Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет ___інформаційно-аналітичних технологій та менеджменту_____
(повна назва)
Кафедра _ __економічної кібернетики та управління економічною безпекою__
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

_____Механізм забезпечення захисту бізнесу в умовах гібридних загроз___
_____
(тема)

Виконав:
студент _2_ курсу, групи __УФЕБм-19-1__
_____Єфіміна О.О._____
(прізвище, ініціали)

Спеціальність __073 Менеджмент_____
_____
(код і повна назва спеціальності)
Тип програми _ __освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма ___Управління фінансово-економічною безпекою_____
(повна назва освітньої програми)

Керівник _____доц. Гришко С.В._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ ____Полозова Т. В.__
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет__інформаційно-аналітичних технологій та менеджменту_____
(повна назва)

Кафедра_економічної кібернетики та управління економічною безпекою___
(повна назва)

Рівень вищої освіти _____другий (магістерський)_____

Спеціальність _____073 Менеджмент_____
(код і повна назва)

Тип програми _____освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)

Освітня програма _____Управління фінансово-економічною безпекою_____
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____ 2020 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові_____Єфіміній Олені Олександровні_____
(прізвище, ім'я, по батькові)

1. Тема роботи _Механізм забезпечення захисту бізнесу в умовах гібридних загроз ____
_____
_____
затверджена наказом університету від _30_ ___жовтня_____2020 р. № _1493 Ст_
2. Термін подання студентом роботи до екзаменаційної комісії _21_ __грудня____ 2020 р.
3. Вихідні дані до роботи _Наукові літературні джерела, періодичні видання, фінансова___звітність підприємства, законодавчо-нормативні акти, електронні джерела._
_____
_____
_____
_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі _____
Вступ. 1 Методичні основи захисту підприємств в умовах гібридних загроз. 2 Аналіз діяльності та напрямів забезпечення економічної безпеки бізнесу ТОВ «Стройобзор». 3 Удосконалення механізму захисту бізнесу в умовах гібридних загроз. Висновки. Перелік джерел посилання. Додаток._____
_____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій_____
1. Об'єкт, предмет, мета і завдання дослідження._____
2-3. Гібридні впливи як загроза екосистемі підприємства._____
4-5. Бізнес як об'єкт та інструмент гібридних загроз._____
6-9. Аналіз результатів діяльності ТОВ «Стройобзор».____
10-12. Механізм протидії гібридним загрозам на рівні бізнесу_____
13. Критичні функції ТОВ «Стройобзор».____
14-15. Організаційні заходи та система індикаторів._____
16. Результати моніторингу гібридних загроз для ТОВ «Стройобзор»._____
17. Результати атестаційної роботи._____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Теоретичні аспекти дослідження захисту підприємств в умовах гібридних загроз	30.10.20-07.11.20	виконано
2	Аналіз виробничо-господарської діяльності ТОВ «Стройобзор»	08.11.20-14.11.20	виконано
3	Розробка шляхів підвищення безпеки бізнесу в умовах гібридних загроз	15.11.20-30.11.20	виконано
4	Оформлення атестаційної роботи	01.12.20-07.12.20	виконано
5	Перевірка атестаційної роботи на плагіат	08.12.20-09.12.20	виконано
6	Підготовка доповіді та ілюстративного матеріалу	10.12.20-14.12.20	виконано
7	Рецензування атестаційної роботи	15.12.20-21.12.20	виконано

Дата видачі завдання _30 жовтня 2020 р.

Студент _____
(підпис)

Керівник роботи _____ _____доц. Гришко С.В._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Атестаційна робота: 68 с., 22 табл., 9 рис., 42 джерела, 1 додаток.

ЕКОНОМІЧНИЙ ЗАХИСТ, ГІБРИДНІ ЗАГРОЗИ, ГІБРИДНІ ВПЛИВИ, СИСТЕМА ІНДИКАТОРІВ, МОНІТОРИНГ ЗАГРОЗ, ВРАЗЛИВОСТІ БІЗНЕСУ, КРИТИЧНІ ФУНКЦІЇ БІЗНЕСУ.

Об’єктом дослідження є управління бізнесом в умовах гібридних загроз. Предметом дослідження є методи оцінки та забезпечення захисту бізнесу в умовах гібридних загроз.

Метою роботи є теоретичне обґрунтування та розробка практичних рекомендацій з побудови механізму захисту бізнесу в умовах гібридних загроз.

Розглянуто методологічні аспекти захисту підприємств в умовах гібридних загроз, розкритий сучасний стан гібридних впливів на бізнес-середовище та охарактеризована стійкість до гібридних загроз як складова економічної безпеки підприємства. Продемонстровано, що бізнес-спільнота та окремі компанії є невід'ємною частиною суспільства, а отже, і об'єктами гібридного впливу. Проаналізовано діяльність та напрями організації економічної безпеки ТОВ «Стройобзор», досліджено існуючі на підприємстві напрями організації економічної безпеки. Визначені шляхи підвищення безпеки бізнесу в умовах гібридних загроз та запропонований організаційно-методичний підхід до забезпечення захисту ТОВ «Стройобзор».

ABSTRACT

Master thesis: 68 p., 22 tables, 9 fig., 42 sources, 1 exhibit.

ECONOMIC PROTECTION, HYBRID THREATS, HYBRID INFLUENCES, INDICATOR SYSTEM, THREAT MONITORING, BUSINESS VULNERABILITY, CRITICAL BUSINESS FUNCTIONS.

The object of the research is business management in the context of hybrid threats. The subject of the research is methods of assessing and ensuring business protection in the context of hybrid threats.

The purpose of the research – theoretical motivation and development practical recommendation for building a business protection mechanism in the context of hybrid threats.

The methodological aspects of protecting enterprises in the context of hybrid threats are considered, the current state of hybrid impacts on the business environment is revealed, and resistance to hybrid threats is characterized as a component of the economic security of an enterprise. It has been demonstrated that the business community and individual companies are an integral part of society, and therefore, objects of hybrid impact. The activity and directions of the organization of economic security of «StroyObzor» are analyzed, the directions of the organization of economic security existing at the enterprise are investigated. The ways of improving business security in the context of hybrid threats are identified and an organizational and methodological approach to ensuring the protection of «StroyObzor» is proposed.

ЗМІСТ

ВСТУП

Бізнес-середовище містить такі системи, інституції та інструменти, які необхідні для життєздатності країни. Напад на таке середовище може мати величезні дестабілізуючі наслідки та серйозно загрожувати функціонуванню суспільства. В умовах гібридних загроз такі напади дуже складно вчасно розпізнати, тому що гібридні дії характеризуються невизначеністю. Вони стирають лінії «бойового простору», розповсюджуючись до людського та економічного вимірів. Окрім прямого нападу на системні інституції (такі як банківська система), гібридні загрози можуть набувати різні форми впливу на бізнес-середовище. Особлива загроза складається в тому, що жодна з цілей не має видимості всієї операції, але ефект від них має каскадний характер. Навіть якщо приватний бізнес тимчасово втрачає здатність здійснювати операції, в критичний період невизначеності та в критичній галузі це призводить до мультиплікативного ефекту.

Але з іншого боку, гібридні загрози – це злісні проблеми. Вони неоднозначні та нечіткі, їм не вистачає перевірених знань та фіксованих стандартів, щоб адекватно їх вирішити. Це робить розробку системи попередження про такі загрози внутрішньо складною. До того, як гібридні загрози матеріалізуються, вони часто надсилають лише слабкі сигнали, які важко виявити і які неможливо легко пов’язати з будь-якою відомою тенденцією чи явищем. Тому гібридні загрози потребують нових рішень для попередження, а розробка механізму забезпечення захисту бізнесу в умовах гібридних загроз є актуальним завданням.

Об’єктом дослідження є управління бізнесом в умовах гібридних загроз. Предметом дослідження є методи оцінки та забезпечення захисту бізнесу в умовах гібридних загроз.

Метою роботи є теоретичне обґрунтування та розробка практичних рекомендацій з побудови механізму захисту бізнесу в умовах гібридних загроз.

Основними завданнями дослідження є:

– розглянути методологічні аспекти захисту підприємств в умовах гібридних загроз;

– розкрити сучасний стан гібридних впливів на бізнес-середовище;

– охарактеризувати стійкість до гібридних загроз як складову економічної безпеки підприємства;

– проаналізувати діяльність та напрями організації економічної безпеки ТОВ «Стройобзор»;

– виявити актуальні загрози безпеці досліджуваного підприємства в умовах гібридних впливів;

– визначити шляхи підвищення безпеки бізнесу в умовах гібридних загроз;

– запропонувати організаційно-методичний підхід до забезпечення захисту ТОВ «Стройобзор» в умовах гібридних загроз.

Методичною основою для проведення дослідження були періодичні наукові видання, законодавство України, фінансова звітність досліджуваного підприємства.

Під час дослідження були використані методи аналізу та синтезу інформації, яка характеризує діяльність підприємства з забезпечення його безпеки; порівняння та узагальнення показників безпеки діяльності підприємства; інтерпретація висновків, що випливають з результатів аналізу ситуації, яка складається у забезпеченні безпеки підприємств.

Практична значущість отриманих результатів полягає у тому, що запропоновані практичні рекомендації можуть бути використані підприємствами будь-якої галузі для забезпечення захисту бізнесу в умовах гібридних загроз.

Апробація результатів дослідження. Основні теоретичні положення і практичні результати проведених досліджень, висновки і рекомендації, які викладені в роботі, доповідались на І Міжнародній науково-практичній конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (Харків. 3 листоп. 2020) та І Всеукраїнській науково-практичній конференції «Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці» (Київ, 7 грудня 2020 р.).

Acknowledgment. Під час дослідження були використані матеріали Еразмус+ проєкту WARN «Academic Response to Hybrid Threats» (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP), який фінансується програмою Європейського Союзу Erasmus+.

Disclaimer: «The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein».

Публікації. Результати досліджень опубліковано у 2 наукових працях в якості 2 матеріалів конференцій (тези доповідей).

1 МЕТОДИЧНІ ОСНОВИ ЗАХИСТУ ПІДПРИЄМСТВ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

1.1 Гібридні впливи як загроза екосистемі підприємства

Термін «гібридна загроза» стосується дій, що проводяться державними або недержавними суб'єктами, метою яких є підрив або заподіяння шкоди цілі, впливаючи на прийняття рішень на місцевому, регіональному, державному чи інституційному рівнях. Такі дії координуються та синхронізуються і навмисно спрямовані на вразливість демократичних держав та інституцій. Діяльність може відбуватися, наприклад, у політичній, економічній, військовій, цивільній або інформаційній сферах. Вони проводяться з використанням широкого спектру засобів і призначені для того, щоб залишатися нижче порогу виявлення та приписування.

Гібридні дії характеризуються неоднозначністю, оскільки гібридні суб’єкти розмивають звичні межі міжнародної політики та діють у взаємозв’язку між зовнішніми та внутрішніми, законними та нелегальними, а також миром та війною. Неоднозначність створюється поєднанням звичайних та нетрадиційних засобів - дезінформації та втручання у політичні дебати чи вибори, критичні порушення інфраструктури або напади, кібер-операції, різні форми злочинної діяльності і, нарешті, асиметричне використання військових засобів та ведення війни.

Застосовуючи згадані вище нетрадиційні та загальноприйняті засоби, гібридні актори завуальовують свої дії невизначеністю та двозначністю, ускладнюючи атрибуцію та відповідь. Використання різних посередників - або довірених осіб - підтримує досягнення цих цілей. Гібридна дія є економічно ефективною, оскільки перетворює вразливість цілі на пряму силу для гібридного актора. Це ускладнює запобігання або реагування на гібридні дії.

Постійний перехід у міжнародні владні структури забезпечує благодатне середовище для гібридних дій. Посилення конфлікту цінностей між Заходом та авторитарними державами розмиває міжнародні норми та інститути та робить відкриті західні суспільства цілями всебічних гібридних дій. Конфлікт цінностей, що поширюється на внутрішню сферу західних суспільств, посилює поляризацію та роз'єднаність усередині та серед західних акторів, роблячи їх більш уразливими до зовнішнього втручання. Останні події в сучасних технологіях та дедалі складніша інформаційна обстановка забезпечують потужні інструменти для гібридних акторів, якщо західна спільнота не отримує належних заходів протидії.

Відповідно, Hybrid CoE (Європейський центр з протидії гібридним загрозам) характеризує гібридні загрози як «координовані та синхронізовані дії, які навмисно спрямовані на системну вразливість демократичних держав та інституцій за допомогою широкого кола засобів» [1]. Це діяльність, яка використовує пороги виявлення та приписування, а також різні інтерфейси (війна-мир, внутрішня-зовнішня безпека, місцева, державна та національно-міжнародна). Це діяльність, спрямована на вплив на різні форми прийняття рішень на місцевому (регіональному), державному чи інституційному рівні, і призначена для подальшого та / або виконання стратегічних цілей агента, одночасно підриваючи та / або завдаючи шкоди цілі. Нові гібридні загрози кидають виклик на кількох рівнях:

– нові загрози призводять до нових вразливостей суспільств;

– суспільства ще не мають достатніх навичок, щоб справлятися з новими загрозами.

Визнання гібридних загроз пройшло через низку важливих документів найвищого рівня (табл.1.1).

Україна є першою країною в Європі, яка серйозно постраждала від гібридного впливу (рис.1.1). Неможливо визначити, скільки років знадобиться, щоб оговтатися від гібридної війни, що триває.

Таблиця 1.1 – Визнання руйнівної сили гібридних загроз

Організація	Документ	Дата	Сутність
Парламентська асамблея Європи	Постанова PACE № 2217 [2]	квітень 2018	Гібридні загрози визнані глобальним викликом
Верховна Рада України	Указ № 219 [3]	27.01.2015	Непідготовленість та недооцінка російських гібридних впливів призвели до вибуху гібридної війни на території України та безпосереднього ворожого вторгнення
Парламентська асамблея НАТО	Спеціальний звіт № 166 CDS 18E [4]	жовтень 2018	
Європейський центр з протидії гібридним загрозам, Hybrid CoE	Експертна доповідь [5]	травень 2018	Україна стала передовою нового покоління воєн, де межі між миром та війною розмиті

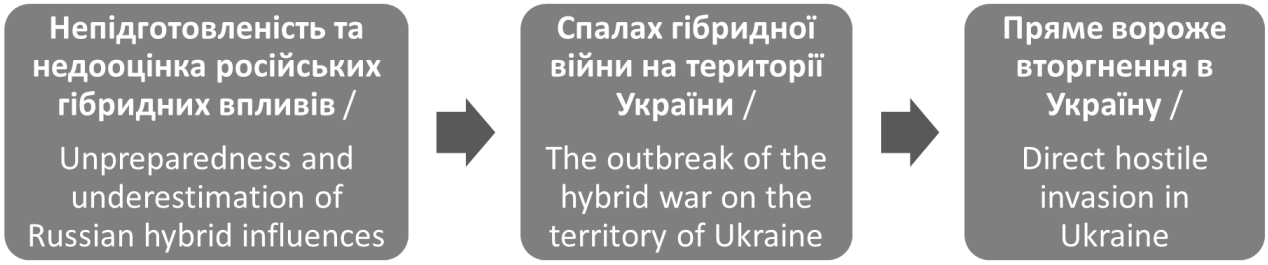

Рисунок 1.1 – Сценарій розвитку гібридних загроз в Україні

Це призвело до катастрофічних наслідків (табл.1.2).

Україна – не єдиний об’єкт гібридних атак. Численні дослідження повідомляють про здійснені напади по всій Європі та в усьому світі. Вони показують системну вразливість демократичних держав, інститутів та суспільств до широкого кола політичних, економічних, військових, соціальних та інших засобів гібридного впливу.

Європейський парламент та Рада розробили та прийняли Спільну основу протидії гібридним загрозам як відповідь ЄС. Європейський центр передового досвіду з протидії гібридним загрозам (Hybrid CoE) був створений як аналітичний центр гібридної оборони в ЄС.

Таблиця 1.2 – Наслідки дії гібридних загроз в Україні

Організація	Документ	Дата	Сутність
ООН, Управління Верховного Комісара з прав людини	Звіт УВКПЛ ООН про ситуацію з правами людини в Україні [6]	Лютий 2020	Україна втратила контроль над частиною своїх територій, Понад; 40 000 людей загинуло 30 000 – поранених
ООН	карта УКГВ "Україна: Огляд переміщення населення" [7]	2015	Майже 1,5 млн. внутрішньо переміщених осіб
The HALO Trust , міжнародна організація з розмінування територій	Огляд Halo: проблема України [8]	2020	Понад 420 га замінованих земель Майже 2 000 жертв - чоловіків, жінок та дітей, які зазнали травм або загинули внаслідок замінування території.
ООН, Управління Верховного Комісара з прав людини	Звіт УВКПЛ ООН про ситуацію з правами людини в Україні [9]	Серпень 2018	понад 40 000 цивільних будівель були пошкоджені або зруйновані
Євразійський центр Atlantic Council	Звіт Atlantic Council [10]	Березень 2018	Втрачені активи в Криму та на Донбасі складають 13,7% ВВП України

Гібридні загрози дуже різноманітні і з ними важко боротися. Ці загрози є дуже плавними та пристосованими, мають високу здатність адаптуватися, і можуть бути матеріалізовані окремими особами або групами, які не можуть бути визнані та контрольовані. Гібридні атаки мають на меті вплинути на прийняття рішень на державному, регіональному чи інституційному рівні, а також на радикалізацію вразливих членів суспільства, перетворюючи їх на «агентів негативних змін».

Гібридна діяльність використовує вразливі місця своїх цілей, незалежно від того, хто це є: люди, організації чи суспільство в цілому. Зазвичай, гібридні загрози та гібридний вплив створюються на державному рівні, коли держави організовано використовують як традиційні, так і

нетипові інструменти влади для досягнення своїх цілей. Вони прагнуть зробити це, не порушуючи «порогу виявлення» або, у більш важких випадках, «порогу традиційної війни» чи «порогу дорогої війни» [11]. Більш детально визначити гібридні загрози складно з кількох причин:

– гібридні «гравці» використовують старі, добре відомі тактики, але в несподіваних або мультиплікаційних комбінаціях;

– вони мають доступ до нових інструментів і методів, які ніколи раніше не застосовувались і навіть не думали, що їх можна використовувати як зброю на підтримку політичного порядку денного, такі заходи включають як старі трюки (як підкуп або примушення людей до співпраці), так й нові інструменти, які діджиталізація впровадила у всьому суспільстві (як кібершпигунство та кібератаки, проникнення до критичної інфраструктури, інформаційні операції за допомогою соціальних медіа тощо);

– часто буває важко віднести гібридну діяльність до певної країни чи організації, оскільки це є може проводитись довіреною особою (третя держава, фронт-організація, організована злочинність або окремий оператор), а іноді політичні чи економічні реалії навіть можуть забороняти цілям-жертвам повідомляти про напади або приписувати їх певному злочинцю;

– гібридна діяльність поєднує в собі не одну форму впливу на підтримку досягнення мети агресора, причому це поєднання не обов'язково відбувається одночасно: заходи можуть бути організовані послідовно, протягом тривалого періоду часу, розподілено як по географічному, так і по організаційному принципу, що ускладнює розпізнавання та визначення гібридної операції.

Таким чином, гібридні загрози – це широке поняття, яке постійно розвивається. Гібридні впливи можуть бути спрямовані на прийняття політичних рішень, діяльність влади, ділової спільноти або на будь-яку їх комбінацію. Але в будь-якому випадку, ця загроза є одним з найбільших викликів оточуючого середовища в глобальному масштабі.

1.2 Сучасний стан гібридних впливів на бізнес-середовище

Використання гібридної тактики не є новацією нинішнього часу. Новою є поява цих тактик в якості стратегічної загрози в так званій «сірій зоні», посилена технологічними досягненнями, які змінили природу глобального суперництва. Як зауважив представник ОБСЄ Дж. Гілмор, «тепер троянський кінь набув абсолютно нового значення» [12].

Гібридні методи за своєю природою задіють усі інструменти влади і застосовуються не у збройному конфлікті, а на порозі збройного конфлікту – в умовах зростаючої «сірої зони» [13]. В результаті стирається межа між війною та миром, зокрема – між конфліктом і конкуренцією, з'являється так звана «сіра зона конкуренції».

В сірій зоні конкуренції, гібридних гравців цікавлять потенційні системні прогалини, які відкривають можливість використовувати гібридний вплив на бізнес та економічні системи для створення порушень в розвитку країни (табл.1.3, за матеріалами [14]).

Підвищення стійкості бізнесу до таких впливів зазвичай вимагає рішень на стратегічному рівні [15]:

– регулювання іноземних інвестицій, протидія відмиванню грошей;

– «вирівнювання конкурентних умов» (санкції, засоби правового захисту тощо);

– економічна стійкість;

– стійкість технічної бази (успіх хоча б у деяких ключових технологіях);

– регулювання даних, особливо в сфері доступу до «технологій подвійного використання» тощо.

Але цього недостатньо, якщо громадське суспільство не готове до протидії гібридним загрозам. Бо в сучасних умовах «спільноти є тим клеєм, який утримує стабільні суспільства» [16].

Таблиця 1.3 – Використання бізнесу як гібридного інструменту (за матеріалами [14])

Ризики / вразливості	Приклади загроз
Розширення бізнесу при ігноруванні безпеки	Експансія російського «руського миру» [17], Експансія китайського «Belt and Road Initiative» [18]
Використання фінансових ресурсів для стратегічних цілей	Кредитування владою Китаю [15]
Відсутність безпекової координації незалежних бізнесів	Криза Covid-19 [19]
Придбання стратегічних активів	Діяльність Росатома в Європі [20]
Вплив через приховане інвестування	Російські сховані ланцюги володіння, оприлюднені через Panama papers leaks [21]
Спотворення моделі ринкової поведінки	Використання Китаєм переваг ВТО при агресивному протекціонізмі [22]
Взяття під контроль потоків	План «Made in China 2025» [23]
Фінансування прихованої діяльності через FinTech	Експансія платіжних систем Alipay, WeChat (Китай), МИР (Росія) [15]

Структури та процеси громадянського суспільства не є традиційною силою та навіть не входять до відповідальності військових у демократичних країнах. Але завдяки соціальним медіа громадянське суспільство стало озброєним простором, в якому проводяться нові гібридні битви. Ось чому підвищення обізнаності та стійкості кожного громадянина та кожного бізнесу є як ніколи важливим.

Бізнес-спільнота та окремі компанії є невід'ємною частиною суспільства, а отже, і об'єктами гібридного впливу. Роль ділової спільноти зросла за останні десятиліття, оскільки приватні компанії дедалі частіше надають послуги у таких секторах, як телекомунікації, медіа та енергетика. Раніше ці послуги надавали або місцеві муніципалітети, регіональні органи влади або держава. Як правило, компанії також продовжують піклуватися про ці критично важливі послуги та інфраструктуру як у звичайних

ситуаціях, так і у випадках кризи. Більше того, державний сектор та органи влади все більше залежать від технологій, ресурсів та послуг, що надаються компаніями в приватному секторі для підтримки своїх основних функцій та місії.

Оскільки гібридний вплив вимагає розуміння вразливостей цілей-жертв, операціям, як правило, передують зусилля зі збору інформації протягом тривалого періоду часу. Можуть бути використані наступні методи:

– проникнення в цільову організацію;

– використання традиційних методів людського інтелекту;

– проникнення в інформаційні системи за допомогою кібератаки або їх комбінації.

Бізнес-спільнота в цілому, і компанії зокрема, відіграють важливу роль у гібридному впливі. Але оскільки суб’єкта такого впливу важко визначити, то ділове співтовариство ще не зрозуміло власної ролі об’єкта гібридного впливу. Так, більше половини компаній у Фінляндії (59%) не змогли пояснити, чому вони можуть бути ціллю діяльності, кінцевою метою якої є вплив на населення або уряд країни [24]. Розглядаючи, як компанія може стати частковою ціллю гібридної операції, слід враховувати, що це залежить від кінцевої мети, цілі, слабких сторін компанії та інших факторів, невідомих всім, крім тих, хто планує та проводить гібридну операцію.

Об'єктом гібридного впливу можуть ставати не лише великі компанії, хоча вони є відомими, часто мають велику клієнтську базу, урядових клієнтів, стосунки з політиками, доступ до суспільної інфраструктури, а також інші фактори, які можуть встановити їх як цілі в гібридних операціях. На практиці кількість компаній, яких можна вважати цікавими об'єктами з точки зору гібридного впливу чи незаконного нагляду, значно вища. Оскільки важко розпізнати зусилля гібридного впливу, тому багато компаній навіть не підозрюють, що є потенційними цілями.

Гібридні агресори можуть отримати доступ до інформації обраної ними компанії шляхом [25]:

– розповсюдження шкідливого програмного забезпечення через зовнішні USB-пристрої чи інші електронні пристрої;

– за допомогою фішингових операцій;

– через використання найманих людей для збору інформації всередині цільової компанії.

Інформація, яка використовується, може здатися досить нешкідливою: хто за які рахунки відповідає, хто відвідує ті самі соціальні клуби, що й відповідальний за політичні рішення, тощо. Коли особу ідентифікують таким чином, і коли ця інформація пов’язана з інформацією про профіль її соціальних мереж, поведінкою в Інтернеті та інформацією, зібраною з інших джерел, – все це може стати зброєю гібридного «гравця» може мати змогу сформувати всебічний огляд, на якому вони може діяти. Інформація, отримана таким чином, може бути використана для впливу на людей. Доступ до інформації також піддає компанії ризику маніпуляції даними та ризику саботажу діяльності.

Використання «шпигунів» може бути дуже плідним: вони можуть отримувати доступ до інформації на основі своїх робочих завдань, вони знають, де шукати конкретну інформацію, і можуть легко виявити слабкі сторони людей, що знаходяться під впливом. Це вважається інформацією, яка може допомогти гібридному акторові визначити, чи варто націлювати гібридну операцію саме на цю компанію. При цьому працівники компанії можуть отримати доступ до такої інформації, майже не залишаючи слідів.

Серед слабких сторін бізнесу, через які гібридні «гравці» можуть впливати на бізнес, можна виділити наступне (рис.1.2).

Прозорість, наївність, недостатня обізнаність та пильність, нездатність розпізнавати проблеми – це питання, які можна виправити шляхом обміну інформацією та проведення навчання.

Гібридна діяльність може призвести до ситуації, коли ресурси та системи, які зазвичай доступні компаніям, для них вже недоступні.

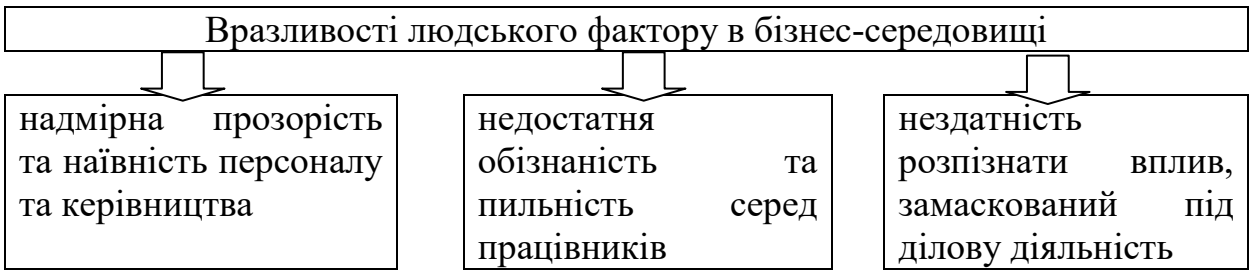

Рисунок 1.2 – Вразливості бізнесу в умовах гібридних загроз: людський фактор

Найбільш критичними факторами з точки зору здатності бізнесу працювати є: електроенергія, Інтернет та інформаційні системи. Цей тип ситуації представляє іншу крайність, в якій гібридний вплив більше не маскується. Ось чому компанія повинна підготувати план безперервності бізнесу, який допомагає їй продовжувати працювати за таких обставин.

1.3 Стійкість до гібридних загроз як складова економічної безпеки підприємства

Бізнес зазвичай стикається з проблемами забезпечення безпеки. Необхідність цього зумовлюється завданням забезпечення стабільності функціонування і досягнення головних цілей підприємницької діяльності в умовах нестабільного середовища [26].

В загальному розумінні економічна безпека підприємства – це організаційна система ефективного використання корпоративних ресурсів, метою якої є запобігання загрозам і створення умов стабільного функціонування підрозділів підприємства [27]. Основними функціональними цілями економічної безпеки підприємства є:

– забезпечення високої фінансової ефективності роботи, фінансової стійкості та незалежності;

– забезпечення технологічної незалежності та досягнення високої конкурентоспроможності технічного потенціалу;

– досягнення високої продуктивності менеджменту, оптимальної та ефективної організаційної структури управління підприємством;

– досягнення високого рівня кваліфікації персоналу та його інтелектуального потенціалу, належної ефективності корпоративних науково-дослідних та дослідно-конструкторських робіт;

– мінімізація руйнівного впливу результатів виробничо-господарської діяльності на стан навколишнього середовища;

– якісна правова захищеність усіх аспектів діяльності;

– забезпечення захисту інформаційного простору, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів та відділів;

– ефективна організація безпеки персоналу підприємства, його капіталу та майна, а також комерційних інтересів.

Як потенційний об'єкт гібридної агресивної діяльності, будь-який бізнес (навіть невеликий приватний бізнес, не задіяний в критичній інфраструктурі) має наступні вразливості (зони ризику) (рис.1.3).

Перша з перелічених вразливостей пов'язана із посиленою цифровізацією бізнесу. У сучасному світі велика кількість окремих фінансових операцій, навіть бізнес-процесів проводиться в цифровому форматі. З одного боку, діджиталізація збільшує ефективність за рахунок зменшення надмірностей, але з іншого боку це також робить системи більш вразливими. В оцифрованому світі вразливі місця можуть бути неактивними протягом тривалого періоду та експлуатуватися на відстані. Це перешкоджає ідентифікації та робить цифровізацію ефективним засобом у гібридному наборі інструментів.

Інший фактор ризику - це відсутність всеохоплюючого офіційного обміну інформацією між приватними гравцями щодо атак та захисних

механізмів. Основним джерелом ризику є те, що кіберсередовище є високо інтегрованим, в той час як політика безпеки залишається суто національною.

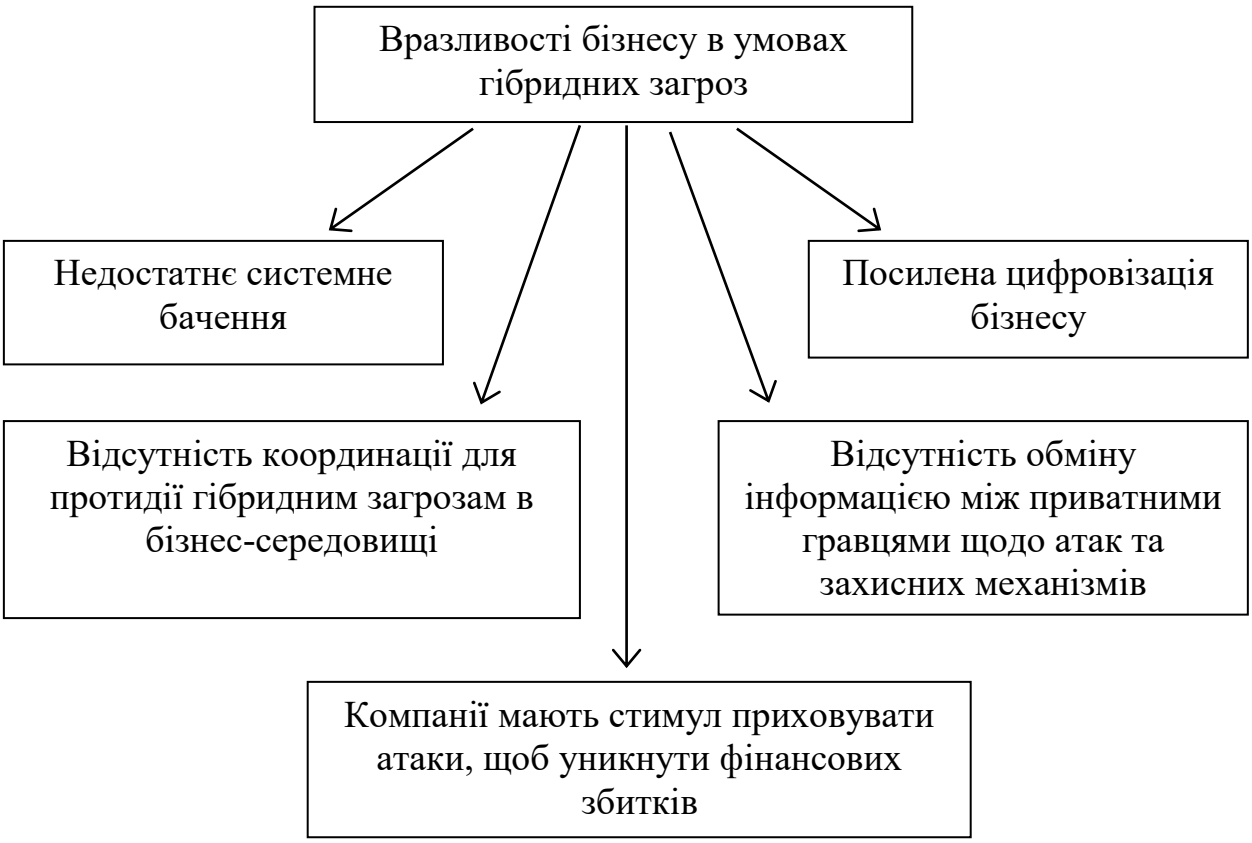

Рисунок 1.3 – Вразливості бізнесу як об'єкта гібридних загроз

Наступний фактор – відсутність координації для протидії гібридним загрозам в бізнес-середовищі. Рівень захисту суттєво відрізняється між різними суб'єктами, й через масштабну бізнес-інтеграцію різних галузей та ринків напад на окремий бізнес може мати значні каскадні наслідки для всього бізнес-середовища.

Недостатнє системне бачення є ще однією суттєвою загрозою бізнес-середовища. Кібератаки в основному розглядаються в типових рамках операційного ризику – це означає, що вони розглядаються як дії здебільшого приватних кримінальних акторів, а не як частина широкомасштабної, скоординованої гібридної операції проти нації. Навіть якщо приватні

компанії прагнуть бути індивідуально добре захищеними, існує недостатній системний захист.

Також компанії мають стимул приховувати атаки, щоб уникнути фінансових збитків. Суспільство в цілому отримує вигоду від посиленого захисту приватних гравців з точки зору конфіденційності та безпеки даних, але компанії не бажають нести витрати на додатковий захист, якщо він перевищує їх приватний рівень вигоди.

Одже, можна зробити висновок, що забезпечення безпеки бізнесу є найважливішим компонентом й у протидії гібридним загрозам.

Однак, як переконливо аргументував Патрік Каллен [28], гібридні загрози – це злісні проблеми. Вони неоднозначні та нечіткі, їм не вистачає перевірених знань та фіксованих стандартів, щоб адекватно їх вирішити. Це робить розробку системи попередження про такі загрози внутрішньо складною та складною.

До того, як гібридні загрози матеріалізуються, вони часто надсилають лише слабкі сигнали, які важко виявити і які неможливо легко пов’язати з будь-якою відомою тенденцією чи явищем. Більше того, ці слабкі сигнали містять величезну кількість недоречної або оманливої інформації, яку часто називають шумом. Крім того, «гібридні загрози покликані розмивати різницю між миром і війною, а також ускладнюють і падають нижче межі виявлення та реагування цілі». Тому гібридні загрози потребують нових рішень для попередження [29].

2 АНАЛІЗ ДІЯЛЬНОСТІ ТА НАПРЯМІВ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ БІЗНЕСУ ТОВ «СТРОЙОБЗОР»

2.1 Загальна характеристика діяльності підприємства

ТОВ «Стройобзор» засновано в 2007 році на власності фізичних осіб, зареєстроване в м. Харкові, форма власності – приватна. Воно функціонує відповідно до Цивільного і Господарського кодексів України і інших законодавчих актів. Організаційно-правова форма підприємства – товариство з обмеженою відповідальністю. Це означає, що учасники відповідають по зобов'язаннях товариства в межах своїх внесків. Будучи суб'єктом підприємницької діяльності, ТОВ «Стройобзор» має правовий статус юридичної особи.

Для забезпечення діяльності ТОВ «Стройобзор» сформований статутний капітал у розмірі 2 266 тис. грн. Зміна структури власності, коли до бізнесу приєдналась компанія Карлтон Індастріз Лімітед, призвела до збільшення власного капіталу на 7 453 тис. грн.

Підприємство функціонує на підставі статуту, в своїй діяльності керується рішеннями органів управління товариством і чинним законодавством. ТОВ «Стройобзор» самостійно здійснює свою діяльність, розпоряджається отриманим прибутком, що залишився в розпорядженні після сплати податків і інших обов'язкових платежів.

Основним видом діяльності підприємства є діяльність з випуску журналів, інтернет-ресурси, рекламна діяльність (КВЕД 22.13.0).

Діяльність підприємства формується навколо медіа-ресурсу https://stroyobzor.ua/ «СтройОбзор. Портал новобудов» – спеціалізований інтернет-ресурс, на якому представлена інформація про всі новобудови і будівельні компанії Харкова і Києва.

На сайті розміщена наступна інформація: ціни, кількість вільних квартир в новобудові, планування квартир, динаміка будівництва об'єкта,

візуалізація та місце розташування новобудови, будівельна активність на об'єкті (ведеться чи ні будівництво), етап будівництва та акції, графіки зміни цін на нерухомість, знижки та інші корисні оголошення.

Серед переваг цього інтернет-ресурсу можна виділити наступне:

– зручний перегляд – новобудови можна подивитися на карті з можливістю фільтрації об'єктів;

– аналітика з «перших рук» – в розділі представлені аналітичні статті, які висвітлюють ринок нерухомості,

– графіки цін – коливання цін на нерухомість за останні кілька років представлені у вигляді таблиці новобудов,

– унікальний пошуковик нерухомості – вся інформація про новобудови систематизована по класу новобудов (економ, бізнес, преміум), району та компанії – забудовника.

Вся інформація систематизована і щомісяця оновлюється шляхом безпосередньої роботи з забудовником. Користувачі заходять на сайт для того, щоб отримати якісну інформацію про нерухомість, новобудови та будівельні компанії, яка надається абсолютно безкоштовно, з прямими контактами компанії – забудовника.

«СтройОбзор» збирає понад 250 тис. користувачів на місяць.

Організаційна структура підприємства представлена на рис.2.1.

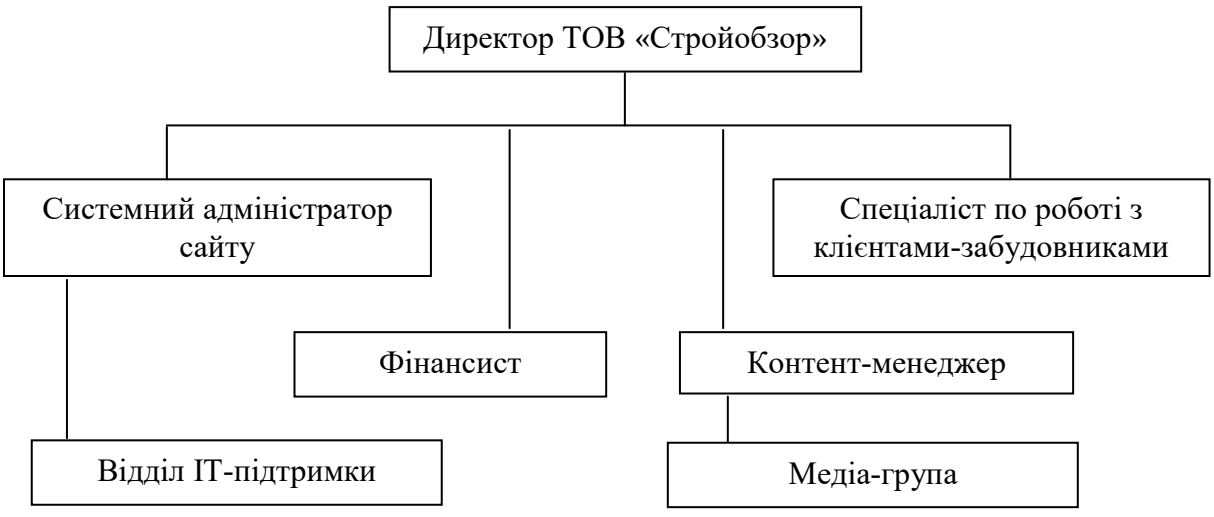

Рисунок 2.1 – Організаційна структура ТОВ «Стройобзор»

Сайт підтримується групою співробітників технічного напряму на чолі із системним адміністратором. Ця група взаємодіє із партнерами «Стройобзору» – IT-компанією, яка займається IT-супроводом бізнесу, оновленням та технічним забезпеченням віртуальної складової бізнесу.

Спеціаліст по роботі з клієнтами-забудовниками забезпечує отримання актуальної майже щоденної інформації в стандартизованій формі від компаній-забудовників про стан будівництва.

Контент-група очолюється контент-менеджером та містить медіа-групу, яка працює над змістовною складовою: створює текстові статті та фото- й відеоматеріал, – зокрема – за допомогою безпілотних летальних апаратів, які дозволяють робити панорамні зйомки ходу будівництва. За потреби контент-менеджер залучає до роботи сторонніх журналістів.

Таким чином невеликий колектив 11 осіб забезпечує роботу ефективного та популярного медіа-ресурсу, який займається висвітлюванням та аналітикою регіонального будівництва.

2.2 Аналіз економічних результатів діяльності підприємства

Економічний аналіз є неодмінним елементом як фінансового менеджменту на підприємстві, так і його економічних взаємин із партнерами, фінансово-кредитною системою.

Техніко-економічний аналіз дозволяє провести оцінку ефективності використання активів підприємства. Для таких цілей передбачений цілий ряд показників, що характеризують як стан основних і оборотних засобів, використання робочої сили на підприємстві, так і фінансово-економічне становище підприємства в цілому. Розглянемо техніко-економічні показники результату роботи ТОВ «Стройобзор» за 2018-2019рр. (табл.2.1) і проведемо їх порівняльний аналіз.

Таблиця 2.1 – Аналіз результатів діяльності ТОВ «Стройобзор»

Стаття	Код	За 2018р.		За 2019р.	
		тис.грн.	%	тис.грн.	%
1	2	3	4	5	6
Чистий дохід від реалізації	2000	3 567	100,0	2 417	100,0
Інші операційні доходи	2120	4 115	115,3	5 591	231,3
Разом доходи		7 682	215,4	8 008	331,3
Матеріальні затрати	2500	1 896	53,2	2 289	94,7
Витрати на оплату праці	2505	2 761	77,4	3 001	124,2
Відрахування на соціальні заходи	2510	884	24,8	999	41,3
Амортизація	2515	162	4,5	215	8,9
Адміністративні, збутові витрати	2130, 2150	1 873	52,5	2 321	96,0
Разом операційні витрати	2550	7 576	212,4	7 997	330,9
Чистий прибуток (збиток)	2350 (2355)	106	3,0	11	0,5

В результаті порівняльного аналізу техніко-економічних показників можна відзначити низку негативних змін:

– протягом 2019 року виручка від реалізації зменшилась на 32% і склала 2 417 тис.грн. на кінець року;

– чистий прибуток підприємства також зменшився на 90% ,

– зменшення чистого прибутку відбувається швидше за зменшення виручки від реалізації; причина цього полягає в зростанні витрат;

– структура виручки стала більш витратною: якщо в 2018р. частка чистого прибутку у виручці була 3%, то в 20192р. вона склала 0,5%.

Але аналіз техніко-економічних показників ТОВ «Стройобзор» виявив і низку наступних позитивних змін:

– результатом діяльності організації є прибуток (в 2018-у році від дорівнюівав 106 тис.грн., в 2019-му 11 тис. грн.);

– серед доходів підприємства головну роль відіграють не доходи від реалізації (створення рекламних банерів, доступ до аналітики тощо), а інші операційні (перш за все доходи від оренди рекламних місць на сайті), а ці доходи збільшились на 37%.

Таким чином, результати діяльності говорять про зростання сукупних доходів організації, що свідчить про розширення діяльності організації. Отже, клієнтів задовольняє якість і ціна товару, тому з цього боку суттєвих проблем немає. Але збільшення витратної частини призводить до зменшення чистого прибутку. Це є фактором ризику з точки зору функціонування бізнесу, бо чистий прибуток є основним джерелом фінансування поточних бізнес-процесів.

Економічний потенціал виробничих потужностей може бути охарактеризований двояко: з позиції майнового становища і з позиції використання наявних потужностей. Обидві ці сторони фінансово-господарської діяльності взаємопов'язані: нераціональна структура майна, його неякісний склад можуть привести до погіршення фінансового становища.

Динаміка майнового становища підприємства може бути охарактеризована наступними показниками (табл.2.2).

Таблиця 2.2 – Майнове становище ТОВ «Стройобзор»

Показники	За 2018р.		За 2019р.		Зміна за рік	
	тис.грн.	%	тис.грн.	%	тис.грн.	частка
1.Необоротні активи	7 986	72,3	7 76 4	69,2	- 222	0,97
2.Оборотні активи (зокрема)	3 060	27,7	3 450	30,8	+ 390	1,13
- запаси	159	1,4	591	5,3	+ 432	3,72
- розрахунки з дебіторами	1 476	13,4	1 415	12,6	- 61	0,96
- грошові кошти	1 399	12,7	1 418	12,6	+ 19	1,01
3.Всього майна	11 046	100	11 214	100	+ 168	1,02

З наведених даних видно, що за минулий рік у підприємства майно майже не змінилося: відбулось незначне зростання на 2%.

Структура майна також майже не змінилася: основну частку складають необоротні активи (комп'ютерна та мережева техніка, програмне забезпечення, безпілотний летальний апарат, апаратура для фото та відеозйомок тощо). І навіть при скороченні частки основного капіталу з 72,3% до 69,2%, він все одно відіграє головну роль в структурі майна.

Оборотні активи складаються в основному з розрахунків з дебіторами та грошових коштів, а запаси мають незначну частку навіть при збільшенні їх вартості за рік з 159 тис. грн. (1,4%) до 591 (5,3%). Це пояснюється особливостями діяльності медіа-ресурсу. Технологія виконання даних робіт не передбачає виробничих запасів та запасів готової продукції.

Велика частка дебіторської заборгованості (майже 13%) пояснюється особливостями розрахунків між замовниками та ТОВ «Стройобзор», які складаються в поступовому освоєнні коштів замовника протягом розміщення інформації на сайті, щоденного занесення даних в базу, розміщення реклами замовників тощо. Тому структуру оборотних активів можна вважати виправданою.

Формалізованими критеріями якісних змін майнового становища підприємства виступають й такі показники, як фондовіддача, фондомісткість, фондоозброєність, коефіцієнт фізичного зносу. У зв'язку з цим розглянемо характеристику основних засобів підприємства, що є одним з найважливіших елементів виробничого потенціалу (табл.2.3).

Таблиця 2.3 – Показники використання основних засобів ТОВ «Стройобзор»

Найменування показника	За 2018 р.	За 2019 р.	Зміни, частка
Фондовіддача	0,96	1,03	1,07
Фондомісткість	1,04	0,97	0,93
Фондоозброєність, тис.грн. /чол.	726	706	0,97
Коефіцієнт фізичного зносу	0,56	0,57	1,02

Фондовіддача показує, який обсяг продукції був випущений з використанням 1 грн. основних фондів. Фондовіддача на підприємстві, що вивчається, збільшилась на 7%. Це пов'язано із збільшенням чистих доходів з 7 682 тис. грн. в 2018р. до 8 008 тис. грн. в 2019р. (на 4%). Тому кожна гривня, яка вкладена в основні фонди, стала приносити більше доходів. Збільшення виручки «перекрило» зменшення вартості основних фондів з

7 986 тис. грн. за 2018р. до 7 764 тис. грн. за 2019р. Таким чином, в 2019р. кожна гривня, вкладена до основних фондів, принесла 1,07 грн. доходу.

Оскільки фондомісткість – це зворотний показник фондовіддачі, то вона відповідно зменшилась, що відображає зменшення витрат основного капіталу на випуск одиниці продукції (роботи, послуги). Ця тенденція є позитивною, особливо в умовах зростання чистих доходів.

Фондоозброєність показує, скільки основних фондів припадає на одного виробничого працівника. Даний показник майже не змінився (зниження відбулось на 3%), оскільки за рік чисельність працівників підприємства не змінилася персонал склав 11 осіб. Отже, на одну людину припадає технічних засобів на суму більш ніж 700 тис. грн. Для IT-середовища така ситуація виправдовується тим, що один працівник використовує не лише комп'ютерну техніку, але й мережеву, а також цілий набір високопрофесійного програмного забезпечення.

Для оцінки ступеня зношеності основних фондів використовують коефіцієнт фізичного зносу, який обчислюється як відношення суми амортизаційних відрахувань від початку служби до первинної вартості основних фондів. Згідно розрахункам устаткування зношене більш ніж на половину. Це свідчить про ще наявний технічний потенціал ТОВ «Стройобзор», оскільки в IT-сфері обладнання та програмне забезпечення мають невеликий термін експлуатації (порівняно із промисловим обладнанням) – в середньому 5 – 7 років. Але дані свідчать, що необоротні активи в той же час потребують розробки та проведення заходів для підвищення ефективності використання потужностей.

Крім показників ефективності використання основних фондів важливо також проаналізувати ефективність використання оборотних засобів. Це можна зробити за допомогою таких показників: коефіцієнт оборотності, тривалість обороту, рентабельність оборотних коштів. Розрахунок цих показників було проведено на основі даних фінансової звітності – балансу і звіту з фінансових результатів і представлений в табл.2.4.

Таблиця 1.4 – Ефективність використання оборотних коштів ТОВ «Стройобзор»

Найменування показника	За 2018р.	За 2019 р.	Зміна, частка
Коефіцієнт оборотності оборотних активів	2,51	2,32	0,92
Тривалість обороту, дні	143	155	1,08
Рентабельність оборотних коштів %	3,5	0,3	0,09

Результати розрахунку свідчать, що ефективність використання оборотних коштів у ТОВ «Стройобзор» знаходиться на нормальному рівні, але є тривожні симптоми. Коефіцієнт оборотності показує кількість оборотів за рік і визначається відношенням реалізованої за рік продукції до середньорічного залишку оборотних коштів. Цей показник зменшився на 8%, тобто капітал почав трохи повільніше обертатися. Це пояснюється тим, що операційні доходи зросли менш, ніж зросли оборотні витрати. Таким чином, в 2019р. оборотні активи зробили більш ніж 2 оберти.

Тривалість одного обороту визначається як відношення кількості днів в році (360 днів) до коефіцієнта оборотності. Відповідно тривалість обороту за даний період зросла на 12 днів і склала 155 днів. Це є свідоцтвом того, що оборотні кошти знаходяться в обороті більшу кількість часу. При цьому підкреслимо, що протягом аналізованого періоду спостерігається достатній рівень оборотності оборотних коштів (виходячи із особливостей бізнес-процесу організації) – оборотні засоби проходять повний цикл і повертаються за півроку. Рентабельність оборотних коштів показує, скільки прибутку підприємство отримало на кожну гривну оборотних коштів. Показники рентабельності є невисокими, кожна гривня оборотних коштів принесла в 2019р. лише 0,3 грн. чистого прибутку. Але негативним є той факт, що їх зміна відбувається у бік погіршення: за 2019р. рентабельність оборотних коштів знизилась на 91%. Таким чином, головні проблеми ефективності виробництва проявляються в динаміці і основних, і оборотних активів, що зменшує рентабельність і робить виробництво більш витратним.

2.3 Аналіз фінансових результатів діяльності підприємства

В процесі функціонування підприємства і величини активів і пасивів, і їх структура зазнають постійних змін (табл.2.5).

Таблиця 2.5 – Аналіз балансу ТОВ «Стройобзор»

Стаття	Код	На 31.12.2018		На 31.12.2019	
		тис.грн.	%	тис.грн.	%
АКТИВИ					
І. Необоротні активи					
Нематеріальні активи	1000	3 195	28,9	3 106	27,7
- первісна вартість	1001	7 292	66,0	7 289	65,0
- накопичена амортизація	1002	4 097	37,1	4 183	37,3
Основні засоби:	1010	4 791	43,4	4 658	41,5
- первісна вартість	1011	10 937	99,0	10 933	97,5
- накопичена амортизація	1012	6 146	55,6	6 275	56,0
Усього за розділом І	1095	7 986	72,3	7 764	69,2
ІІ. Оборотні активи					
Запаси	1100	159	1,4	591	5,3
Дебіторська заборгованість за товари	1125	1 468	13,3	1 374	12,3
Дебіторська заборгованість / розрахунк.	1135	8	0,1	41	0,4
Інша поточна дебіт. заборгованість	1155	26	0,2	26	0,2
Гроші кошти та їх еквіваленти	1165	1 399	12,7	1 418	12,6
Усього за розділом ІІ	1195	3 060	27,7	3 450	30,8
Баланс	1300	11 046	100,0	11 214	100,0
ПАСИВИ					
І. Власний капітал					
Зареєстрований капітал	1400	2 266	20,51	2 266	20,2
Додатковий капітал	1410	7 453	67,47	7 453	66,5
Нерозподілений прибуток (збиток)	1420	866	7,84	877	7,8
Усього за розділом І	1495	10 585	95,83	10 596	94,5
ІІІ. Поточні зобов’язання					
Кредит. заборгованість за товари	1615	258	2,34	476	4,2
Поточна кредиторська заборгованість за розрахунками:					
- з бюджетом	1620	87	0,79	38	0,3
- зі страхування	1625	33	0,30	0	0,0
- з оплати праці	1630	81	0,73	104	0,9
Інші поточні зобов'язання	1690	2	0,02	0	0,0
Усього за розділом ІІІ	1695	461	4,17	618	5,5
Баланс	1900	11 046	100,00	11 214	100,0

Найбільш загальні уявлення про якісні зміни, що мали місце в структурі засобів та їх джерел, можна отримати за допомогою аналізу звітності. Аналіз фінансової діяльності ТОВ «Стройобзор» за період 2018 – 2019 років проводився за даними балансу і звіту про фінансові результати.

Проаналізувавши і порівнявши дані балансу за два роки можна зробити наступний висновок: за рік масштаб діяльності організації майже не змінилися, збільшення підсумку балансу відбулось лише на 2%.

Для детальнішого вивчення фінансового стану ТОВ «Стройобзор» необхідно проаналізувати розміщення засобів і джерел їх формування.

Щоб говорити про ефективність потенціалу ТОВ «Стройобзор», необхідно перевірити дане підприємство на ліквідність і платоспроможність і з'ясувати чи зможе підприємство погасити всі свої короткострокові зобов'язання без порушень термінів погашення, і чи має підприємство достатню кількість грошових коштів і їх еквівалентів, необхідних для розрахунків за кредиторською заборгованістю, яка вимагає негайного погашення. Мета аналізу ліквідності – визначити здатність підприємства протягом року сплатити свої короткострокові зобов'язання. Розрахунок показників ліквідності представлений в табл.2.6.

Таблиця 2.6 – Показники ліквідності ТОВ «Стройобзор»

Показник	Норматив	2018	2019
Поточна ліквідність	від 1 до 2,5	6,6	5,6
Термінова ліквідність	більше 1,0	6,3	4,6
Абсолютна ліквідність	від 0,2 до 0,5	3,0	2,3

Коефіцієнти абсолютної ліквідності знаходяться істотно вище за норму. Це означає, що станом на 31.12.2019р. ТОВ «Стройобзор» в змозі сплатити більш ніж в 5 разів за короткострокову кредиторську заборгованість грошовими коштами, що є на рахунку. Це свідчить про

велику ліквідність підприємства, але з іншого боку перевищення верхньої межі говорить про неефективність використання наявних коштів. Хоча в порівнянні з попереднім роком, коли грошових коштів на рахунку у товариства було ще більше, є позитивна динаміка.

Коефіцієнт термінової ліквідності також занадто високий, але демонструє позитивну динаміку. У 2018р. цей показник був в 6 разів вище за норму. Це означає, що платіжні можливості підприємства при своєчасному розрахунку з дебіторами також були відмінними. І в 2019р. показник також вищій за свою норму, але зменшується до 4,6. Це свідчить про більш ефективне використання платіжних можливостей.

Коефіцієнт поточної ліквідності також є настільки високим, що не задовольняє вимогам ефективності, причому за обидва періоди. Це свідчить про те, що підприємство в змозі своєчасно ліквідовувати борги, оскільки оборотні активи більше зобов'язань. Позитивною динамікою є зменшення і цього показника. Таким чином, можна зробити висновок, що підприємство є платоспроможним. Тому у ТОВ «Стройобзор» на фоні відсутності проблем із виконанням свої поточних зобов'язань є проблеми з ефективністю діяльності.

Однією з найважливіших характеристик фінансового стану підприємства є стабільність його виробничо-господарської діяльності, тобто фінансова стійкість. Вона оцінюється співвідношенням власних і позикових коштів. Перелік показників фінансової стійкості, розрахованих для ТОВ «Стройобзор» представлений в табл.2.7.

Таблиця 2.7 – Показники фінансової стійкості ТОВ «Стройобзор»

Показники	Норматив	2018р.	2019 р.
Коефіцієнт фінансової автономії	>0,5	0,96	0,94
Коефіцієнт фінансової залежності (левериджу)	<1	0,04	0,06
Коефіцієнт фінансового ризику	<0,5	0,04	0,06
Коефіцієнт маневреності	>0	0,38	0,44

За два роки ТОВ «Стройобзор» демонструє міцну фінансову стійкість.

Коефіцієнт фінансової автономії характеризує частку власників підприємства в загальній сумі коштів, авансованих в його діяльність. Чим вище значення цього коефіцієнта, тим більш стійким, стабільним і незалежним від зовнішніх кредиторів є підприємство. В економічній практиці нормальним вважається значення показника, що дорівнює 0,5 - 0,6. Коефіцієнт фінансової автономії в за обидва роки майже дорівнював одиниці. Це означає, що майже всі кошти, вкладені в діяльність підприємства, належать власникам. Тобто підприємство є фінансово стійким, але знову виникає питання щодо ефективності такої діяльності, бо потенціал власного капіталу є недовикористаним.

Коефіцієнт левериджу характеризує співвідношення між позиковими і власними коштами. Межа показника, що рекомендується, дорівнює 1 і нижче. Розраховані значення цього показника демонструють таку ж ситуацію – позикові кошти майже відсутні, діяльність здійснюється за рахунок власних засобів. Отже, ТОВ «Стройобзор» є незалежним від зовнішніх джерел.

Коефіцієнт фінансового ризику відображає частку позикових коштів у валюті балансу. Межа показника, що рекомендується, – не більше 0,5. Перевищення верхньої межі свідчить про великий ступінь залежності підприємства від зовнішніх фінансових джерел. Природно, що і цей показник відображає таку ж ситуацію щодо фінансової стійкості, що і попередні показники. Більш того, вони майже однакові з показниками фінансового левериджу, що пояснюється тим, що валюта балансу складається майже повністю із власних коштів.

Коефіцієнт маневреності (або співвідношення мобільних і необоротних активів) відображає, скільки оборотних активів припадає на кожну гривну необоротних активів. Значення показників свідчать про те, що протягом аналізованого періоду переважаюча частина коштів ТОВ «Стройобзор» була спрямована на фінансування необоротних активів. Є незначне зростання

показника протягом аналізованого періоду, яке свідчить про те, що підприємство почало вкладати більше коштів в оборотні активи.

Таким чином, показники фінансової стійкості свідчать про те, що підприємство ТОВ «Стройобзор» має надто стійке фінансове становище. Таке підприємство не має погрози з боку зовнішніх інвесторів, але іншим боком фінансової незалежності є неефективність використання наявних ресурсів.

Можна зробити висновок, що для підприємства важливо відновити баланс власного і позикового капіталу.

Ділова активність підприємства може бути оцінена за допомогою відносних показників, що характеризують результати і ефективність основної діяльності. Для оцінки ділової активності в практиці використовують показники, представлені в табл. 2.8.

Таблиця 2.8 – Показники ділової активності ТОВ «Стройобзор»

Показник	2018р.	2019р.	Зміна, частка
Оборотність активів, обертів за рік / днів	0,7 / 518	0,71 / 504	1,03
Оборотність необоротних активів, обертів за рік / днів	0,96 / 374	1,03 / 349	1,07
Оборотність власного капіталу, обертів за рік / днів	0,73 / 496	0,76 / 476	1,04
Оборотність дебіторської заборгованості, обертів за рік / днів	5,2 / 69	5,7 / 64	1,09
Оборотність запасів обертів за рік / днів	48,3 / 7	13,5 / 27	0,28
Оборотність кредиторської заборгованості, обертів за рік / днів	16,7 / 22	13,0 / 28	0,77
Операційний цикл, дні	77	90	1,18
Фінансовий цикл, дні	55	62	1,13

Показники оборотності свідчать про низьку ефективність діяльності, оскільки їх абсолютні значення дуже низькі.

Оборотність активів показує, скільки разів за період здійснюється повний цикл виробництва і обігу. Значення показника свідчать про те, що в цілому оборотність майже не змінилась, її зростання складає 3%. Швидкість обороту складає 504 дні на один цикл.

Оборотність необоротних активів також є дуже низькою і має тенденцію до незначного зростання – за аналізований період значення показника зросло на 7%. Підвищення цього коефіцієнта досягнуте перш за все за рахунок зростання обсягів продажів. Про це свідчать дані техніко-економічного аналізу.

Оборотність власного капіталу за 2019 рік зросла на 4%. За результатами 2019р. власний капітал здійснив 0,76 обороту.

Оборотність дебіторської заборгованості відображає ефективність кредитної політики. Вона показує, скільки обертів за рік зробили кошти, вкладені в розрахунки. Показники розраховані в днях, відображаючи період погашення дебіторської заборгованості. Цей період зменшився в порівнянні з 2018 р. на 5 днів і в 2019р. склав 64 дні.

Оборотність запасів, характеризує швидкість їх використання. Розрахунки свідчать, що тривалість одного обороту запасів в 2019 р. складає близько 27 днів.

Оборотність кредиторської заборгованості визначає швидкість оплати боргів підприємством. Оцінку цього показника не можна проводити однозначно, оскільки короткострокова кредиторська заборгованість по суті своїй є безкоштовним кредитом для даного бізнесу. Результати розрахунків показали, що термін погашення кредиторської заборгованості в 2019 р. склав 28 днів, що на 6 днів більше, ніж в попередньому.

На підставі вище розглянутих даних проведемо розрахунок показників, які характеризують основні етапи обігу грошових коштів в ході діяльності товариства. Даними показниками є:

– тривалість операційного циклу;

– тривалість фінансового циклу.

Розрахунок цих показників також представлений в табл.2.8.

Результати розрахунків дозволяють судити про те, що на аналізованому підприємстві відбулося істотне збільшення періоду повного виробничого циклу і зниження швидкості обігу в цілому.

Операційний цикл узагальнює показники оборотності дебіторської заборгованості і виробничих запасів. Отже, загальний час, протягом якого фінансові ресурси вилучені в запаси і дебіторську заборгованість, складає в 2019 р. 90 днів.

Крім того, найважливішу характеристику має показник фінансового циклу, який характеризує час, протягом якого грошові кошти витягують із обороту. В 2019 р. фінансовий цикл склав 62 дні.

Прибутковість підприємства характеризується сумою прибутку і рівнем рентабельності. Рентабельність – це показник ефективності виробництва, що характеризує співвідношення між результатами виробничої діяльності і витратами на виробництво продукції або іншими активами, які використовуються у виробництві. Розрахунок показників рентабельності для ТОВ «Стройобзор» наведений в табл. 2.9.

Таблиця 2.9 – Показники рентабельності ТОВ «Стройобзор»

Показник	2018 р.	2019 р.
Рентабельність всього капіталу %	0,96	0,098
Валова рентабельність продажів%	1,38	0,137
Рентабельність власного капіталу %	1,001	0,104
Рентабельність основних фондів %	1,327	0,142

Рентабельність всього капіталу є узагальнюючим показником і характеризує чистий прибуток, який приносить кожна гривня, що вкладена в активи. Таким чином, в 2019р. віддача від використання всіх активів, якими володіє ТОВ «Стройобзор», є дуже низькою і складає 0,098%.

Рентабельність реалізації відображає, якою є частка чистого прибутку у виручці від реалізації. Це дозволяє визначити, чи відповідає ціна на

продукцію інтересам підприємства, тому що прибуток визначається саме на етапі формування ціни. Показник рентабельності реалізації також має дуже низькі значення: частка чистого прибутку у розмірі виручки від реалізації складає 0,137%.

Рентабельність власного капіталу дає можливість оцінити, чи вигідно вкладати кошти в дане підприємство. Згідно розрахункам, в 2019р. прибуток склав лише 0,104 % від власного капіталу. Така низька ефективність власного капіталу відповідає і ефективності всього капіталу і свідчить, що не користуючись чужими коштами (зокрема, – поточними зобов'язаннями), власники значно зменшують ефективність своїх засобів.

Рентабельність основних фондів характеризує обсяг прибутку, який був отриманий на 1 грн. коштів, що вкладені в основні фонди. Значення цього показника в 2019 р. – 0,142%.

Показники рентабельності свідчать про погіршення ситуації з прибутковістю. За 2019р. сума чистого прибутку зменшилась в абсолютному значенні на 95 тис.грн. (табл. 2.1), зменшення його частки в структурі виручки з 3% до 0,5% відбилося на показниках рентабельності негативно.

Висновки за результатами фінансового аналізу:

– ТОВ «Стройобзор» є платоспроможним за всіма показниками ліквідності, що відкидає загрозу для виконання поточних зобов'язань, які виявились занадто незначними для товариства,

– фінансове становище ТОВ «Стройобзор» характеризується як надто стійке, що означає майже абсолютну незалежність від зовнішніх інвесторів,

– прибутковість ТОВ «Стройобзор» є дуже низькою і протягом 2019 р. вона стала ще менше,

– оборотність усіх активів, як в цілому, так і за елементами, є також дуже низькою і протягом 2019 р. ще знижується.

Таким чином фінансовий аналіз дозволив виявити ряд проблематичних моментів: підприємство має в розпорядженні суттєві ресурси (зокрема, необоротні активи), забезпечує ліквідність та фінансову стійкість, але все це

відбувається за рахунок низької ефективності, що проявляється в низький прибутковості та оборотності капіталу. Це означає, що підприємству необхідно оживити діяльність підприємства шляхом підвищення ефективності використання наявних ресурсів.

2.4 Напрями організації економічної безпеки на підприємстві

Розробка механізму захисту ТОВ «Стройобзор» в умовах гібридних загроз перш за все вимагає аналізу існуючої системи забезпечення безпеки бізнесу, оскільки захист в умовах гібридних загроз додається до загальної системи захисту.

Результати аналізу існуючої системи захисту бізнесу ТОВ «Стройобзор» дозволили сформувати наступну схему забезпечення безпеки бізнесу, представлену на рис.2.2.

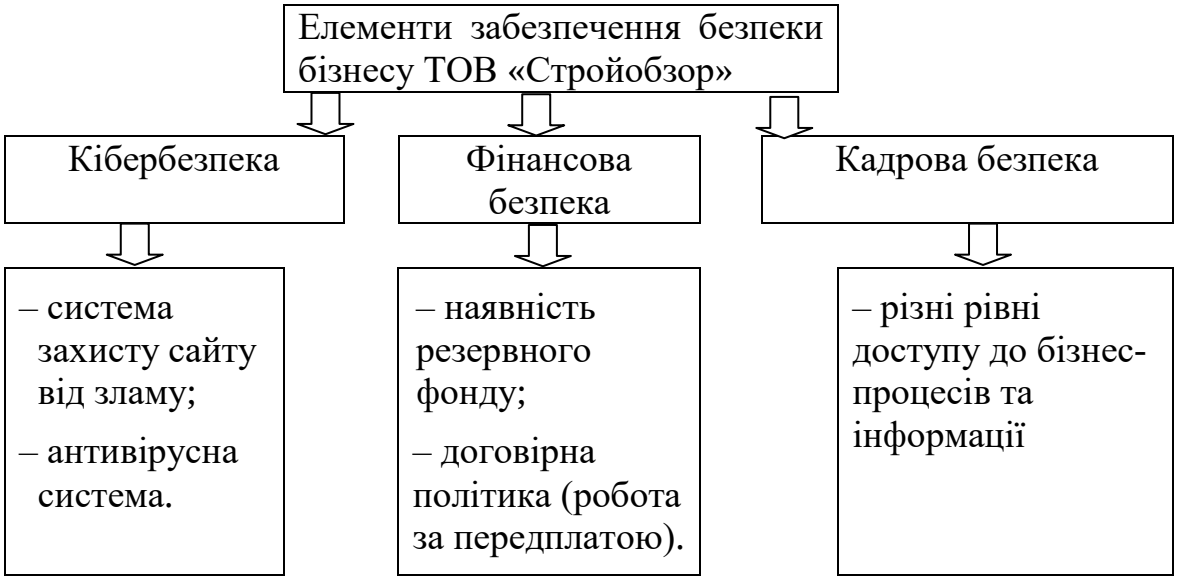

Рисунок 2.10 – Існуюча система захисту бізнесу ТОВ «Стройобзор»

Підприємство в своїй практиці стикалось із недружніми впливами, пов'язаними із кібератаками на сайт. Але щодо гібридних загроз – такі

загрози не розглядались керівництвом як актуальні загрози бізнесу та не досліджувались.

Таким чином, підприємство ТОВ «Стройобзор», що працює в медіа-просторі будівничої галузі, характеризується наявним попитом на свої послуги, фінансовою стійкістю бізнес-моделі та наявністю безпекових елементів її захисту. Але питанням для практичного дослідження залишається, чи збережеться надійність захисту даного бізнесу в умовах гібридних загроз.

3 УДОСКОНАЛЕННЯ МЕХАНІЗМУ ЗАХИСТУ БІЗНЕСУ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

3.1 Шляхи підвищення безпеки бізнесу в умовах гібридних загроз

3.1.1 Побудова механізму протидії гібридним загрозам на рівні бізнесу

Бізнес-середовище містить такі системи, інституції та інструменти, які необхідні для життєздатності країни. Напад на таке середовище може мати величезні дестабілізуючі наслідки та серйозно загрожувати функціонуванню суспільства. В умовах гібридних загроз такі напади дуже складно вчасно розпізнати, тому що гібридні дії характеризуються невизначеністю [1]. Вони стирають лінії «бойового простору», розповсюджуючись до людського та економічного вимірів. Окрім прямого нападу на системні інституції (такі як банківська система), гібридні загрози можуть набувати різні форми впливу на бізнес-середовище: економічний тиск, кібератаки на критичну інфраструктуру, втручання у вибори, використання COVID-19 у векторі гібридних дій, підживлювання громадської нетерпимості, оскарження міжнародної підтримки незалежного громадянського суспільства тощо.

Хоча окрема компанія не обов’язково може бути кінцевою або навіть ключовою метою операції, вона може сприяти досягненню кінцевої стратегічної мети (рис.3.1) [30].

Під час гібридної операції одна компанія може зазнати кібератаки, інша – інформаційної, третя – ворожого захоплення, а четверта – класичного проникнення. Особлива загроза складається в тому, що жодна з цілей не має видимості всієї операції. Але ефект від таких операцій має каскадний характер, поступово розповсюджуючи шкоду на різні домени. Навіть якщо приватний бізнес тимчасово втрачає здатність здійснювати операції, в критичний період невизначеності та в критичній галузі це призводить до мультиплікативного ефекту, від якого постраждають різні частини суспільства.

Рисунок 3.1 – Використання бізнесу в гібридній діяльності

Невеликі компанії також можуть стати інструментом гібридних впливів на кшталт того, як шпіонське програмне забезпечення залучає мільйони комп'ютерів пересічних користувачів для скоєння DOS-атаки. Якщо скоординовані гібридні операції виконуються одночасно через багато частин критичної інфраструктури та ланцюгів поставок, суспільство отримає аналогічний руйнівний ефект [31].

Окремий бізнес не має можливостей держави. Тому бізнес-суб'єктам слід зосередитись на зменшенні вразливості та підвищенні стійкості бізнесу на противагу пошуку та покаранню винних, зокрема через наступне[15]:

– побудова резервних систем в критичних для бізнесу сферах (зокрема – створення запасу ліквідності та перегляд JIT-підходів до логістики);

– створення системи захисту бізнесу із кібер-безпековим компонентом;

– підвищення обізнаності персоналу про гібридні загрози;

– обмін інформацією: створення відповідних протоколів між учасниками бізнес-екосистеми, взаємодії з національними безпековими організаціями при виявленні вразливостей (особливо незрозумілої природи);

– проведення тестування, коли моделюються та імітуються реальні атаки з метою перевірити стійкість бізнес-процесів;

– презентування безпеки даних як конкурентної переваги бізнесу, яка запобігає репутаційним та діловим ризикам.

Ці рекомендації мають доповнювати звичайні механізми забезпечення безпеки, логічно вбудовуючись в них та не порушуючи бізнес-діяльність.

Механізм будемо розглядати як «сукупність та взаємодію певних структурних елементів (можливостей, станів, процесів, властивостей), які забезпечують функціонування будь-якої соціально-економічної системи» [32].

Взявши за основу загальну структуру механізму економічної безпеки, розроблену в дисертаційній роботі Тимощенко К.С. [33], був розроблений механізм протидії гібридним загрозам на рівні підприємства (рис.3.2). Він може розглядатись як самостійний механізм або як додатковий інсталяційний блок до існуючого на підприємстві механізму економічної безпеки.

Для забезпечення комплексного підходу система захисту бізнесу в умовах гібридних загроз має містити наступні елементи:

– керівні принципи роботи компанії в умовах гібридних загроз;

– операційні моделі для захисту даних, інформації та працівників;

– план безперервності бізнесу в умовах дефіциту важливих ресурсів;

– механізми підвищення обізнаності (навчання, інформування) власників, керівництва та службовців;

– механізми обміну інформацією, пов’язаною з безпекою, між компаніями в ланцюгах поставок та вартості;

– механізми співпраці компаній з владою та службами безпеки для створення платформи з протидії гібридним загрозам.

Кожен з напрямів потребує окремої розробки для врахування небезпеки, пов'язаних із гібридними загрозами, асиметричними впливами, нечіткими сигналами тощо. На основі цих міркувань запропоновані наступні елементи механізму протидії гібридним загрозам на рівні бізнесу (рис.3.3.).

Рисунок 3.2 – Загальні принципи побудови механізму захисту бізнесу від гібридних загроз (на базі моделі Тимощенко К.С. [33])

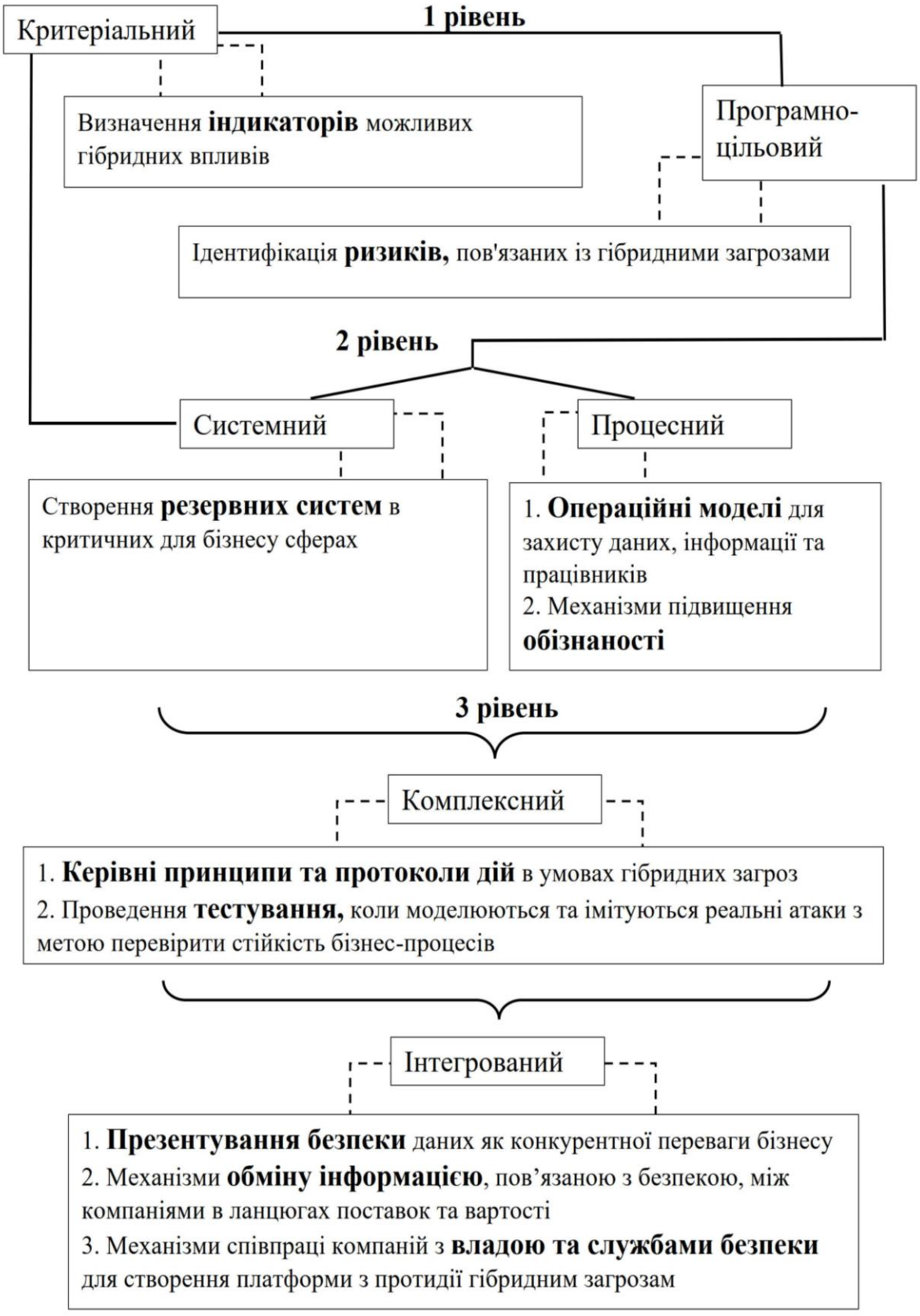

Рисунок 3.3 – Елементи механізму протидії гібридним загрозам на рівні бізнесу

3.1.2 Ідентифікація ризиків, пов'язаних із гібридними загрозами

Для ідентифікації ризиків гібридних загроз пропонується спиратись на дослідження Кампанії з розвитку міжнаціональних можливостей (Multinational Capability Development Campaign, MCDC) [35]. За їх визначенням, евристична модель для розуміння гібридних впливів складається з трьох взаємозалежних частин:

– критичні функції та уразливості цілі гібридних впливів (тобто бізнесу);

– синхронізоване використання зловмисником декількох засобів та горизонтальної ескалації (тобто одночасний прояв несподіваних проблем одночасно в кількох різних сферах);

– лінійні та нелінійні ефекти гібридної атаки.

На рис.3.4 показано, як актор гібридних впливів може синхронізувати свої військові, політичні, економічні, цивільні, інформаційні (MPECI) інструменти влади для вертикальної та горизонтальної ескалації ряду конкретних заходів для створення ефектів.

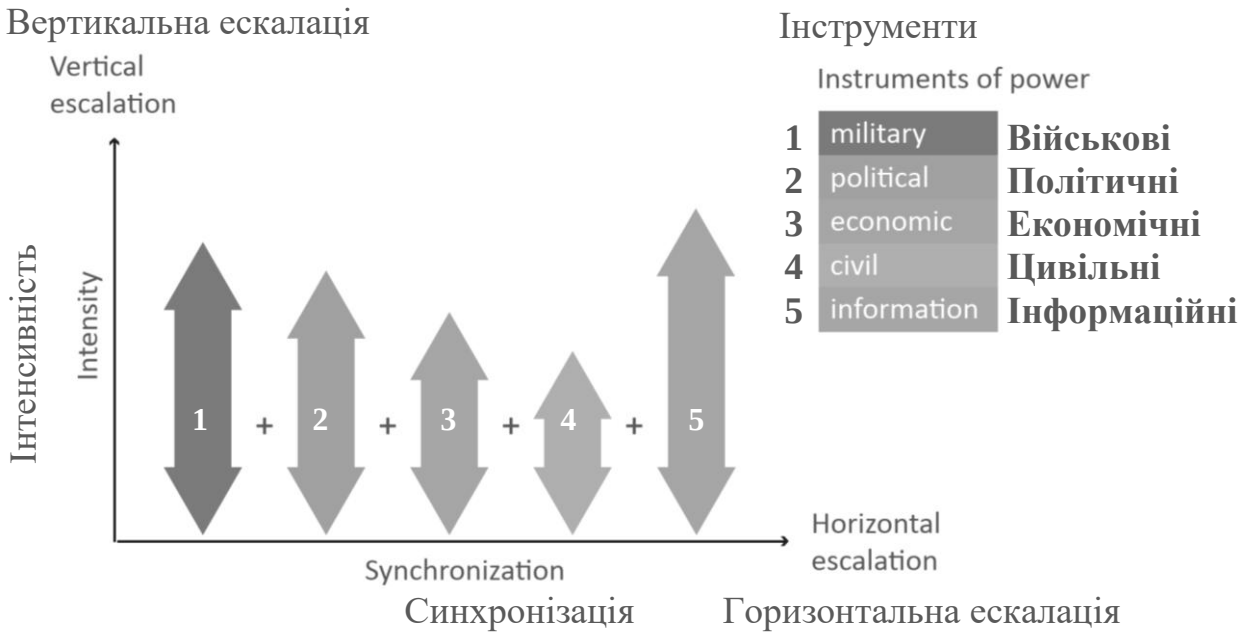

Рисунок 3.4 – MPECI-інструменти гібридних впливів [35]

Це також показує, як гібридний зловмисник може або вертикально ескалатувати загрози, збільшуючи інтенсивність одного або багатьох інструментів влади, та / або горизонтально ескалатувати за допомогою синхронізації декількох інструментів влади, щоб створити ефекти більші, ніж лише вертикальною ескалацією.

З огляду на ці можливості, розуміння гібридного супротивника не піддається лише традиційному аналізу загроз, що базується на його спроможності та намірах з ряду важливих причин:

– по-перше, гібридні впливи використовують ширший набір інструментів та методів MPECI, які зазвичай не розглядаються в традиційних оцінках загроз;

– во-друге, гібридні загрози націлені на вразливі місця в суспільствах таким чином, про які ми традиційно не думаємо;

– по-третє, гібридний зловмисник синхронізує свої засоби новими способами (наприклад, розглядаючи лише різні інструменти сили, якими володіє супротивник, не можна точно передбачати, як і наскільки вони можуть бути синхронізовані для створення певних ефектів), тобто функціональні можливості противника гібридної війни, хоч і важливі, але не обов'язково даватимуть потрібну інформацію для розуміння проблеми.

– по-четверте, гібридні впливи навмисно використовують двозначність, креативність та наше звичайне розуміння війни та миру, щоб зробити напади менш «помітними»; це пов’язано з тим, що вони можуть бути пристосовані для того, щоб залишатися нижче певних порогових значень виявлення та реагування, включаючи міжнародно-правові, тим самим ускладнюючи процес прийняття рішень та ускладнюючи реакцію на атаку гібридної війни.

– по-п’яте, кампанію гібридних впливів можна не побачити, доки вона вже добре розпочата, із шкідливими наслідками, які вже почали проявлятися і погіршують здатність цілі захищатися.

Ці проблеми є основою для розширення традиційного аналізу загроз, орієнтованого на ворога. З цією метою слід фокусуватись на вразливостях цілі, здатності зловмисника гібридної війни синхронізувати широкий спектр

своїх можливостей під час атаки та ефектах, створених в результаті цих дій проти конкретних вразливостей.

Аналітична основа базується на трьох дискретних, але взаємопов'язаних категоріях:

– критичні функції та уразливості;

– синхронізація засобів (горизонтальна ескалація);

– ефекти та нелінійність.

Хоча ці категорії відокремлені, їх потрібно розуміти узгоджено, оскільки сума гібридних впливів більша за кожну окрему частину.

Критичні функції – це діяльність або операції, розподілені по політичному, військовому, економічному, соціальному, інформаційному, інфраструктурному (ПМЕСІІ) спектрі, які, якщо їх припинити, можуть призвести до порушення функціонування служб, що діють в системі (наприклад, весь бізнес або його окрема процедура чи функція) залежить від них [34].

Критичні функції можуть бути розбиті на комбінацію суб'єктів (наприклад, окремих осіб), інфраструктури (наприклад, силова електропроводка чи інтернет-сполучення) та процесів (наприклад, технологічних, юридичних) (рис.3.5).

Рисунок 3.5 – Сутність та складові критичних функцій

В усіх критичних функцій є вразливості, що надають суб'єкту гібридних впливів можливі умови експлуатації, залежно від засобів, що є в їх розпорядженні. Однак не всі вразливості обов'язково є можливостями для використання противником. Альтернативно, супротивник може вибрати опцію «не використовувати» певну вразливість залежно від його намірів. Крім того, вразливості в межах критичних функцій можуть бути невідомі

цільовій системі (наприклад, невідомі вразливості, такі як кібер-атака нульового дня), і можуть проявлятися лише із розгортанням подій.

Протидія гібридним атакам вимагає оцінки критичних функцій, взаємозалежності цих функцій та їх вразливості. Цей «погляд на себе» вимагає процесу оцінки ризику, який враховує вразливі місця в усьому ланцюгу доданої вартості, а не лише у секторі фінансово-економічної безпеки. Хоча така оцінка цінна сама по собі, незалежно від гібридних впливів, розуміння гібридних впливів як типу дії, які спеціально пристосовані до вразливостей, означає, що гібридні впливи неможливо зрозуміти без посилання на ці вразливості. Результати цієї самооцінки гібридних впливів суттєво відрізнятимуться від однієї цільової системи (бізнесу) до іншої, що робить кожну оцінку унікальною та дуже контекстуальною.

Для ідентифікації ризиків, пов'язаних із гібридними загрозами, ключовим є розуміння того, що різні силові інструменти використовуються в різних вимірах і на кількох рівнях одночасно синхронізовано.

Цей тип мислення дозволяє гібридному нападнику використовувати різні засоби MPECI, які є в їх розпорядженні, для створення синхронізованих пакетів атак (synchronized attack packages, SAP), які спеціально адаптовані до вразливостей цільової системи. Використані інструменти влади будуть залежати від:

– можливостей гібридного нападника;

– від передбачуваної вразливості його опонента;

– від політичних цілей учасника гібридного нападника;

– запланованих способів досягнення цих цілей.

Як і у всіх конфліктах та війнах, характер гібридної війни залежить від контексту.

3.1.3 Визначення індикаторів гібридних впливів

Гібридні атаки зосереджуються на конкретних вразливостях цілі, що робить їх дуже контекстуальними. Щоб відповісти на цю загрозу, потрібно дотримуватися певних кроків.

Перш за все, бізнес, який розглядається в даному досліджені як ціль, потребує оцінки своїх критичних функцій та вразливостей. Після виявлення критичних функцій та вразливостей необхідно встановити порогові значення для моніторингу змін у функціональному стані критичних функцій (наприклад, загальний стрес). Порогові значення допомагають визначити та визначити ступінь серйозності гібридного нападу (або підозри на атаку) шляхом попереднього визначення рівнів (наприклад, нормальності, кризи або надзвичайної ситуації) разом із величиною або інтенсивністю, яку потрібно перевищити, щоб перейти від одного рівня статусу до наступного.

Слід також побудувати конкретні показники, які допоможуть визначити, чи відбувається гібридна дія, а якщо так – то де й коли відбувається. Побудова базової лінії (наприклад, статус нормальний) є критичним першим кроком у визначенні активності гібридного впливу. Не маючи уявлення про те, що є нормальним, важко «побачити» дії, які можуть бути частиною двозначної гібридної атаки (рис.3.6).

Важливим моментом при визначенні порогових значень є й те, що гібридні впливи працюють «на межі», розмиваючи поняття норми та відхилення від норми. Оскільки завдання гібридних впливів - залишатися нижче певних порогових значень виявлення та реагування, то відхилення від норми (або знаходження на межі) може не відчуватись системою тривалий період. Атака учасника гібридної війни за допомогою силових інструментів MPECI може бути підривною, але не настільки, що можна відрізнити їх від звичайних інцидентів. Однак, якщо це трапляється багато разів або одночасно в інших секторах, це може переступити порогові значення через те, що синхронізовані зусилля можуть призвести до кумулятивних та нелінійних ефектів.

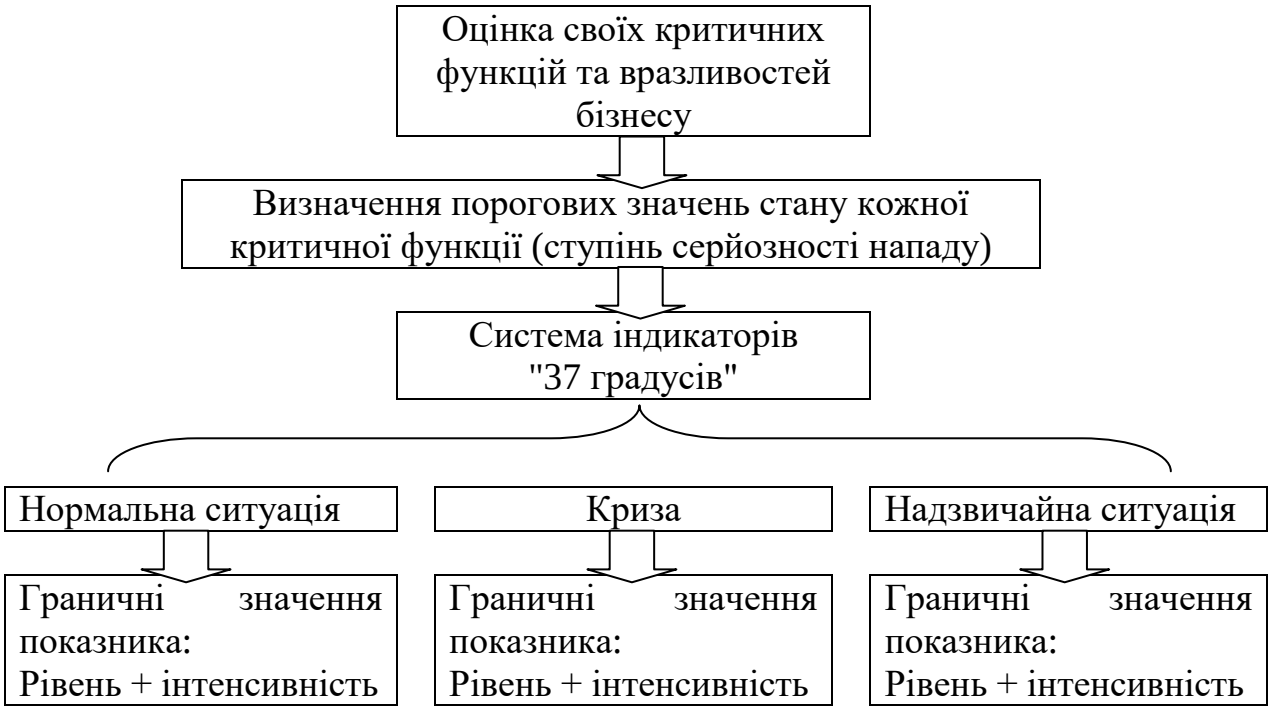

Рисунок 3.6 – Основні елементи механізму визначення індикаторів гібридних впливів

Це має пряму медичну аналогію: нетривалі підйоми температури тіла до 37 градусів можуть не відчуватись людиною. Але якщо при цьому відбувається розвиток хвороби – через якійсь період часу людина отримає різке раптове погіршання, яке може мати непередбачувані фатальні наслідки. Але щоденний моніторинг температури тіла дозволяє виявляти такі фактори та знаходити проблему навіть якщо людина її зовсім не відчуває. Медична аналогія дозволила назвати систему індикаторів гібридних загроз «37 градусів».

Система індикаторів гібридних загроз має так само працювати, вимірюючи навіть незначні відхилення від норми та порівнюючи інтенсивність їх прояву.

Гібридна війна не вкладається в традиційне мислення на фазі нападу. Це не обов'язково еволюціонує лінійно через фази ескалації до стратегічно визначеного кінцевого стану. Замість того, щоб діяти поетапно, гібридна атака розвивається через одночасну ескалацію та деескалацію на тактичному

та оперативному рівні через вертикальну та горизонтальну вісь, гнучко експлуатуючи та використовуючи переваги ефектів у міру їх виникнення.

Таким чином, розуміння гібридної атаки та способу реагування на неї вимагає моніторингу майже в режимі реального часу:

– своїх вразливостей;

– можливостей та дій актора гібридних впливів;

– можливих наслідків атак проти системи.

3.1.4 Розробка операційних моделей моніторингу гібридних загроз

Можливість діяти на випередження багато в чому залежить від можливості отримання своєчасного сигналу про появу небезпеки. Але ж гібридні загрози створюють «невизначеність на межі», тобто розмивають межі між безпечними та небезпечними ситуаціями. Але в будь-якому випадку ефективний аналіз і раннє розпізнавання базуються на основі збору інформації з різних джерел.

Тому для створення захисту від гібридних впливів, обов'язково мають бути вбудовані в існуючі системи захисту підприємств відповідні індикатори та попереджувальний моніторинг.

Реагування на гібридні загрози вимагає їх контекстуалізації відповідно до конкретних можливостей та вразливостей цільової системи (бізнесу). Оскільки важко, а то й неможливо передбачити місце нападу, засоби, які будуть використані, або уразливості, які будуть використані (або навіть «створені») актором гібридного нападу, постійний моніторинг критичного стану функцій необхідний бізнесу. Тільки оцінивши статус цільової системи (критичні функції та уразливості) та склавши на карту дії, що вживаються актором гібридного впливу, можна зрозуміти, як розвивається загроза та де цільова система перебуває з точки зору її стану (нормальний, криза або надзвичайна ситуація).

Для візуалізації роботи моніторингової системи пропонується використовувати матрицю станів (рис. 3.7).

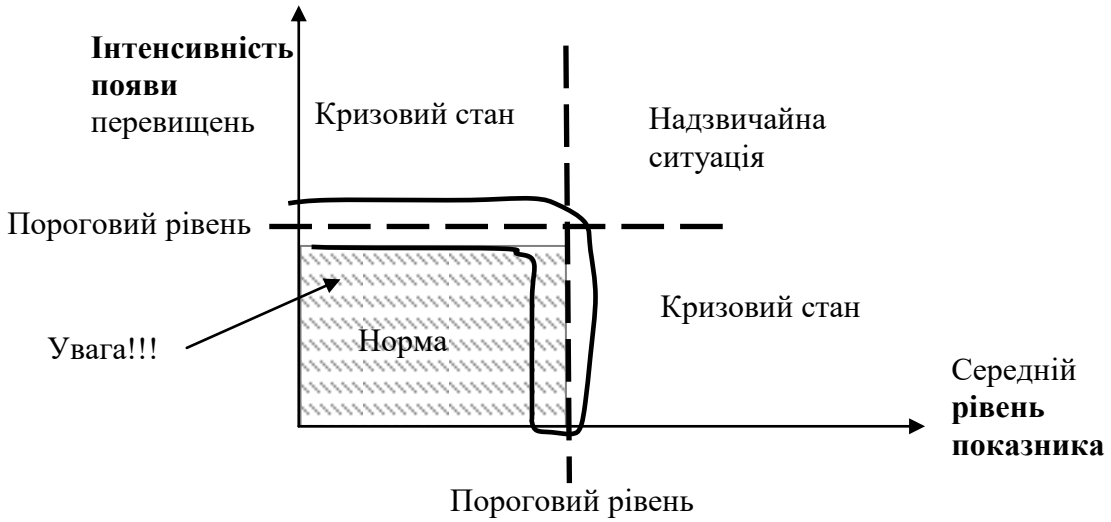

Рисунок 3.7 – Матриця станів критичних функцій бізнесу в умовах гібридних загроз

Цей процес моніторингу включає виявлення подій як потенційних ризиків для критичних функцій людини, можливих спроб використання конкретних вразливих місць, а потім «з'єднання крапок», що дозволяє цілі ідентифікувати, реагувати і, зрештою, протидіяти гібридній атаці.

3.1.5 Розробка операційних моделей захисту від гібридних загроз

Важливою характеристикою загрози є її потенціал. Зазвичай під потенціалом розуміються приховані здатності, сили для якої небудь діяльності, що можуть виявитися за певних умов; запас чого-небудь, резерв. Під «потенціалом загрози» будемо розуміти ступінь прихованих здатностей загрози [35]. Наприклад, енергетичних, ресурсних (матеріальних або нематеріальних, технічних та людських), діапазону кліматичних факторів та ін. Оцінка потенціалу загрози має важливе значення для визначення

масштабів ураження бізнесу загрозами і ризиків від них. Чим більшим є потенціал у загрози, тим більшим є ризик від неї для бізнесу.

Для оцінки стійкості бізнесу до потенціалу загрози традиційно використовують такі показники:

– час для відновлення нормального функціонування бізнесу (його окремої функції) після дії на нього певної загрози (ураження): чим менший час відновлення бізнесу, тим більшою є його стійкість до впливу загрози;

– втрата продуктивності: зниження втрати продуктивності підвищує стійкість бізнесу до впливу загроз.

Підвищення стійкості бізнесу досягається різними шляхами, саме вони є основою для формування операційних моделей захисту. Операційні моделі захисту бізнесу від гібридних загроз виконують три базові функції [36] (рис.3.8).

Рисунок 3.8 – Функції операційних моделей захисту бізнесу від гібридних загроз

Це не обов'язково послідовні дії, але функції, які, можливо, доведеться виконувати одночасно, щоб забезпечити стійкість і ефективне реагування на гібридні загрози, в залежності від того, як гібридна кампанія застосовується і розвивається.

Створення резервних систем є традиційним елементом механізмів захисту бізнесу [37], також він розглядається як обов'язковий елемент захисту критичної інфраструктури [38-39], особливо в умовах гібридних загроз [40]. Роль резервних систем в операційних механізмах захисту бізнесу від гібридних загроз представлена на рис.3.9.

Рисунок 3.9 – Роль резервних систем в операційних механізмах захисту бізнесу від гібридних загроз

Для комплексного захисту компанії (а через них – й суспільства) від гібридних загроз, система корпоративної безпеки має містити окремі керівні принципи та операційні моделі для захисту даних та працівників. Але оскільки існує широкий спектр злочинних дій, спрямованих на використання гібридного впливу, неможливо створити операційні моделі для всіх сценаріїв. У цих ситуаціях вирішальним є загальна пильність працівників, пов’язана з безпекою [41].

3.2 Організаційно-методичний підхід до забезпечення захисту ТОВ «Стройобзор» в умовах гібридних загроз

3.2.1 Дослідження критичних функцій підприємства

Для ідентифікації ризиків були проаналізовані бізнес-процеси підприємства та на основі рис.3.5 виділені його критичні функції.

Після визначення критичних функцій здійснюється пошук показників, значення яких відображають стан (функціональність) кожної критичної функції. Також встановлюються їх порогові значення (за рис.3.6)

Таблиця 1.3 – Критичні функції ТОВ «Стройобзор»

Складові	Критично вразливі елементи
Суб'єкти	- системний адміністратор (доступ до управління сайтом) - автори контенту (доступ до змістовної складової) - директор (прийняття рішень та доступ до фінансових ресурсів) - партнери (програмна підтримка сайту, доступ до інтернету) - клієнти (формують замовлення на інформаційні блоки)
Інфраструктура	- програмна інфраструктура (програмне забезпечення як власне, так й аутсорсне, хмарні потужності як власні, так й аутсорсні, програмна взаємодія із клієнтами через кабінет користувача) - мережева інфраструктура (серверне обладнання, мережеве обладнання, робочі місця працівників) - доступ до електроенергії (електромережа, разгалуджувачі) - інформаційна інфраструктура (правила отримання інформації, її обробки та розміщення на сайті) - фінансова інфраструктура (забезпечення грошових потоків через інтернет-банкінг)
Процеси	- створення контенту (отримання польової інформації, обробка, створення змістовного наповнення та аналітики), - забезпечення роботи сайту (програмне та технічне функціонування) - відносини з клієнтами (рекламодавцями), аутсорсними спеціалістами (журналісти) та постачальниками (перш за все – ІТ-фірма для супроводу сайту) - надходження та витрати фінансового ресурсу

Для дослідження в атестаційній роботи був обраний критичний процес, безпосередньо пов'язані із технологією створення доданої вартості бізнесу: забезпечення роботи сайту (IT-складова).

3.2.2 Механізм захисту IT-складової бізнесу ТОВ «Стройобзор» в умовах гібридних загроз

Існуюча система кібер-захисту ТОВ «Стройобзор» є достатньо опрацьованою та містить базові елементи захисту від зламу на основі прийнятого на підприємстві Протоколу організаційного захисту.

Цей документ визначає регламентацію виробничої діяльності і взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне заволодіння конфіденційною інформацією. Організаційний захист забезпечує:

– організацію охорони, режиму, роботу з кадрами, з документами;

– використання технічних засобів безпеки.

ТОВ «Стройобзор» вживає низку організаційні заходи, які створюють захист в сфері IT. Для запобігання раптових перебоїв в роботі підприємству була запропонована низка додаткових заходів, які підвищують стійкість процесів, низка з них – за рахунок створення додаткових резервних систем (табл.3.2).

Більшість із запропонованих заходів спрямована на отримання додаткових резервів або процесів, які захищають вразливі елементи бізнесу від нападу, тобто коли бізнес є об'єктом атаки. Але ж використання бізнесу в гібридних впливах може мати на меті перетворення такого бізнесу на засіб атаки (або на один з багатьох засобів). Тому саме для бізнесу такі впливи не представляють загрози, але для громади, суспільства, оточуючого середовища це може мати руйнівний характер. Руйнуючи оточуюче середовище, бізнес руйнує й власні перспективи не тільки розвитку, але й існування.

Тому для ТОВ «Стройобзор» була запропонована низка індикаторів за принципом «37 градусів», яка відстежує несанкціоновані слабо помітні дії на інформаційному ресурсі (сайті) – табл.3.3.

Таблиця 3.2 – Організаційні заходи ТОВ «Стройобзор», які створюють захист в сфері ІТ

Тип захисту	Існують на підприємстві	Запропоновані
Організаційні заходи	- організація режиму і охорони для виключення можливості таємного проникнення сторонніх осіб; - організація роботи зі співробітниками (ознайомлення з заходами відповідальності тощо); - організація роботи з документами.	- організація роботи зі співробітниками (навчання правилам роботи з конфіденційною інформацією); - організація використання технічних засобів.
Засоби захисту від несанкціонованого доступу	- засоби авторизації; - мандатне управління доступом.	- журналювання (резервна система)
Системи аналізу інформаційних потоків.	відсутні	- системи аналізу інформаційних потоків (CASE-системи)
Системи моніторингу мереж	- системи запобігання витоків конфіденційної інформації (DLP-системи).	- системи виявлення й запобігання вторгнень (IDS / IPS).
Криптографічні засоби	- шифрування; - цифровий підпис.	Не запропоновано
Системи резервування	відсутнє	- резервне копіювання (резервна система)
Системи безперебійного живлення	- джерела безперебійного живлення	Резервна система: - резервні лінії електроживлення; - генератори електроживлення.
Системи аутентифікації на основі	- пароля	- електронного ключа доступу

Таблиця 3.3 – Система індикаторів «37 градусів» для IT-середовища ТОВ «Стройобзор»

№	Індикатор	Сутність	Од. вим.	Порогове значення	
				показника	інтенсивності
1	Гальмування власне	затримка швидкості типової операції	%	10	Більш ніж 200
2	Трафік	Необґрунтована зміна трафіку	%	30	Більш, ніж 5 – менш ніж 15 разів за місяць
3	"Ти попав"	Потрапляння у ворожу банерну систему (інфобот-ру)	так чи ні	Так (факт виявлення)	1 (з першого разу)
4	Автопілот-IT	Перехоплення управління скриптами	так чи ні	Так (факт виявлення)	1 (з першого разу)
5	Автопілот-менеджмент	Перехоплення управління папками адміністратора – зараження локальної мережі	так чи ні	Так (факт виявлення)	1 (з першого разу)
6	Троянський кінь	Контроль IP партнерів (при запиті власний сайт зависає)	так чи ні	Так (факт)	1 (з першого разу)
7	Гальмування стороннє	Зростання часу видачі API від партнера	%	100	Більше 5 разів

За результатами цілодобового моніторингу вказаних технічних параметрів (протягом місяця з 1 по 30 листопада 2020 року) були отримані наступні значення вказаних показників (табл.3.4).

В результаті проведеного моніторингу було виявлене незначне гальмування як часу проведення як внутрішніх операцій, так й зовнішніх. Результати стали підставою для запиту на проведення аудиту з боку партнерів, які здійснюють супровід сайту.

Таблиця 3.4 – Результатами цілодобового моніторингу системи «37 градусів» ТОВ «Стройобзор» (з 1 по 30 листопада 2020 року)

№	Індикатор	показник	інтенсивність
1	Гальмування власне	12 %	200
2	Трафік (середня динаміка)	7 %	28 днів
3	«Ти попав»	0	0
4	Автопілот-IT	0	0
5	Автопілот-менеджмент	0	0
6	Троянський кінь	0	0
7	Гальмування стороннє	90	7

Візуалізація отриманих результатів відображена у матриці станів (рис.3.11)

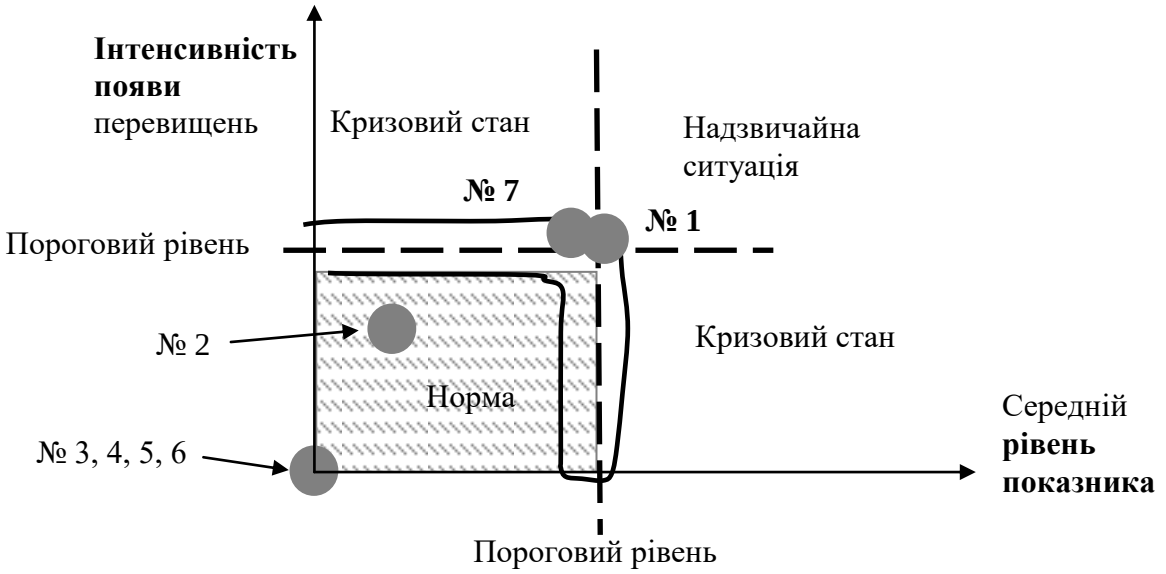

Рисунок 3.11 – Матриця станів критичної функції «Забезпечення роботи сайту (IT-складова)» для ТОВ «Стройобзор»

Зокрема, аудитом був виявлений скрипт, який використовується для генерування атаки-віддзеркалення, що використовує протокол Connectionless Lightweight Directory Access Protocol (CLDAP). Й хоча кінцеву мету

використання цього скрипта встановити не вдалось, показовим є те, що зафіксована активізація цього скрипта, зокрема й 17.02.2020 – день, коли були здійснені наймасштабніші атаки на сервери Amazon [42].

Таким чином, моніторингова система «37 градусів» дозволила виявити непомітні для звичайних систем симптоми неправомірного використання ресурсів сайту для спричинення шкоди третім особам.

А запропоновані заходи для створення додаткового захисту дозволяють відфільтрувати мережевий трафік та попередити більшу частину ситуацій, коли IT-бізнес використовується як засіб атаки.

ВИСНОВКИ

У першому розділі роботи розглянуто теоретичні засади захисту підприємств в умовах гібридних загроз. Розглянуті методологічні аспекти захисту підприємств в умовах гібридних загроз, розкритий сучасний стан гібридних впливів на бізнес-середовище та охарактеризована стійкість до гібридних загроз як складова економічної безпеки підприємства.

При цьому гібридні загрози визначені як широке поняття, яке постійно розвивається, яке спрямоване на прийняття політичних рішень, діяльність влади, ділової спільноти або на будь-яку їх комбінацію. Але в будь-якому випадку, ця загроза є одним з найбільших викликів оточуючого середовища в глобальному масштабі. Продемонстровано, що бізнес-спільнота та окремі компанії є невід'ємною частиною суспільства, а отже, і об'єктами гібридного впливу.

В другому розділі проаналізовано діяльність та напрями організації економічної безпеки ТОВ «Стройобзор», надана загальна характеристика діяльності підприємства, проведено аналіз його економічних та фінансових результатів діяльності, визначено напрями організації економічної безпеки на підприємстві. В результаті було зроблено наступний висновок: підприємство ТОВ «Стройобзор», що працює в медіа-просторі будівничої галузі, характеризується наявним попитом на свої послуги, фінансовою стійкістю бізнес-моделі та наявністю безпекових елементів її захисту. Але питанням для практичного дослідження залишається, чи збережеться надійність захисту даного бізнесу в умовах гібридних загроз.

В третьому розділі визначені шляхи підвищення безпеки бізнесу в умовах гібридних загроз та запропонований організаційно-методичний підхід до забезпечення захисту ТОВ «Стройобзор».

Запропоновані шляхи побудови механізму протидії гібридним загрозам на рівні бізнесу; способи ідентифікації ризиків, пов'язаних із гібридними

загрозами; прийоми для визначення індикаторів гібридних впливів; підходи до розробки операційних моделей моніторингу гібридних загроз, названі «37 градусів», та до розробки операційних моделей захисту від гібридних загроз.

Результати практичного дослідження продемонстрували, що запропонована моніторингова система «37 градусів» дозволяє виявити непомітні для звичайних систем симптоми неправомірного використання ресурсів сайту для спричинення шкоди третім особам.

А запропоновані заходи для створення додаткового захисту дозволяють відфільтрувати мережевий трафік та попередити більшу частину ситуацій, коли IT-бізнес використовується як засіб атаки.

Основні результати досліджень опубліковано у двох роботах, копії яких наведено у додатку А.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. HybridCoE: Hybrid threats as a concept. URL: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (дата звернення: 15.11.2020).

2. Legal challenges related to hybrid war and human rights obligations: PACE Resolution № 2217, Apr. 2018. URL: https://assembly. coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24762&lang=en

3. Про Звернення Верховної Ради України до Організації Об'єднаних Націй, Європейського Парламенту, Парламентської Асамблеї Ради Європи, Парламентської Асамблеї НАТО, Парламентської Асамблеї ОБСЄ, Парламентської Асамблеї ГУАМ, національних парламентів держав світу про визнання Російської Федерації державою-агресором: Постанова Верховної ради від 27 січня 2015 року № 129-VIII. URL: https://zakon.rada.gov.ua/laws/show/129-19#Text

4. Countering Russia's hybrid threats: an Update. NATO PA Special Report 166 CDS 18E, Oct. 2018. – URL: https://www.nato-pa.int/view-file?filename=/sites/default/files/2018-12/166%20CDS%2018%20E%20fin%20-%20HYBRID%20THREATS%20-%20JOPLING_0.pdf

5. Treverton G., Thvedt A., Chen A., Lee K., McCue M. Addressing Hybrid Threats: HybridCoE Report. Swedish Defence University, 2018. 101p.

6. Ситуація з правами людини в Україні: доповідь Управління Верховного Комісара ООН з прав людини, лютий, 2020. URL: https://www.ohchr.org/Documents/Countries/UA/29thReportUkraine_UA.pdf

7. UN, map OCHA «Ukraine: Overview of population displacement», 2015. URL: https://reliefweb.int/sites/reliefweb.int/files/resources/ ukr_ displacement_21_august_2015.pdf (дата звернення: 17.11.2020)

8. The HALO Trust: Making Land Safe In Ukraine. URL: https://www.halotrust.org/where-we-work/europe-and-caucasus/ukraine/ (дата звернення: 17.11.2020)

9. Ситуація з правами людини в Україні: доповідь Управління Верховного Комісара ООН з прав людини, серпень, 2018. URL: https://www.ohchr.org/Documents/Countries/UA/ReportUkraineMay-August 2018 _UKR.pdf

10. Åslund A. Kremlin Aggression in Ukraine: The Price Tag. The Atlantic Council Report, 2018. URL: https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Kremlin_Aggression_web_040218_revised.pdf

11. Joint communication to the European Parliament and the Council. Joint framework on countering hybrid threats, a European Union response, join (2016) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

12. Gilmore, J.S. Security Dialogue: Hybrid Threats and Modern Warfare. Permanent Council OSCE, Vienna, July 15, 2020 режим доступу: https://osce.usmission.gov/security-dialogue-hybrid-threats-and-modern-warfare/ (дата звернення: 10.11.2020)

13. Mazarr, M. J. Mastering the gray zone: understanding a changing era of conflict. US Army War College Carlisle, 2015. 157 p.

14. Гришко С., Пересада О. Підвищення обізнаності як елемент стійкості бізнес-середовища в умовах гібридних загроз. *Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці:* матеріали Всеукраїнської науково-практичної конференції, м.Київ, 7 грудня 2020 р. Київ: ДУІТ, 2020 *(подано до друку)*

15. Aho A., Midões C., Šnore A. Hybrid threats in the financial system: Hybrid CoE Working Paper 8. June, 2020. Helsinki, Finland: Hybrid CoE. 24 p.

16. Falk B. Hybrid CoE Strategic Analysis. Strategic citizens: Civil society as a battlespace in the era of hybrid threats. Helsinki, Finland: Hybrid CoE, 2020. 8 p.

17. Lutsevych O. Agents of the Russian World: Proxy Groups in the Contested Neighbourhood. Chatham House, 2016. 45 p.

18. Empty Shell No More: China's Growing Footprint In Central And Eastern Europe, AMO Policy Paper. Praha: AMO, 2020. 95 p.

19. Borchert, H. Looking Beyond the Abyss. Eight Scenarios on the Post-COVID-19 Business Landscape. Germany: HEDGE21 Strategic Assessments, 2020. 45 p.

20. Hybrid CoE Report: Nuclear Energy and the Current Security Environment in the Era of Hybrid Threats. Helsinki, Finland: Hybrid CoE, 2019 46 p.

21. Conley H. etc. The Kremlin Playbook Understanding Russian Influence in Central and Eastern Europe. USA: CSIS, 2016. 67 p.

22. Leonard, M. etc. Redefining Europe's economic sovereignty // Policy Contribution Issue. # 9. 2019. P. 1–23.

23. Sørensen C. Hybrid CoE Strategic Analysis 19: The ice dragon – Chinese interests in the Arctic. Helsinki, Finland: Hybrid CoE June, 2020. 8 p.

24. Business community and hybrid threats: Report of Pasi Eronen Foundation for Defense of Democracies. Helsinki, 2018. 20 p.

25. Vilmer J.-B., Escorcia A., Guillaume M., Herrera J. Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018. 210 p.

26. Живко З. Економічна безпека підприємств, організацій, установ. К.: «Правова єдність», 2009. 544 с.

27. Салоїд С. Механізм управління економічною безпекою підприємства: теоретичний аспект. *Економічний Вісник НТУУ «КПІ»*. 2017. С. 250 – 254. DOI: https://doi.org/10.20535/2307-5651.14.2017.108778

28. Cullen P. Hybrid CoE Strategic Analysis May 2018: Hybrid threats as a new ‘wicked problem’ for early warning. Helsinki, Finland: Hybrid CoE, May 2018. 8 p.

29. Rietjens S. Hybrid CoE Strategic Analysis 22: A warning system for hybrid threats – is it possible? – Helsinki, Finland: Hybrid CoE, June, 2020. 10p.

30. Єфіміна О., Гришко С. Від чого та як захищати бізнес в умовах гібридних загроз. *Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці:* матеріали Всеукраїнської науково-практичної конференції, м.Київ, 7 грудня 2020 р. Київ: ДУІТ, 2020 *(подано до друку)*

31. Savolainen, J. Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi): Hybrid CoE Working Paper. Helsinki, Finland: Hybrid CoE, 2019. 22 p.

32. Полозова Т. В. Формування інноваційно-інвестиційного механізму забезпечення конкурентоспроможності підприємства: монографія. Херсон: Видавничий дім «Гельветика», 2017. 592 с.

33. Тимощенко К.С. Фінансовий механізм фінансової безпеки суб'єктів підприємництва: дис. канд. екон. наук: 08.00.08. Дніпропетровськ, 2015. 310 с.

34. Cullen, P., Reichborn-Kjennerud, E. Countering hybrid warfare project: Understanding hybrid warfare (MCDC Report). A Multinational Capability Development Campaign project, London, 2017. 36 p.

35. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф. / О.П. Єрменчук. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

36. Hybrid Threats: Overcoming Ambiguity, Building Resilience / Ed. J.Hajek. Lithuania, Vilnius: NATO ENSEC COE, 2017. 52 p.

37. Забезпечення фінансово-економічної безпеки підприємництва: навчальний посібник/ Г.В. Соломіна. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. 234 с.

38. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, постанова КМУ від 19 червня 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF

39. Концепція створення державної системи захисту критичної інфраструктури, розпорядження КМУ від 6 грудня 2017 р. № 1009. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

40. Limnéll J. Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed. Helsinki, Finland: Hybrid CoE, 2018. 8 p.

41. Гришко С., Єфіміна О. Особливості захисту бізнесу в умовах гібридних загроз. *Матеріали І Міжнародної науково-практичної конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта»* (Харків. 3 листоп. 2020) / За заг. ред. Т.В. Полозової. Харків: ХНУРЕ, 2020. С. 71 – 76.

42. AWS Shield Threat Landscape Report – Q1 2020. –URL: https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf (дата звернення: 01.12.2020)