо не вдасться вберегттися від заплямування репутації, цілком можливо, що позитивне сприйняття компанії так і не вдасться відновити повністю, оскільки антиреклама спрацбовує глибше та швидше.

Важливо вчитися на прикладах минулого, розуміти і дотримуватися правових зобов’язань, наприклад, в рамках Загального регламенту з питань захисту даних (GDPR). GDPR вводить зобов’язання для організацій повідомляти про порушення даних відповідному наглядовому органу протягом 72 годин з моменту виявлення порушення. У випадку Великої Британії за Законом про захист даних 2018 року цей звіт повинен бути поданий в Інформаційний комісаріат (ICO).

Використаємо TalkTalk як історичний приклад. Представники ICO заявили, що кібератаку та витік даних, яких зазнала TalkTalk у жовтні 2015 року, можна було

б запобігти, якби TalkTalk вжив основних заходів для захисту інформації клієнтів. Наслідки для компанії були ширшими, ніж просто вплив на безпеку.

У жовтні 2016 року Злата Родіонова в The Independent повідомила, що за рік після кібератаки прибуток TalkTalk скоротився більш ніж удвічі, при цьому прибуток до оподаткування впав з 32 мільйонів фунтів стерлінгів у попередньому році до 14 мільйонів фунтів стерлінгів. Таким чином, можна стверджувати, що кіберзлам негативно вплинув на довіру клієнтів, які потім, ймовірно, змінили свого постачальника на постачальника з кращою репутацією.

Витік даних Mumsnet у 2019 році – це інша історія. Веб-сайт пишається конфіденційністю своїх учасників, головним чином тому, що теми, які обговорюються на сайті, можуть бути особливо делікатними або особистими. Декілька користувачів попередили веб-сайт про те, що під час входу вони можуть отримати доступ до чужого облікового запису – проблема, яка виникала, коли два користувачі входили в систему одночасно.

Mumsnet, мабуть, вжив правильних дій у цій ситуації: він попередив своїх користувачів про проблему, скасував оновлення програмного забезпечення, які спричинили проблему, вийшов із усіх користувачів із їхніх облікових записів (примусивши їх увійти знову та, отже, скасувавши будь-який нелегітимний доступ до іншого обліковий запис) і повідомили про себе ICO [1].

Незважаючи на те, що Mumsnet зазнала, мабуть, меншого зламу, ніж той, який зазнав TalkTalk, і той факт, що це було випадково, а не зловмисно, різні реакції компаній заслуговують на увагу. Mumsnet був набагато прозорішим у своєму підході та швидким у своїх діях, що мінімізувало будь-який вплив на його репутацію.

Першим кроком для мінімізації ризику витоку даних є розуміння ризиків, з якими стикається організація. Як правило, найкраще почати з оцінки ризику, використовуючи визнаний стандарт або структуру, щоб зрозуміти області низької зрілості, які потребують уваги. Дуже важливо розуміти загрози для організації, критичні активи організації (які можуть бути фізичними чи інформаційними) і вразливість організації.

Як завжди, було б нерозумно стверджувати, що атаки можна уникнути, для

організації було б помилкою не вживати заходів обачності, не запровадити протекційні заходи. Як згадувалося вище, будь-якій організації необхідно не лише керувати кіберризиками, виявляти й пом'якшувати ризики, але й постійно проводити оборонні кібероперації. Іншими словами, для постійного моніторингу мережі та реагування на події безпеки, щойно вони відбуваються.

Інформаційна безпека, кібербезпека, кіберстійкість або забезпечення кібермісії не повинні бути просто функцією відділу безпеки. Безпека є обов'язком кожного працюючого та дотичного до функціонуючого підприємства.

Процеси кібербезпеки мають бути вбудовані в бізнес-процеси та пояснюватися таким чином, щоб працівники їх розуміли та дотримувалися. Співробітників потрібно стимулювати та заохочувати дотримуватись процесів безпеки, і вони повинні розуміти переваги цього – або, можливо, наслідки, якщо їх не робити.

Найефективнішими засобами кіберзахисту завжди будуть ті, які концентрують ресурси там, де вони потрібні. Важливо, щоб будь-яка організація зосереджувалася як на людському, так і на технічному вимірі.

1.2. Репутаційні ризики та їх вплив на інформаційну безпеку компанії

Роль репутації в галузі інформаційної безпеки, як ми переконалися із вищевикладеного, зростає, власники та керівництво усвідомлюють, що втрата репутації є великою загрозою для бізнесу, але інколи перебуває не у полі уваги підприємства, оосбливо з точки зору технічної команди.

Однією з найбільших загроз, пов'язаних з ризиком репутації, є непередбачуваність. Вона може буквально з'явиттися неочікувано, і часто без сигналів та попереджень, не відслідковується. У таких випадках репутаційна шкода може бути руйнівною для організації, залежно від ступеня її тяжкості. Репутаційні ризики включають різні аспекти, які можуть негативно вплинути

на сприйняття та оцінку компанією своїх клієнтів, партнерів, інвесторів та громадськості загалом. Інформаційна безпека грає ключову роль у забезпеченні та управлінні цими ризиками. Ось кілька видів репутаційних ризиків, інформаційна безпека яких є критичною:

Витік конфіденційної інформації:

Ризик: Несанкціонований доступ чи витік конфіденційної інформації, такої як особисті дані клієнтів чи внутрішні плани компанії.

Значення для репутації: Витік конфіденційної інформації може спричинити втрату довіри з боку клієнтів, інвесторів та інших стейкхолдерів, що негативно вплине на репутацію компанії.

Кібератаки та порушення безпеки:

Ризик: Атаки на інформаційні системи, включаючи хакерські атаки, віруси та інші зловмисні дії.

Значення для репутації: Успішні кібератаки можуть призвести до втрати довіри споживачів та інвесторів, а також нанести шкоду репутації у великому масштабі.

Несприятливі події в інтернеті:

Ризик: Негативний вплив від відгуків, коментарів чи новин, що поширюються в інтернеті.

Значення для репутації: Негативна інформація в інтернеті може швидко поширюватися та впливати на відносини з клієнтами і рішення інвесторів.

Неадекватне управління кризою:

Ризик: Невідповідне реагування на кризові ситуації або відсутність планів управління кризою.

Значення для репутації: Інтенсивні кризові ситуації можуть вимагати ефективного управління та взаємодії зі стейкхолдерами для мінімізації впливу на репутацію.

Інформаційна безпека стає важливою для захисту від цих ризиків, оскільки вона допомагає уникати витоку конфіденційної інформації, захищати системи від кібератак, моніторити онлайн-активність та ефективно управляти

кризовими ситуаціями. Забезпечення інформаційної безпеки не лише допомагає уникнути потенційних загроз, а й підтримує довіру та позитивний імідж компанії, що впливає на її репутацію та ринкову вартість.

Класифікація ризиків становить важливий інструмент управління, який допомагає підприємствам ефективно ідентифікувати, аналізувати та управляти різноманітними загрозами. Вона грає ключову роль у систематизації ризиків, роблячи їх менш складними для сприйняття та керування. Вона також дозволяє визначати ризики за різними параметрами, такими як їх джерело, вплив, часовий характер чи фінансові наслідки. Такий підхід допомагає підприємствам краще розуміти природу ризиків та приймати обгрунтовані рішення для їх управління.

Об’єктивні та суб’єктивні ризики можуть бути розрізнені завдяки класифікації. Об’єктивні ризики, які можна виміряти та кількісно оцінити, дозволяють більш точно прогнозувати їхні наслідки. Суб’єктивні ризики, які ґрунтуються на особистих оцінках та враженнях, можуть бути піддані детальному аналізу для зменшення ступеня невизначеності.

Іншим важливим аспектом є визначення ризиків за джерелами їх виникнення та видами втрат. Класифікація допомагає ідентифікувати конкретні сценарії, які можуть призвести до фінансових чи нефінансових втрат.

Залежно від ступеня зміни ризиків у часі, їх можна розділити на статичні та динамічні. Це важливо для врахування того, як ризики можуть змінюватися під впливом зовнішніх чинників чи внутрішніх процесів.

У контексті репутаційних ризиків, які можуть виникати як зовнішні, так і внутрішні, класифікація дозволяє зосередитися на конкретних джерелах інформації та виділяти основні напрямки управління цими ризиками.

Таблиця нижче надає огляд різних аспектів класифікації репутаційних ризиків підприємства. Ця класифікація допомагає систематизувати та визначити основні характеристики ризиків для подальшого аналізу та управлін

Таблиця 1.2

Класифікація репутаційних ризиків підприємства

Класифікаційна ознака	**Види репутаційних ризиків**
За сферою виникнення ризиків	Зовнішні
	Внутрішні
За точністю оцінки ризиків	Об’єктивні
	Суб’єктивні
За ступенем зміни ризику в часі	Статичні
	Динамічні
За видом втрат	Фінансові
	Нефінансові
За видом стейкхолдерів, які розповсюджують негативну інформацію	Клієнти
	Партнери
	Співробітники
	Акціонери
	Владні структури
	Журналісти
	Суспільство
За джерелом отримання негативної інформації	Різні види стейкхолдерів як джерела інформації
	ЗМІ-ТВ, радіо, газети, журнали
	Інтернет
	Офіційні матеріали підприємства

Джерело: [55]

Ризик репутації може загрожувати навіть найбільшим і найкраще керованим підприємствам, знищуючи мільйони або мільярди доларів ринкової капіталізації або майбутні прибутки.

Останній Звіт компанії IBM про вартість порушення даних 2021, який узагальнює незалежні дослідження Понемона Інституту, звертається до вартості втрат бізнесу в результаті порушення даних, що тісно пов'язано з втратою репутації. Згідно з цим дослідженням [11], дії, пов'язані із втратою бізнесу в результаті порушення даних, включають:

- Збільшення обороту клієнтів
- Відмова системи, що призводить до втрати доходів
- Зусилля отримати новий бізнес зі зіпсованою репутацією.

Дані з кожним роком набувають все більшої ваги, та відповідно їх витоки коштують компаніям все більше і більше. У середньому ціна витоку даних по всьому світу дорівнює $4,24 млн.

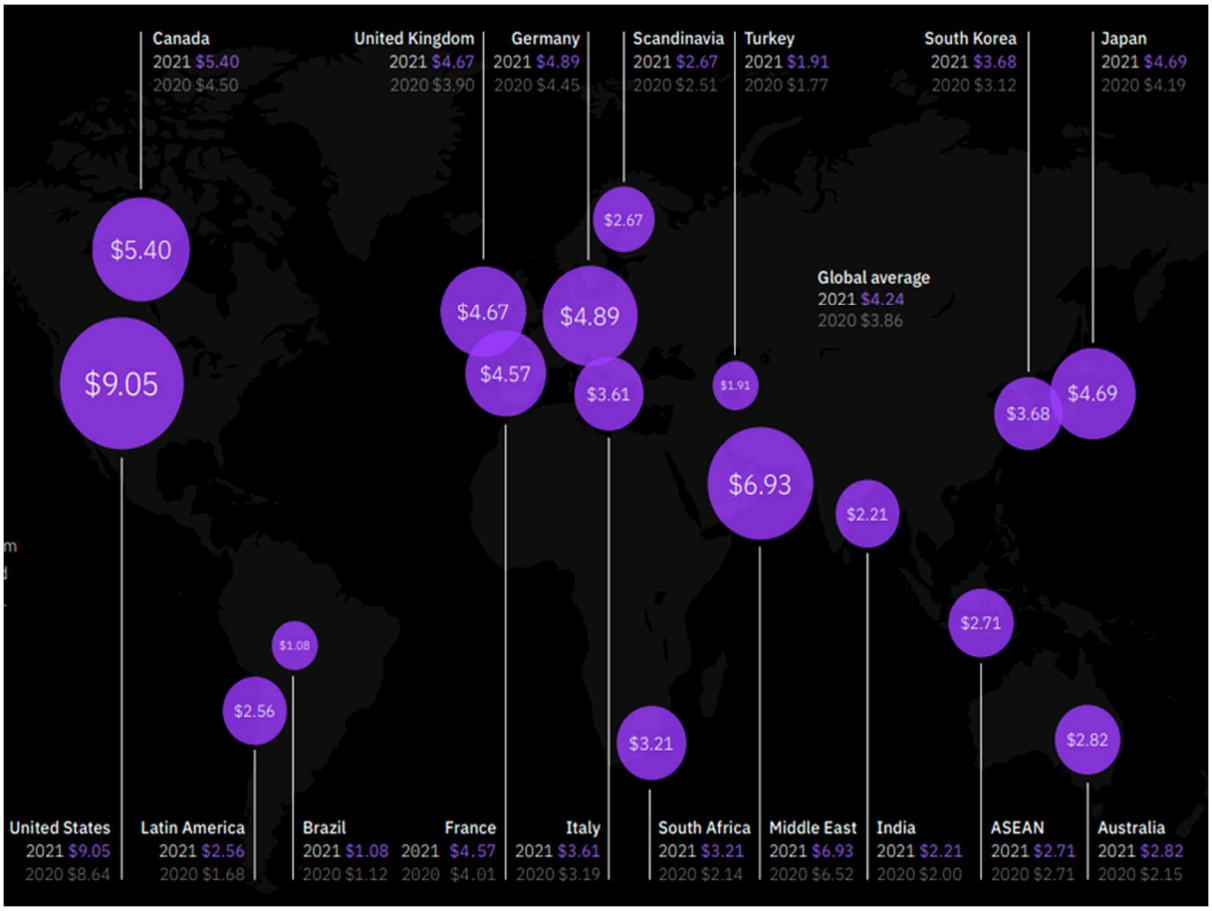

Рис. 1.2. Середня загальна вартість (млн дол.) витоку даних за країнами та регіонами

Джерело: [11]

За результатами досліджень також було наведено інфографіку середнього часу, який було витрачено на виявлення та локалізацію порушення залежно від початкового вектора атаки.

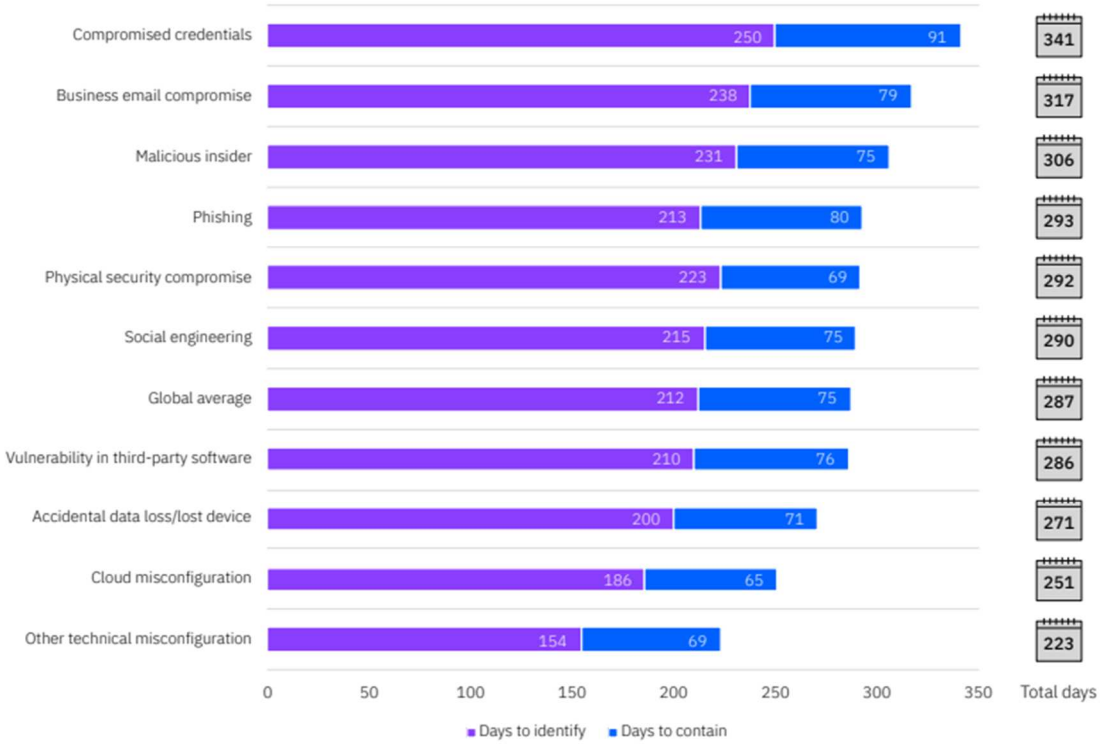

Рис. 1.3. Середній час (в днях) на виявлення і локалізацію порушення

Джерело: [10]

Порівняно з іншими факторами, такими як виявлення та ескалація, сповіщення, реагування після витоку, втрачений бізнес став найбільшим фактором витрат, на який припадає майже 38% середньої загальної вартості витоку даних у звіті за 2021 рік. .

Кіберризик - це будь-який ризик з цифрового світу, включаючи збитки репутації компанії від фінансових втрат, операційних розладів та впливу порушень даних. Кіберризик може виникнути різними способами, включаючи:

- Прориви для отримання несанкційного доступу до інформаційних систем
- Ненавмисні або випадкові порушення безпеки
- IT-ризики через фактори, такі як неправильна конфігурація або низька цілісність

Хоча причина кіберпрориву - це більш широка тема, яку потрібно розглядати, наслідки репутаційної шкоди невідомі, і в багатьох випадках це призводить до втрати бізнесу.

Як приклад, порушення даних від Target у 2013 році, яке сталося через те, що злочинці отримали доступ до постачальника послуг в цифровому ланцюжку постачання компанії. Порушення тривало з 27 листопада по 15 грудня 2013 року і, нарешті, виявило особисті дані 110 мільйонів клієнтів.

Target виявили порушення протягом 16 днів і повідомили громадськість про це через 20 днів після виявлення. Багато хто поклав вину на Target за час, який вони витратили на розкриття події громадськості.

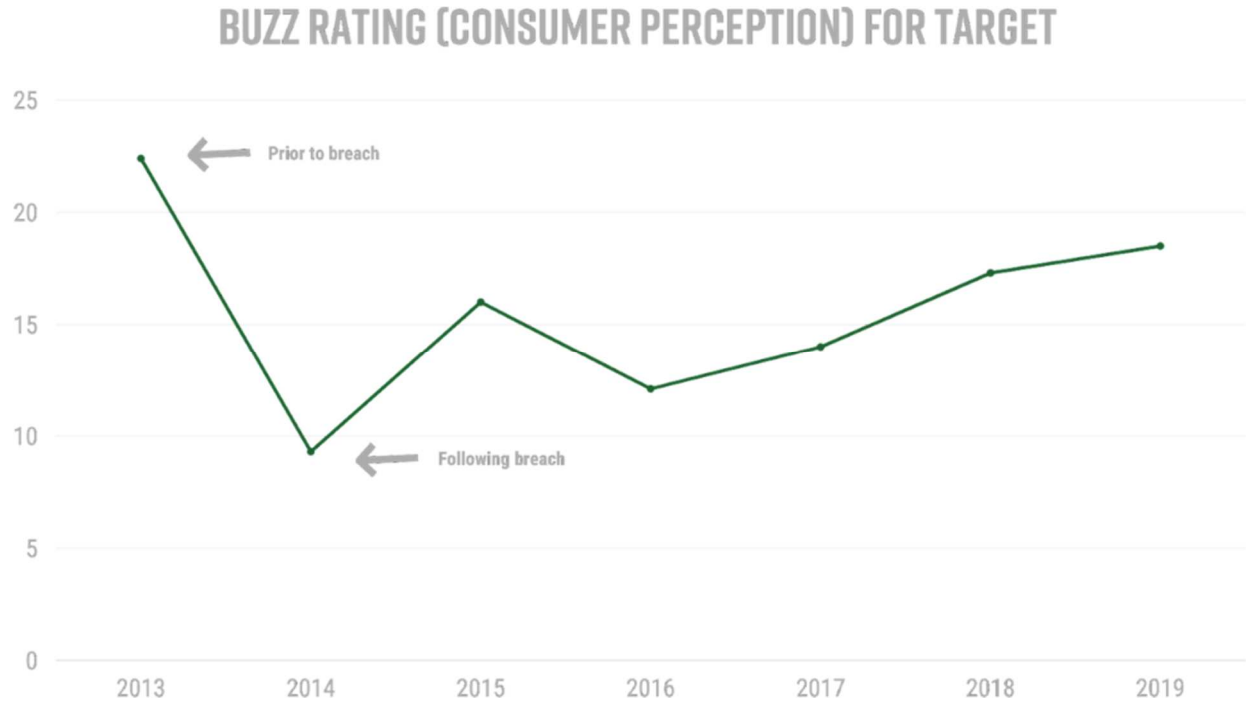

Рис. 1.4. Рейтинг шуму (сприйняття споживачами) для Target

Джерело: [10]

Графік вище базується на відповідях респондентів, які відповіли на запитання BrandIndex: "Якщо ви чули щось про бренд протягом останніх двох тижнів через рекламу, новини або із вуста в вуста, чи було це позитивним чи негативним?" Оцінки є чистими балами, розрахованими шляхом віднімання негативних відсотків і позитивних відсотків для кожного бренду.

Після того як порушення стало відоме громадськості, багато клієнтів відмовилися від REDcards та перестали робити покупки. Як видно з графіка BrandIndex вище, сприйняття клієнтів впало на 54,6% у рік після порушення даних [10].

Порушення Target було одним із найбільших на той час, викликаючи розмову про захист POS-систем, безпеку даних клієнтів і багато інших питань, часто ігнорованих у минулому. Через п'ять місяців після порушення Target опублікував перелік заходів [9] щодо безпеки, який включав у себе підвищений моніторинг і логування, впровадження сегментації, перегляд та обмеження доступу постачальників та підвищену безпеку облікових записів.

Хоча Target вдалося підняти свою невигідну репутацію, їх бренд у 2019 р. все ще на 18% нижче, ніж у 2013 р.

Ще одне значуще порушення варто розглянути - це Uber у 2016 році. Uber вирізняється тим, що спочатку не повідомив про деталі порушення, а замість цього спробував замести сліди, виплативши винагороду. Таким чином, Uber пошкодив свої стосунки з клієнтом, втративши довіру і вірогідність.

Під час першого витоку даних у 2016 році до рук зловмисників потрапила особиста інформація 57 мільйонів користувачів Uber, а також дані водійських прав 600 000 водіїв Uber. Однак замість того, щоб негайно повідомити про порушення та попередити постраждалих, Uber заплатив хакерам 100 000 доларів, щоб «позбутися інформації», дозволивши деталям залишатися прихованими до 2017 року.

Подібні випадки змушують до крайніх дій і наслідків, щоб відновити стосунки та відновити довіру. Тодішній генеральний директор Тревіс Каланік і Джо Салліван, головний керівник Uber, покинули свої посади після того, як стало відомо про масштаби порушення.

Генеральний прокурор Каліфорнії Ксав’єр Бесерра добре резюмував це [7]: «Рішення Uber приховати порушення було відвертим порушенням довіри громадськості».

Для порівняння з Target, у якого за рік після зламу сприйняття клієнтами впало на 54,6 відсотка, у Uber було колосальне падіння на 141,3 відсотка [10] після розкриття злому в 2017 році.

Злам Target — це приклад використання для демонстрації наслідків витоку даних і того, як це може вплинути на репутацію. Це також показує, як

організації можуть не справлятися з репутаційним ризиком, просто реагуючи на кіберподії та зміцнюючи зламані активи.

Організаціям слід застосовувати проактивний підхід до управління репутаційними ризиками так само, як і до управління ризиками постачальників. Репутаційний ризик може бути визначений кількісно та адекватно регулюватися компанією. Така методологія може допомогти менеджерам краще визначати поточні та майбутні ризики для репутації їхнього бізнесу, а також визначити, чи прийняти певний ризик чи вжити заходів для його уникнення чи пом’якшення.

1.3 Взаємозв’язок: забезпечення інформаційної безпеки – управління репутаційними ризиками – капітал бренду

Здатність компанії захищати дані може безпосередньо вплинути на те, чи клієнти довіряють організації та залишаються лояльними з часом. Відповідно до звіту Shred-it’s Data Protection Report за 2021 рік [13], понад 8 із 10 споживачів вирішують, з якими компаніями вести бізнес, ґрунтуючись на їхній репутації у сфері інформаційної безпеки. Частково це пояснюється тим, що споживачі менш впевнені в безпеці своїх персональних даних, ніж десять років тому, і у них є підстави для цього. Майже 70% опитаних споживачів особисто постраждали від витоку даних у 2021 році порівняно з 53% у 2020 році.

На жаль, споживачі, як правило, не довіряють бізнесу та безпеці даних. Кожен третій споживач вважає, що компаніям не вдається своєчасно прозоро повідомити про витік даних, і існує загальна думка, що ці інциденти виявляються лише тоді, коли компанію спіймають або вимушено розкривають подію.

Довіра може швидко зруйнуватися, якщо організація зазнає зламу, але

не впорається з ним належним чином. Хоча споживачі можуть почекати і побачити, як компанія відреагує на помилку безпеки, перш ніж приймати будь-які рішення щодо своїх майбутніх відносин з організацією, люди можуть вирішити розірвати зв’язки, особливо якщо вони вважають, що організація не була прозорою та належним чином реагувала. Майже 1 з 4 споживачів припинить співпрацю з компанією, якщо його особисту інформацію буде скомпрометовано.

За останнє десятиліття закони та нормативні акти щодо захисту даних розвивалися, щоб стримувати злочинців і змушувати компанії покращувати свої зусилля щодо безпеки та конфіденційності. Витрачати час на розуміння поточного нормативного ландшафту має вирішальне значення не лише для задоволення існуючих вимог, але й для підготовки до того, що буде на горизонті.

У всьому світі багато країн уже мають широкомасштабне законодавство про конфіденційність, включаючи Канаду, Великобританію та Європейський Союз. Якщо компанія працює на міжнародному рівні, вона також повинна знати про ці вимоги, оскільки країни продовжують регулярно приймати нове або оновлювати існуюче законодавство.

Перший крок у створенні повного плану безпеки даних — це знати, які типи даних збирає компанія, де вони зберігаються, з ким і як ними ділиться. Далі компанія повинна визначити потенційні ризики для цих даних і визначити, чи зберігається інформація в електронній чи фізичній формі (або в обох).

Ризики для електронних даних включають компрометацію або втрату через зловмисне програмне забезпечення, фішинг, крадіжку або людську помилку. Фізичні ризики можуть бути схожими й виникати внаслідок крадіжки паперових документів або обладнання, на якому зберігається конфіденційна інформація, як-от ноутбуки, зовнішні носії інформації, мобільні телефони тощо. Коли компанія дізнається, які дані вона має та ризики, які загрожують цим даним, він може визначити відповідну

комбінацію заходів безпеки та контролю.

Щоб захистити фізичні дані, компаніям слід розглянути можливість використання служби знищення документів через регулярні проміжки часу, щоб отримати та безпечно знищити конфіденційну інформацію, яка більше не потрібна. Подібним чином він може застосувати процес збору та знищення застарілих жорстких дисків або ноутбуків, які не використовуються.

Щоб захистити електронні дані, компанії знадобиться потужна програма кібербезпеки, яка охоплює технології, бізнес-процеси та, звичайно, людей, які ними користуються. З цією метою важливо доповнювати навчання практикою, наприклад симуляцією фішингу, яка допомагає співробітникам краще розпізнавати загрози та розвивати «м'язову пам'ять», щоб уникати їх і повідомляти про них. Сучасні викрадачі даних є набагато досвідченішими та постійно вдосконалюються. З цієї причини важливо переконатися, що всі співробітники повністю розуміють свої ролі та обов'язки щодо захисту даних компанії.

Враховуючи поточне гібридне робоче середовище, особливо важливо забезпечити персоналу доступ до інструментів, необхідних для підтримки безпеки даних, коли вони працюють віддалено — у домашньому офісі чи громадському місці.

Впровадження стратегій захисту даних, таких як вимога використання віртуальних приватних мереж (VPN) і багатофакторної автентифікації, може зменшити ризик компрометації або крадіжки, незалежно від того, звідки входить співробітник. З точки зору фізичної безпеки, подумайте про навчання співробітників, які працюють віддалено надійно зберігати документи в закритій шафі або в іншому безпечному місці, доки вони не зможуть повернути їх до офісу, щоб помістити в безпечні контейнери для знищення.

Безпека даних є ключовим елементом утримання клієнтів, і компанії повинні використовувати багатогранний підхід до захисту інформації. Звертаючи увагу як на фізичні, так і на цифрові ризики та впроваджуючи стратегії їх зменшення, компанія може уникнути дорогих порушень, які

можуть мати наслідки протягом багатьох років.

Однією з найбільших поточних загроз для репутації організації є витік даних. Очікується, що компанії захищатимуть особисті дані своїх клієнтів, тому інцидент із безпекою може вплинути на громадські настрої щодо організації. Ця хвиля негативу та втрати репутації може призвести до того, що клієнти розірвуть зв’язок із компанією. Мало того, репутація бренду впливає на те, чи зможе він залучити найкращих талантів або постачальників, а також впливає на їхні ділові партнерства. Таким чином, успішна кібератака безпосередньо впливає на кінцевий результат[12].

Оскільки все більше компаній переводять свою інфраструктуру на хмарні системи, зростає загроза інциденту кібербезпеки. Багато компаній покладаються на застарілу мережеву інфраструктуру та процеси або використовують застаріле та вразливе програмне забезпечення. У нещодавньому звіті Deloitte про управління ризиками генерального директора та правління [15] було проведено опитування 400 генеральних директорів та членів правління щодо того, як вони визначають пріоритетність інвестицій у певні сфери ризику. З цих 400 41% назвали «безпеку, включаючи фізичні та кіберзломи» найбільшою загрозою для своєї репутації

Багато програм кібербезпеки зосереджені на традиційній перспективі інвестування в технології запобігання. Однак Інтернет речей (IoT) і штучний інтелект (AI) становлять величезний ризик для організацій. Навіть компанії, які запровадили плани забезпечення безперервності бізнесу та аварійного відновлення, не обов’язково стійкі до нових загроз. Крім того, багато бізнес-лідерів часто не орієнтуються на кібербезпеку та не знають, куди інвестувати в IT. Як показано нижче, турбота про кібербезпеку не перетворюється на зобов’язання керівництва керувати ризиками.

Рис. 1.5. Звіт про управління ризиками генерального директора та правління

Джерело: [15]

Хоча створення репутації може зайняти роки, заплямувати репутацію так само легко, як один пролом у безпеці. Для компаній стратегічно важливо демонструвати прозорість і зміцнювати суспільну довіру. Клієнти більше, ніж будь-коли, усвідомлюють потенційні ризики для їхніх особистих даних, і вони краще усвідомлюють, який захист вони мають отримати від компаній.

Загальний регламент захисту даних (GDPR) мав глобальний вплив на обізнаність громадськості щодо захисту персональних даних. Оскільки GDPR набув чинності в 2018 році, GDPR зобов'язує компанії дотримуватися вимог. Він також гарантував, що громадяни ЄС будуть сповіщені про будь-яке порушення їх особистої інформації. Ці споживачі можуть легше отримати доступ до власних даних і зрозуміти, як їх дані використовуються.

GDPR також надихнув інші країни світу запровадити законодавство щодо персональних даних. Оскільки громадськість стає все більш обізнаною щодо захисту даних, компанії повинні визнати, що витік даних може мати значний вплив на їхню репутацію.

Дослідження Ponemon Institute у 2018 році показало, що середня вартість витоку даних становить 3,86 мільйона доларів. З цього числа непрямі

витрати від втрати репутації часто переважають прямі витрати на штрафи або судові баталії. Для більш масштабних атак, які включають від 1 до 50 мільйонів записів, витрати можуть бути надзвичайними. Порушення даних такого розміру може коштувати від 29 до понад 400 мільйонів доларів, і це не включає витрати, понесені через пошкоджену репутацію. Це може включати витрати на вирішення проблеми та сповіщення клієнтів, а також витрати на втрату продажів і пошкодження бренду.

Організації, які активно працюють над формуванням довіри клієнтів як до, так і після порушення, краще захищені від шкоди репутації. Тому стратегії управління кіберризиками та репутацією повинні йти рука об руку. Корпоративні керівники, як правило, зосереджуються на пріоритетах, які, на їхню думку, мають велике значення для компанії, а кібербезпеці, як правило, приділяється мало уваги. Тож не дивно, що компанії витрачають у середньому лише 3,3% свого доходу на IT, і лише незначна частина цього виділяється на кібербезпеку.

Коли справа доходить до визначення репутаційного впливу потенційних ризиків, треба враховувати зору клієнтів. Чому вони довіряють компанії? Що б вони вважали непростимим порушенням цієї довіри? Перед кризою управлінські команди повинні зустрітися, щоб обміркувати потенційні проблеми. Важливо визначити майбутні ризики до того, як вони відбудуться.

Однією з найбільших проблем для будь-якої компанії є організаційна роз'єднаність. Іншими словами, співробітники (або навіть цілі відділи) не мають можливості ділитися важливими знаннями один з одним. Відокремленість — це як бар’єр для змін і комунікації та може ускладнити співпрацю, коли виникають критичні проблеми. Коли комунікація процвітає, легше виявляти нові загрози та боротися з ними.

IT-лідерам часто важко визначити відповідні сфери, на які можна витратити свій обмежений бюджет. Багато разів виникає боротьба за те, щоб перекласти IT-ризики мовою, яку можуть зрозуміти нетехнічне виконавче

керівництво та члени правління. Однак стратегія управління репутаційними ризиками має бути пріоритетом безпеки для будь-якої організації, а участь керівництва є ключем до успіху. Ви повинні працювати над реалізацією стратегічного плану, який передбачає вплив на репутацію, а не просто реагувати на шкідливу подію.

Виконавча команда відіграє важливу роль не лише у підтримці стратегії, але й у контролі збитків. Генеральний директор та інші керівники старшого класу відіграють вирішальну роль у встановленні тону після події. Встановлюючи стратегію управління кризою, організація повинна працювати разом, щоб вибрати представників керівництва в усіх бізнес-підрозділах. Найкращий спосіб боротьби з дезінформацією — це призначити осіб, які є єдиними людьми, уповноваженими служити голосом компанії під час кризи.

Так само, потрібно мати співробітників, які слідкують за репутацією. Це є центральним для виявлення нових загроз репутації. Не кожен інцидент кібербезпеки зашкодить бренду компанії, але завжди треба стежити за реакцією клієнтів. У епоху цифрових технологій це означає цілодобовий моніторинг соціальних мереж.

Під час кризи зазвичай є два пріоритети, що працюють паралельно: стримування та вирішення інциденту та усунення коротко- та довгострокових ризиків для репутації. Якщо ціль зберегти довіру клієнтів, треба переконатись, що є відповідна комунікацію та послідовна розповідь.

Відновлення довіри може зайняти багато часу після порушення даних, але дотримання обіцянок є критичним. Нездатність ефективно впоратися з кризою може бути руйнівною для довгострокової репутації.

Технологія розвивається зі швидкістю, яка значно випереджає засоби захисту. Зважаючи на вимоги глобальної економіки, очікується, що підприємства будуть підтримувати безперервну діяльність. Сторонні постачальники керованих послуг пропонують такі послуги, як резервне копіювання як послуга (BaaS) і аварійне відновлення як послуга (DRaaS), щоб забезпечити захист даних. Однак захист безперервності бізнесу та аварійного

відновлення становить лише половину загальної стійкості бізнесу або здатності швидко виявляти збої та реагувати на них. Втрата даних може призупинити бізнес-операції та призвести до значних фінансових втрат, але це також може завдати шкоди репутації та призвести до ще більших довгострокових витрат.

Треба згадати про великі організації, які зазнали широкого розголосу порушень за останні кілька років. Для багатьох із них громадськість не дізналася про порушення через довгий час після того, як воно сталося. Інформація про кібератаку може поширюватися онлайн за лічені хвилини. Приховування події завдасть ще більшої шкоди репутації, якщо її розкриють пізніше. Проактивний план управління ризиками репутації, інтегрований із стратегією кібербезпеки, значною мірою допоможе створити справді стійкий бізнес.

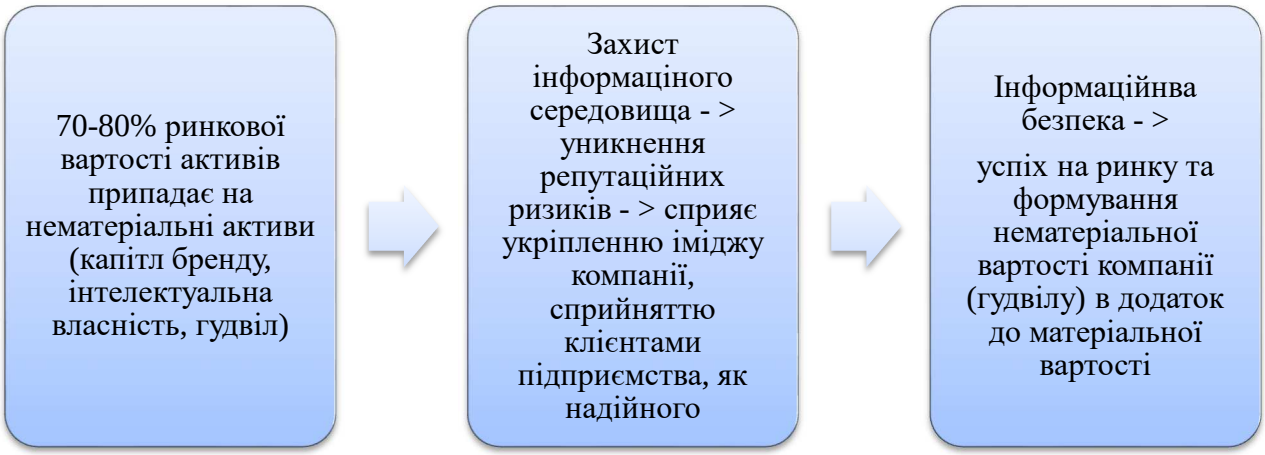

Рис. 1.6. Взаємозв`язок репутаційних ризиків, інформаційної безпеки та вартості компанії

Джерело: узугальнено за результатами досліджень

У сучасній економіці від 70% до 80% ринкової вартості припадає на нематеріальні активи, такі як капітал бренду, інтелектуальна власність і гудвіл [8]. Це співвідношення робить бізнес особливо вразливим до ситуацій, що шкодять репутації.

Гудвіл є нематеріальним активом, що виникає при придбанні компанії та

включає надбання, яке перевищує ринкову вартість її конкретних активів. Цей надмір може виникати з репутації, клієнтської бази, зв'язків та інших аспектів, що призводять до приросту вартості компанії понад його матеріальні складові.

Капітал бренду представляє собою безформний актив, визначений вартістю іміджу компанії та ступенем його впізнаваності серед споживачів. Він виникає з унікального об'єднання емоційних та раціональних аспектів, що формують позитивний образ бренду та сприяють його успіху на ринку.

Узагальнюючи, гудвіл і капітал бренду є ключовими аспектами, які визначають нематеріальну вартість компанії. Гудвіл формується при придбанні, включаючи різноманітні активи, тоді як капітал бренду виражає вартість унікального іміджу, що приводить до визнання та впізнаваності бренду на ринку. Ці елементи сприяють укріпленню позицій компанії та її привабливості для споживачів. Важливість захисту інформаційного середовища компаній стає визначальною для збільшення їх ринкової вартості, оскільки це впливає на збереження репутації, конфіденційності даних та стабільності бізнес-процесів.

Висновки до першого розділу

У першому розділі розглядається важливий аспект забезпечення інформаційної безпеки підприємства – управління репутаційними ризиками. Відзначається ключове поняття "репутація" та розглядаються "репутаційні ризики" компанії. Досліджується вплив цих ризиків на діяльність підприємства, включаючи можливі негативні наслідки для стосунків з клієнтами, партнерами та іншими зацікавленими сторонами

Важливим аспектом є розгляд взаємозв'язку репутаційних ризиків із сферою інформаційної безпеки компанії. Визначається, як негативна репутація може виникнути внаслідок порушень інформаційної безпеки, і навпаки, які заходи можуть бути вжиті для мінімізації ризиків в цих областях.

Цей розділ ставить під сумнів традиційний підхід до забезпечення інформаційної безпеки, підкреслюючи необхідність врахування репутаційних аспектів в рамках стратегій управління ризиками. Забезпечення інформаційної безпеки тепер вимагає інтегрованого підходу, що враховує не лише технічні аспекти, а й репутаційні ризики, що можуть суттєво впливати на стабільність та успішність діяльності компанії.

РОЗДІЛ 2
АНАЛІЗ РЕПУТАЦІЙНИХ РИЗИКІВ КОМПАНІЇ ТА ЇХ ОЦІНКА ПРИ ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

2.1. Характеристика та особливості функціонування компанії

Розглядаючи особливості функціонування компанії Huawei в рамках дипломної роботи, подивимося на історію її бізнесу та надамо коротку характеристику цього підприємства.

Huawei — китайська транснаціональна технологічна корпорація зі штаб-квартирою в Шеньчжені, провінція Гуандун. Вона проєктує, розробляє, виробляє та продає телекомунікаційне обладнання, споживчу електроніку, розумні пристрої та різноманітні сонячні пристрої для дахів [18].

Корпорацію заснував у 1987 році Рен Чженфей, колишній офіцер Народно-визвольної армії (НВАК). Спочатку Huawei була торговим агентом для систем приватної АТС (PBX) [19].

Рен намагався розробити іноземні технології разом із місцевими дослідниками. Щоб вийти на ринок, Китай багато запозичив у Qualcomm та інших лідерів галузі. У той час, коли вся телекомунікаційна технологія Китаю була імпортована з-за кордону, Рен сподівався створити вітчизняну китайську телекомунікаційну компанію, яка могла б конкурувати з іноземними конкурентами та, зрештою, замінити їх.

Щоб розвиватися, незважаючи на складну конкуренцію з боку Alcatel, Lucent і Nortel Networks , у 1992 році Huawei зосередилася на малодохідних і важкодоступних ринкових нішах. Торговий персонал Huawei мандрував від села до села в слаборозвинутих регіонах, поступово переміщаючись у більш розвинені регіони.

Перший великий прорив компанії стався в 1993 році, коли вона запустила

програмно керований телефонний комутатор C&C08. На той час це був найпотужніший перемикач, доступний у Китаї. Спочатку розгорнувши роботу в невеликих містах і сільській місцевості та зробивши акцент на обслуговуванні та налаштуванні, компанія завоювала частку ринку та спромоглася вийти на основний ринок [23].

Huawei також виграла ключовий контракт на будівництво першої національної телекомунікаційної мережі для Народно-визвольної армії, угоду, яку один із співробітників назвав «невеликою з точки зору нашого загального бізнесу, але великою з точки зору наших відносин». У 1994 році засновник Рень Чженфей зустрівся з генеральним секретарем Комуністичної партії Китаю Цзян Цземінем , сказавши йому, що «технологія комутаційного обладнання пов’язана з національною безпекою, і що нація, яка не має власного комутаційного обладнання, схожа на країну, яка не має свою власну армію». Як повідомляється, Цзян погодився з цією оцінкою.

У 1990-х роках канадський телекомунікаційний гігант Nortel передав виробництво всієї лінійки своїх продуктів компанії Huawei. Згодом вони також передали значну частину розробки своїх продуктів компанії Huawei [24].

Питання щодо ступеня державного впливу на Huawei стосуються її ролі національних лідерів у Китаї, субсидій і фінансової підтримки з боку державних установ, а також реакції китайського уряду у світлі протидії в деяких країнах участі Huawei в 5G .

Іншим важливим поворотним моментом для компанії став 1996 рік, коли уряд у Пекіні прийняв чітку політику підтримки вітчизняних виробників телекомунікацій та обмеження доступу іноземних конкурентів. Як уряд, так і військові просували Huawei як національного чемпіона , а також заснували нові відділи досліджень і розробок.

Починаючи з кінця 1990-х років, Huawei побудувала комунікаційні мережі по всій Африці на південь від Сахари та на Близькому Сході . Вона стала найважливішою китайською телекомунікаційною компанією, що працює в цих регіонах [25].

Таблиця 2.1

Динаміка розвитку компанії Huawei

Рік	Досягнення
1987	Huawei- торговельний агент для систем приватної АТС (PBX)
1993	Запуск першого програмно-керованого комутатора
1997	Виграш контракту на постачання продуктів фіксованого зв'язку гонгконгській компанії Hutchison Whampoa
2003	Співпраця з 3Com у спільному підприємстві, відомому як H3C, яке було зосереджено на корпоративному мережевому обладнанні
2004	Кредитна лінія на суму 10 мільярдів доларів із Банком розвитку Китаю
2005	Контракт з Vodafone
2007	Спільне підприємство з Symantec Corporation
2008	Спільний технологічний дослідницький центр з перевізником Optus
2010	Входить до списку Global Fortune 500
2016	Розширення діяльності в Ірландії
2017	Створення вузькосмугової мережі Інтернет речей
2019	Заснування Глобального навчального центру Huawei Malaysia

Джерело: узугальнено за даними [56]

У 1997 році Huawei виграла контракт на постачання продуктів фіксованого зв’язку гонконгській компанії Hutchison Whampoa . Пізніше того ж року Huawei випустила бездротові продукти на базі GSM і з часом розширила пропозицію до стандартів CDMA та UMTS . У 1999 році компанія відкрила науково-дослідний центр (R&D) у Бенгалуру, Індія, для розробки широкого спектру телекомунікаційного програмного забезпечення.

У травні 2003 року Huawei співпрацює з 3Com у спільному підприємстві, відомому як H3C, яке було зосереджено на корпоративному мережевому обладнанні. Це ознаменувало повернення 3Com на ринок високоякісних базових маршрутизаторів і комутаторів після того, як у 2000 році вона відмовилася від

нього, щоб зосередитися на іншому бізнесі. У 2006 році компанія 3Com викупила частку компанії Huawei за 882 мільйони доларів США [26].

У 2004 році компанія Huawei підписала кредитну лінію на суму 10 мільярдів доларів із Банком розвитку Китаю, щоб надати недороге фінансування клієнтам, які купують її телекомунікаційне обладнання для підтримки продажів за межами Китаю. Ця кредитна лінія була збільшена втричі до 30 мільярдів доларів у 2009 році.

У 2005 році зовнішні контрактні замовлення Huawei вперше перевищили продажі на внутрішньому ринку. Huawei підписала глобальну рамкову угоду з Vodafone. Ця угода стала першим випадком, коли постачальник телекомунікаційного обладнання з Китаю отримав статус схваленого постачальника від Vodafone Global Supply Chain.

У 2007 році Huawei заснувала спільне підприємство з американським постачальником програмного забезпечення для безпеки Symantec Corporation , відомою як Huawei Symantec , яке мало на меті надавати наскрізні рішення для мережевого зберігання та безпеки даних. Huawei викупила частку Symantec у цьому підприємстві в 2012 році, при цьому The New York Times зазначила, що Symantec побоюється, що партнерство «завадить їй отримати секретну інформацію уряду Сполучених Штатів про кіберзагрози» [28].

У травні 2008 року австралійський перевізник Optus оголосив, що створить технологічний дослідницький центр разом із Huawei у Сіднеї . У жовтні 2008 року компанія Huawei досягла угоди про внесок у нову мережу HSPA+ на базі GSM , яку спільно розгортають канадські оператори Bell Mobility та Telus Mobility , а також Nokia Siemens Networks . У 2009 році Huawei поставила одну з перших у світі комерційних мереж LTE /EPC для TeliaSonera в Осло, Норвегія. Норвезька телекомунікаційна компанія Telenor натомість вибрала Ericsson через проблеми безпеки Huawei.

У 2009 році Huawei Marine Networks поставила підводну кабельну систему зв’язку HANNIBAL для Tunisie Telecom через Середземне море до Італії.

У липні 2010 року компанія Huawei вперше була включена до списку

Global Fortune 500 2010, опублікованого американським журналом Fortune , завдяки річному обсягу продажів у 21,8 мільярда доларів США та чистому прибутку у 2,67 мільярда доларів США [29].

У жовтні 2012 року було оголошено, що Huawei перенесе свою британську штаб-квартиру в Грін-Парк , Редінг, Беркшир.

З 2016 року Huawei також розширює діяльність в Ірландії. Окрім штаб-квартири в Дубліні , у неї є підприємства в Корку та Вестміті.

У вересні 2017 року Huawei створила вузькосмугову мережу Інтернету речей, орієнтовану на місто, використовуючи модель побудови «одна мережа, одна платформа, N додатків», використовуючи « Інтернет речей » (IoT), хмарні обчислення , великі дані та іншу інформацію наступного покоління та комунікаційних технологій , він також прагне стати одним із п’яти найбільших світових хмарних гравців у найближчому майбутньому.

У квітні 2019 року компанія Huawei заснувала Глобальний навчальний центр Huawei Malaysia (MGTC) у Кіберджаї, Малайзія.

У листопаді 2020 року Telus відмовився від Huawei на користь Samsung, Ericsson і Nokia для їхньої мережі 5G/радіодоступу [30].

Huawei класифікує себе як «колективну » компанію і до 2019 року не вважала себе приватною компанією. Річард МакГрегор , автор книги «Партія: Таємний світ комуністичних правителів Китаю» , сказав, що це «визначальна відмінність, яка була важливою для отримання компанією державної підтримки на вирішальних етапах її розвитку». МакГрегор стверджував, що «статус Huawei як справжнього колективу сумнівний». Позиція Huawei змінилася в 2019 році, коли доктор Сонг Люпін, головний юридичний директор Huawei, прокоментував заборону уряду США, сказав: «Політики в США використовують силу цілої нації, щоб напасти на приватну компанію» [31].

Рен Чженфей є засновником і генеральним директором Huawei і має право накласти вето на будь-які рішення, прийняті радою директорів. У Huawei також є співвиконавчі директори, що змінюються.

Huawei вперше оприлюднила свій список ради директорів у 2010 році.

Нинішнім головою правління є Лян Хуа . Станом на 2019 рік членами правління є Лян Хуа, Гуо Пін, Сюй Чжіцзюнь, Ху Хоукунь, Мен Ваньчжоу (фінансовий директор і заступник голови), Дін Юнь, Ю Чендун, Ван Тао, Сюй Веньвей, Шень-Хань Чіу, Чень Ліфан , Пен Чжунян, Хе Тінбо, Лі Інтао, Рень Чженфей, Яо Фухай, Тао Цзінвен і Янь Ліда.

Го Пінг є головою Huawei Device, підрозділу мобільних телефонів Huawei. Чжоу Дайкі , який також є секретарем Комітету Комуністичної партії Китаю, є головним спеціалістом Huawei з питань етики та відповідності . Їхнім головним юристом є Сонг Люпін.

Корпоративна культура Huawei така: служити людям означає бути орієнтованим на клієнта та відповідальним перед суспільством». Рен часто заявляє, що філософія та стратегія управління Huawei є комерційним застосуванням маоїзму.

На теперешній час компанія Huawei є однією із провідних телекомунікаційних компаній, яка окрім цього, зайняла багато опосередкованих ніш, таких як виробництво різноманітних пристроїв (включаючи телефони, годинники, девайси для смарт-будинків, ноутбуки, планшети, тощо), розробка програмного забезпечення, виробництво сонячних панелей та іншого обладнання, що стосується енергетики і навіть презентувала декілька власних автомобілей (табл. 2.2)

Проте, із великою історією розвитку компанії, слідує і велика кількість скандалів, в тому числі, пов’язаних їз репутацією бренда, інформаційними витоками, порушенням прав інтелектуальної власності, санкцій і т.д.

Таблиця 2.2

Продукція та мобільні послуги компанії «Huawei» [57]

Продукція	Мобільні послуги
Мобільні телефони, ноутбуки, планшети, телевізори, аксесуари	Розвиток і впровадження мереж нового покоління
Пристрої Інтернет-речей	Технічна підтримка і обслуговування

Продовження табл. 2.2

Телекомунікаційне обладнання (базові станції, роутери, комутатори, кабеля, SFP)	Корпоративні рішення для обробки
Обчислювальні пристрої і обладнання для зберігання інформації (сервери, стореджі)	Розробка та впровадження IoT (Internet of Things) рішень
Пристрої енергетичної сфери (зарядні станції, сонячні панелі, тощо)	Хмарне зберігання та обчислення
Автомобілі	Консультації щодо впровадження нових технологій

Джерело: [57]

2.2. Аналіз інформаційних та репутаційних ризиків компанії

У першій частині другого розділу лише віддалено було згадано про відносини компанії із комуністичною партією Китаю, Народно-визвольною армією і урядом США. У цій же частині навпаки – будуть розглянуті найгостріші і найбільш кризисні ситуації через які пройшла компанія і з якими наслідками суперечок доводилось мати справи.

Компанія Huawei звинувачується в тому, що її продукти містять бекдори для китайського урядового шпигунства, а внутрішні закони вимагають від громадян і компаній Китаю співпраці з державною розвідкою, коли це виправдано. Керівництво Huawei спростувало ці заяви, заявивши, що компанія не отримувала запитів від китайського уряду на впровадження бекдорів у своєму обладнанні, відмовиться це робити, і що китайське законодавство не зобов'язує їх робити це. Станом на 2019 рік Сполучені Штати не надали доказів скоординованого злому з боку Huawei [16].

На ранніх етапах розвитку Huawei використовувала складну систему угод з місцевими державними телефонними компаніями, яка, здавалося, включала

незаконні виплати працівникам місцевого телекомунікаційного бюро. Наприкінці 1990-х років Huawei створила кілька спільних підприємств зі своїми державними телекомунікаційними компаніями-клієнтами. До 1998 року Huawei підписала угоди з муніципальними та провінційними телефонними бюро про створення Shanghai Huawei, Chengdu Huawei, Shenyang Huawei, Anhui Huawei, Sichuan Huawei та інших компаній. Спільні підприємства фактично були підставними компаніями і були способом перекачування грошей місцевим працівникам телекомунікацій, щоб Huawei могла отримати угоди про продаж їм обладнання. У випадку Sichuan Huawei, наприклад, місцеві партнери могли отримати 60–70 відсотків своїх інвестицій у вигляді річних «дивідендів».

Мартін Торлі з Ноттінгемського університету зазначив, що «компанія розміру Huawei, яка працює в тому, що вважається чутливим сектором, просто не може досягти успіху в Китаї без широких зв’язків із партією» [16]. Klon Kitchen припустив, що домінування 5G має важливе значення для Китаю для досягнення його бачення, коли «процвітання державного капіталізму поєднується зі стабільністю та безпекою технологічно обумовленого авторитаризму». Найджел Інкстер з Міжнародного інституту стратегічних досліджень припустив, що «залучення Huawei до основної магістральної інфраструктури 5G розвинутих західних ліберальних демократій змінює стратегічну гру, оскільки 5G змінює правила гри», при цьому «чемпіони національного телекомунікацій» відіграють ключову роль. , що, у свою чергу, є частиною «амбітної стратегії Китаю з перебудови планети відповідно до його інтересів» через ініціативу «Один пояс, один шлях » . 7 жовтня 2020 року Комітет оборони парламенту Великої Британії опублікував звіт, у якому було зроблено висновок про наявність доказів змови між компанією Huawei та китайською державою та Комуністичною партією Китаю на основі моделі власності та державних субсидій, які вона отримувала [17].

Китайський уряд надав Huawei повну підтримку, у противагу щодо інших вітчизняних компаній, які стикаються з проблемами за кордоном, такі як ByteDance, оскільки Huawei вважається «національним чемпіоном» разом з

Alibaba Group і Tencent. Наприклад, після того, як фінансового директора Huawei Мен Ваньчжоу було затримано в Канаді в очікуванні екстрадиції до Сполучених Штатів за звинуваченнями в шахрайстві, Китай негайно заарештував Майкла Ковріга та Майкла Спавора в тому, що багато хто розглядав як «дипломатію заручників». У 2020 році Китай також запровадив мита на імпорт з Австралії, очевидно, як помсту за те, що Huawei та ZTE були виключені з австралійської мережі 5G у 2018 році. У червні 2020 року, коли Велика Британія розглядала скасування попереднього рішення дозволити Huawei брати участь у 5G, Китай пригрозив помстою в інші сектори шляхом припинення інвестицій у виробництво електроенергії та високошвидкісну залізницю. Комітет із захисту Палати громад виявив, що «Пекін чинив тиск через «таємні та явні погрози», щоб зберегти Huawei у мережі 5G Великобританії». Держсекретар США Майк Помпео запевнив Сполучене Королівство, заявивши, що «США виступають разом із нашими союзниками та партнерами проти насильницької тактики залякування Комуністичної партії Китаю», і «США готові допомогти нашим друзям у Великобританії з будь-якими потребами, починаючи від будівництва безпечних і надійних атомних електростанцій для розробки надійних рішень 5G, які захищають конфіденційність громадян» [20].

«Погляд пекінських дипломатів, які стали на захист [Huawei]» в Європейському Союзі, також суперечить заявам Huawei про те, що вона «повністю незалежна від китайського уряду». Згідно зі звукозаписом, отриманим Kringvarp Føroya , у листопаді 2019 року посол Китаю в Данії під час зустрічей із високопоставленими політиками Фарерських островів прямо пов’язав розширення Huawei 5G із китайською торгівлею . Як повідомляє Berlingske , посол погрожував відмовитися від запланованої торгової угоди з Фарерськими островами, якщо фарерська телекомунікаційна компанія Føroya Tele не дозволить Huawei побудувати національну мережу 5G. У Huawei заявили, що не знали про зустрічі. Посол Китаю в Німеччині Ву Кен попередив, що «будуть наслідки», якщо Huawei буде виключено, і заявив про «можливість заборони німецьких автомобілів з міркувань безпеки» [21].

The Wall Street Journal припустив, що Huawei отримала приблизно «46 мільярдів доларів у вигляді позик та іншої підтримки, а також 25 мільярдів доларів у вигляді зниження податків», оскільки уряд Китаю був зацікавлений у створенні компанії, яка б конкурувала з Apple і Samsung [22]. Зокрема, державні банки Китаю, такі як Китайський банк розвитку та Експортно-імпортний банк Китаю, надають позики клієнтам Huawei, що значно знижує фінансування конкурентів за рахунок нижчих відсотків і готівки наперед, а Китайський банк розвитку надає кредитну лінію на загальну суму 30 мільярдів доларів США між 2004 і 2009 роками. У 2010 році Європейська комісія розпочала розслідування щодо субсидій Китаю, які спотворили глобальні ринки та завдали шкоди європейським постачальникам, і Huawei запропонувала початковому скаржнику 56 мільйонів доларів США, щоб відкликати скаргу, намагаючись припинити розслідування. . Тодішній єврокомісар з питань торгівлі Карел де Ґухт виявив, що Huawei використовувала державну підтримку, щоб знизити ціни конкурентів на 70 відсотків [32].

Компанії також доводилось переживати і звинувачення у зв’язках з військовими та розвідкою Китаю [33].

У 2019 році Рен Чженфей заявив, що Huawei не займається шпигунством і не встановлює бекдори, навіть якщо цього вимагає китайське законодавство. Проте, експерти вказують на нечіткість і широкий обсяг законів про розвідку та контршпигунство в Китаї, які можуть зобов'язати компанії співпрацювати з розвідувальними операціями. Деякі дослідники вказують на тісний зв'язок між Huawei і китайською державою, включаючи осіб з військовим досвідом та зв'язки з китайськими спецслужбами. Аналіз резюме працівників Huawei вказує на їхнє зв'язок із структурами китайської армії та розвідки. Крім того, нові закони про кібербезпеку та національну розвідку вимагають від компаній використовувати державно сертифіковане обладнання та програмне забезпечення, що викликає обурення щодо приватності та безпеки даних.

Майкл Вессел, член американсько-китайської комісії з огляду економіки та безпеки, порівняв Huawei зі слюсарем, який встановлює замки на дверях

громади. Звіти вказують на те, що австралійська розвідка виявила бекдор у телекомунікаційній мережі в 2012 році, який містив шкідливий код, відправляючи дані до Китаю. Huawei відкидає звинувачення, назвавши їх "наклепом". В Уганді та Замбії визнали, що Huawei грав роль у шпигунстві за політичними опонентами. В Африканському союзі системи, встановлені Huawei, передавали дані до Китаю. Виявлено, що Huawei Mediapad M5 надсилав дані на сервери в Китаї без дозволу. Сполучені Штати повідомили Великобританії та Німеччині про можливість використання Huawei бекдорів для співробітників правоохоронних органів. Великобританська лабораторія, фінансована Huawei, не виявила бекдорів, але визнала помилки, які можуть бути використані хакерами [34].

Одним із ключових звинувачень у бік компанї Huawei є порушення інтелектуальної власності. Головними опонентами у судових позовах проти китайської компанії виступали Cisco, PanOptis і Motorola. За результатами позовів у 2018 році німецький суд виніс рішення проти Huawei на користь MPEG LA, яка володіє партнерами пов’язаними з Advanced Video Coding [35].

Huawei звинувачують, зокрема в порушенні патентів Cisco Systems у 2003 році. У той період компанію також звинувачували у незаконному копіюванні вихідного коду, використаного в її маршрутизаторах і комутаторах. У 2004 році на технічній конференції Supercomm у Чикаго співробітник Huawei, за слуханнями, відкрив мережеве обладнання інших компаній, щоб здійснити фотографію друкованих плат.

Більше того, колишній керівник служби безпеки Nortel, Брайан Шилдс, стверджує, що компанію зламали китайські хакери в 2004 році, що призвело до отримання ними конфіденційних даних, включаючи дорожні карти продукту та технічні документи. Хоча безпосередня причетність Huawei залишається питанням спору, є підозра, що компанія могла скористатися вигодою від цього вторгнення [36].

У 2017 році Huawei було визнано винним у незаконному привласненні комерційної таємниці T-Mobile US, однак компенсація була призначена лише за

порушення контракту [37]. У 2020 році Міністерство юстиції США висунуло нові обвинувачення щодо рекету та змови на рахунок Huawei у викраденні комерційної таємниці шести американських фірм. Незважаючи на це, Huawei відкидає звинувачення, називаючи їх підставою для серйозних юридичних наслідків [38].

Питання про етичність та діяльність компанії Huawei стає предметом уваги через ряд обвинувачень та витоків інформації. Однією з ключових тем є спроби з'ясувати можливу співпрацю Huawei з країнами, які перебувають під санкціями, а також звинувачення використання технологій компанією в ситуаціях, пов'язаних із систематичним спостереженням та порушеннями прав людини. Розглянемо кілька інцидентів для кращого розуміння цих питань.

Витік документів у 2019 році підштовхнув до розгляду можливого таємного бізнесу Huawei з Північною Кореєю, яка перебуває під санкціями США [39]. Крім того, компанію обвинувачують у наданні технологій для масового спостереження та утримання уйгурів у таборах інтернованих Сіньцзян. Документи вказують на розробку програмного забезпечення для розпізнавання облич та подачу заявки на патент у Китаї для ідентифікації етнічних особливостей. Звинувачення також стосуються використання примусової праці, що викликає санкції з боку Державного департаменту Сполучених Штатів. Варто відзначити, що Huawei заперечує звинувачення та використання таких технологій [40].

Важливою темою у цьому питанні є також санкції. Санкції, що стосуються компанії Huawei, представляють собою складний міжнародний випадок, що визначає взаємовідносини Китаю та інших країн, зокрема Сполучених Штатів.

До 2020 року компанію Huawei обмежували санкціями у США через обвинувачення в порушенні безпеки та контролі над експортом. У серпні 2018 року був підписаний закон NDAA 2019, який забороняв використання обладнання Huawei та ZTE федеральним урядом США. Huawei подала позов щодо його конституційності, але він залишався чинним [41].

У травні 2019 року Міністерство торгівлі США додало Huawei до списку

організацій, обвинувачених у сприянні експорту до Ірану [42]. Це призвело до обмежень для американських компаній, які заморозили бізнес з Huawei. Заборона була поетапною, але в серпні 2020 р. стала повною, охоплюючи усі напівпровідники, виготовлені за американською технологією. Загальна заборона стала чинною у вересні 2020 р.

Внаслідок санкцій, введених проти Huawei з вересня 2020 року, компанія відчула серйозні труднощі в різних аспектах свого бізнесу. Однією з ключових обмежень стала заборона на виробництво напівпровідників, що використовують американську технологію. Це відбулося після попереднього розширення санкцій у травні 2020 р., коли США заборонили постачання американських напівпровідників для Huawei. Також у листопаді 2020 р. була введена заборона для американських компаній та осіб на володіння акціями компаній, пов'язаних із Народно-визвольною армією Китаю, до якої входить Huawei.

Адміністрація Трампа активно домагалася обмежити діяльність Huawei в США, а також намагалася переконати інші країни у важливості уникання використання технологій Huawei з огляду на національну безпеку [43]. Зокрема, в червні 2021 р. адміністрація Джо Байдена взяла на себе завдання переконати Об'єднані Арабські Емірати відмовитися від обладнання Huawei у своїх телекомунікаційних мережах [44].

Ці кроки супроводжувалися різними обмеженнями, такими як відкликання ліцензій для американських компаній, заборона на субсидії та участь в американських проектах. FCC також визначила Huawei як загрозу національній безпеці та заборонила використання її обладнання в телекомунікаційних мережах США [45].

Під впливом санкцій і обмежень, Huawei зосереджується на стратегії накопичення ключових компонентів, витрачаючи значні суми (23,45 мільярда доларів у 2019 р.) на придбання мобільних процесорів 5G, мікросхем Wi-Fi та інших матеріалів [46]. Зокрема, компанія утримує запаси від провідних виробників, таких як Samsung, SK Hynix, TSMC, MediaTek, забезпечуючи собі резерв на 1,5-2 роки в сегментах телекомунікаційного та серверного бізнесу [47].

Цей стратегічний хід дозволяє Huawei забезпечити стабільність у виробництві та захистити себе від можливих перешкод у подальшому розвитку, враховуючи динаміку сучасного ринку та геополітичні виклики.

У кінці 2020 р. Huawei визначила стратегічний курс на власне виробництво напівпровідників, розгортаючи справжню індустрію в Китаї та намагаючись уникнути американських санкцій [48]. Заводи, розташовані у різних регіонах, створюють тіньову мережу виробництва, що дозволяє компанії подолати обмеження. Західні аналітики визнали технічний прогрес Huawei, коли в вересні 2023 року вона представила смартфон Mate 60 з чіпом Kirin 9000s, виготовленим в Китаї та використовуючи технологію 7 НМ [49]. Цей крок вказує на готовність компанії ефективно функціонувати в умовах санкцій, навіть інвестуючи в внутрішні технологічні рішення. Однак такий курс може призвести до подальших конфліктів та санкцій, зокрема від США, щодо обхідної співпраці зі світовими гравцями в сфері напівпровідників.

Під час введення санкцій США влітку 2018 року Huawei розпочала розробку власної операційної системи під кодовою назвою "HongMeng OS". Зазначалося, що ця система може слугувати альтернативою у разі обмежень використання Android або Windows через дії США. Harmony OS було офіційно представлено у серпні 2019 року, а Huawei подала заявки на торговельні марки "Ark", "Ark OS" і "Harmony" в Європі для цієї ОС [50]. Ця операційна система стала стандартною для смартфонів Huawei в Китаї з червня 2021 р., піднявши свою частку ринку до 10% китайського сегмента протягом двох років, хоча в Європі залишалася версія EMUI на базі Android.

Рис. 2.1. Репутаційні ризики компанії «Huawei»

Джерело: складено за результатами досліджень[10-15]

Продукти Huawei були заборонені або обмежені в ряді країн, включаючи Австралію, Нову Зеландію та десять країн Європейського Союзу. Тайвань заборонив використання обладнання Huawei в 2013 році, Японія відмовила компанії в державних контрактах у 2018 р., а В'єтнам утрималася від тендерів на будівництво мережі 5G у 2019 р.

Індія планує вилучити телекомунікаційне обладнання Huawei через національні безпекові обгрунтування, а Канада вже заборонила використання їхнього обладнання в мережі 5G до червня 2024 р. [52].

Велика Британія і Коста-Ріка також прийняли заходи щодо вилучення

обладнання Huawei з мереж, а Німеччина пропонує видалити китайське обладнання, включаючи Huawei, зі своєї мережі 5G до 2026 р. [51].

Китайська громадськість загалом вважає недовіру Заходу та націлювання на Huawei невиправданими. Це призвело до того, що серед китайської громадськості та міської влади виникла думка, що заступництво Huawei допомагає Китаю підтримувати геополітичну та технологічну конкуренцію зі Сполученими Штатами. Таким чином, Huawei отримала високий рівень підтримки з точки зору громадських настроїв, від чого її конкурентні фірми не виграють такою ж мірою. Ці настрої зміцнили першу позицію Huawei на ринку технологій розумних міст Китаю.

2.3. Оцінка репутаційних ризиків та інформаційної безпеки компанії

Тепер, знаючи, через який тиск і випробування пройшла компанія з моменту її створення і як реагувала на кризисні ситуація, можна зосередитись на оцінці репутаційних ризиків з якими вона мала справу на кожному етапі свого існування.

Перш за все, необхідно розпочати з класифікації, яка включає розгляд різних аспектів, що можуть вплинути на репутацію підприємства.

1. Керівництво та Поведінка:

На початковому етапі розвитку Huawei виникли фінансові скандали та порушення етичних стандартів, включаючи підтримку переслідування уйгурів в Китаї. Ці аспекти залишають тінь невпевненості щодо репутації компанії на глобальному ринку.

2. Виробництво та Продукти:

Звинувачення у створенні бекдорів для шпіонажу та складні угоди з телеком-операторами піднімають загрозу для безпеки користувачів та фінансового стану компанії. Ці аспекти створюють нестабільність та питання

щодо якості продукції.

3. Соціальна відповідальність:

Звинувачення у рекеті та порушення прав людини суттєво впливають на соціальну відповідальність компанії. Незважаючи на це, відсутність публічних розслідувань підкреслює важливість прозорості та відкритості.

4. Кібербезпека:

Критика США та інших країн у справі кібербезпеки та підозри щодо співпраці з китайськими спецслужбами піддають сумніву довіру споживачів та партнерів. Звинувачення у шпіонажі ставить під питання безпеку продуктів Huawei, хоча відсутність публічних витоків свідчить про вдосконалені практики в цифровій безпеці.

5. Стосунки з Громадськістю та ЗМІ:

Huawei активно працює над уникненням звинувачень у порушеннях прав людини через мас-медіа. Негативні медіа-публікації можуть завдати шкоди репутації компанії, і важливо ефективно управляти кризовими ситуаціями.

6. Ринкові Фактори:

Санкції викликали втрату ринків та технологій, що призвело до неудач на ринку та обмежень у конкурентоспроможності. Невдачі через санкції вимагають постійного адаптування стратегій та підходів.

7. Кадрові Ризики:

Інформації про дискримінацію на робочому місці немає, але компанія стикається із суперечливими питаннями, пов'язаними із переслідуванням уйгурів та дотриманням прав людини в Китаї. Збереження балансу різноманіття та уникнення дискримінації на робочому місці є важливою задачею, особливо в контексті геополітичних та соціальних проблем.

Серед наведених вище ризиків можна чітко розділити їх на внутрішні та зовнішні:

Зовнішні Ризики:

1. Геополітичні Напруги:

Опис: Втручання політичних сил та конфлікти міжнародного рівня можуть

призвести до санкцій та втрати ринкових можливостей.

Приклад: Заборона у використанні продукції Huawei у США через питання кібербезпеки.

2. Торговельні Блокади:

Опис: Міжнародні торговельні обмеження та бар'єри можуть вплинути на логістику, вартість виробництва і розподіл продукції.

Приклад: Заборона на торгівлю технологіями між Huawei та американськими компаніями.

3. Технологічні Тренди:

Опис: Різке зміни у технологічному середовищі можуть призвести до застаріння продуктів та втрати конкурентоспроможності.

Приклад: Швидкий розвиток нових технологій, які замінюють існуючі продукти Huawei.

Внутрішні Ризики:

1. Етичні Питання:

Опис: Внутрішні порушення етичних стандартів та співпраця з контроверсійними проектами можуть пошкодити репутацію компанії.

Приклад: Звинувачення Huawei у співпраці з урядом Китаю у сфері прав людини.

2. Технічні Неполадки:

Опис: Невдачі в розробці продуктів та технічні проблеми можуть призвести до втрат фінансів та репутації.

Приклад: Дефекти в новому продукті, що призводять до відкликання чи погіршення іміджу.

3. Фінансові Обмеження:

Опис: Невдачі в фінансових стратегіях та складнощі з отриманням кредитів можуть вплинути на ліквідність та розвиток.

Приклад: Фінансові втрати через санкції та обмеження у фінансовому доступі.

Таблиця 2.3

Оцінка та наслідки репутаційних ризиків компанії «Huawei»

Причина порушення репутації	Рівень ризику	Реакція стекхолдерів	Наслідки
Питання щодо безпеки мережі 5G і телекомунікаційного обладнання.	Високий. Звинувачення у використанні технології для шпигунства може поглибити довіру до компанії та порушити безпеку комунікаційних інфраструктур.	Оператори можуть відмовитися від використання продукції Huawei, перейшовши до інших постачальників. Уряди і регулятори можуть вводити обмеження та заборони на використання продукції Huawei в мережах.	Втрата ринкової частки та можливі штрафи від регуляторів.
Співпраця з урядом і спецслужбами Китаю.	Високий. Звинувачення в тісних зв'язках з урядом може підірвати довіру в компанію та спричинити питання щодо конфіденційності.	Інвестори можуть вимагати додаткової прозорості та впливу на корпоративне управління. Уряди і регулятори можуть реагувати проведенням додаткових розслідувань і контроль за діяльністю компанії.	Втрата довіри та можливі правові наслідки.
Обмеження участі в міжнародних операціях і непрозорість фінансової історії.	Середній. Обмеження в міжнародних операціях може вплинути на ринкову присутність, а фінансова непрозорість може викликати сумніви в корпоративній відповідальності.	Інвестори і аналітики вимагатимуть докладної фінансової звітності та пояснень стосовно обмежень в операціях. Клієнти і партнери можуть обирати більш прозорих партнерів для своїх потреб.	Можливий знижений інтерес з боку інвесторів і втрата деяких бізнес-можливостей.
Інтелектуальна власність та патентні суперечки.	Середній. Судові та патентні суперечки можуть призвести до втрати інтелектуальної власності та фінансових втрат.	Інвестори можуть бути обурені можливими втратами та вимагають захисту інтелектуальної власності. Конкуренти можуть виграти від судових рішень та зміцнити свої позиції на ринку.	Фінансові втрати та втрата конкурентоспроможності.

Продовження таблиці 2.3

Санкції та торгові обмеження.	Високий. Санкції можуть призвести до обмежень в торгівлі та втрати доступу до ключових ринків.	Уряди та регулятори вводять санкції та обмеження, контролюючи діяльність компанії. Акціонери стурбовані можливими втратами вартості акцій.	Втрата ринкового доступу та фінансові втрати.
Залежність від постачальників та виробників.	Високий. Залежність від обладнання чи компонентів може стати вразливістю при проблемах з постачанням. Особливо в умовах санкцій.	Клієнти та партнери шукають альтернативні рішення в разі перебоїв в постачанні. Інвестори стурбовані можливими втратами виробництва та продажів.	Повна зупинка або затримка виробництва та можливі втрати клієнтів.
Конкуренція на ринку.	Високий. Зростання конкуренції може вплинути на ринкову долю та призвести до падіння цін.	Клієнти мають більше варіантів вибору та можуть вимагати кращих умов. Інвестори турбуються про вплив конкуренції на прибутковість компанії.	Зниження прибутків та можливі втрати ринкової позиції.

Джерело: [53]

Компанія Huawei зіткнулася з низкою викликів, розглянемо яким чином вона їх вирішувала.

Проактивне управління комунікаціями: Huawei активно використовує свої внутрішні PR-команди, щоб забезпечити більше доступу до журналістів, аналітиків та інших впливових осіб. Це допомагає будувати справжні відносини, в яких люди будуть прислухатися. Це включає в себе регулярні інтерв'ю з журналістами, навіть коли компанія переживає складні періоди [53].

Внутрішні програми комунікацій: Huawei розробила внутрішню програму, яка пояснює своїм 180 000 співробітникам, чому важливо мати доступ до інформації, як репутація компанії впливає на її успіх і її підхід до комунікацій. Цей підхід не змінить культуру та ментальність за одну ніч, це довгострокова гра [53].

Взаємодія з пресою: Huawei активно взаємодіє з пресою, щоб забезпечити

більше доступу до інформації про компанію. Це допомагає забезпечити справжні відносини, в яких люди будуть слухати вас справедливо [53].

Управління зовнішніми ризиками: Huawei також активно працює над управлінням зовнішніми ризиками, включаючи геополітичні ризики, фінансові кризи, нестабільне економічне зростання, зменшення інвестицій, колебальні обмінні курси, суворі контролі за іноземною валютою, антиглобалізм, захист, анти-дюмпінг, трудові конфлікти, зміни в моделях бізнесу клієнтів та інші виклики [54].

Управління внутрішніми ризиками: Huawei також активно працює над управлінням внутрішніми ризиками, включаючи ризики, пов'язані з розширенням, якості продукту, продовження бізнесу, постачання, невикористаний інвентар, невикористані рахунки за очікувані платежі, кібербезпеку, захист приватності користувачів, оподаткування, торговельне

Huawei, як компанія, стикалася з низкою критичних викликів та кризових ситуацій протягом свого існування. Важливо розглянути, як саме вона вирішувала ці питання і яку політику реагування обрала.

Законодавство, пов'язане з правами людини, відрізняється від країни до країни, і Huawei опинилася під впливом специфічного законодавства Китаю та комуністичної партії. Це створює складність у вирішенні проблем, таких як порушення прав людини та соціальна відповідальність.

Компанія Huawei використовується Китаєм як інструмент для втілення закритої політики з тотальним контролем. Розробка програмного забезпечення для ідентифікації за расовими чинниками піднімає етичні питання, але Huawei, ймовірно, визначила свої інтереси відповідно до політичного контексту Китаю.

Втрата ринків у США, Європі та частині Близького Сходу зумовила стратегічний розворот на нові ринки, зокрема в Африці, а також подальше співпрацювання з Росією навіть після повномасштабного вторгнення (ринки в Росії, Південній Кореї і Ірані досі не ліквідовано). Це призвело до фінансових втрат, які, за звітами, сягають мільярдів доларів. Проте, компанія демонструє гнучкість та стійкість, зберігаючи технологічне лідерство в розробці 5G, власних

операційних систем і навіть розширюючи свою діяльність в інші галузі, такі як автомобільна і напівпровідникова промисловість.

Розглядаючи велику кількість кризових ситуацій, можна зробити висновок, що, нажаль, Huawei, незважаючи на значні труднощі, зуміла зберегти своє існування та технологічний рівень. Справжнім випробуванням була здатність компанії адаптуватися до нових умов, змінювати стратегії та залишатися конкурентоспроможною.

Висновки до другого розділу

Другий розділ присвячений детальному аналізу репутаційних ризиків компанії Huawei та їх оцінці в контексті забезпечення інформаційної безпеки. Використовуючи характеристики та особливості функціонування компанії, було проведено аналіз інформаційних та репутаційних ризиків, розглядаючи їх можливі виникнення та вплив на діяльність підприємства. Оцінка репутаційних ризиків та інформаційної безпеки слугує фундаментом для розробки стратегій управління ризиками, спрямованих на збереження стабільності та репутації компанії.

У контексті компанії Huawei, яка опинилася під впливом геополітичних напруг та технологічних обмежень, аналіз репутаційних ризиків є особливо важливим. Інтеграція характеристик функціонування компанії з оцінкою ризиків дозволяє виявити найбільш вразливі аспекти та прийняти засоби запобігання.

Оцінка репутаційних ризиків та інформаційної безпеки для Huawei слугує підґрунтям для подальших стратегій, спрямованих на підтримку і зміцнення стійкості компанії в умовах непередбачуваного бізнес-середовища. Розгляд репутаційних ризиків у контексті інформаційної безпеки підкреслює важливість їх комплексного управління для досягнення успішності та стабільності на ринку.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ РЕПУТАЦІЙНИМИ РИЗИКАМИ КОМПАНІЇ

3.1 Розробка комплексної технології управління репутаційними ризиками та загрозами

Комплексна технологія управління репутаційними ризиками і загрозами є стратегічним інструментом, спрямованим на систематичне та ефективне управління репутаційним середовищем компанії в умовах змін технологічного простору, глобалізації та геополітичних «турбулентностей». Ця технологія враховує різноманіття загроз та ризиків, які можуть вплинути на репутацію підприємства, і пропонує інтегрований підхід для їх передбачення, управління та мінімізації.

Рис. 3.1. Комплексна технологія управління репутаційними ризиками і загрозами

Джерело: складено за результатами досліджень

На рис. 3.1. зображено власне бачення комплексної технології управління репутаційними ризиками і загрозами. Для розуміння змісту, представленого на рисунку, необхідно проаналізувати кожен з етапів і зупинятися на кожному із них окремо.

Аналіз репутаційного ландшафту. Етап аналізу репутаційного ландшафту включає в себе докладне вивчення аудиторії та взаємодії, а також моніторинг як онлайн, так і офлайн простору. Щоб ефективно аналізувати аудиторію, ключовим є використання платформ соціальних медіа та інших онлайн ресурсів. Наприклад, створення сторінок на Facebook чи LinkedIn дозволить не лише залучити увагу цільової аудиторії, але й взаємодіяти з нею.

Під час аналізу аудиторії, важливо вивчати реакцію потенційних клієнтів на ключові ініціативи, події та повідомлення. Наприклад, збільшення кількості лайків, коментарів та репости може свідчити про позитивне сприйняття аудиторією. З іншого боку, відповіді на аудієнційні опитування можуть надати важливі відгуки.

Щодо моніторингу онлайн та офлайн простору, сучасні інструменти соціального медіа відіграють ключову роль.

Для аналізу репутаційного ландшафту доцільно використовувати:

- Hootsuite: Цей інструмент дозволяє планувати та відстежувати публікації на різних соціальних мережах, а також відслідковувати згадки та обговорення про компанію.
- Google Alerts: Надсилання сповіщень про нові згадки ключових слів або фраз в онлайн-публікаціях, що дозволяє оперативно реагувати на події.
- Brandwatch: Інструмент для медіа-моніторингу, який аналізує мільйони джерел для отримання відгуків та взаємин.

Ці інструменти допомагають виявляти ключові теми, тенденції та реакції аудиторії, що є важливим для успішного управління репутаційним ландшафтом.

Ідентифікація ризиків і загроз. Етап ідентифікації ризиків і загроз включає в себе системи раннього виявлення та аналіз геополітичних та регуляторних

чинників. Це передбачає:

Використання передових технологій штучного інтелекту (AI) для прогнозування та попередження можливих ризиків і виявлення негативних тенденцій. Наприклад, аналіз великих обсягів даних з використанням AI може допомогти ідентифікувати зміни у споживчому ставленні або в реакції аудиторії на конкретні події.

Використання спеціалізованих систем аналізу, щоб оцінити вплив глобальних подій та змін у регуляторному середовищі на репутацію компанії. Прикладами можуть бути:

- Stratfor: Система, яка аналізує геополітичні події та розробляє прогнози, допомагаючи компаніям розуміти можливі ризики.
- The EIU (Economist Intelligence Unit): Платформа, яка надає аналіз геополітичних та економічних подій, допомагаючи підприємствам адаптуватися до змін у світовому середовищі.
- Regulatory Intelligence Platforms: Наприклад, Bloomberg Law або Thomson Reuters Regulatory Intelligence, які допомагають відстежувати та аналізувати зміни в законодавстві та регуляторних стандартах.
- Compliance Management Software: Інструменти, такі як MetricStream чи IBM OpenPages, які використовують аналітичні засоби для ефективного управління регуляторними ризиками.

Впровадження цих технологій сприяє оперативному виявленню ризиків та розумінню їхнього впливу на репутацію компанії, що дозволяє ефективно реагувати та пристосовувати стратегії управління.

Розробка стратегій та заходів. Етап розробки стратегій та заходів включає в себе комунікаційні стратегії та ефективне кризове управління. Це включає:

Створення персоналізованих та адаптивних стратегій комунікацій, які враховують різноманітні культурні та географічні контексти. Наприклад:

- Створення адаптивної комунікаційної стратегії на популярних соціальних мережах для адекватного взаємодії з різними

аудиторіями та уникнення конфліктів.

- Врахування місцевих традицій та медійних платформ для створення персоналізованих повідомлень, спрямованих на конкретні регіони.
- Впровадження планів дій та сценаріїв для реагування на кризові ситуації з використанням технологій симуляції та тренувань персоналу. Наприклад:
- Використання програм симуляції кризових ситуацій, таких як CrisisCast чи Simudyne, для тренування персоналу у віртуальному середовищі.
- Проведення регулярних тренувань із використанням планів дій та підготовлених сценаріїв для відповіді на різні кризові ситуації.

Адаптивні стратегії можуть включати гнучкі підходи до комунікацій, зміну стратегій в залежності від зміни обставин та активне використання засобів зворотного зв'язку від аудиторії. Такі стратегії дозволяють компаніям ефективно взаємодіяти з різними групами та ефективно вирішувати кризові ситуації.

Аналіз дієвості запропонованих заходів.

Етап моніторингу та відслідковування запропонованих заходів передбачає використання автоматизованих засобів для постійного відслідковування реакцій аудиторії та обґрунтування результативності застосованих заходів.

Для проведення моніторингу можуть застосовуватися технології для неперервного спостереження за різними аспектами репутації компанії. Прикладами таких систем можуть бути:

- Brand24: Інструмент для моніторингу відгуків у соціальних мережах та в інтернеті.
- Meltwater: Платформа, що виявляє згадки та аналізує медійний звіт про компанію.

Застосування методів аналізу даних для оцінки динаміки змін у репутаційному ландшафті та впровадження необхідних заходів корегування. Приклади включають:

- Sentiment Analysis: Визначення настрою (позитивний, негативний,

нейтральний) коментарів та відгуків для визначення загального сприйняття бренду.

- Social Network Analysis (SNA): Вивчення зв'язків та взаємодій між користувачами в соціальних мережах для виявлення ключових впливових фігур та тенденцій.

Ці автоматизовані системи та техніки аналізу даних дозволяють компаніям ефективно відстежувати та оцінювати стан своєї репутації, реагувати на зміни та приймати обґрунтовані управлінські рішення.

Контингенційне планування. Етап контингенційного планування зосереджений на підготовці компанії до можливих репутаційних викликів шляхом розробки сценаріїв, моделей та тестування контингенційних планів. Це включає:

Створення докладних сценаріїв можливих репутаційних викликів, таких як кризи, скандали чи негативні події:

- Криза у соціальних мережах: Сценарій, де компанія стикається із великим обсягом негативних коментарів у соціальних мережах щодо якоїсь своєї діяльності або продукту.
- Витік конфіденційної інформації: Сценарій, де стає відомо про витік конфіденційної інформації, що може негативно вплинути на довіру клієнтів.

Створення детальних планів відповіді на кожен з розроблених сценаріїв, таких, як:

- Соціальні медіа-стратегія в кризових ситуаціях: План дій для ефективного взаємодії з аудиторією та зменшення негативного впливу через соціальні мережі.
- Комунікації та публічні виступи: План, який визначає, як організувати комунікацію та публічні виступи для зменшення ризиків та відновлення репутації.

Ці заходи сприяють глибокому розумінню та готовності компанії до потенційних репутаційних криз та забезпечують ефективний відгук у випадку

негативних сценаріїв.

Отримавши комплексну систему управління репутаційними ризиками, можна з ефективністю застосовувати її до ризиків середнього та високого рівня. Треба наголосити на тому, що ризики низького рівня можна вдало ігнорувати або уникати ще на етапі їхнього формування, оскільки така система дозволяє вчасно ідентифікувати та управляти потенційними загрозами, забезпечуючи оптимальний контроль над репутаційними процесами.

3.2 Вияв прогалин у інформаційній безпеці та репутаційних ризиків за використання комплексної технології управління

Запропонована комплексна технологія управління репутаційними ризиками і загрозами має бути використана для того, щоб виокремити та виявити прогалини у інформаційній безпеці (в частині репутаційних ризиків) з метою їх упередження. Тому доцільно покроково розглянути її та використати для досліджуваного підприємства. Першим кроком є аналіз репутаційного ландшафту.

Для аналізу репутаційного ландшафту компанії використано сучасний інструмент соціального медіа «Hootsuite». Інструмент дозволяє планувати та відстежувати публікації на різних соціальних мережах, а також відслідковувати згадки та обговорення про компанію.

Інструмент надав дані стосовно компанії у медіа-просторі, найбільш показовими обрано дані Global Data Huawei найчастіше згадували в соціальних мережах під час MWC 2022.

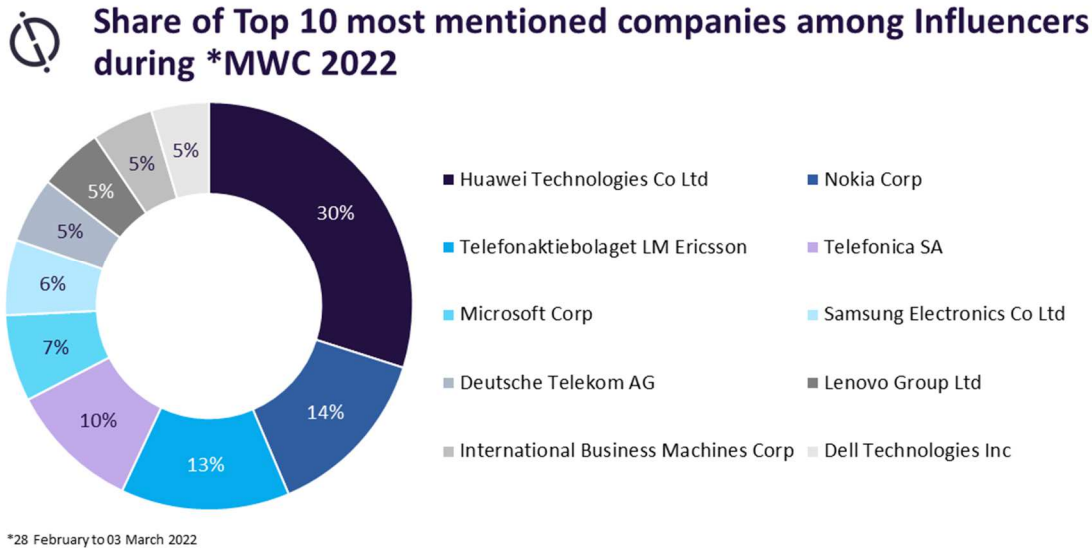

Рис. 3.2. Топ 10 згадуваних компаній

Джерело: складено за даними [61]

На частку Huawei припало 30% розмов із впливовими особами на MWC 2022. Дискусії навколо Huawei були зосереджені в основному на широкому спектрі інновацій компанії, включаючи її останній флагман MateBook X Pro 2022, розвиток напряму 5G та інші розумні рішення, які зосереджені на можливостях розумного офісу. Це свідчить про те, що, незважаючи на існуючі виклики, компанія продовжує залишатися актуальною та привабливою для клієнтів завдяки впровадженню нових технологій та виробів.

Водночас, складно зробити остаточні висновки щодо позитивної чи негативної реакції громадськості на компанію Huawei, оскільки навіть у цьому аспекті проводилася прокитайська кампанія в соціальних мережах. За даними The New York Times, було виявлено певний перелік акаунтів, фотографії яких були створені нейромережею, а самі пости цих осіб спрямовані на лобіювання інтересів китайської компанії [61].

Важливо відзначити цікавий підхід до роботи з громадськістю для запобігання погіршенню репутації. Завдяки репостам подібних повідомлень, багато людей особисто дізнаються про це, що може підвести їх під вплив висловлюваних тез.

Рис. 3.3. Аналіз залучення і твітів компанії Huawei в соцмережах

Джерело: складено за даними [61]

На основі представленого на рис. 3.2 можна припустити, що компанія Huawei успішно взаємодіє з громадськістю, переважно за параметрами онлайн-згадувань, кількості лайків, твітів, що дозволяє їй випереджати конкурентів на ринку телекомунікацій та техніки.

Проте важливо врахувати, що ключовою аудиторією для компанії є китайці. Huawei у Китаї займає високі позиції поряд з іншими гігантами, такими як Xiaomi, і стикається із відмінними умовами, оскільки тут відсутні проблеми з законодавством, яке підтримує, зокрема, слідкування за особистими даними населення та передачу розвідданих даних комуністичній партії Китаю.

Для об`єктивності щодо сприйняття компанії «Huawei» доцільно перевірити кількість запитів аудиторії. Не дивлячись на лінійку товрі і послуг компанії цікавість з боку широкого загалу спадає. Пік щодо запитів припадав на травень 2019 року, потім відбувалося поступове, стабільне їх зменшення (рис. 3.4).

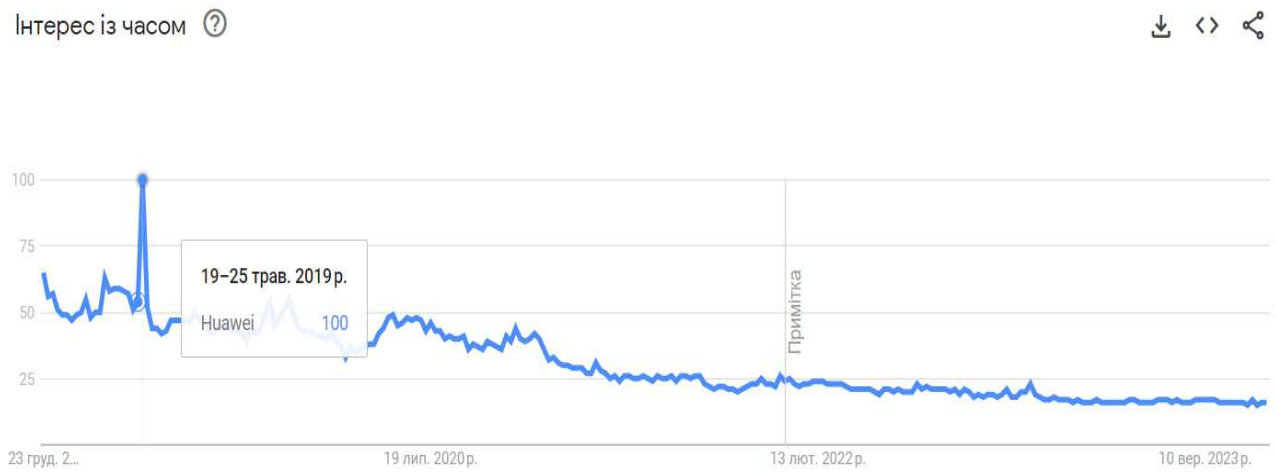

Рис. 3.4. Лінія тренду запитів щодо компанії «Huawei» за 2019-2023 рр.

Звісно, що така тенденція пояснюється політикою компанії щодо збирання інформації та даних про клієнтів компанії. Для того, щоб покращити дану ситуацію потрібно терміново вжити заходів щодо їх усунення.

З причини відмови у співпраці із компанією Австралії (у 2020 році), Америки та інших країн, цікавість щодо продукції та саме компанії «Huawei» проявляли споживачі із африканських країн (рис. 3.5.)

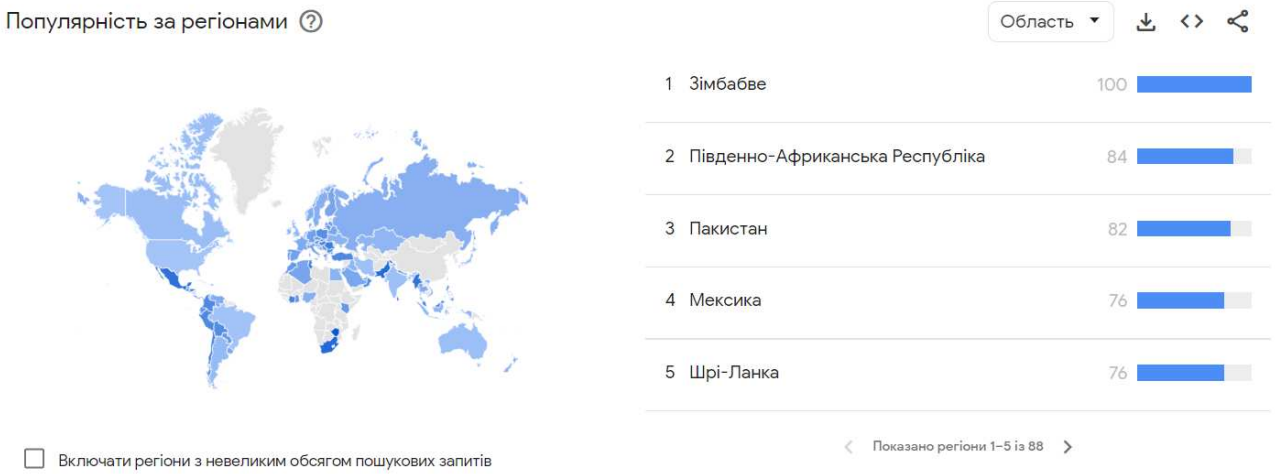

Рис. 3.5. Відображення запитів щодо компанії «Huawei» за країнами впродовж 2019-2023 рр.

У розрізі запитів за країнами світу, вбачається важливість питань розробки заходів заходів щодо покращення репутації компанії, її реабілітації для

підвищення інтересу до компанії та її продуктів споживачами із різних країн світу.

Для забезпечення об’єктивності в дослідженні та ідентифікації актуальних ризиків та загроз для компанії Huawei слід використатии SWOT-аналіз. SWOT враховує чотири основні аспекти: Сильні сторони (Strengths), Слабкі сторони (Weaknesses), Можливості (Opportunities) та Загрози (Threats).

Спеціалісти, які займаються SWOT-аналітикою, можуть включати в себе стратегічних консультантів, бізнес-аналітиків, маркетингових експертів та інших фахівців з управлінської сфери. Цей вид аналізу часто використовується компаніями для розробки стратегій, управлінського прийняття рішень та планування майбутніх кроків.

Незалежні дослідники, такі як бізнес-аналітики та консультанти, можуть надавати свої послуги для проведення SWOT-аналізу для компаній, що допомагає їм зрозуміти їхню внутрішню та зовнішню ситуацію, а також визначити стратегічні напрямки розвитку (рис. 3.6.).

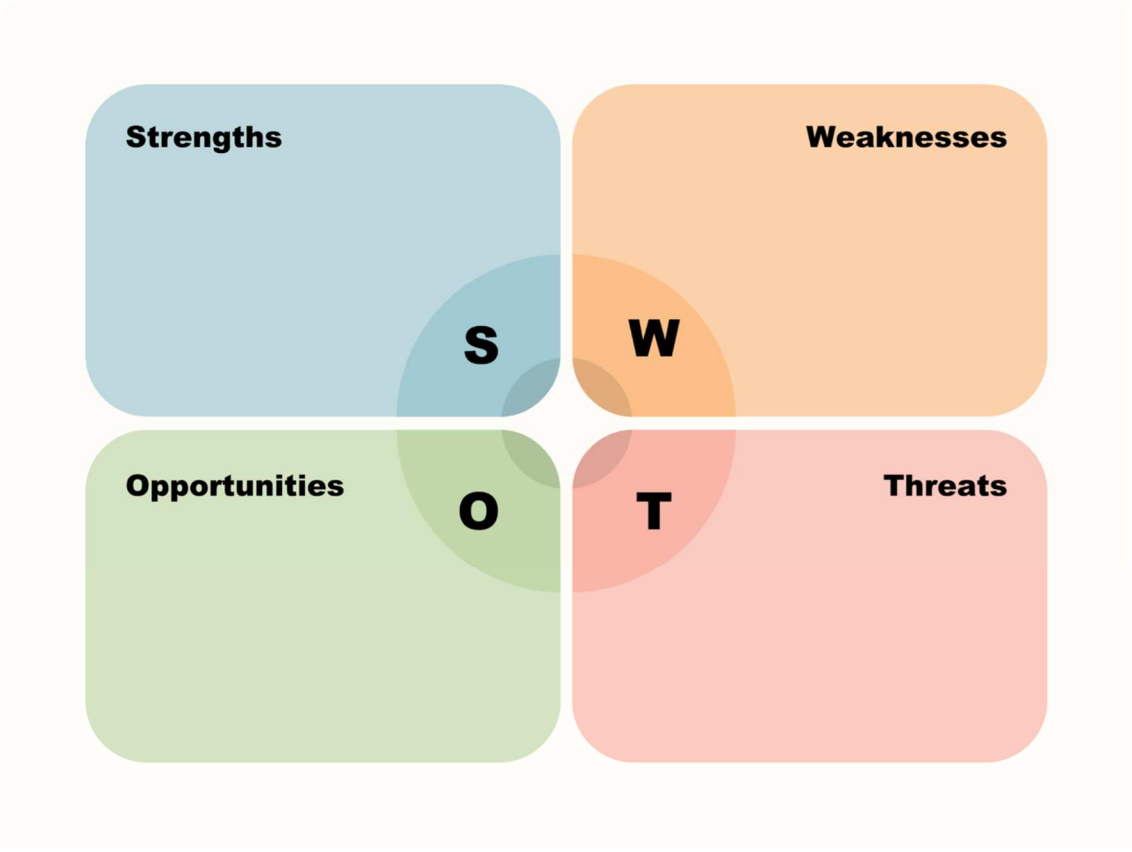

Рис. 3.6. SWOT-аналіз

Джерело: складено за даними [58]

Команія є ключовим гравцем у світовому телекомунікаційному та технологічному секторах, комплексний SWOT-аналіз Huawei проливає світло на його стратегічне становище в технологічній індустрії, яка жорстко конкурує[58].

Оскільки нас цікавлять прогалини у інформаційній безпеці та наявні репутаціні ризики, виокремимо саме слабкі сторони та загрози. Результати представимо у вигляді таблиці зі слабкими сторонами компанії та загрозами по SWOT-аналізу (табл. 3.1).

Таблиця 3.1

Слабкі сторони та загрози компанії Huawei по SWOT

Слабкі сторони	**Загрози**
Занепокоєння безпекою: Huawei зіткнулась із звинуваченнями у створенні загроз безпеці через тісні зв’язки з урядом Китаю, що призвело до заборон і обмежень у країнах Європи, США, Австралії.	Геополітична напруженість: поточна геополітична напруженість між Китаєм та іншими країнами може призвести до нових заборон і обмежень на діяльність Huawei. Продовження співпраці з російською федерацією в умовах повномасштамного вторгнення в Україну.
Залежність від закордонних ринків: значна частина доходів Huawei надходить з міжнародних ринків, що робить її вразливою до геополітичної напруженості та торгових суперечок.	Конкуренція: Huawei стикається з жорсткою конкуренцією з боку інших технологічних гігантів, таких як Apple, Samsung і Cisco, у різних категоріях продуктів.
Сприйняття бренду: негативна реклама та проблеми безпеки вплинули на сприйняття бренду Huawei та довіру споживачів. Найбільшими антирепутаційними кейсами були: Справа з США, Безпека та Шпигунство, Спроби Вилучення з Ринку.	Збої в ланцюжку постачання: збої в ланцюзі постачання, наприклад нестача компонентів, можуть вплинути на виробництво та час доставки. Найбільше постраждали мікропроцесори і центральні процесори, дисплеї, камери та сенсори, батареї, пам'ять (RAM і внутрішній накопичувач), чіпи та інтегровані схеми.

Продовження табл. 3.1

Проблеми з інтелектуальною власністю: компанія зіткнулася з судовими проблемами, пов’язаними з інтелектуальною власністю та порушенням патентів. Найвідомішими судовими справами є: Звинувачення у фінансових порушеннях та шпигунстві, Затримання Мен Ванчжоу в Канаді.	Регуляторні проблеми: розвиток норм, пов’язаних із конфіденційністю даних, кібербезпекою та телекомунікаційними стандартами, може створити проблеми з відповідністю щодо цих норм і стандартів. Була помічена невідповідність у конфіденційності даних, кібербезпеці, телекомунікаційних стандартах і т.д.
Відсутність доступу до ключових технологій: санкції та обмеження, які унеможливлюють доступ Huawei до критично важливих технологій і компонентів, таких як передове виробництво напівпровідників.	Втрата висококваліфікованих фахівців: вичерпання талантів через обмеження та негативне сприйняття може вплинути на здатність Huawei до інновацій.

Джерело: складено за даними [57-60]

Як не дивно, але більшість ризиків та загроз, які були розглянуті у другому розділі, залишаються актуальними для компанії, і деякі з них навіть підсилюються в умовах сучасності. Важливо зазначити, що крім турбот про безпеку, витоків інформації, інтелектуальної власності, регуляторних проблем та залежності від закордонних ринків, також зросли загрози на геополітичному рівні.

На даний момент немає повного підтвердження щодо виходу компанії з російського ринку у зв'язку з повномасштабним вторгненням в Україну. За інформацією від Leave Russia: Huawei припинив укладання нових контрактів на постачання мережевого обладнання російським операторам. Було призупинено виконання нових замовлень і частково звільнено персонал. З 1 липня 2022 року: активовано прийом на роботу. З 19 серпня 2022 року: Магазини Huawei в Росії припинили продаж товарів відвідувачам через відсутність офіційних поставок. З 6 вересня 2022 року: китайські та російські менеджери та керівники підрозділів були переведені до Казахстану та Узбекистану. Наразі відомо, що Росія та Китай вже мають певний досвід співпраці в сфері IT. Один з російських розробників співпрацює з китайською компанією Alibaba Group, а компанія "Ред Софт"

реалізує власний проект спільно з Huawei [60].

Незважаючи на те, що деякі контракти не продовжуються, існує можливість укладання додаткових угод, які доповнюють існуючі контракти. На думку автора, саме це і відбувається в поточний час.

Huawei, китайський телекомунікаційний гігант, не тільки залишається на російському ринку, але й підозрюється в допомозі режиму Путіна боротися з кібератаками на урядові та пропагандистські ресурси.

Про це навіть повідомляли китайські ЗМІ, але згодом усі подібні повідомлення були видалені. Зазначалося, що Huawei має намір використовувати свої дослідницькі центри в Росії (їх п'ять) для підготовки 50 тис. технічних фахівців для захисту російської інтернет-мережі від кіберзагроз.

Очевидно, Huawei відкидає всі звинувачення, але заявам китайських монополістів мало хто вірить. Зокрема, 7 березня один із найкращих футболістів XXI століття, форвард мюнхенської «Баварії» Роберт Левандовскі розірвав багатомільйонний спонсорський контракт з Huawei на тлі інформації про співпрацю китайського гіганта з Росією [59].

Насправді, це важливий аспект, який виникає з ситуації. Втрата ключових талантів може бути наслідком рішень компанії, яка утримується від виходу з ринку агресора та продовжує співпрацю з ним. Така позиція може негативно вплинути на імідж компанії серед професіоналів, які можуть утриматися від працевлаштування або співпраці з такою організацією.

Враховуючи ризики, пов'язані із санкціями проти компанії Huawei, існує реальна загроза того, що ці санкції можуть не тільки збільшитись, але й стати повноцінними загрозами для компанії. Це може взяти форму втрати активів, переважно в грошовому еквіваленті та на ринках, що може значно вплинути на фінансовий стан та конкурентоспроможність компанії. Також важливо враховувати можливі ризики, пов'язані з іміджем компанії, що можуть виникнути внаслідок продовження співпраці з країною-агресором.

Доцільно визначити стану інформаційних загроз репутації компанії «Huawei» (табл. 3.2)

Таблиця 3.2

Визначення стану інформаційної безпеки та ризиків репутації компанії «Huawei»

Роки	Кількість запитів	Темп росту, %	Стан	
2019	100	-53	загрозливий	
2020	53	-49	загрозливий	
2021	26	-96	загрозливий	
2022	25	-72	загрозливий	
2023	18			

Інтерпритація показників (приріст) стану інформаціної безпеки (загрози репутації):

0-10 – позитивний

0 - (-10) - середній

Нижче 0 - (-10) – загрозливий/

За результатами дослідження, стан інформаційної безпеки та репутаційних ризиків визначається як загрозливий, тому доцільно застосувати запропоновану технологію управління репутаційними ризиками до конкретних загроз та запропонувати шляхи удосконалення управління ними.

3.3 Застосування технології до конкретних загроз та пропозиції щодо удосконалення управління репутаційними ризиками компанії

Запропоновану комплексну технологію управління репутаційними ризиками та загрозами, доцільно використати, спираючись на результати власних досліджень та аналізу даних Інтернету на прикладі актуальної проблеми геополітичних змін.

У світлі стрімких змін у геополітичному, технологічному та регуляторному середовищі компанія Huawei стикається із викликами, що можуть вплинути на її репутацію та стабільність на міжнародних ринках. Для ефективного управління

репутаційними ризиками та мінімізації негативних впливів, необхідно ретельно розглядати та розробляти стратегічні заходи.

Доцільно розпочати з аналізу репутаційного ландшафту. Більша частина країн Європейського Союзу, Сполучених Штатів та України виступають проти співпраці Huawei з російським ринком. У той же час існують країни, які залишаються нейтральними стосовно виходу компанії з російського ринку, такі як країни Африки, Близького Сходу та частково країни Азії.

У разі відсутності реакції та внесення змін у політику можливі серйозні наслідки для компанії. Сполучені Штати та Європейський Союз вже ввели санкції проти Huawei та обмежують продаж її технологій на власній території. Якщо не реагувати на цей ризик, перед компанією може постати загроза втрати ринку в Україні та інших країнах, які висловлюють підтримкунашій країні.

Щодо аналізу аудиторії, важливо відзначити, що компанія Huawei активно присутня у соціальних мережах, зокрема на LinkedIn, де має значну аудиторію. Більшість цієї аудиторії, однак, не виявляє особливого інтересу до подій в Україні. Їхні головні інтереси стосуються придбання бюджетного обладнання та надання доступних сервісів підтримки.

У контексті взаємодії з Україною, компанія Huawei може розглядати розробку стратегій та заходів для зміцнення своєї репутації та сприяння стабільності в регіоні. Однією з можливих стратегій реагування на геополітичний ризик є активна участь компанії в соціальних проєктах, спрямованих на розвиток освіти та екологічних ініціатив.

Наприклад, компанія може встановити партнерство з місцевими освітніми установами в Україні, сприяти впровадженню програм підтримки освіти та науки. Це може включати створення стипендіальних програм, фінансову підтримку для освітніх ініціатив, а також розвиток інноваційних освітніх технологій.

Компанія не стоїть на місці і вже вживає подібні заходи. Вона має численні партнерські угоди з українськими вузами та реалізує освітній проект Seeds For the Future, який також передбачає навчання студентів у своїй фірмі.

Зокрема, компанія може прийняти участь у гуманітарних програмах, що спрямовані на надання допомоги постраждалим від конфліктів та катастроф в Україні. Це може включати надання фінансової допомоги, матеріальних ресурсів чи технологічної підтримки для відновлення інфраструктури та соціальних об'єктів.

Окрім того, компанія може активно сприяти екологічним ініціативам в Україні, зокрема, участь у програмах з екологічного управління, відновлення природних резерватів чи енергоефективності.

У випадку неможливості повного виходу з ринку Росії, компанії Huawei слід активно розглядати можливості поліпшення відносин та репутації в контексті взаємодії з Україною. Зокрема, важливо вжити конструктивних заходів, включаючи встановлення діалогу з представниками української влади та бізнес-спільноти, надання гуманітарної допомоги та розвиток спільних освітніх ініціатив. Компанії також варто припинити ігнорування війни і активно сприяти мирним ініціативам для зміцнення своєї репутації.

Компанії рекомендується уважно вивчити різницю між законодавством Китаю та тими країнами, де вони планують розвиватися. Законодавство Китаю дозволяє збір персональних даних користувачів, що відрізняється від підходу багатьох інших країн Заходу. Важливо враховувати цей факт і отримати відповідні дозволи для здійснення такої діяльності. Або, як мінімум, це не повинно бути прихованою інформацією, і компанія повинна відкрито ставитися до цього, навіть якщо раніше не було подібних прецедентів, а вони були.

Для покращення репутації Huawei важливо знаходити певний компроміс між урядовими вимогами та вподобаннями клієнтів. Однак ключовою відмінністю полягає в тому, що клієнти в довгостроковій перспективі приносять більше користі, ніж урядові відносини.

В конкурентному середовищі між телекомунікаційними та іншими гігантами, такими як Apple, Cisco і Samsung, важливо використовувати можливості для адаптації досвіду їхньої взаємодії з клієнтською базою. Зазначено, що ці компанії уникають гучних скандалів щодо збору інформації,

тому китайське підприємство можуть взяти у них приклад у цьому аспекті. Участь у конкуренції, враховуючи та підлаштовуючись під правила ринку та навіть застосовуючи деякі елементи поведінки конкурентів, може призвести до позитивних результатів у майбутньому.

Міжнародна компанія Huawei повинна абсолютно дотримуватись стандартів безпеки, зокрема щодо порушень цілісності інформації, відповідно до норм серії ISO 27000. Розуміючи необхідність надавання розвідданню Комуністичної Партії Китаю для функціонування в межах країни, важливо враховувати, що такий підхід може ускладнити участь компанії на міжнародному ринку. Актуальною також стає тема досягнення компромісу з усіма країнами, де Huawei розгортала свою діяльність на міжнародному рівні.

Щодо існуючих санкцій проти компанії Huawei, рекомендацією є відповідальне виконання зобов'язань, накладених санкціями, що може сприяти їх подальшому зняттю і поліпшенню виробничих та репутаційних показників. З метою вирішення можливих майбутніх загроз пропонується використовувати наявний досвід для уникнення подібних ситуацій. Наприклад, провести превентивний аналіз можливих дій з урахуванням можливості настання додаткових санкцій проти компанії.

Для вирішення проблеми відтоку висококваліфікованих кадрів із компанії рекомендується взаємний обмін досвідом з партнерами на короткостроковій основі або продовження політики стажування для студентів. Останнє може призвести до утворення значної кількості висококваліфікованих фахівців по всьому світу в довгостроковій перспективі.

Один із суттєвих аспектів для компанії на сучасному етапі - припинити провадження бізнесу у тіньовому режимі. Це означає припинення укладання додаткових угод з Російською Федерацією та постачання їй технологій, підтримки та обладнання через посередницькі країни. Крім того, це також може відноситися до інших країн, наприклад, Ірану, який, навіть у умовах санкцій, економічної блокади та необхідності так званого "паралельного імпорту", успішно функціонує на близькому сході.

В цілому, розробка та впровадження таких стратегій дозволять компанії Huawei зберегти та зміцнити свою репутацію в Україні і в світі, виступаючи як соціально відповідальний партнер та сприяючи розвитку регіональних ініціатив.

Додатково, важливо розглядати можливість диверсифікації ринків та зосередження на розвитку нових напрямків. Наприклад, активна експансія в регіони з меншою геополітичною напруженістю може допомогти зменшити ризик втрати ринків у зонах конфлікту.

Ще однією порадою є підтримка відкритого діалогу із зацікавленими сторонами, такими як громадські організації, правозахисні групи та інші. Спроба зрозуміти та враховувати їхні погляди може сприяти покращенню стосунків та зменшенню ризиків.

Нарешті, важливо впроваджувати додаткові заходи з внутрішньої та зовнішньої комунікації, такі як вебінари, відкриті листи та прес-конференції, щоб роз'яснити позицію компанії та її зобов'язання. Це може сприяти кращому сприйняттю публікою та іншими зацікавленими сторонами.

Узагальнюючи розглянуті аспекти, таблиця надає відображення ключових рекомендацій для компанії, охоплюючи прогалини виявлені з використанням запропонованої комплексної системи управління ризиками. Поради щодо усунення загроз та слабких сторін

Таблиця 3.3

Поради щодо усунення загроз та слабких сторін

Загрози і слабкі сторони	**Поради по вирішенню**
Занепокоєння безпекою	Активна участь у розробці та дотримання стандартів безпеки, а також забезпечення прозорості у зборі та використанні персональних даних. Це також можуть бути заходи щодо розвідувальної інформації, партнерство із незалежними організаціями.
Залежність від закордонних ринків	Диверсифікація ринків та збільшення внутрішньої стійкості, шляхом розвитку місцевих ринків та залучення нових клієнтів. Клієнтів можна залучити завдяки локалізації продуктів та послуг, партнерства та співпраці з місцевими компаніями, маркетингу та реклами, залучення до освітніх та інноваційних проектів, соціальній відповідальності та сприяння громаді.
Сприйняття бренду	Активне управління репутацією, враховуючи специфіки різних культур та уникнення контроверсійних практик. Слід враховувати мову та комінікацію, символи та кольори, звичаї та свята, соціокультурні цінності, етичні стандарти, історичні та політичні аспекти.
Проблеми з інтелектуальною власністю	Ефективний захист прав інтелектуальної власності, в тому числі через партнерство та відкритий обмін технологіями. Цього можно досягти завдяки патентуванню та реєстрації ІВ, моніторингу та виявленню порушень, виявленню та управлінню ризиками в постачальному ланцюзі, відкритому обміну технологіями і стандартами, ефективної комунікації, освіті та тренінгу.
Відсутність доступу до ключових технологій	Розробка власних технологій та активне партнерство з інноваційними компаніями для забезпечення доступу до передових розробок. Ключові актуальні технології на даний момент це: IoT, штучний інтелект, 5G, кібербезпека і блокчейн, енергоефективні технології та відновлювана енергія, біотехнології і медичні розробки.
Геополітична напруженість	Прогнозування та адаптація до змін у геополітичному середовищі, а також активне налагодження дипломатичних стосунків. З чого почати налагодження зв’язків
Конкуренція	Систематичний моніторинг конкурентів, аналіз їхніх стратегій та невпинне вдосконалення власних продуктів та послуг.
Збої в ланцюжку постачання	Диверсифікація постачальників та регулярна оцінка ризиків, включаючи розробку резервних планів для управління кризовими ситуаціями.
Регуляторні проблеми	Активне співробітництво з регуляторами, попередження можливих проблем та вчасне вирішення регуляторних питань. Пошукати в доменах стандарту ISO 27000
Втрата висококваліфікованих фахівців	Розвиток привабливого робочого середовища, надання можливостей для розвитку та утримання висококваліфікованих працівників. Конкретні кроки по досягненню цієї цілі, наприклад: впровадження програм розвитку та перепідготовки, кар’єрних можливостей, гнучких умов роботи, корпоративної культури і командного духу, конкурентоспроможної заробітньої плати, бонусних систем, забезпечення робочих місць, доступу до знань і збереженню робочого досвіду (документації).

Джерело: узагальнено автороом за результатами дослідження

Виконання стратегічних заходів, спрямованих на покращення безпеки, диверсифікацію ринків, управління репутацією та інноваційний розвиток, може суттєво позитивно позначитися на репутації компанії Huawei. Прозорість у використанні персональних даних, адаптація до різноманітних культурних контекстів і етичний підхід до бізнесу можуть сприяти збільшенню довіри споживачів та позиціонуванню Huawei як відповідального учасника ринку.

Це, в свою чергу, може призвести до підвищення конкурентоспроможності компанії, збільшення привабливості для інвесторів та розширення клієнтської бази. За умови успішної реалізації цих стратегічних напрямків, Huawei може закріпити свою репутацію як надійного та інноваційного лідера в галузі телекомунікацій та технологій, що відіграє важливу роль у розвитку глобальної індустрії.

Після часткового впровадження наведених вище рекомендацій, слід провести аналіз реакції суспільства та оцінити ефективність обраної стратегії. У висновку важливо зауважити, що після перевірки результатів дій можна перейти до контингентного планування. Це дозволить знизити ймовірність повторення аналогічних ризиків, а компанія буде володіти готовим планом дій в разі виникнення подібних обставин.

Висновки до третього розділу

Третій розділ спрямований на удосконалення системи управління репутаційними ризиками компанії, враховуючи виявлені прогалини у інформаційній безпеці та репутаційні ризики.

На етапі виявлення прогалин та ризиків, зокрема у контексті компанії Huawei, визначено, що небезпечність виникає внаслідок геополітичної напруженості, особливо в Україні та інших регіонах.

Розроблено комплексну технологію управління репутаційними ризиками, що враховує нестабільність глобального середовища та потребу адаптивних стратегій.

Застосування цієї технології до конкретних сценаріїв ризиків включає у себе активну участь у соціальних проектах, зокрема гуманітарній допомозі та освітніх програмах, що може сприяти покращенню репутації та відносин з українською спільнотою.

Ураховуючи висновки попередніх розділів, можна визначити, що успішне управління репутаційними ризиками потребує інтегрованого підходу, включаючи технологічні інновації, соціальні взаємодії та стратегії глобальної взаємодії. Зокрема, у випадку компанії Huawei, важливо виокремити необхідність активної участі у розв'язанні глобальних проблем, що допомагатиме сприяти позитивній репутації та покращенню відносин із всіма зацікавленими сторонами.

ВИСНОВКИ

Репутаційні ризики є суттєвим аспектом забезпечення інформаційної безпеки компанії, що вимагає комплексного та систематичного підходу до їх управління. У першому розділі роботи було розглянуто поняття "репутація" та "репутаційні ризики" компанії, а також визначено їх вплив на діяльність підприємства. Також встановлено взаємозв’язок між репутаційними ризиками та інформаційною безпекою компанії.

У другому розділі було проведено аналіз репутаційних ризиків, їх оцінка та визначені особливості функціонування компанії. Важливим етапом є оцінка ризиків, пов'язаних з інформаційною та репутаційною сферами, для ефективного забезпечення інформаційної безпеки.

У третьому розділі обговорено шляхи удосконалення управління репутаційними ризиками компанії. Виявлено прогалини у інформаційній безпеці та виникнення репутаційних ризиків, що підкреслює важливість розробки комплексної технології управління цими ризиками. Запропоновано застосування цієї технології до конкретних загроз з подальшими порадами щодо їх вирішення.

У цій роботі надано загальний погляд на управління репутаційними ризиками як важливої складової інформаційної безпеки компанії. Отримані висновки та рекомендації можуть служити основою для розробки та впровадження ефективних стратегій управління репутаційними ризиками для підприємств та слугувати підгрунтям для розробки пропозицій захисту від репутаційних ризиків для унеможливлення нанесення шкоди у разі їх появи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Reputation and cyber: why it matters. BCS, The Chartered Institute for IT | BCS. URL: https://www.bcs.org/articles-opinion-and-research/reputation-and-cyber-why-it-matters/ (дата звернення: 18.12.2023).

2. Управління ризиками інформаційної безпеки | ALP. URL: https://bohemia-club.com.ua/posts/uk/bezopasnost-upravlinna-rizikami-informacijnoi-bezpeki.shtml (дата звернення: 18.12.2023).

3. 2014 global survey on reputation risk. Deloitte. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf (дата звернення: 18.12.2023).

4. Reputation Risk in the Cyber Age. THE IMPACT ON SHAREHOLDER VALUE. Better Decisions | Aon. URL: https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf?utm_source=aoncom&utm_medium=storypage&utm_campaign=reprisk2018 (дата звернення: 18.12.2023).

5. Global Risk Management Survey. Better Decisions | Aon. URL: https://www.aon.com/getmedia/8d5ad510-1ae5-4d2b-a3d0-e241181da882/2019-Aon-Global-Risk-Management-Survey-Report.aspx#:~:text=A%20key%20insight%20from%20Aon%E2%80%99s%202019%20Global%20Risk,stakeholders%20.%20Top-of-mind%20concerns%20include%20a%20slowing%20economy (дата звернення: 18.12.2023).

6. Reputational Cyber Risk - How to Avoid Business Loss - Black Kite. Black Kite. URL: https://blackkite.com/blog/reputational-cyber-risk-how-to-avoid-business-lost/ (дата звернення: 18.12.2023).

7. Uber Pays $148 Million Over Yearlong Cover-Up Of Data Breach. NPR. URL: https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-

long-cover-up-of-data-breach (дата звернення: 18.12.2023). Uber Pays $148 Million Over Yearlong Cover-Up Of Data Breach. NPR. URL: https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-long-cover-up-of-data-breach (дата звернення: 18.12.2023).

8. Reputation and Its Risks. Harvard Business Review. URL: https://hbr.org/2007/02/reputation-and-its-risks (дата звернення: 18.12.2023).

9. Updates on Target's security and technology enhancements. News, Careers, Investors, Sustainability & Governance | Target Corporation. URL: https://corporate.target.com/news-features/article/2014/04/updates-on-target-s-security-and-technology-enhanc (дата звернення: 18.12.2023).

10. Buckbee M. Analyzing Company Reputation After a Data Breach. Varonis: We Protect Data. URL: https://www.varonis.com/blog/company-reputation-after-a-data-breach (дата звернення: 18.12.2023).

11. Cost of a data breach 2023 | IBM. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: https://www.ibm.com/reports/data-breach (дата звернення: 18.12.2023).

12. Data security is critical to your organization's reputation strategy | Security Magazine. Security Magazine | The business magazine for security executives. URL: https://www.securitymagazine.com/articles/96741-data-security-is-critical-to-your-organizations-reputation-strategy (дата звернення: 18.12.2023).

13. Shred-it's 2021 Data Protection Report Reveals the Need to Protect Data Has Never Been More Important. Paper Shredding Services & Document Destruction. URL: https://www.shredit.com/en-us/data-protection-report-2021 (дата звернення: 18.12.2023).

14. Reputation Risk Management and Cybersecurity - ivision. ivision. URL: https://ivision.com/blog/reputation-risk-management-cybersecurity/ (дата звернення: 18.12.2023).

15. CEO and Board Risk Management Survey Report. Deloitte United States. URL: https://www2.deloitte.com/us/en/pages/risk/articles/ceo-board-of-directors-risk-management-survey.html (дата звернення: 18.12.2023).

16. Kharpal A. Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice. CNBC. URL: https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html (дата звернення: 18.12.2023).

17. Corera G. Huawei: MPs claim 'clear evidence of collusion' with Chinese Communist Party. BBC News. URL: https://web.archive.org/web/20201014044835/https://www.bbc.com/news/technology-54455112 (дата звернення: 18.12.2023).

18. China's Tech Giant Huawei Spans Much Of The Globe Despite U.S. Efforts To Ban It. NPR. URL: https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it (дата звернення: 18.12.2023).

19. Huawei People. Huawei - Building a Fully Connected, Intelligent World. URL: https://www.huawei.com/minisite/whoishuawei/journey.html (дата звернення: 18.12.2023).

20. Lee D., Brandao S. Huawei Is Bad for Business. Foreign Policy. URL: https://foreignpolicy.com/2021/04/30/huawei-china-business-risk/ (дата звернення: 18.12.2023).

21. Chinese ambassador ‘threatens German car industry’ if Huawei is banned. South China Morning Post. URL: https://www.scmp.com/news/china/diplomacy/article/3042190/chinese-ambassador-accused-threatening-german-car-industry-if (дата звернення: 18.12.2023).

22. Y. Chuin-Wei, State Support Helped Fuel Huawei’s Global Rise. The Wall Street Journal. URL: https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736 (дата звернення: 18.12.2023).

23. BUSINESS TODAY - HUAWEI TECHNOLOGIES A Chinese Trail Blazer In Africa. Wayback Machine. URL: https://web.archive.org/web/20111009035828/http://www.businesstoday.lk/article.php?article=931 (дата звернення: 18.12.2023).

24. Smith J., Did Outsourcing and Corporate Espionage Kill Nortel? |

ASSEMBLY. Assembly Magazine | Manufacturing automation and design | ASSEMBLY. URL: https://www.assemblymag.com/blogs/14-assembly-blog/post/90631-did-outsourcing-and-corporate-espionage-kill-nortel (дата звернення: 18.12.2023).

25. China's rise in the Global South : the Middle East, Africa, and Beijing's alternative world order | WorldCat.org. WorldCat.org. URL: https://search.worldcat.org/title/1249712936 (дата звернення: 18.12.2023).

26. 3Com buys out Huawei joint venture for $882 million. Network World. URL: https://www.networkworld.com/article/835843/wireless-3com-buys-out-huawei-joint-venture-for-882-million.html (дата звернення: 18.12.2023).

27. Mcmorrow R. Huawei a key beneficiary of China subsidies that US wants ended. Phys.org - News and Articles on Science and Technology. URL: https://phys.org/news/2019-05-huawei-key-beneficiary-china-subsidies.html (дата звернення: 18.12.2023).

28. Perlroth N., Markoff J. Symantec Dissolves a Chinese Alliance (Published 2012). The New York Times. URL: https://www.nytimes.com/2012/03/27/technology/symantec-dissolves-alliance-with-huawei-of-china.html#:~:text=SAN%20FRANCISCO%20–%20Less%20than%20four,States%20government%20classified%20information%20about (дата звернення: 18.12.2023).

29. Financial Highlights - About Huawei. Wayback Machine. URL: https://web.archive.org/web/20150803223143/http://www.huawei.com/en/about-huawei/corporate-info/financial/index.htm (дата звернення: 18.12.2023).

30. Fife R., Chase S. Telus to build out 5G network without China’s Huawei. The Globe and Mail. URL: https://www.theglobeandmail.com/politics/article-telus-to-build-out-5g-network-without-chinas-huawei/ (дата звернення: 18.12.2023).

31. Huawei asks court to rule US ban unconstitutional. CNET. URL: https://www.cnet.com/tech/mobile/huawei-asks-court-to-rule-us-ban-unconstitutional/ (дата звернення: 18.12.2023).

32. Souppouris A. ZTE and Huawei face EU investigation over predatory

pricing. The Verge. URL: https://www.theverge.com/2013/5/18/4342884/zte-and-huawei-eu-investigation-karel-de-gucht-anti-competitive-dumping (дата звернення: 18.12.2023).

33. Gollom M. Huawei is 'growing astronomically' despite spying allegations | CBC News. CBC. URL: https://www.cbc.ca/news/business/huawei-china-telecom-arrest-spying-1.4934905 (дата звернення: 18.12.2023).

34. Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack - BNN Bloomberg. BNN. URL: https://www.bnnbloomberg.ca/chinese-spies-accused-of-using-huawei-in-secret-australia-telecom-hack-1.1697167 (дата звернення: 18.12.2023).

35. German Court Slams Huawei, ZTE Over AVC Patent Infringement. The News Chronicle. URL: https://web.archive.org/web/20181121192849/https://thenews-chronicle.com/german-court-slams-huawei-zte-over-avc-patent-infringement/ (дата звернення: 18.12.2023).

36. Blackwell T. Exclusive: Did Huawei bring down Nortel? Corporate espionage, theft, and the parallel rise and fall of two telecom giants. nationalpost. URL: https://nationalpost.com/news/exclusive-did-huawei-bring-down-nortel-corporate-espionage-theft-and-the-parallel-rise-and-fall-of-two-telecom-giants (дата звернення: 18.12.2023).

37. Jury awards T-Mobile $4.8M in trade-secrets case against Huawei. | The Seattle Times. URL: https://www.seattletimes.com/business/technology/july-awards-t-mobile-48m-in-trade-secrets-case-against-huawei/ (дата звернення: 18.12.2023).

38. Corinne R., O’Keeffe K. China’s Huawei Charged With Racketeering, Stealing Trade Secrets. https://www.wsj.com/articles/chinas-huawei-charged-with-racketeering-11581618336. URL: https://www.wsj.com/articles/chinas-huawei-charged-with-racketeering-11581618336 (дата звернення: 18.12.2023).

39. Nakashima E., Shih G., Hudson J. Leaked documents reveal Huawei’s secret operations to build North Korea’s wireless network. Washington Post. URL: https://www.washingtonpost.com/world/national-security/leaked-documents-reveal-huaweis-secret-operations-to-build-north-koreas-wireless-

network/2019/07/22/583430fe-8d12-11e9-adf3-f70f78c156e8_story.html (дата звернення: 18.12.2023).

40. Wheeler C. Chinese tech giant Huawei ‘helps to persecute Uighurs’. The Times & The Sunday Times. URL: https://www.thetimes.co.uk/article/chinese-tech-giant-huawei-helps-to-persecute-uighurs-7dfcb56nw (дата звернення: 18.12.2023).

41. Lecher C. Huawei is challenging its US contracting ban as unconstitutional. The Verge. URL: https://www.theverge.com/2019/5/29/18644040/huawei-government-ban-lawsuit-policy-unconstitutional (дата звернення: 18.12.2023).

42. Addition of Entities to the Entity List. Federal Register. URL: https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list (дата звернення: 18.12.2023).

43. Chen S. Trump bans Americans from investing in 31 companies with links to Chinese military. Axios. URL: https://www.axios.com/2020/11/12/china-military-trump-investments-ban (дата звернення: 18.12.2023).

44. Wadhams N., Westall S. Biden Prods UAE to Dump Huawei, Sowing Doubts on Key F-35 Sale. Bloomberg. URL: https://www.bloomberg.com/news/articles/2021-06-11/biden-prods-uae-to-dump-huawei-sowing-doubts-on-key-f-35-sale (дата звернення: 18.12.2023).

45. Schaffer A., Starks T. FCC steps up campaign against Huawei and other Chinese tech companies. The Washington Post. URL: https://www.washingtonpost.com/politics/2022/11/28/fcc-steps-up-campaign-against-huawei-other-chinese-tech-companies/ (дата звернення: 18.12.2023).

46. Writer S. Huawei in 'survival mode' as suppliers race to beat US deadline. Nikkei Asia. URL: https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-in-survival-mode-as-suppliers-race-to-beat-US-deadline (дата звернення: 18.12.2023).

47. Writer S. Huawei builds up 2-year reserve of 'most important' US chips. Nikkei Asia. URL: https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-builds-up-2-year-reserve-of-most-important-US-chips (дата звернення: 18.12.2023).

48. Kathrin Hille, Yuan Yang and Qianer Liu. Huawei develops plan for chip plant to help beat U.S. sanctions. Los Angeles Times. URL:

https://www.latimes.com/business/story/2020-11-01/huawei-chip-plant (дата звернення: 18.12.2023).

49. In Chip Race, China Gives Huawei the Steering Wheel: Huawei's New Smartphone and the Future of Semiconductor Export Controls. CSIS | Center for Strategic and International Studies. URL: https://www.csis.org/analysis/chip-race-china-gives-huawei-steering-wheel-huaweis-new-smartphone-and-future (дата звернення: 18.12.2023).

50. Faulkner C. Huawei developed its own operating systems in case it's banned from using Android and Windows. The Verge. URL: https://www.theverge.com/2019/3/14/18265646/huawei-operating-systems-android-windows-ban (дата звернення: 18.12.2023).

51. UK extends deadline to remove Huawei equipment from 5G network core. Reuters. URL: https://www.reuters.com/business/media-telecom/uk-extends-deadline-remove-huawei-equipment-5g-network-core-2022-10-13/ (дата звернення: 18.12.2023).

52. China's Huawei, ZTE Set To Be Shut Out of India's 5G Trials. Bloomberg. URL: https://www.bloomberg.com/news/articles/2020-08-13/china-s-huawei-zte-set-to-be-shut-out-of-india-s-5g-trials (дата звернення: 18.12.2023).

53. A Clinical Look at Huawei's Reputation Management. Ishmael's Corner ~ Storytelling Techniques For Business Communications. URL: https://www.ishmaelscorner.com/a-clinical-look-at-huaweis-reputation-management/ (дата звернення: 18.12.2023).

54. Huang W. Strengthening Risk Control and Compliance Management. SpringerLink. URL: https://link.springer.com/chapter/10.1007/978-981-13-7507-1_5 (дата звернення: 18.12.2023).

55. Ковтун В. ТЕОРЕТИЧНІ АСПЕКТИ ВИЗНАЧЕННЯ РЕПУТАЦІЙНИХ РИЗИКІВ ПІДПРИЄМСТВА. Київський національний економічний університет. URL: https://kneu.edu.ua/userfiles/ec_pidpr_th_pr_4/5/Kovtun.doc (дата звернення: 18.12.2023).

56. Success Story of Huawei | Milestones & Achievements [Infographic].

Mailing List - Sales Leads - Email Marketing List | InfoClutch. URL: http://www.infoclutch.com/infographic/huawei-company-history-timeline/ (дата звернення: 18.12.2023).

57. Product List | HUAWEI Support Global. HUAWEI Deutschland. URL: https://consumer.huawei.com/en/support/product/ (дата звернення: 18.12.2023).

58. SWOT Analysis of Huawei: Strengths & Weaknesses 2023. Ultimate Marketing Blogs in Simple Words. URL: https://writohub.com/swot-analysis-of-huawei/ (дата звернення: 18.12.2023).

59. Oliiarnyk M. Sponsors of Russian fascism. What global brands consciously decided to stay put in Russia. ZABORONA. URL: https://zaborona.com/en/colas-black-list-what-global-brands-consciously-kept-their-ties-to-russia/ (дата звернення: 18.12.2023).

60. Huawei. #LeaveRussia: The List of Companies that Stopped or Still Working in Russia. URL: https://leave-russia.org/uk/huawei (дата звернення: 18.12.2023).

61. Satariano A. Inside a Pro-Huawei Influence Campaign (Published 2021). The New York Times. URL: https://www.nytimes.com/2021/01/29/technology/commercial-disinformation-huawei-belgium.html (дата звернення: 18.12.2023).