DOI: 10.26565/2310-9513-2025-21-09
Класифікація JEL: C 42, C 89, D 74, L 86, O 19, R 59

НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЦИФРОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КРАЇНАХ ОСТРОВІВ ПІВДЕННО-СХІДНОЇ АЗІЇ

Лубенець Сергій Васильович
кандидат технічних наук, доцент
доцент кафедри міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 4, м. Харків, 61022
e-mail: s.lubenec@karazin.ua
ORCID: https://orcid.org/0000-0003-1061-8763

Шелестова Анна Миколаївна
кандидат наук із соціальних комунікацій, доцент
доцент кафедри економічної кібернетики та прикладної економіки
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 4, м. Харків, 61022
e-mail: anna.shelestova@karazin.ua
ORCID: https://orcid.org/0000-0003-4866-1767
ID автора Scopus: 58277829400

Чернишова Лариса Олексіївна
кандидат економічних наук, доцент
доцент кафедри міжнародних відносин
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 4, м. Харків, 61022
e-mail: lchernyshova@karazin.ua
ORCID: https://orcid.org/0000-0002-3589-9154

Розглянуто проблеми та напрями забезпечення міжнародної цифрової інформаційної безпеки в країнах островів Південно-Східної Азії (SEA), зокрема щодо захисту від програм-вимагачів, які основані на рекомендаціях Сінгапурської цільової групи боротьби з програмами-вимагачами (CRTF), а також на аналітичних матеріалах науковців, експертів та фахівців, що спеціалізуються на проблематиці регіональної інформаційної безпеки та розробці відповідних інструментів для її забезпечення. Предметом дослідження в статті є питання забезпечення міжнародної цифрової інформаційної безпеки в країнах островів SEA у контексті боротьби з програмами-вимагачами. Мета – полягає в дослідженні поточного стану, актуальних проблем і тенденцій міжнародної цифрової інформаційної безпеки для пошуку можливих напрямів підвищення її ефективності в країнах островів SEA на прикладі інформаційних загроз з боку програм-вимагачів та методів боротьби з ними. Завдання: визначити основні сучасні інформаційні загрози та особливості забезпечення цифрової інформаційної безпеки у досліджуваному регіоні; дослідити тенденції розвитку інформаційних загроз з боку програм-вимагачів, їх вплив на міжнародний бізнес та існуючі рекомендації по боротьбі з ними; розробити керівні принципи, рекомендації та методи захисту даних, які можуть бути використані організаціями та міжнародними компаніями країн островів SEA для підвищення ефективності цифрової інформаційної безпеки. Використовується загальнонауковий метод системного аналізу – для визначення поточного стану, викликів та ключових тенденцій цифрової інформаційної безпеки у боротьбі з програмами-вимагачами, а також для дослідження можливих напрямів підвищення її ефективності. Отримано такі результати: на основі обробки звітності, що стосуються сучасного стану міжнародної цифрової інформаційної безпеки та програм-вимагачів, визначено стан, особливості та проблеми забезпечення кібербезпеки в країнах островів SEA. Надано рекомендації щодо боротьби з програмами-вимагачами та методи захисту від них на основі висновків провідних компаній, що працюють у сфері інформаційного захисту, а також з урахуванням керівних рекомендацій CRTF. Визначено можливі напрямки та перспективи подальших наукових досліджень щодо розглянутої проблематики. Висновки: отримані результати

досліджень, а також реалізація викладених у статті рекомендацій, зокрема щодо боротьби з програмами-вимагачами, сприяє забезпеченню ефективної цифрової інформаційної безпеки та формуванню надійного стійкого цифрового середовища проти складних інформаційних загроз. Запропоновані в роботі керівні принципи, рекомендації та методи захисту корпоративних даних можуть бути використані як передова практика для приватних організацій та міжнародних компаній країн островів SEA. Додаткові рекомендації для державних і приватних організацій регіону вказують на те, як найкраще захиститися від різних інформаційних загроз, з акцентом на висновки та рекомендації цільової групи CRTF. Внаслідок цього, реалізуючи ефективні заходи та практики, організації острівного регіону можуть значно зміцнити свої позиції інформаційної безпеки щодо захисту даних та відновлення після збоїв, а також значно скоротити кібератаки як від внутрішніх, так і зовнішніх загроз.

Ключові слова: *цифровізація світової економіки, цифрова інформаційна безпека, програми-вимагачі, резервне копіювання, країни островів Південно-Східної Азії.*

Як цитувати: Лубенець С.В., Шелестова А.М., Чернишова Л.О. Напрями підвищення ефективності цифрової інформаційної безпеки в країнах островів Південно-Східної Азії. *Вісник ХНУ імені В. Н. Каразіна. Серія «Міжнародні відносин. Економіка. Країнознавство. Туризм»*. 2025. № 21. С. 81–88. DOI: https://doi.org/10.26565/2310-9513-2025-21-09
In cites: Lubenets S., Shelestova A., & Chernyshova L. (2025) Directions for improving the efficiency of digital information security in the island countries of Southeast Asia. *The Journal of V. N. Karazin Kharkiv National University. Series International Relations. Economics. Country Studies. Tourism*, (21), 81–88. https://doi.org/10.26565/2310-9513-2025-21-09 (in Ukrainian)

Постановка проблеми. В останні роки з розвитком цифрової трансформації країн світу та цифровізації світової економіки повсюдно продовжують виявлятися численні проблеми цифрової інформаційної безпеки. Не винятком у цьому плані є такий специфічний регіон, як країни островів Південно-Східної Азії (SEA). У даний час в урядів та компаній цього острівного регіону особливо великі побоювання викликають інформаційні загрози, пов'язані з програмами-вимагачами.

Зокрема, у Сінгапурі та інших країнах островів SEA інциденти з програмами-вимагачами зростають як за частотою, так і за складністю, становлячи серйозну загрозу для інфраструктури цифрової інформаційної безпеки всього острівного регіону. Тому для ефективної боротьби з даною загрозою урядам і приватним компаніям цих країн вкрай важливо зміцнювати свій інформаційний захист задля забезпечення безперервності діяльності та розвитку організацій регіону.

Важливість даної проблематики для країнах островів SEA підтверджується значною увагою урядів цих країн до питань забезпечення інформаційної безпеки щодо програм-вимагачів. Так, для ефективної протидії зростаючим інформаційним загрозам з їх боку урядом Сінгапуру створена Сінгапурська цільова група боротьби з програмами-вимагачами (CRTF) [5], яка покликана розробляти відповідні керівні принципи та рекомендації.

Аналіз останніх досліджень і публікацій. Напрямки, задачі та проблеми регіональної безпеки в контексті забезпечення ефективної інформаційної безпеки та кіберзахисту з урахуванням особливостей того чи іншого регіону світу досліджувалися рядом аналітиків, науковців та профільних фахівців.

Зокрема, в науковій статті [1] на основі аналізу статистичних даних щодо регіону EMEA розглянуто питання підвищення ефективності корпоративної інформаційної безпеки компаній та установ шляхом розробки універсальної консолідованої стратегії взаємодії служб інформаційної безпеки та інформаційних технологій.

У статті [2] аналізуються питання поточного ландшафту та основні сучасні виклики інформаційної безпеки в регіоні Центральної та Східної Європи. В роботі [6] проводиться огляд та аналіз розвитку програм-вимагачів та актуальних інформаційних загроз з їх використанням. У публікації [7] досліджуються сучасні тренди цифрової інформаційної безпеки у світі, а також проведено огляд та аналіз спеціалізованих програмних рішень, щодо забезпечення цифрового інформаційного захисту та резервного копіювання даних.

У науковій статті [3] викладено загальний політичний огляд регіону Південно-Східної Азії в контексті східноазійської інтеграції та регіональної безпеки. В роботі встановлено, що економічне співробітництво в регіоні дедалі більш виходить за межі економічних інтересів і поширюється на сферу регіональної безпеки.

У той же час існує потреба в подальших дослідженнях, що стосуються цифрової міжнародної інформаційної безпеки в різних важливих регіонах і країнах світу, оскільки кожен регіон чи навіть країна можуть мати певні особливості та нюанси щодо інформаційних загроз і методів боротьби з ними. Зокрема, актуальними є питання розробки та аналізу дієвих рекомендацій щодо забезпечення ефективного захисту від програм-вимагачів та надійного резервного копіювання корпоративних конфіденційних даних з урахуванням специфічних умов та особливостей країн островів Південно-Східної

Азії, що є важливим регіоном з точки зору забезпечення безпечних умов і неперервності діяльності міжнародних компаній та організацій.

Мета статті, завдання дослідження. *Метою* роботи є дослідження поточного стану, актуальних проблем і тенденцій міжнародної цифрової інформаційної безпеки для пошуку можливих напрямів підвищення її ефективності в країнах островів Південно-Східної Азії на прикладі інформаційних загроз з боку програм-вимагачів та методів боротьби з ними.

Відповідно до мети дослідження в роботі були поставлені та вирішувалися наступні основні *завдання*:

– визначити основні сучасні інформаційні загрози та особливості забезпечення цифрової інформаційної безпеки у досліджуваному регіоні;

– дослідити тенденції розвитку інформаційних загроз з боку програм-вимагачів, у тому числі в регіоні країн островів SEA;

– проаналізувати вплив програм-вимагачів на міжнародний бізнес та існуючі рекомендації по боротьбі з ними;

– розробити керівні принципи, рекомендації та методи захисту даних, які можуть бути використані організаціями та міжнародними компаніями країн островів Південно-Східної Азії для підвищення ефективності цифрової інформаційної безпеки.

Основні результати дослідження. Питання підвищення ефективності цифрової інформаційної безпеки в країнах островів Південно-Східної Азії в першу чергу доцільно дослідити на прикладі Сінгапуру, як країни регіону з найбільш розширеними цифровими зв'язками. Проте, хоча результати цих досліджень покликані вияснити особливості необхідних захисних дій насамперед сінгапурських організацій та фірм відповідно до рекомендацій Сінгапурської цільової групи боротьби з програмами-вимагачами, вони однаково актуальні й для інших країн досліджуваного острівного регіону.

CRTF була скликана урядом Сінгапуру для вирішення зростаючих проблем з такою інформаційною загрозою як програми-вимагачі, з якими дедалі більше стикається країна та регіон островів SEA загалом. CRTF прагне об'єднати урядові установи у відповідних галузях, можливостях та оперативних планах для зміцнення зусиль країни щодо боротьби з програмами-вимагачами та надання Сінгапуру й регіону більш вигідних позицій для просування міжнародних дій проти глобальної загрози програм-вимагачів.

Програми-вимагачі та їх вплив на міжнародний бізнес. Дослідження особливостей забезпечення цифрової інформаційної безпеки на прикладі боротьби саме з програмами-вимагачами викликано тим, що зловмисні атаки з їх боку представляють серйозну загрозу інфраструктурі інформаційної безпеки всього регіону островів Південно-Східної Азії. Для боротьби з цією загрозою, що зростає, урядам і приватному сектору країн даного регіону необхідно посилити інформаційний захист, запроваджуючи відповідні передові практики.

У зв'язку з цим також важливо відзначити, що чи не останньою «лінією інформаційної оборони» організації, яка забезпечує доступність, готовність і, що важливіше, безперервність бізнесу та цілісність даних, є резервне копіювання. Рішення ряду профільних компаній у сфері цифрового інформаційного захисту та резервного копіювання, зокрема компанії Veeam [6], можуть бути важливою частиною цього процесу, надаючи розширені можливості захисту даних, резервного копіювання та відновлення, які відповідають рекомендаціям CRTF.

Для вирішення поставлених у роботі завдань для початку слід дослідити поточну ситуацію з програмами-вимагачами у світі, і зокрема в країнах островів Південно-Східної Азії, а також визначити їх вплив на міжнародний бізнес, спираючись на звіти авторитетних профільних компаній даної галузі.

Швидкий розвиток програм-вимагачів викликає тривогу, а їхні кібератаки ростуть безпрецедентними темпами. У своєму звіті 2024 року про тенденції в галузі програм-вимагачів компанія Veeam виявила [6], що 75% організацій у світі хоча б раз на рік зазнавали атак програм-вимагачів. Крім того встановлено, що зловмисники переважно націлені на резервні копії – 96% атак були націлені саме на них, причому 76% з цих атак були успішними.

Сінгапур, як провідна країна острівного регіону, останніми роками також пережила кілька серйозних атак програм-вимагачів. Зокрема, атаку зазнала велика професійна організація в країні, внаслідок чого були скомпрометовані персональні дані, що належать понад 16000 членів організації. Один з найбільших постачальників телекомунікаційних послуг країни також став жертвою кібератаки, яка призвела до крадіжки персональних даних у 129000 клієнтів, а зловмисники вимагали від компанії викуп у розмірі 250000 доларів США в біткоїнах.

У той же час вражає стрімке зростання кількості варіантів програм-вимагачів: за останні півроку було зафіксовано понад 10 тисяч варіантів таких програм порівняно з 5400 за попередній шестимісячний період. Це є майже 100% зростання кількості варіантів програм-вимагачів за півроку. Крім того, середній розмір виплат за ліквідацію шкоди від програм-вимагачів також зріс до більш ніж 1,8 млн. доларів США в 2024 році, що втричі більше, ніж у 2020 році.

Проте фінансовий тягар від програм-вимагачів виходить за межі самого викупу – фактично було виявлено, що виплати становлять лише 32% від фінансових втрат, які зазнають організації. Додатково сюди також входять:

– простої в обслуговуванні інформаційних систем;

– час, витрачений на відновлення даних та систем;

– підрив довіри клієнтів, що призводить до втрати доходу;

– негативне висвітлення у ЗМІ;

– юридичні санкції.

Це все приховані витрати від програм-вимагачів та пов'язаної з ними втрати даних, з якими стикаються організації через відсутність адекватного захисту, збоїв в обслуговуванні корпоративних інформаційних систем та неналежного планування безперервності бізнесу.

У ході опитування, проведеного компанією Veeam серед 1200 респондентів, та їхнього досвіду з програмами-вимагачами у 2024 році було виявлено, що кібержертви не змогли відновити 43% даних, які постраждали від атак програм-вимагачів. Ця статистика наголошує на важливості забезпечення адекватного захисту та гарантованої можливості відновлення даних.

Згідно результатів аналізу звітних матеріалів [7], чотири з п'яти організацій-респондентів досліджуваного острівного регіону вважають, що вони мають розрив між тим, наскільки швидко, за їхніми очікуваннями, продовжуватимуться кібератаки програм-вимагачів, і тим, що IT-послуги можуть фактично надати для захисту від них. 63% організацій також вважають, що для них потрібне або значне покращення, або повна перебудова у забезпеченні цифрової інформаційної безпеки, щоб узгодити роботу своїх команд резервного копіювання та інформаційного захисту. При цьому на даний час основною причиною неузгодженості є відсутність інтеграції між інструментами резервного копіювання та інструментами цифрової інформаційної безпеки. Щоб краще підготуватися до боротьби з програмами-вимагачами, саме резервне копіювання має вирішальне значення – 95% організацій, що зазнали атак, мали завчасно створену групу реагування на інциденти із заздалегідь визначеним планом на випадок виникнення інформаційних загроз.

У даний час атаки програм-вимагачів стали більш витонченими. Відомими прикладами є атаки, вчинені такими кіберзлочинними групами, як Wizard Spider і Conti. Широко відомими програмами-вимагачами є програма ScareCrow, а також різновиди програм-вимагачів від Conti. Раніше у 2022 році були поширені інші сімейства програм-вимагачів, такі як STOP та REvil. Їхні атаки насамперед були спрямовані на компрометацію операційної системи MS Windows, роблячи відновлення даних неможливим без належного захисту резервного копіювання. Операційна система Linux хоч і піддається меншому ризику в порівнянні з Windows, все одно залишається вразливою для програм-вимагачів та інших зовнішніх і внутрішніх загроз, якщо не вжито належних заходів управління та контролю облікових даних.

Розширені атаки програм-вимагачів також використовують так звані «сплячі файли» з ефектом бомби уповільненої дії на виробничих серверах, настільних комп'ютерах та загальних файлових ресурсах. Навіть якщо пошкоджені файли повністю відновлені до шифрування, існує ймовірність, що зараження може залишатися сплячим у самих файлах резервних копій, що призводить до атак, які повторюються. Зловмисники та злочинні організації використовують цю ситуацію, щоб зробити резервні копії неефективними або зажадати кілька викупів від критично важливих організацій, які шукають швидке рішення.

Подібні атаки з використанням сплячих файлів спеціально розроблені для затримки заподіяння шкоди на тижні або навіть місяці замість негайної крадіжки, стирання або вимагання даних після зламування комп'ютера чи сервера. Цей варіант програми-вимагача створює великі проблеми для їх відстеження та відновлення даних. Навіть якщо викуп за розшифрування файлів виплачується, багато організацій виявляють, що вони не можуть розшифрувати всі свої дані або стикаються з помилками розшифровки, якщо не буде здійснено додаткові виплати викупу. Більше того, кібератаки часто націлені на організації, які мають страховку від програм-вимагачів, оскільки є більш висока ймовірність отримання платежу [4].

У даний час національна позиція Сінгапуру полягає в тому, що виплата викупу зловмисникам з використанням програм-вимагачів настійно не рекомендується, з чим погоджується CRTF. Згідно з висновками цільової групи, виплата викупу тільки підживлює проблему програм-вимагачів. CRTF відмовляє від сплати викупу, зазначаючи, що це не гарантує розшифровку викуплених даних або те, що дані не будуть опубліковані зловмисником, який використовує програму-вимагач. До того ж організація, яка вже заплатила, також може бути ідентифікована зловмисниками як «м'яка» мета і зазнати повторного нападу.

Рекомендації щодо боротьби з програмами-вимагачами та методи захисту від них. За результатами аналізу звітів CRTF визначено [5], що дана цільова група рекомендувала урядам Сінгапуру та інших країн островів SEA зосередитись на наступних чотирьох ключових діях захисту від програм-вимагачів:

1. У першу чергу зміцнити захист високоризикових цілей, таких як державні установи, критично важлива інформаційна інфраструктура та підприємства, щоб зловмисникам, які використовують програми-вимагачі, було складніше проводити успішні атаки.

2. Зруйнувати бізнес-модель програм-вимагачів, щоб зменшити віддачу від їх атак.

3. Підтримувати відновлення даних, щоб жертви атак програм-вимагачів не відчували тиску щодо примусу платити викуп, який підживлює індустрію програм-вимагачів.

4. Працювати з міжнародними партнерами для забезпечення скоординованого глобального підходу до протидії програмам-вимагачам.

Цільова група також розробила еталонний ланцюжок дій програм-вимагачів, в якому зазначені наступні п'ять етапів атаки цих програм:

– отримання початкового доступу до інформаційної системи та даних;

– зміцнення початкових позицій;

– вилучення корпоративних даних з подальшим резервним копіюванням/відновленням/знищенням даних;

– активація вірусу-вимагача;

– здирництво, переведення в готівку вилучених коштів.

При цьому CRTF продемонстровано, де організація може вжити заходів для запобігання або припинення такої атаки. Зокрема, згідно з висновками цільової групи, пріоритетом має бути виявлення та зупинка прогресу в атаці на перших двох її етапах, де шкідлива кібератака прагне отримати доступ та зміцнити своє становище. Оскільки ці етапи схожі на етапи інших, більш типових кібератак, основна увага має бути приділена посиленню та вдосконаленню існуючих заходів щодо підвищення інформаційної безпеки й стійкості користувачів та організацій.

До викладеного слід додати, що якщо зловмиснику вдалося перейти до останніх етапів ексфільтрації даних/знищення резервних копій, активації програм-вимагачів та здирництва, то зусилля мають бути спрямовані на пом'якшення й усунення наслідків. Ці дії мають містити використання ключів дешифрування та активацію існуючих резервних копій.

Важливо відзначити, що хоча зазначені вище заходи дозволяють жертвам кібератак вилучати та/або відновлювати дані, випадки подвійного здирництва – коли зловмисник і шифрує дані, і загрожує опублікувати конфіденційну інформацію – роблять їх лише частково ефективними для повного пом'якшення атак програм-вимагачів. Все частіше зловмисники використовують ще агресивнішу тактику, наприклад, потрійне вимагання. Ці багатоаспектні загрози вимагають від компаній більш комплексного підходу до цифрової інформаційної безпеки – використання надійніших превентивних та швидких стратегій реагування.

Незважаючи на те, що агентствам CRTF рекомендується впроваджувати багаторівневі заходи безпеки для усунення інформаційних загроз, резервне копіювання є скоріш одним із найважливіших заходів безпеки. Воно є останньою «лінією оборони» від програм-вимагачів і життєво важливе для забезпечення безперервності бізнесу в досліджуваному регіоні.

Однак багато рішень для резервного копіювання не мають можливості автоматизувати тестування відновлення та переходу на інший ресурс, що робить його ручним та вкрай трудомістким процесом. Просте відновлення та завантаження сервера з резервної копії автоматично не виявляє і не усуває жодних сплячих або неактивних загроз, які все ще можуть бути присутніми. Тому при зараженні інформаційні системи часто відновлюються з нуля за допомогою ризикованого багаторівневого процесу відновлення. Це суттєво затримує безперервність бізнесу та відновлення його послуг.

У зв'язку з цим виникає потреба в ефективних інтегрованих рішеннях з акцентом на передові методи цифрової інформаційної безпеки для розширеного захисту від програм-вимагачів, а також для резервного копіювання, здатних допомогти урядам та бізнес-сектору країн островів SEA відповідати основним рекомендаціям CTRF із масштабованістю та ефективністю.

Зокрема, пропонуються наступні розширені можливості захисту від програм-вимагачів:

– наявність багатофакторної автентифікації (MFA);

– необхідність прогнозувати та усувати вразливості системи, підвищуючи стійкість в умовах ескалації інформаційних загроз;

– регулярне резервне копіювання;

– зберігання резервних копій важливих даних, програмного забезпечення та налаштувань конфігурації безпечним і стійким способом;

– відновлення важливих даних, програмного забезпечення та параметрів конфігурації із резервних копій тестувати в рамках навчань з аварійного відновлення;

– привілейовані облікові записи (за винятком акаунтів адміністратора резервного копіювання) не можуть отримувати доступ до резервних копій, що належать іншим обліковим записам, а також привілейованим обліковим записам заборонено змінювати та видаляти резервні копії протягом періоду їх зберігання;

– непривілейовані облікові записи не можуть отримувати доступ до резервних копій, що належать своїм та іншим обліковим записам, а також непривілейовані облікові записи не можуть змінювати та видаляти резервні копії.

На додаток до переліченого вище також рекомендується дотримуватися таких галузевих практик та правил для забезпечення доступності файлів резервних копій:

– створювати три копії важливих даних (одна виробнича та дві резервні копії);

– файли записувати на двох різних типах носіїв (наприклад, на диску та у хмарі/об'єкті або на стрічці);

– принаймні одна резервна копія повинна зберігатися поза місцем розташування виробничих даних;

– одна (або кілька) з цих резервних копій мають бути автономними/незмінними;

– виконувати перевірку цілісності резервних копій щодо пошкодження.

Слід звернути увагу на те, що ці правила не потребують певного типу обладнання і є досить універсальними, щоб справитися практично з будь-яким сценарієм відмови.

Таким чином, усі наведені рекомендації та стратегії в сукупності забезпечують ефективний спосіб захисту резервних копій від внутрішніх та зовнішніх загроз, а також значно скорочують терміни відновлення даних та знижують багато ризиків у разі аварій, викликаних кібератаками з боку програм-вимагачів.

Висновки та перспективи подальших розробок. Результати проведених досліджень, а також викладені у статті рекомендації з їх подальшою практичною реалізацією, зокрема щодо боротьби з програмами-вимагачами, здатні забезпечити ефективну інформаційну безпеку та надійне стійке цифрове середовище проти складних інформаційних загроз. Запропоновані в роботі керівні принципи, рекомендації та методи захисту корпоративних даних можуть бути використані як передова практика для приватних організацій та міжнародних компаній, що працюють у Сінгапурі та в інших країнах островів Південно-Східної Азії.

Додаткові рекомендації для державних і приватних організацій регіону, що містяться в статті, вказують на те, як найкраще захиститися від різних інформаційних загроз, з акцентом на висновки та рекомендації звіту цільової групи CRTF. Внаслідок цього, реалізуючи правильні можливості та практики, організації острівного регіону SEA можуть значно зміцнити свої позиції інформаційної безпеки щодо захисту даних та відновлення після збоїв, а також значно скоротити кібератаки як від внутрішніх, так і зовнішніх загроз.

У роботі також зазначено, що наявність у компанії ефективної стратегії безперервності бізнесу, включаючи стратегію посиленого резервного копіювання, дозволяє організаціям країн островів SEA мати дієвий підхід до процесу відновлення даних. Крім того, розглянуто декілька інших аспектів, які складають рішення посиленого резервного копіювання у контексті інформаційної безпеки та захисту від програм-вимагачів.

Основні напрямки подальших досліджень. Як було зазначено вище, близько 80% організацій країн островів Південно-Східної Азії вважають, що в їхньому функціонуванні існує розрив між очікуванням інтенсивності кібератак та фактичним рівнем захисту від них, де переважає перше. При цьому встановлено, що є два типи розривів, з якими стикаються компанії цього регіону:

– розрив доступності, який визначає, чи достатньо надійна корпоративна інформаційна система для забезпечення продуктивності бізнесу компанії;

– розрив захисту, який гарантує, що конфіденційні дані компанії не будуть втрачені.

У зв'язку з цим актуальними є питання подальших досліджень цих розривів, зокрема більш детальне з'ясування причин їх появи та розширення, для можливості їх усунення та забезпечення надійного, адекватного загрозам, інформаційного захисту з метою досягнення високоефективної цифрової інформаційної безпеки, покликаної забезпечити безперервність діяльності та зростання організацій досліджуваного регіону.

Іншим важливим напрямком подальших досліджень щодо програм-вимагачів може стати дослідження агресивних тактик зловмисників (потрійне вимагання тощо) для розробки більш ефективних комплексних підходів до інформаційного захисту з використанням надійних та швидких стратегій реагування на інформаційні загрози.

СПИСОК ЛІТЕРАТУРИ

1. Сергій Лубенець, Ігор Харченко, Людмила Новікова. (2021). Проблеми побудови консолідованих корпоративних стратегій управління корпоративною інформаційною безпекою в регіоні EMEA. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Міжнародні відносини. Економіка. Країнознавство. Туризм*, (14), 24-34. https://doi.org/10.26565/2310-9513-2021-14-03

2. Сергій Лубенець, Ігор Харченко, Тетяна Шедякова. (2024). Тенденції, виклики та рішення цифрової інформаційної безпеки в Центральній та Східній Європі. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Міжнародні відносини. Економіка. Країнознавство. Туризм*, (19), 16-24. https://doi.org/10.26565/2310-9513-2024-19-02

3. Шергін, С. (2024). Східноазійська інтеграція та регіональна безпека. *Проблеми всесвітньої історії*, (26), 123-136. https://doi.org/10.46869/2707-6776-2024-26-7

4. Palmer, D. (2021, June 28). Cyber insurance isn't helping with cybersecurity, and it might be making the ransomware crisis worse, say researchers [Web log post]. Retrieved from https://www.zdnet.com/article/ransomware-has-become-an-existential-threat-that-means-cyber-insurance-is-about-to-change/

5. The Cyber Security Agency of Singapore. (2025). *Advisories. Information on high-impact cybersecurity activity affecting Singapore*. Retrieved from https://www.csa.gov.sg/alerts-and-advisories/advisories/

6. Veeam Software. (2024). *2024 Ransomware Trends Report*. Retrieved from https://www.veeam.com/resources/wp-2024-ransomware-trends-report.html
7. Veeam Software. (2024). *Data Protection Trends Report 2024*. Retrieved from https://www.veeam.com/resources/wp-data-protection-trends-report-insights.html

Внесок авторів: всі автори зробили рівний внесок у цю роботу.
Конфлікт інтересів: автори повідомляють про відсутність конфлікту інтересів.

Стаття надійшла до редакції 04.03.2025
Стаття рекомендована до друку 07.04.2025

Serhii Lubenets, Candidate of Technical Sciences (Ph. D.), Associate Professor, Associate Professor of the Department of International Relations, V.N.Karazin Kharkiv National University, Svobody sq., 4, 61022, Kharkiv, Ukraine, e-mail: s.lubenec@karazin.ua, ORCID: https://orcid.org/0000-0003-1061-8763

Anna Shelestova, PhD in Social Communications, Associate Professor, Associate Professor of the Department of Economic Cybernetics and Applied Economics, V.N.Karazin Kharkiv National University, Svobody sq., 4, 61022, Kharkiv, Ukraine, e-mail: anna.shelestova@karazin.ua, ORCID: https://orcid.org/0000-0003-4866-1767, Scopus Author ID: 58277829400

Larysa Chernyshova, Candidate of Economic Sciences (Ph. D.), Associate Professor, Associate Professor of the Department of International Relations, V.N.Karazin Kharkiv National University, e-mail: lchernyshova@karazin.ua, ORCID: https://orcid.org/0000-0002-3589-9154

DIRECTIONS FOR IMPROVING THE EFFICIENCY OF DIGITAL INFORMATION SECURITY IN THE ISLAND COUNTRIES OF SOUTHEAST ASIA

The problems and directions of ensuring international digital information security in the countries of the Southeast Asian islands (SEA), in particular regarding protection against ransomware, are considered, which are based on the recommendations of the Singapore Task Force on Combating Ransomware (CRTF), as well as on analytical materials of scientists, experts and specialists specializing in the issues of regional information security and the development of appropriate tools for its provision. The subject of the study in the article is the issue of ensuring international digital information security in the countries of the SEA islands in the context of combating ransomware. The goal is to study the current state, current problems and trends of international digital information security in order to find possible directions for increasing its effectiveness in the countries of the SEA islands using the example of information threats from ransomware and methods of combating them. Tasks: to identify the main modern information threats and features of ensuring digital information security in the studied region; to investigate the trends in the development of information threats from ransomware, their impact on international business and existing recommendations for combating them; to develop guidelines, recommendations and methods of data protection that can be used by organizations and international companies of the SEA island countries to improve the effectiveness of digital information security. The general scientific method of system analysis is used to determine the current state, challenges and key trends of digital information security in the fight against ransomware, as well as to study possible directions for increasing its effectiveness. The following results were obtained: based on the processing of reports on the current state of international digital information security and ransomware, the state, features and problems of ensuring cybersecurity in the SEA island countries were determined. Recommendations for combating ransomware and methods of protecting against them were provided based on the conclusions of leading companies working in the field of information security, as well as taking into account the CRTF guidelines. Possible directions and prospects for further scientific research on the issue under consideration were identified. Conclusions: The research findings, as well as the implementation of the recommendations set out in the article, in particular on combating ransomware, contribute to ensuring effective digital information security and the formation of a reliable, resilient digital environment against complex information threats. The guidelines, recommendations and methods for protecting corporate data proposed in the work can be used as best practices for private organizations and international companies in the SEA island countries. Additional recommendations for public and private organizations in the region indicate how best to protect themselves from various information threats, with an emphasis on the conclusions and recommendations of the CRTF task force. As a result, by implementing effective measures and practices, organizations in the island region can significantly strengthen their information security positions in terms of data protection and disaster recovery, as well as significantly reduce cyberattacks from both internal and external threats.

Keywords: *digitalization of the world economy, digital information security, ransomware, backup, Southeast Asian island countries.*

REFERENCES

1. Serhii Lubenets, Igor Harchenko, & Ljudmyla Novikova. (2021). Problems of building consolidated corporation strategies for corporate information security management in the EMEA region. *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism*, (14), 24-34. https://doi.org/10.26565/2310-9513-2021-14-03 (in Ukrainian)

2. Serhii Lubenets, Igor Harchenko, & Tetiana Shediakova. (2024). Trends, challenges and solutions of digital information security in Central and Eastern Europe. *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism*, (19), 16-24. https://doi.org/10.26565/2310-9513-2024-19-02 (in Ukrainian)

3. Sherhin, S. (2024). East Asia Integration and Regional Security. *Problems of World History*, (26), 123-136. https://doi.org/10.46869/2707-6776-2024-26-7 (in Ukrainian)

4. Palmer, D. (2021, June 28). Cyber insurance isn't helping with cybersecurity, and it might be making the ransomware crisis worse, say researchers [Web log post]. Retrieved from https://www.zdnet.com/article/ransomware-has-become-an-existential-threat-that-means-cyber-insurance-is-about-to-change/

5. The Cyber Security Agency of Singapore. (2025). *Advisories. Information on high-impact cybersecurity activity affecting Singapore*. Retrieved from https://www.csa.gov.sg/alerts-and-advisories/advisories/

6. Veeam Software. (2024). *2024 Ransomware Trends Report*. Retrieved from https://www.veeam.com/resources/wp-2024-ransomware-trends-report.html

7. Veeam Software. (2024). *Data Protection Trends Report 2024*. Retrieved from https://www.veeam.com/resources/wp-data-protection-trends-report-insights.html

Authors Contribution: All authors have contributed equally to this work.
Conflict of Interest: The authors declare no conflict of interest.

The article was received by the editors 04.03.2025
The article is recommended for printing 07.04.2025