

відбуваються чи можуть виникнути на ринку та вплинути на компанію, яка функціонує в цьому середовищі.

2) Системи прогнозування: дозволяють використовувати дані, щоб прогнозувати потенційний попит на товари та послуги, рівень очікуваних продажів, зміни цін на товари під впливом зміни кон'юнктури на ринку та інші фактори, що впливають на бізнес. Це може допомогти компанії спланувати своє виробництво, запаси та інші операції (наприклад, керуючись концепцією "just-in-time"), щоб забезпечити максимальну економічність та прибутковість.

3) Системи управління логістикою: дозволяють компаніям відстежувати рух товарів від постачальника до клієнта, тобто на всій протяжності глобального ланцюга постачання. Вони можуть допомогти у визначенні оптимального маршруту доставки, оптимальних термінів і вартості доставки, що зможе значно покращити показники діяльності підприємства через оптимізацію витрат та підвищення ефективності різноманітних логістичних операцій.

4) Системи економічного прогнозування: дозволяють використовувати моделі та аналітичні методи для макропрогнозування розвитку економіки та ринків. Вони можуть допомогти компанії в ідентифікації потенційних ризиків та можливостей у міжнародному середовищі.

Таким чином, можна зробити висновок, що інформаційно-аналітичні системи та технології є невід'ємною і критично важливою частиною сучасної економіки, оскільки дозволяють підвищити ефективність та якість прийнятих рішень в умовах обмеженості ресурсів. З-поміж інших переваг і позитивних результатів, можна забезпечити інформаційно-аналітичних систем та технологій нового покоління для ідентифікації найефективніших маркетингових стратегій з урахуванням конкретних умов розвитку смарт-економіки, оптимізації логістичної діяльності та управління запасами, зменшення виробничих витрат та підвищення рівня якості продукції відповідно до потенційних змін у потребах споживачів на різних ринках.

Список використаних джерел

1. Клепікова О.А. Інформаційно-аналітичні системи прийняття рішень в управлінні підприємством. Вісник соціально-економічних досліджень. *Вісник соціально-економічних досліджень*. 2017. №1. С. 196-204.
2. Blau B., van Dinther C., Flath C. M., Knapper R., Rolli D. Data Analytics for Smart Decision-Making and Resilient Systems. URL: https://www.researchgate.net/publication/351112446_Data_Analytics_for_Smart_Decision-Making_and_Resilient_Systems
3. Novak A., Bennett D., Klietk T. Product Decision-Making Information Systems, Real-Time Sensor Networks, and Artificial Intelligence-driven Big Data Analytics in Sustainable Industry 4.0. *Economics, Management, and Financial Markets*. 2021. №16(2). P. 62–72.

Науковий керівник: Литвиненко Л. Л., к.е.н., доцент.

Білявська Ю.В., к.е.н., доцент

Державний торговельно-економічний університет

y.biliavska@knute.edu.ua

ДОВІРА ДО ЦИФРОВИХ ТЕХНОЛОГІЙ: НОВА ЕРА КІБЕРБЕЗПЕКИ

Цифрові технології нині є ключовим фактором розвитку підприємств, відтак кібербезпека стає дедалі актуальнішим напрямком наукових досліджень. Розвиток Суспільства 5.0. та перехід на 5G-мережі несе із собою нові виклики, які беззаперечно пов'язані з коректною роботою програмного забезпечення, активне користування яким, у свою чергу, несе кіберзагрози. Саме тому поняття кібербезпеки постійно розширюється паралельно із диджиталізацією суспільства.

Значна частина персоналу підприємств в усьому світі переведена в режим дистанційної роботи внаслідок пандемії COVID-19 та війни, а тому необхідно беззаперечно слідкувати за обізнаністю ризиків, які пов'язані з віддаленою роботою: атаками на акаунти в соціальних мережах; незахищеним віддаленим підключенням до установи; спробами фішингових атак; поширеним використанням офісної техніки в особистих цілях; шахрайством та незахищеністю інформаційних даних. Електронні підписи та послуги електронної ідентифікації є двома з основних рішень, які прискорюють цифрову взаємодію між учасниками, наприклад, для підтвердження особи під час доступу до державних послуг або підписання юридичних контрактів.

Сучасний світ давно зробив перший крок до принципово нової технологічної, економічної та соціальної реальності – нової епохи цифрової глобалізації. Забезпечення кібербезпеки є одним з вагомих пріоритетів в загальній системі національної безпеки України. Впроваджуючи новітні технології, цивілізація у XXI ст. сприяє активному формуванню супутніх ризиків. Також спостерігаємо зростання питомої ваги кіберзагроз, і ця тенденція в міру розвитку цифрових технологій в поєднанні зі штучним інтелектом лише посиляться, а зростання такого впливу сприятиме формуванню нової безпекової ситуації. Фундаментом дієвої системи кібербезпеки, безумовно, є ефективна нормативно-правова база, а тому слід зауважити на актуальності Указу Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 26.08.2021 р. [1], відповідно до якої передбачено перспективи створення максимально вільного та безпечного, відкритого і стабільного кіберпростору в інтересах забезпечення прав людини.

На сьогоднішній день кібербезпека здатна не лише реагувати на інциденти, але й запобігати атакам до їх початку, застосовуючи різні технології та накопичені знання. З метою покращення ефективності діяльності підприємства керівники з кібербезпеки сфокусовані на технологіях, а також на тісній співпраці з бізнес-командами. Нещодавні зміни бізнес-моделей спонукали багато підприємств прискорити реалізацію програм цифровізації. Керівники підприємств дедалі частіше звертаються до фахівців з інформаційної безпеки за допомогою у питаннях підвищення стійкості інформаційної системи та створення цінності захисту для бізнесу.

Останні роки відзначені сплеском випадків кіберзагроз. За результатами опитування респондентів сформовано карту впливу кіберзагроз на підприємство, що складається з чотирьох сегментів, кожен з яких має певні межі (рис. 1). Представлені на карті кіберзагрози можна узагальнити в сегментах залежно від масштабу впливу та масштабу рівня ймовірності. Таким чином, сегмент А «Аутсайдер» це група, в якій кіберзагрози мають незначну відносну частку. У результаті проведеного опитування визначено ступінь, а також оцінено їхній вплив на підприємство. До сегменту А потрапили такі види кіберзагроз, як колишні працівники, конкуренти та співробітники.

Кіберзагрози, що належать до групи В – «Потенціал», мають високі темпи росту: інформаційні інциденти, які пов'язані з дезінформацією. Такі види кіберзагроз як хакери та атаки за допомогою програм, спрямованих на порушення роботи важливих бізнес-сервісів, знаходяться на межі від сегменту В до сегменту С «Лідер» (найпоширеніші загрози). Беззаперечними лідерами кіберзагроз визначено діяльність кіберзлочинців та атака на хмарні сервіси.

І, останній сегмент D – «Генератор», що мають дуже слабкі позиції у списку кіберзагроз. Це зумовлене недостатнім рівнем функціонування. До таких належать постачальники хмарних сервісів, туманних технологій, інтернет речей і мобільні технології.

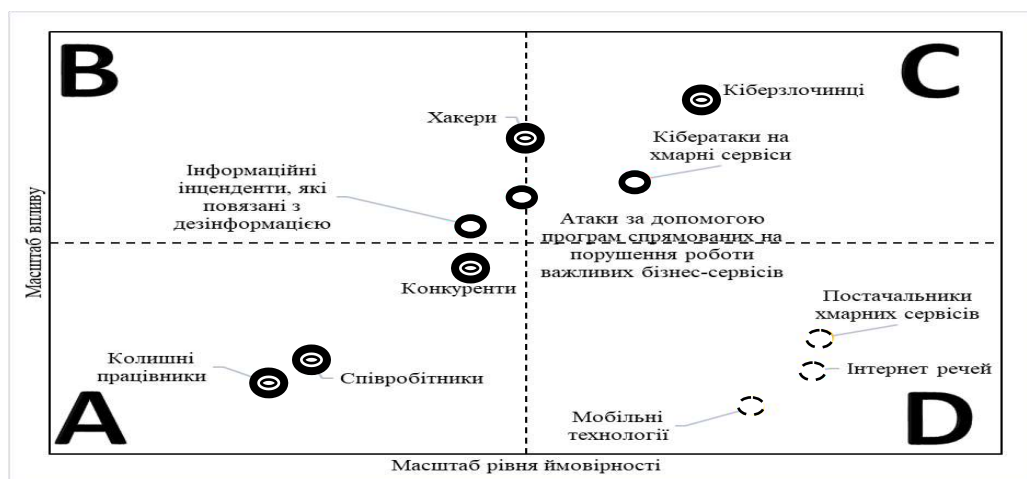


Рис. 1. Карта впливу кіберзагроз на підприємство

Примітка: - потужні і успішні атаки; - потенційні загрози;
 - прогноз інцидентів на 2022 р.; - потенційних загроз;

Джерело: розраховано авторами за даними анкетного опитування 217 респондентів 45 підприємств України у грудні 2021 р.

Таким чином, встановлено, що нова ера кібербезпеки вимагає цілком нових підходів до управління підприємством та його ресурсами, зокрема інформаційними. Успіх таких змін значною мірою залежить від того, як гнучко організовані бізнес-процеси на підприємстві, а також як імплементуються нові моделі та методи роботи. Через недоліки в організаційній роботі та невміння управляти змінами підприємства відчують наслідки кібер-ризиків, а тому вважаємо доречним дотримання кібергігієни за умов COVID-реальності

Список використаних джерел

1. Про рішення РНБО України від 14.05.2021 р. «Про Стратегію кібербезпеки України» від 26.08.2021 р. № 447/2021.: Указ Президента України. URL: <https://www.president.gov.ua/documents/4472021-40013>

Букраба О.М., аспірант
 Одеський національний економічний університет
aleksandrbrukraba@gmail.com

ПРОЕКТ СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Україна впевнено тримає курс на цифровізацію. Її мета полягає у тому аби реформувати усі процеси в нашій державі та об'єднати всі відомства в єдину зручну й дієву систему за допомогою інформаційних технологій. Це дозволить органам влади завжди мати актуальні дані для ухвалення ефективних рішень, спростить та зробить прозорим надання державних послуг громадянам та бізнесу, що призведе до зниження рівню корупції. Цифровізація має торкнутися не тільки галузі надання адміністративних послуг та електронного урядування, а й галузей освіти, охорони здоров'я, транспорту, судів, питань демократії тощо. Так, наразі, створений проект Електронна демократія (е-Демократія), який