Список використаних джерел:
1. Собкевич О. Перспективи модернізаційних зрушень у промисловості України в процесі євроінтеграції. URL: https://niss.gov.ua/news/komentari-ekspertiv/perspektyvy-modernizatsiynykh-zrushen-u-promyslovosti-ukrayiny-v-protsesi (дата звернення: 18.11.2023).
2. KPMG in Ukraine. Post-war Reconstruction of Economy: Case Studies. URL: https://assets.kpmg.com/content/dam/kpmg/ua/pdf/2023/01/post-war-reconstruction-of-economy-en.pdf (дата звернення: 18.11.2023).
3. Гуткевич С.О., Сидоренко П.О., Соломко А.С., Смик Р. Інвестування: міжнародний досвід: монографія. Харків "Діса плюс", 2017. 216 с.

ІНДИКАТОРИ КІБЕРЗАГРОЗ В СИСТЕМАХ МОНІТОРИНГУ БЕЗПЕКИ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

ПАКУЛІНА Алевтина Анатоліївна,
канд. екон. наук, доцент,
Харківський національний університет
міського господарства імені О. М. Бекетова
ЄВСЄЄВА Ольга Олексіївна,
д-р екон. наук, професор,
Український державний університет залізничного транспорту

Кіберзагроза для підприємства – це потенційна можливість виникнення шкідливих дій або подій в інформаційних технологіях (ІТ), які можуть завдати шкоди бізнес-процесам, даним чи іншим аспектам діяльності підприємства. Це може включати в себе різні види атак, такі як кіберпроникнення, віруси, шкідливі програми, фішінг, DDoS-атаки та інші загрози для інформаційної безпеки. Видами кіберзагроз для підприємства можуть: втрата даних (атаки, спрямовані на вкрадення або пошкодження конфіденційної інформації, можуть призвести до серйозних фінансових втрат та порушення довіри клієнтів); переривання бізнес-процесів (DDoS-атаки чи інші форми атак можуть призвести до призупинення роботи важливих систем, що може вплинути на продуктивність та призвести до фінансових втрат; пошкодження репутації (у випадку витоку важливої інформації або втрати даних, підприємство може зазнати шкоди своїй репутації, що може вплинути на відносини з клієнтами та партнерами); втрати фінансових активів (кіберзагрози можуть вплинути на фінансові активи підприємства, такі як рахунки, інвестиції або фінансові транзакції); порушення вимог щодо захисту даних (кіберзагрози можуть призвести до порушення правових вимог стосовно захисту особистих даних і викликати правові наслідки для підприємства); втрата доступу до систем та послуг (атаки, такі як розкрадання аутентифікаційних даних, можуть призвести до втрати доступу до систем та послуг, що може важко відновити та вимагати великих зусиль для відновлення) та інше.

Для захисту від кіберзагроз підприємства повинні вживати системних заходів інформаційної безпеки, таких як встановлення відповідних заходів захисту, навчання персоналу щодо кібербезпеки та використання сучасних технологій захисту даних з урахуванням можливостей в межах чинного законодавства. Зокрема в цьому питанні, основоположним нормативним документом є Закон України «Про основні засади забезпечення кібербезпеки України» [1], який визначає «… правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки».

Серед низки термінів, які вживаються у тлумаченні Закону України «Про основні засади забезпечення кібербезпеки України» [1] (індикатори кіберзагроз, кібератака, кібербезпека, кіберзагроза, кіберзахист, кіберзлочин (комп'ютерний злочин), кіберзлочинність, кібероборона, кіберпростір, кіберрозвідка, кібертероризм, кібершпигунство, критична інформаційна інфраструктура, Національна телекомунікаційна мережа, національні електронні інформаційні ресурси, Національний центр резервування державних інформаційних ресурсів, об'єкт критичної інформаційної інфраструктури, система управління технологічними процесами, системи електронних комунікацій, система активної протидії агресії у кіберпросторі, активна протидія агресії у кіберпросторі), з точки зору концептуально-модельного розуміння, на наш погляд, з метою побудови міцної системи кібербезпеки є такі поняття як сама «кібербезпека», «кіберпростір», «кіберзагроза», «кібератака» та «індикатори кіберзагроз».

На наш погляд, саме індикатори кіберзагроз є конкретними ознаками чи подіями, які вказують на наявність або можливість кіберзагрози. Вони використовуються для виявлення та реагування на потенційні загрози і дозволяють вчасно виявити порушення безпеки і запобігти їх подальшому розвитку.

Індикатори кіберзагроз можна розділити на дві основні категорії [2]: *індикатори компрометації* (IoC - Indicators of Compromise) – ці індикатори вказують на конкретні ознаки або сліди того, що система чи мережа була атакована або компрометована; та *індикатори атаки* (IoA - Indicators of Attack) - ці індикатори вказують на певні етапи або методи, які зловмисники використовують під час атаки, вони допомагають виявити атаку на ранніх стадіях, навіть до того, як система буде компрометована.

Індикатори кіберзагроз використовуються в системах моніторингу безпеки та аналізу подій для виявлення потенційно небезпечних ситуацій. Спостереження за такими індикаторами дозволяє вчасно реагувати на кіберзагрози, відокремлювати їх та забезпечувати безпеку інформаційних ресурсів підприємства [3].

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України [Закон України]: № 2163-VIII від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Державна служба спеціального захисту зв’язку та захисту інформації [державні сайти України]. URL: https://cip.gov.ua/ua.

3. Ievsieieva O., Kovalova D., Ievsieiev A. Organization of e-document management as a component of cloud technologies in strengthening the information segment of economic security. Science and technology: problems, prospects and innovations. Proceedings of the 5th International scientific and practical conference. CPN Publishing Group. Osaka, Japan. February 16-18, 2023.

ЕКОНОМІЧНІ ВИКЛИКИ В УМОВАХ ВОЄННОГО СТАНУ

ПАКУЛІНА Алевтина Анатоліївна,
канд. екон. наук, доцент,
СОКОЛОВ Владислав Андрійович,
здобувач вищої освіти
Харківський національний університет
міського господарства імені О. М. Бекетова

Умови воєнного стану не тільки тестують стійкість суспільства, але й створюють суттєві економічні виклики для суб'єктів господарювання. Цей період несе в собі низку унікальних проблем та загроз, які вимагають креативного та стратегічного підходу для подолання. Давайте поглибимося у світ економічних викликів в умовах воєнного стану:

- зменшення інвестицій та фінансова нестабільність. Воєнний стан призводить до невизначеності, що робить інвесторів обережними. Зменшення інвестицій та коливання фінансового стану стають серйозним викликом для підприємств. Розвиток креативних методів залучення капіталу та фінансова стратегія стають ключовими факторами для виживання.
- необхідність адаптації ланцюгів постачання та виробничих процесів. Умови воєнного стану породжують перешкоди у ланцюгах постачання та виробничих процесах. Суперечності та перерви у транспорті можуть призвести до затримок та втрат. Підприємства повинні пристосовувати свої виробничі процеси та знаходити альтернативні шляхи забезпечення ресурсами [1].
- зміни в попиті та споживчій психології. Воєнний стан супроводжується не тільки економічною, але й психологічною нестабільністю. Попит та споживча активність зменшуються через стресову обстановку. Ділові суб'єкти повинні адаптувати свої стратегії маркетингу та пристосовувати продуктові пропозиції до змін споживчої поведінки.
- правові та податкові зміни. Умови воєнного стану часто ведуть до змін в правовому та податковому середовищі. Суб'єкти господарювання повинні