ДОДАТОК А

Копії публікацій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Кафедра економічної кібернетики та управління економічною безпекою

СУЧАСНІ СТРАТЕГІЇ ЕКОНОМІЧНОГО РОЗВИТКУ: НАУКА, ІННОВАЦІЇ ТА БІЗНЕС-ОСВІТА

І Міжнародна науково-практична конференція

3 листопада 2020 року

Харків 2020

УДК 330.341; 338.24; 005 (06)
ББК 65; 65.050.2
Я 431

Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта. Матеріали І Міжнародної науково-практичної конференції (м. Харків, 3 листопада 2020 р.) / За заг. ред. Т. В. Полозової [та ін.]. Харків. ХНУРЕ. 2020. 380 с.

У збірнику містяться матеріали, що були подані на І Міжнародну науково-практичну конференцію «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (м. Харків, 3 листопада 2020 року).

Для науковців, викладачів, аспірантів, а також фахівців, що займаються дослідженням питань соціально-економічного розвитку та забезпечення економічної безпеки підприємств, галузей, регіонів та країни.

УДК 330.341; 338.24; 005 (06)
ББК 65; 65.050.2
Я 431

ЗМІСТ

Гришко С. В.,
к.е.н., доцент кафедри економічної кібернетики
та управління економічною безпекою,
Харківський національний університет радіоелектроніки
Єфіміна О. О.,
студент,
Харківський національний університет радіоелектроніки

ОСОБЛИВОСТІ ЗАХИСТУ БІЗНЕСУ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

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. 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» [1]. 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.

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.

Хоча окрема компанія не обов'язково може бути кінцевою або навіть ключовою метою операції, вона може сприяти досягненню кінцевої стратегічної мети, наприклад, отримання довгострокового доступу до осіб, що приймають рішення або до їх мереж. Під час гібридної операції одна компанія може зазнати кібератаки, інша – інформаційної атаки, третя – ворожого захоплення, а четверта – класичного проникнення. При цьому жодна з цілей-жертв не може побачити та зрозуміти всієї операції.

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 Фінляндии (59%) не змогли пояснити, чому вони можуть бути ціллю діяльності, кінцевою метою якої є вплив на населення або уряд країни [2]. 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:

– 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 гібрідні «гравці» можуть впливати на бізнес, можні виділити наступне:

– надмірна прозорість та наївність персоналу та керівництва,
– недостатня обізнаність та пильність серед працівників,
– нездатність розпізнати вплив, замаскований під ділову діяльність.

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. 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.

Для комплексного захисту компанії (а через них – й суспільства) від гібридних загроз, система корпоративноїх 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.

Саме тому система корпоративної безпеки 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.

Перелік джерел посилання

1. Joint communication to the European Parliament and the Council. Joint framework on countering hybrid threats, a European Union response, join (2016) URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC00 18

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

3. 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.

Всеукраїнська науково-практична конференція

«УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ В УМОВАХ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ»

7 грудня 2020 року

Подано до друку

ВІД ЧОГО ТА ЯК ЗАХИЩАТИ БІЗНЕС В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Єфіміна О.О.,
магістрант кафедри економічної кібернетики та управління економічною безпекою Харківського національного університету радіоелектроніки
Гришко С.В.
к.е.н., доцент, доцент кафедри економічної кібернетики та управління економічною безпекою Харківського національного університету радіоелектроніки

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 громандської нетерпимісті, 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.1). 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 мультипликативного ефекту, від якого постраждають різні частини суспільства.

Невеликі компанії також можуть стати інструментом гібридних впливів на кшталт того, як шпіонське програмне забезпечення залучає мільони

ком'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 [2].

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[3]:

- побудова резервних систем в критичних для бізнесу сферах (зокрема – створення запасу ліквідності та перегляд JIT-підходів до логістики),
- створення системи захисту бізнесу із кібербезпековим компонентом,
- підвищення обізнаності персонала 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 імплементуючись в них та не порушуючи бізнес-діяльність.

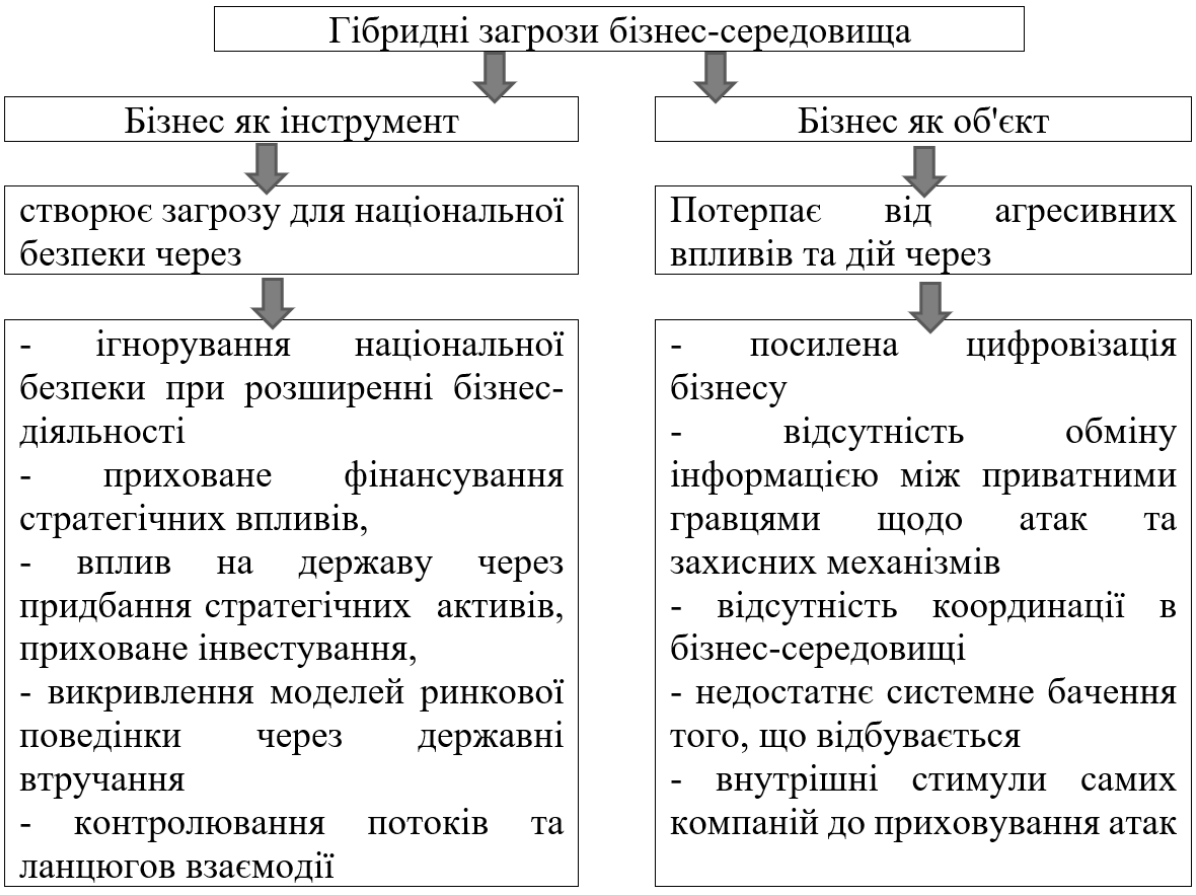

Рисунок 1 – Використання бізнесу в гібридній діяльності

Список використаних джерел

1. HybridCoE: Hybrid threats as a concept. – режим доступу: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

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

3. Aho A., Midões C., Šnore A. Hybrid threats in the financial system: Hybrid CoE Working Paper. - Helsinki, Finland: Hybrid CoE, 2020. -– 24 p.