

до таргетування.

Фінансова позиція України покращилася, і за період з 24 лютого по 20 вересня Міністерство фінансів України забезпечило фінансування на суму 33,9 млрд доларів, але лише 19 млрд доларів із них надали міжнародні донори. І під час перегляду цього міжнародного фінансування очевидними є кілька яскравих проблем.

Цілком очевидно, що цей тягар непропорційно лягає на плечі США, які надали Україні фінансування в розмірі 8,5 млрд доларів США переважно у формі грантів. Європейський Союз (ЄС) та європейські двосторонні кредитори надали трохи більше 5 млрд доларів – ЄС дійсно обіцяв 9 млрд євро фінансування, але виплатив лише близько 2,4 мільярда.

Крім того, трохи більше половини з 19 млрд доларів США, наданого на сьогоднішній день, було надано у формі позик. Якщо так триватиме й надалі, після завершення війни Україна опиниться під непосильним борговим тягарем. Це може закінчитися черговою руйнівною реструктуризацією боргу саме тоді, коли знадобиться швидкий доступ до фінансових ресурсів, щоб забезпечити повну участь приватного сектора у величезних потребах відбудови країни.

Протягом 2022 року гривня продовжувала слабшати, головна небезпека полягала в тому, що макрофінансова стабільність знаходиться під загрозою, з ризиком втечі банків і більш широкою втратою довіри до валюти та фінансової системи. Та вже починаючи з середини січня 2023 року курс стабілізувався, почали надходити грошові потоки від експорту (ускладнення логістики призвело до збільшення циклу життя продукту), можемо спостерігати навіть укріплення гривні.

Сьогодні, Україні потрібно зосередитися на веденні війни та досягненні перемоги, а це можливо лише за підтримки міжнародних партнерів, як військової так і бюджетної. Україна веде війну і бореться, з однієї сторони, за свою свободу, населення та землю, а з іншої, захищає демократію та цінності своїх союзників, ставши бар'єром між агресором та цивілізованим світом

Перелік джерел посилань:

1. Офіційний сайт Міністерства фінансів України – [Електронний ресурс]. – Режим доступу: <https://mof.gov.ua/uk>
2. Офіційний сайт Національного банку України – [Електронний ресурс]. – Режим доступу: <https://bank.gov.ua/>
3. Timothy Ash, “International finance”, Chatham House, The Royal Institute of International Affairs, 2022

Демченко В.О.

*к.е.н., доцент кафедри банківської справи та страхування
Київський національний економічний університет
імені Вадима Гетьмана*

БЕЗПЕКА БІЗНЕСУ ЯК ФАКТОР МІНІМІЗАЦІЇ ІНФОРМАЦІЙНИХ

РИЗИКІВ

Інформаційні ризики стали елементом безпеки бізнесу в сучасному світі. За останнє десятиліття, зростаючий обсяг інформації та її значущість для розвитку бізнесу призвів до збільшення кількості загроз, пов'язаних з її обробкою, зберіганням та передачею.

Інформаційні ризики можуть бути класифіковані як загрози безпеці даних, які можуть призвести до втрати чутливої інформації або її порушення, а також до збитків для бізнесу та його репутації. Такі ризики можуть включати в себе кібератаки, витоки даних, несанкціонований доступ до інформації, помилки в програмному забезпеченні та багато іншого. Пошкодити можуть як неправомірні дії нашого власного персоналу, так і зовнішні атаки.

Основні типи інформаційних ризиків включають:

Кібератаки: це спроби несанкціонованого доступу до комп'ютерних систем і мереж.

Втрата даних: це може відбутися через помилкову дію працівників, технічні проблеми або кібератаки.

Фінансові ризики: це може відбутися через крадіжку інформації про платіжні картки, обман клієнтів, а також через фінансові злочини власного персоналу.

Ризики в області дотримання законів: індивідуально відповідності різних законів, зокрема в галузі захисту персональних даних, авторських прав і прав інтелектуальної власності.

Мінімізація інформаційних ризиків є критично важливою для будь-якого я компанії, щоб забезпечити захист своєї інформації, а також зберегти довіру клієнтів та партнерів. Для цієї компанії необхідно проводити заходи, щоб захистити свої комп'ютерні системи та мережі від зловживань та несанкціонованого доступу [1].

Деякі рекомендації для мінімізації інформаційних ризиків включають:

Надавати доступ до комп'ютерних систем лише авторизованим працівникам і періодично змінювати паролі.

Використовувати програмне забезпечення для блокування шкідливих програм, через які можуть витікати дані.

Зберігати копії своїх даних у безпечному місці та перевіряйте їх на наявність вірусів.

Контролювати доступ до інформації та захищати дані клієнтів і партнерів.

Регулярно навчати співробітників політиці конфіденційності і процедурі безпеки даних.

Для запобігання несанкціонованому доступу використовуються різні методи шифрування та захисту даних.

Аудит даних безпеки виконується для перевірки дійсності введених даних безпеки. Різниця полягає в тому, що компанії можуть скористатися послугами компаній зі зберігання даних і кібербезпеки, щоб забезпечити додатковий рівень захисту даних.

Підсумовуючи, інформаційні ризики які сьогодні є реальною загрозою для бізнесу. Завдяки проактивному захисту даних і належним заходам дані компаній

збережуть їх репутацію та довіру клієнтів і партнерів, а також захистять їхні інвестиції та фінансові ресурси від можливих порушень даних.

Отже, збільшення використання інформаційних технологій у сучасному бізнесі призвело до збільшення кількості інформаційних ризиків, з якими доводиться стикатися компаніям. Відсутність належної безпеки бізнесу щодо мінімізації таких ризиків може мати серйозні наслідки, які можуть значно погіршити фінансовий стан та репутацію компанії[2]. Щоб уникнути негативних наслідків, підприємства повинні приділяти всю увагу мінімізації інформаційних ризиків. Для цього необхідно провести аудит інформаційної безпеки, застосувати будь-які загрози та небезпеки, розробити план превентивних дій, запровадити в компанії системи контролю та моніторингу інформаційних процесів.

Необхідно також пам'ятати, що мінімізація інформаційних ризиків – це постійний процес безпеки, який потребує постійного оновлення та вдосконалення заходів інформаційної безпеки.

Тому підвищення обізнаності про інформаційний ризик і розуміння необхідності його мінімізації в сучасному бізнесі може допомогти компаніям уникнути негативних наслідків, зберегти репутацію та захистити свої інвестиції.

В цілому, мінімізація інформаційних ризиків у сучасному бізнесі є кількома елементами успішної стратегії безпеки компаній. Це зауважують як великих корпорацій, так і малих підприємств. Крім того, інформаційні ризики не обмежуються лише комп'ютерними або кібернетичними атаками, вони також можуть виникати в результаті людських помилок, фізичних загроз та інших факторів.

З'ясовуючи з вищевикладеного, інформаційні ризики – це суттєва загроза для сучасного бізнесу. Через збільшення кількості цифрових технологій та використання Інтернету значно збільшується кількість негативних загроз для компаній. Щоб мінімізувати ці ризики, необхідно забезпечити безпеку даних та мережі, вдосконалити технічні та організаційні заходи безпеки, а також навчити своїх співробітників правилам безпеки даних.

Забезпечення безпеки даних є важливою складовою успіху та довіри споживачам та партнерам, тому компанії повинні приділяти увагу цьому питанню як пріоритетному. Виконання рекомендацій з мінімізації інформаційних ризиків дозволяє компаніям збільшити свою безпеку та довіру споживачів та партнерів, які в свою чергу позитивно відобразяться на їхньому бізнесі та доходах.

Перелік джерел посилання:

1. Говорун, О.В., Литвин, О.В., Наумов, О.А. (2020). Інформаційні ризики в сучасному бізнесі: причини та наслідки. URL:<http://repository.kpi.kharkov.ua/handle/KhPI-Press/53632>
2. Hoffman, P., & Marelli, S. (2016). Management of information security in organizations: an integrated structure. Journal of Business Ethics, 137(3), 639-658. doi: 10.1007/s10551-015-2614-6

Довбуш І.В.
«Економіка», 2 курс