DOI: 10.18372/2410-7840.25.17672
УДК 004.624

АНАЛІЗ ВПЛИВУ ІНОЗЕМНОГО ІТ БІЗНЕСУ НА ЛАНДШАФТ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ДЕРЖАВИ

Юлія Хохлачова, Андрій Давидюк, Віталій Зубок

Розвиток ІТ індустрії сприяє масштабуванню бізнесу з надання цифрових сервісів. Зростає рівень автоматизації процесів в державних та приватних організаціях. Зростає попит на обчислювальні ресурси. Бізнес в сфері центрів обробки даних починає масштабуватися щоб задовольнити потреби не тільки користувачів однієї країни, а й інших. Водночас користувачі з різних країн світу не обмежені у виборі надавача цих послуг. Вони будують власний ІТ бізнес з використанням ресурсу центрів обробки даних інших держав. Система таких транскордонної взаємодії будується вже багато років і її вплив на внутрішні економічні та соціальні процеси в різних державах зростає також. В наш час доцільно виокремити поняття мережі даних, що можна визначити як сукупність бізнес зв'язків між громадянами різних країн в сфері надання цифрових сервісів та зв'язків центрів обробки даних між собою. На сьогоднішній день відсутній контроль за розвитком мереж даних, зокрема відсутні підходи до вимірювання впливу ризиків кібербезпеки іноземного ІТ бізнесу на економічні та соціальні процеси в державі. Таким мережам притаманний синергетичний розвиток. Війна в Україні показала, що наявність російського ІТ бізнесу сприяла ряду кібератак з метою порушення функціонування об'єктів критичної інфраструктури, державних органів влади та бізнесу. Тому, звісно, не можна заперечувати причетність державних спецслужб до розгортання власної мережі даних для впливу на інші країни. Дана робота присвячена аналізу впливу іноземного ІТ бізнесу на кібербезпеку держави.

Ключові слова: *датацентр, ІТ бізнес, кібербезпека, кіберзахист, Україна, кіберстійкість.*

ВСТУП

Проблема ризиків іноземного ІТ бізнесу вже неодноразово підіймалася світовими вченими та експертами в галузі кібербезпеки, зокрема розкрито тематику промислового шпигунства в праці Вільяма Ханнаса [18], кібероперацій – Ніколасом Самбелу [24], кібероперацій геополітичного характеру – Білом Марчаком [12], описані кіберзагрози з боку Ірана Коліном Андерсоном [10]. Водночас доцільним є абстрагування від конкретних випадків і виокремлення загальних загроз для розуміння подій в кіберпросторі і їх причинно-наслідкових зв'язків. Метою роботи є аналіз загальних загроз кібербезпеці держави від іноземного ІТ бізнесу та демонстрація їх реалізації на прикладі російсько-української війни.

В умовах війни в Україні значна кількість організацій з метою резервування і збереження власних інформаційних активів здійснює міграцію до хмарних обчислювальних ресурсів [22]. Це дозволяє мінімізувати ризики втрати інформаційних ресурсів в наслідок ракетних ударів. Водночас зростає попит на використання хмарних послуг, що спричиняє появу нових датацентрів і в інших країнах. Збільшення пропозицій на ринку хмарних послуг впливає на зниження вартості і робить їх більш доступними. Отже, збільшується кількість клієнтів, а ряд користувачів починають стрімко масштабувати власні ресурси. Відкриття іноземних ІТ компаній може призвести до збільшення використання їхньої інфраструктури та послуг даних держави. Це створює залежність від цих компаній і може спричинити потенційні загрози безпеці, якщо доступ до цієї інфраструктури неправомірно отримають сторонні суб'єкти. Не винятком є і бажання ряду бізнесу російського походження уникнути ризиків санкційної політики та тиску влади, що стимулює їх мігрувати в іноземні датацентри і будують там нові відносини.

Рис. 1. Залежність держави від датацентрів та його клієнтів

Такий тренд впливає не тільки на розвиток бізнесу датацентрів, а й на надходження фінансів у вигляді податків до казни інших держав. Це створює економічні зв'язки ІТ бізнесу і держави.

Водночас важливо розуміти, що можлива ситуація, коли декілька користувачів датацентру, які приносять йому значний прибуток, роблять бізнес датацентру залежним від них. Враховуючи це існує імовірність наявності ланцюгів залежностей, як представлено на рис. 1.

З рис. 1 стає зрозумілим, що користувач, який бажає захистити свій бізнес повинен підвищувати свій вплив на економічний розвиток датацентру та держави. Основним шляхом збільшення такого впливу є масштабування бізнесу, міжнародна кооперація з іноземними партнерами, впровадження власних сервісів у різні критичні сфери життя. Наприклад складним питанням залишається оцінки впливу виходу з ринку корпорацій гігантів Microsoft, Google, Amazon. Іноземні ІТ компанії можуть пропонувати різні продукти та послуги, які використовуються в державних структурах і бізнес-середовищі. Аналіз впливу іноземного ІТ бізнесу повинен враховувати можливі вразливості в цих продуктах та послугах, оскільки це може створити ризики з точки зору кібербезпеки. Які локальні збитки отримає кожна організація або держава, на скільки це критично для ряду сервісів? Також не варто виключати можливість створення потенціалу для кібератак з різними цілями. Така невизначеність є джерелом великих ризиків. Отже, актуальним є питання оцінки впливу ІТ бізнесу іноземного походження на кібербезпеку держави.

ОСНОВНА ЧАСТИНА

Масштабування ІТ бізнесу як кібероперація

З огляду на необмежені можливості у масштабуванні ІТ бізнесу та його впливу на внутрішні процеси в державі є цілком можливим отримання контролю над процесами держави не військовим шляхом. Іноземний ІТ бізнес може мати доступ до важливих даних та інфраструктури держави. Це створює потенційний ризик зловживання доступом, якщо компанії не забезпечують достатніх заходів безпеки для захисту цих даних. Залучення іноземних ІТ компаній може підвищити ризик зовнішніх кібератак, оскільки збільшується потенційна точка входу для зловмисників. Аналіз впливу іноземного ІТ бізнесу на ландшафт загроз кібербезпеці держави має враховувати цей аспект та визначати заходи безпеки для запобігання таким атакам. Вплив іноземного ІТ бізнесу на кібербезпеку держави може бути також пов'язаний з геополітичними чинниками. Певні держави можуть мати вплив на іноземні ІТ компанії, що може мати наслідки для кібербезпеки держави. Така концепція частково відображає стратегію захоплення кіберпростору однією країною іншої. На прикладі України, рф постійно працювала над впровадженням російськомовного контенту створюючи велику різницю в контенті, сприяла різними шляхами впровадженню власних ІТ технологій, масштабувала власний ІТ бізнес в критичні сфери життя, наприклад інформаційно-комунікаційні технології, інформаційна та кібербезпека, системи навігації, системи фінансового обліку тощо. Побудова такої складної системи тривала багато років, водночас і зростав вплив рф на процеси в Україні. З початком захоплення територій України в 2014 році різко почала збільшуватися кількість кібератак на об'єкти критичної інфраструктури України, сервіси державних органів, приватні компанії. Введення санкційної політики стимулювало закупівлі та впровадження нового програмного та апаратного забезпечення, що, звісно, мінімізувало ризики появи нових кібератак та їх наслідків, але водночас виснажувало економіку держави в непростий для неї час. Ряд процесів потребували змін, що потребувало часу та додаткових витрат на адаптацію та навчання персоналу. Цілком справедливим є твердження, що Україна починаючи з 2014 року бореться за очищення власного кіберпростору від ІТ російського походження.

З огляду на це, актуальним стає визначення меж кіберпростору країни, її незалежності та суверенітету в кіберпросторі. Виникають питання визначення оптимального відсотку ІТ бізнесу власного походження, наявність аналогів програмного та програмно-апаратного забезпечення власного виробництва, наявність вітчизняних фахівців, оцінки впливу мереж даних з іншими країнами. Розробка механізмів контролю за процесами формування монополій ІТ бізнесу однієї країни в іншій. Ці процеси є вкрай важливими для безпеки держави. Водночас є і дуже небезпечними, так як ряд держав крім оцінки власних залежностей можуть здійснити оцінку залежностей інших країн від неї і, усвідомивши власну перевагу, можуть здійснити негативний вплив на іншу країну, слідуючи власним інтересам. Вирішення такої проблеми полягає

у створенні міжнародних організацій з забезпечення колективної безпеки у кіберпросторі та розробки міжнародних нормативних документів в рамках процесів кібердипломатії.

Переходячи від глобального розуміння проблем кібербезпеки, пов'язаних з іноземним ІТ бізнесом, до локальних, доцільним є розглянути можливість впровадження процедур «стрес тестування» з метою визначення необхідного потенціалу для зміни ІТ рішень на аналоги в рамках однієї організації, ряду організацій в одній сфері економіки. Визначення необхідного часу для такої заміни, ресурсів для підготовки персоналу. Незнання таких речей приводить до катастрофічних наслідків. Таким чином, стає зрозумілим, що чим швидше країна усвідомить загрозу, тим більше шансів протистояти їй з мінімальними втратами.

Мінімізація ризиків впливу ІТ бізнесу інших держав

Звісно, доцільним є почати з інвентаризації активів. Здійснити збір даних з державних організацій, об'єктів критичної інфраструктури про використовуване в них програмне та програмно-апаратне забезпечення, після чого визначити залежності організації від вендорів конкретної країни. Провести облік договорів з надання послуг в сфері ІТ та кібербезпеки і визначити відсоток інформованості країн надавачів послуг. З урахуванням зібраних даних стане можливим оцінити залежності та набори чутливих даних, що можуть бути в інших країн про власні ІТ ресурси держави. Водночас варто виділити інформацію про ІТ інфраструктуру, що доступна з відкритих джерел, зокрема з сайтів державних закупівель, сервісів сканування пристроїв, підключених до мережі Інтернет [11], технічної документації тощо. Вся ця інформація та залежності, у разі конфлікту, можуть бути використані проти держави. Використання кібератак в сьогоденні є частиною мультидоменних операцій[13]. Кібероперації мають на меті здійснення впливу на іншу країну з використанням кіберзброї [20]. Звісно, кібероперації також можуть бути використані як стримуючий фактор, або для попередження кібератак з боку противника. Проте, наявність ІТ ресурсів одної країни на території іншої в нинішній час можна порівняти з наявністю військових баз. Кожній країні варто здійснювати систематичний контроль власних залежностей, впроваджувати міжнародні договори для підтримання колективної безпеки. Присутність іноземного ІТ бізнесу не тільки може становити загрозу використання цих ресурсів проти країни, це також сприяє появі різниці в технологіях. Країна у якій ІТ забезпечено імпортом не відчуває потреби у створенні власного, монополізація бізнесу та конкуренція придушує будь-які можливості малого локального бізнесу створювати і впроваджувати власні технічні рішення для сприяння суверенітету і незалежності держави в кіберпросторі. Побудова бізнесу в ІТ базується на принципах масового використання сервісів користувачами. Зі стрімким розвитком криптовалюти стали популярними криптобіржі, які приносять досить великі гроші своїм власникам та до казни держав, під юрисдикцією яких вони функціонують. Такий бізнес є певного роду щитом для інших речей, таких як VPN сервіси, хостинги, DNS сервіси, які можуть бути застосовані для зловмисних дій в кіберпросторі.

Цілком реальним є планування масштабних кібероперацій, коли здійснюється впровадження рішень однієї країни у всі установи однієї зі сфер економіки, зокрема фінансової чи енергетичної, де важливим є уніфіковані підходи до обміну інформацією. Зокрема від цих сфер залежать процеси і в інших галузях. Таким чином порушення процесів в одній зі сфер економіки може призвести до каскадних ефектів в інших. Отже доцільним постає питання кіберстійкості держави.

Кіберстійкість України під час війни з рф на прикладі енергетичної галузі

Російсько-українська війна має гібридний характер. Кібератаки становлять значну загрозу в цій гібридній війні [19]. У 2014 році російські війська вторглися в Україну [4], створивши пряму загрозу територіальній цілісності та національній безпеці країни. Через окупацію росією Криму та частини Луганської та Донецької областей змінилася енергетична система України, а також система маршрутизації українського сегменту Інтернету [3]. Ці зміни безпосередньо впливають на стійкість як енергетичної системи, так і системи комунікацій (кіберпростору) і є джерелом значних загроз для цих галузей.

Українська енергетика є унікальною в Європі через наявність великої транспортної системи з вузлами до 3000 МВт та унікальними трансформаторами на 750 кВ, яких немає більше в Європі. Однак

саме ці вузли є найлегшою мішенню для масованих ракетних ударів противника. Більша розгалуженість і локалізація генерації (до чого, до речі, прагне ЄС) підвищує стійкість енергетики до фізичних впливів. Однак для великомасштабної генерації потрібне інтелектуальне цифрове управління, яке виводить проблему кіберзагроз на перший план нового енергетичного сектору.

Росія використовує для кібератак потенціал своїх спецслужб [23] та країн, які підтримують росію у цій війні [15]. Росія становить серйозну загрозу в кіберпросторі, оскільки кілька російських IT-компаній все ще мають функціонуючі обчислювальні ресурси по всьому світу [25]. Значну загрозу становить широке використання програмного забезпечення російського виробництва [21]. Ще однією проблемою є залучення російських експертів і співробітників російських представництв міжнародних компаній до побудови систем зв'язку, кібербезпеки та енергетики в Україні до 2014 року. З відходом таких компаній з російського ринку ці співробітники були звільнені, що служить спонукання до співпраці з хакерськими угрупованнями противника в цій війні [17].

Усі ці фактори становлять кіберзагрозу критичній інфраструктурі. Енергетичний сектор України безпосередньо впливає на інші галузі економіки. Цілями кібератак на об'єкти критичної інфраструктури в Україні є порушення функціонування систем розподілу електроенергії, збір інформації, порушення процесів обміну даними та вплив на інші залежні галузі (об'єкти критичної інфраструктури).

Інформація, отримана шляхом кібератак на критичну інфраструктуру, допомагає противнику планувати ракетні удари [2]. Порушення процесів обміну інформацією використовується як відволікаючий захід від основного вторгнення з метою виведення системи з ладу. Порушення системи використовується для впливу на суміжні галузі. Кібератаки рф на енергетичні системи також мають політичні мотиви [26].

Кібератаки на енергетичні компанії більш складні, і їх важко виявити. Також під постійною загрозою знаходяться компанії, які постачають апаратне та програмне забезпечення енергетичним компаніям. Таким чином, атаки на ланцюги поставок залишаються джерелом зростаючої загрози [14].

Статистика кібератак на енергетичний сектор підтверджує необхідність постійного підвищення його стійкості та безпеки [9] (рис. 2).

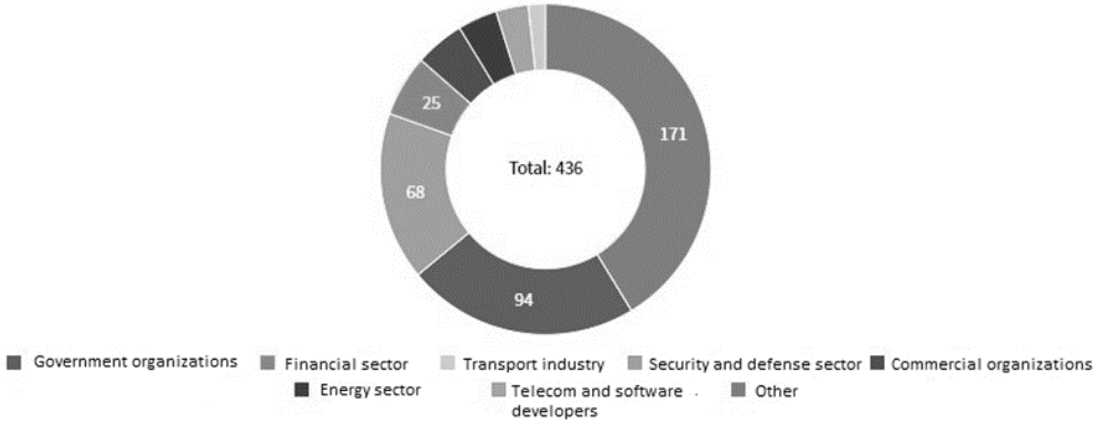

Рис. 2. Кіберстатистика CERT-UA [1]

З огляду на вищезазначене, метою цього дослідження аналіз впливу іноземного IT бізнесу на появу проблем стійкості в кіберпросторі, їх потенційних наслідків та аналізу причин їх виникнення.

Для розуміння поточних проблем доцільно проаналізувати дії зловмисника. Дії зловмисника залежать від його кінцевої мети, яка може полягати не тільки в порушенні енергетичного об'єкта. Тому існує потреба проаналізувати залежність кібербезпеки критичної енергетичної інфраструктури від інших галузей (каскадні ефекти).

Використовуючи отриману інформацію про каскадні ефекти, можна буде запропонувати

процедури для підвищення стійкості (компенсаторні заходи).

Знаючи мету зловмисника, ми можемо простежити процес кібератаки. Для аналізу кібератак на критичну інфраструктуру використовується модель «Cyber kill chain» [16].

Першим кроком цієї моделі є розвідка (збір інформації) про ціль. Вектор кібератаки визначається обсягом інформації про ціль і компетентністю зловмисника. Збираючи таку інформацію, зловмисник прагне отримати максимальну кількість даних за допомогою засобів OSINT і HUMINT [27], не виявляючи себе до етапу здійснення зловмисних дій.

Таблиця 1

Приклади існуючих та нових факторів кіберзагроз для енергетичної інфраструктури

Існуючі загрози	Застарілі версії операційних систем в операційних технологіях (ОТ).
	Багато систем ОТ світових брендів розроблені та впроваджені в Україні офісами та персоналом де-факто російських компаній.
	Широке використання антивірусного програмного забезпечення російських програмних компаній.
	Бухгалтерське програмне забезпечення, розроблене російськими розробниками програмного забезпечення.
	Логістичне програмне забезпечення російського виробництва.
	Можливі російські інсайдери серед співробітників об'єктів критичної інфраструктури.
	Атаки на ланцюги постачання.
Нові загрози	Захоплення обладнання державних установ та об'єктів критичної інфраструктури з окупацією територій військами рф.
	Отримання примусового доступу до критичних систем на окупованих територіях.
	Застосування ворогом засобів (уразливостей) українських хактивістів. без аналізу таких проблем у захисті критичної інфраструктури України.
	Створення ботферм і ботмереж (для DDoS атак).

Вибравши вектор кібератаки, зловмисник вибирає інструменти для кібератаки (експлойт з бекдором тощо). Додатковою загрозою є використання супротивником інструментів (уразливостей), які українські активісти використовували проти рф, не аналізуючи можливі ризики зворотної атаки. Після цього інструменти доставляються в цільову мережу. При вході в цільову мережу шкідливий код використовується з інсталяцією шкідливого програмного забезпечення на комп'ютер цільової мережі. Встановлення такого програмного забезпечення дозволяє зловмиснику отримати контроль над системою. Маючи контроль, зловмисник може здійснювати деструктивні дії.

Таким чином, ландшафт кіберзагроз для критичної інфраструктури можна описати в таблиці 1.

Існуючі обставини, наведені в табл. 1, свідчать про значний вплив рф. У контексті російсько-української війни поняття кордонів кіберпростору країни доцільно визначити як ступінь залежності однієї країни від ІТ-рішень та інформаційних ресурсів іншої. Зокрема, залежність можна розраховувати як частку ІТ-рішень, що використовуються в державі одного класу продукції однієї країни, до кількості ІТ-рішень інших країн. З огляду на зазначене, кібербезпека країни у 2014 році перебувала у критичному стані та потребує чітких та системних рішень. При цьому рф значно випереджає Україну за технічною підтримкою та має значний потенціал у розвитку кібербезпеки та інформаційних технологій.

Водночас рф вживає заходів щодо підвищення рівня кібербезпеки шляхом переходу на програмне забезпечення власного виробництва. Цей захід є досить ефективним і також необхідним для критичної інфраструктури України.

Ще однією проблемою стабільності критичної інфраструктури енергетичної галузі є використання типових рішень кібербезпеки, які постачаються на український ринок обмежена кількість вендорів та системних інтеграторів. Ці інтегратори також є потенційно менш захищеною мішенню для кібератак противника з метою отримання даних про їхні операції на об'єктах критичної інфраструктури.

Використання шаблонів конфігурації кібербезпеки допомагає збільшити масштаби атак і, як наслідок, збільшити збитки.

Організаційно-технічні засади кібербезпеки України

За обмежений період з 2014 року в Україні розпочато розбудову власної організаційно-технічної моделі кібербезпеки [6], розробляються нормативні документи, впроваджуються технічні рішення. Проте варто зазначити, що об'єктивна оцінка ефективності вжитих у 2022 році кроків свідчить про недостатнє покращення. Водночас Україна починає адаптуватися до нових процесів у кіберпросторі:

-створено центр активної протидії російській агресії в кіберпросторі [5];

-сформовано кібервійська [7];

-визначено орган державної влади з безпеки критичної інфраструктури [5];

-створено систему виявлення вразливостей [8].

Безперечно, в умовах війни ворог має перевагу через Україну в технологічних і часових ресурсах. Фізичне руйнування об'єктів енергетики російськими ракетними ударами та обстрілами посилює цю перевагу.

Таблиця 2

Приклад факторів ризику пов'язаних з робочим місцем

Робота на об'єкті	Небезпека транспортування на об'єкт і додому.
	Небезпека перебування на об'єкті, який є ціллю ракетного удару.
Віддалена робота вдома	Нестійкість електропостачання будинку.
	Незахищені електронні комунікації та віддалений доступ.
	Потенційно скомпрометовані домашні комп'ютери.
	Ризики помилок через відволікання уваги співмешканцями.
Кадрові зміни	Відсутність достатнього часу для детального вивчення інфраструктури.
	Недостатній досвід і кваліфікація.
	Інсайдерський ризик.

Ризики ракетних ударів впливають на ряд процесів у критичній інфраструктурі. Ці наслідки включають смерть або інвалідність працівників, порушення емоційного та психологічного стану, стрес, плинність кадрів тощо. Там, де це можливо, організації відправляють співробітників працювати з дому, де існують додаткові кіберризики. Загальні ризики для критичної інфраструктури енергетики в умовах систематичних ракетних ударів включають наступні ризики (табл. 2).

Україна адаптовує, закуповує та широко встановлює альтернативні джерела живлення (генератори, батареї), виконує резервне копіювання даних у хмарних сховищах як в Україні, так і за кордоном, навчає персонал. Проте слід зазначити, що Україна не була готова до масштабних відключень електроенергії. Тривала адаптація, безумовно, впливає на процеси кібербезпеки.

Пропозиції щодо аналізу даних і прогнозування

Досвід України свідчить про необхідність розробки моделей для аналізу стійкості енергетичної системи. Основою таких моделей повинні стати системи збору та аналізу великих даних. Основні необхідні набори даних включають:

-телеметричну інформацію від датчиків на периметрі інформаційно - комунікаційних систем критичної інфраструктури;

-дані, зібрані сервісами збору даних, що використовуються для OSINT (приклад Shodan, Censys, ZoomEye та інші);

-інформація засобів масової інформації про юридичну особу-власника або оператора критичної інфраструктури, персонал, підрядників, управлінські рішення (особливо кадрові питання);

-діяльність хакерських груп з недружніх країн (росія, Білорусь, Іран, Північна Корея);

-дії з кібербезпеки на стороні противника;

-інформація про закупівлі в сферах IT та кібербезпеки;

-зв'язок дій у кіберпросторі з активними військовими діями проти окремих об'єктів, у тому числі масовими ракетними ударами по енергетичним установкам (мультидоменні операції).

Цей перелік не є вичерпним, але такі набори інформації є складовими моделі інформаційного поля об'єкта захисту критичної інфраструктури. Модель такого інформаційного поля складається з інформації введення/виведення та процесів її обробки.

Можна стверджувати, що стійкість критичної інфраструктури в цілому залежить від здатності

зловмисника впливати на вміст вхідної інформації або процес її обробки. Таким чином, моделювання негативних впливів з використанням інформації з інформаційного поля об'єкта захисту критичної інфраструктури з метою порушення властивостей введення/виведення інформації та процесів її обробки є складовою стійкості критичної інфраструктури.

Одним із ефективних підходів до протидії таким впливам є впровадження моделі «Нульової довіри» (див. рис. 3) [28].

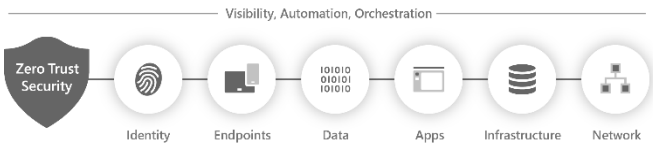

Рис. 3. Модель «Нульової довіри»

Результати такого моделювання можуть включати заходи для приховування конфіденційних даних і впровадження відповідних заходів резервного копіювання (лінії електропостачання, комунікації тощо).

Водночас ці дані є основою для аналізу ризиків як невід'ємної частини забезпечення стійкості.

ВИСНОВКИ

Глибока інтегрованість та недиверсифікованість іноземного ІТ бізнесу в критичних секторах може становити загрозу кібербезпеці країни. Основними ризиками закордонного ІТ бізнесу є залежність від інфраструктури, вразливості в продуктах та послугах, ризик зловживання доступом, зовнішні атаки, геополітичні чинники. Обчислювальні ресурси на території країни, що знаходяться у власності іноземця можуть бути використані при проведенні кібероперацій. ІТ бізнес може впливати на різні галузі економіки, збільшуючи власний вплив. Досвід України показав негативний вплив російського ІТ в Україні. Доцільними є зусилля держав щодо розбудови систем кіберстійкості.

Стійкість до кіберзагроз в енергетичному секторі України у воєнний час можна визначити як комплекс заходів зі збору та обробки великих обсягів даних, управління ризиками, адаптаційних заходів та можливостей аналітичного прогнозування. Проблеми енергозабезпечення України підтвердили необхідність ресурсного та матеріального забезпечення розробки ефективних планів забезпечення функціонування енергетичної системи.

Актуально акцентувати увагу на можливостях аналітичного прогнозування, оскільки ці процеси можуть значно підвищити ефективність реалізованих заходів стійкості. Завданням аналітичного прогнозування є розробка принципів кореляції між наданими масивами даних. Результатом такого співвідношення є вибірка подібних за своїми властивостями об'єктів критичної інфраструктури (інтегратор, вендор, обладнання, програмне забезпечення тощо). Така вибірка дає змогу швидко визначити можливий масштаб кібератаки та вжити відповідних заходів для локалізації скомпрометованого середовища. Зворотний підхід також використовується супротивником під час кібероперацій, коли він виявляє вразливу систему та шукає схожі цілі для збільшення масштабу атаки. Швидка локалізація сприяє якісному розслідуванню кібератак і зменшує наслідки кібератак.

Результати дослідження можуть бути використані при написанні доктрин національної безпеки, розробці стратегії кібербезпеки, формування політик безпеки організацій і при проєктуванні нових інформаційно-комунікаційних та технологічних систем в рамках післявоєнної відбудови України.

ЛІТЕРАТУРА

[1] Довідкова інформація з питань діяльності CERT-UA за фактами впливу на стан кібербезпеки у 2022 році [Електронний ресурс] // cert. gov. ua. Режим доступу: https://cert.gov.ua/article/37121 (дата звернення: 06.06.2023).

[2] Кібератаки, артилерія, пропаганда. загальний огляд вимірів російської агресії [Електронний ресурс] // https://cip.gov.ua. Режим доступу: https: //cip.gov.ua/en/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv - rosiiskoyi - agresiyi (дата звернення: 06.06.2023).

[3] Нечай О. Як працює інтернет у "ДНР" - лист читача з окупованих територій, tokar.ua [Електронний ресурс] / Олександр Нечай // Tokar.ua. Режим доступу: https: // tokar.ua /read/ 44924 (дата звернення: 06.06.2023).

[4] Повномасштабне вторгнення Росії в Україну: історичний контекст [Електронний ресурс] // uinp. gov.ua. Режим доступу: https: // uinp. gov. ua/ aktualni-temy/povnomasshtabne-vtorgnennya-rosiyi-v-

ukrayinu - istorychnyy - kontekst (дата звернення: 06.06.2023).

[5] Про Державну службу спеціального зв'язку та захисту інформації України [Електронний ресурс]: Закон України від 23.02.2006 р. № 3475-IV: станом на 31 берез. 2023 р. Режим доступу: https://zakon. rada.gov.ua /laws /show / 3475-15#Text (дата звернення: 06.06.2023).

[6] Про затвердження Положення про організаційно-технічну модель кіберзахисту [Електронний ресурс]: Постанова Каб. Міністрів України від 29.12. 2021 р. № 1426. Режим доступу: https:// zakon. rada. gov.ua / laws / show /1426-2021-п#Text (дата звернення: 06.06.2023).

[7] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" [Електронний ресурс]: Указ Президента України від 26.08.2021 р. № 447/2021. Режим доступу: https://zakon.rada. gov.ua/laws/show/447/2021#Text (дата звернення: 06.06.2023).

[8] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" [Електронний ресурс]: Указ Президента України від 26.08.2021 р. № 447/2021. Режим доступу: https://zakon.rada. gov.ua/laws/show/447/2021#Text (дата звернення: 06.06.2023).

[9] Російські хакери намагалися позбавити доступу до електроенергії значну кількість українців [Електронний ресурс] // https://cip.gov.ua. Режим доступу: https: // cip.gov.ua /ua/news/ rosiiski-khakeri-namagalisya-pozbaviti- dostupu - do - elektroenergiyi-znachnu-kilkist-ukrayinciv (дата звернення: 06.06. 2023).

[10] Anderson C. Iran's cyber threat espionage, sabotage, and revenge [Electronic resource] / Collin Anderson, Karim Sadjadpour. Washington: Carnegie Endowment for International Peace Publications Department, 2018. 73 p. Mode of access: https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134 (date of access: 07.06.2023).

[11] Best network scanning tools (network and IP scanner) of 2023 [Electronic resource] // Software Testing Help. Mode of access: https://www.softwaretestinghelp.com / network-scanning-tools / (date of access: 06.06.2023).

[12] Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert. "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," Citizen Lab Research Report No. 135, University of Toronto, December 2020.

[13] Black J. Cyber Threats to NATO from a Multi-Domain Perspective [Electronic resource] / James Black, Alice Lynch. 2020. pp. 126-150. Mode of access: https: // ccdcoe. org / uploads / 2020/ 12/ 7-Cyber_ Threats_NATO_Multidomain_Perspective_ebook. pdf.

[14] CERT-UA від початку року опрацювала більше двох тисяч кібератак на Україну [Електронний ресурс] // https://cip.gov.ua. Режим доступу: https:/ / cip.gov.ua/ ua / news / cert-ua-vid-pochatku-roku-opracyuvala-bilshe-dvokh-tisyach-kiberatak-na-ukrayinu (дата звернення: 06.06.2023).

[15] Corera G. Iranian and Russian hackers targeting politicians and journalists, warn UK officials [Electronic resource] / Gordon Corera // BBC News. Mode of access: https: // www. bbc. com /news/uk-64405220 (date of access: 06.06.2023).

[16] Cyber kill chain® [Electronic resource] // Lockheed Martin. Mode of access: https://www.lockheedmartin. com / en-us / capabilities / cyber/cyber-kill-chain.html (date of access: 06.06.2023).

[17] Ericsson divests its local customer support business in Russia [Electronic resource] // www.ericsson.com. Mode of access: https: // www. ericsson. com /en/ press-releases/2022/12/ericsson-divests-its-local-customer-support-business-in-russia (date of access: 06.06.2023).

[18] Hannas W. C. Chinese industrial espionage [Electronic resource] / William C. Hannas. [S. l.]: Routledge, 2013. Mode of access: https://doi.org/10. 4324/9780203630174 (date of access: 07.06.2023).

[19] Hasratyan N. Cyberattacks in hybrid warfare: the case of Russia/Ukraine War [Electronic resource] / Nina Hasratyan // HeadMind Partners. Mode of access: https: // www.headmind.com /en/cyberattacks-hybrid - warfare/ (date of access: 06.06.2023).

[20] International cyber law: interactive toolkit. Scenario 10: legal review of cyber weapons [Electronic resource] / International cyber law: interactive toolkit // International cyber law: interactive toolkit. Mode of access: https: // cyberlaw. ccdcoe.org / wiki / Scenario_10:_Legal_review_of_cyber_weapons (date of access: 06.06.2023).

[21] Levy I. Use of Russian technology products and services following the invasion of Ukraine [Electronic resource] / Ian Levy // NCSC. Mode of access: https: //www.ncsc.gov.uk/blog-post/use-of-russian-technology-products-services-following-invasion-ukraine (date of access: 06.06.2023).

[22] Moss S. Escaping Ukraine: data migration during an invasion [Electronic resource] / Sebastian Moss // Data center industry news, analysis and opinion - DCD. Mode of access: https://www.datacenterdynamics.com/en/analysis/escaping-ukraine-data-migration-during-an-invasion/ (date of access: 06.06.2023).
[23] Russian state-sponsored and criminal cyber threats to critical infrastructure | CISA [Electronic resource] // Cybersecurity and Infrastructure Security Agency CISA. Mode of access: https://www.cisa.gov/news-events/ cybersecurity-advisories / aa22-110a (date of access: 06.06.2023).
[24] Sambaluk N. M. Myths and realities of cyber warfare: conflict in the digital realm / Nicholas Michael Sambaluk, Eugene H. Spafford. [S. l.]: ABC-CLIO, LLC, 2020.
[25] Soldatov A. Russian cyberwarfare: unpacking the kremlin's capabilities [Electronic resource] / Andrii Soldatov, Irina Borogan // CEPA. Mode of access: https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities / (date of access: 06.06.2023).
[26] "Ukrenergo" under war conditions: Attacks increased threefold to block joining European power network". https://cip.gov.ua. Mode of access: https://cip.gov.ua/en/news/ukrenergo-v-umovakh-viini- kiberataki-zrosli-vtrichi-shob-zupiniti-priyednannya- do - yevropeiskoyi-energomerezhi (date of access: 06.06.2023).
[27] Warner C. Attribution of advanced persistent threats [Electronic resource] / Chad Warner // https://warnerchad.medium.com. Mode of access: https://warnerchad.medium.com/attribution-of-advanced-persistent-threats-notes-94008ea1f365 (date of access: 06.06.2023).
[28] What is zero trust? [Electronic resource] // Microsoft Learn: Build skills that open doors in your career. Mode of access: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview (date of access: 06.06.2023).

ANALYSIS OF THE IMPACT OF FOREIGN IT BUSINESS ON THE LANDSCAPE OF CYBERSECURITY THREATS TO THE STATE

The development of the IT industry contributes to the scaling of businesses providing digital services. The level of process automation in both public and private organizations is increasing. There is a growing demand for computing resources. Businesses in the data centre sphere are scaling to meet the needs not only of users within one country but also of others. At the same time, users from different countries are not limited in their choice of service providers. They are building their own IT businesses using the resources of data centres in other countries. Such a system of trans bordered relations has been built for many years, and its impact on internal economic and social processes in different countries is also growing. In our time, it is relevant to define the concept of a data network, which can be understood as a set of business connections between citizens of different countries in the field of providing digital services and relationships between data centres. Currently, there is no control over the development of data networks, particularly no approaches to measuring the impact of cyber risks of foreign IT businesses on economic and social processes in a country. These networks are characterized by synergistic development. The war in Ukraine has shown that the presence of Russian IT businesses facilitated a series of cyber-attacks aimed at disrupting the functioning of critical infrastructure, government authorities, and businesses. Therefore, it is undeniable that state security services are involved in deploying their own data networks to influence other countries. This work is dedicated to analyzing the impact of foreign IT businesses on a country's cybersecurity.

Keywords: data center, IT business, cybersecurity, cyber defense, Ukraine, cyber resilience.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій НАУ.
Yulia Khokhlachova, candidate of technical sciences, associate professor, associate professor of the Department of information technology security of NAU.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Давидюк Андрій Вікторович, аспірант кафедри безпеки інформаційних технологій НАУ, молодший науковий співробітник ІПМЕ ім. Г.Є. Пухова НАН України.
Andrii Davydiuk, Phd student of the Department of information technology security of NAU, junior scientific researcher G.E. Pukhov IMEE NAS of Ukraine, Technical researcher NATO CCDCOE.
E-mail: andrey19941904@gmail.com.
Orcid ID: 0000-0003-1238-2598.

Зубок Віталій Юрійович, доктор технічних наук, старший дослідник, професор кафедри Комп'ютеризованих систем управління НАУ.
Vitalii Zubok, Doctor of Technical Sciences, senior researcher, professor of the Department of Computerized Management Systems of NAU.
E-mail: vit@visti.net.
Orcid ID: 0000-0002-6315-5259.