DOI: 10.26565/2310-9513-2023-17-04
УДК 65.012.8(613)

# АКТУАЛЬНІ ПРОБЛЕМИ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**Лубенець Сергій Васильович**
кандидат технічних наук, доцент
кафедра міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 6, м. Харків, 61022
E-mail: s.lubenec@karazin.ua
Контактний тел.: 097-361-55-09
ORCID: https://orcid.org/0000-0003-1061-8763

**Харченко Ігор Михайлович**
кандидат технічних наук, доцент
кафедра міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет імені В.Н. Каразіна
майдан Свободи, 6, м. Харків, 61022
E-mail: kharchenko@karazin.ua
Контактний тел.: 067-576-63-21
ORCID: https://orcid.org/0000-0002-1372-0408

**Павленко Євген Петрович**
кандидат технічних наук, доцент
кафедра спеціалізованих комп'ютерних систем
Український державний університет залізничного транспорту
площа Фейєрбаха, 7, Харків, 61050
E-mail: evgenijpavlenko821@gmail.com
Контактний тел.: 098-817-60-29
ORCID: https://orcid.org/0000-0003-0699-6294

Розглянуто проблеми та напрями забезпечення ефективної міжнародної інформаційної безпеки, які ґрунтується на аналізі поточного стану світової кіберзлочинності, існуючих основних напрямків глобальних кібератак і вироблення можливих методів та засобів протидії їм, з використанням актуальних дослідницьких та звітних матеріалів профільних міжнародних компаній, що спеціалізуються на проблематиці міжнародної інформаційної безпеки та розробці відповідних комплексних інструментів її забезпечення. Предметом дослідження в статті є питання забезпечення міжнародної інформаційної безпеки, кіберзахисту та боротьби з кіберзлочинністю. Мета – полягає в аналізі сучасного стану та актуальних проблем міжнародної інформаційної безпеки для забезпечення ефективного управління нею на державному та корпоративному рівнях у різних країнах та регіонах світу. Завдання: обробка й аналіз останньої звітності та висновків, що стосуються сучасного стану міжнародної інформаційної безпеки в різних країнах і регіонах світу; дослідження основних інформаційних загроз, їх типів, актуальних напрямків та джерел; аналіз існуючих та перспективних напрямків і засобів протидії інформаційним загрозам для забезпечення ефективної міжнародної інформаційної безпеки. Використовується загальнонауковий метод системного аналізу – для визначення існуючих інформаційних і кіберзагроз та аналізу їх особливостей, а також для дослідження існуючих та перспективних напрямів боротьби з ними. Отримано такі результати: на основі результатів обробки звітності та висновків Microsoft Digital Defense Report, що стосуються сучасного стану міжнародної інформаційної безпеки в різних країнах та регіонах світу, досліджено основні інформаційні загрози, їх типи, актуальні напрямки, цілі та джерела. Визначено актуальні питання міжнародної кіберзлочинності, основаної на використанні програми вимагачів, а також основні цільові галузі відповідних кібератак. Проаналізовано існуючі та перспективні напрямки і засоби протидії інформаційним загрозам для забезпечення ефективної міжнародної інформаційної безпеки. Визначено основні тенденції щодо підвищення рівня кіберзахисту та інформаційної безпеки у світі. Висновки: показано, що в міру збільшення кількості, витонченості та впливу сітьових загроз, для протидії їм міжнародні організації, компанії та окремі особи повинні вжити заходи для зміцнення так званої першої лінії захисту, зокрема, використовувати строгу багатофакторну автентифікацію. Визначено, що на даний момент існують три основні тенденції щодо підвищення рівня кіберзахисту та інформаційної безпеки у світі: здійснення безпрецедентних кроків провідними країнами світу для вирішення проблеми кібербезпеки з використанням вже існуючих законів та повноважень; прийняття і введення урядами по всьому світу нових законів, які вимагають від організацій обов'язкової звітності щодо виявлення кібератак; добровільне інформування урядами та міжнародними компаніями громадськість, коли вони стають жертвами атак. Тенденцією також є подальше зростання кількості та масштабів кібератак для будь-яких політичних цілей, чи то шпигунства, підриву чи руйнації. При цьому очікується, що все більше країн приєднуватимуться до списку тих, хто бере участь у наступальних кіберопераціях, і що ці операції стануть більш зухвалими, наполегливими та руйнівними, з більш серйозними наслідками. Одночасно, для протидії цьому, урядами та міжнародними компаніями прикладається все більше зусиль щодо протидії вказаним інформаційним небезпекам.

**Ключові слова:** *інформаційна безпека, кібербезпека, кіберзахист, кіберзлочинність, програми-вимагачі.*

**Як цитувати:** Лубенець С.В., Харченко І.М., Павленко Є.П. Актуальні проблеми міжнародної інформаційної безпеки. *Вісник ХНУ імені В. Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм»*. 2023. № 17. С. 42-48. DOI: https://doi.org/10.26565/2310-9513-2023-17-04

**In cites:** Lubenets S., Harchenko I., & Pavlenko Y. (2023) Current problems of international information security. *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism*, (17), 42-48. https://doi.org/10.26565/2310-9513-2023-17-04 (in Ukrainian)

**Постановка проблеми.** На даний час уряди країн світу, міжнародні корпорації та неурядові організації стикаються з серйозними ризиками і проблемами, що стосуються інформаційної безпеки. Однак без належного глибокого аналізу сучасного стану міжнародної інформаційної безпеки, без виявлення основних інформаційних загроз та визначення їх ландшафту, без оцінки тенденцій у діяльності держав та організацій, аналізу кіберзлочинності, безпеки логістики, гібридних дій та дезінформації, часто досить складно протистояти даним викликам. У зв'язку з цим актуальним є аналіз поточного стану світової кіберзлочинності, існуючих основних напрямків глобальних кібератак і вироблення можливих напрямків та засобів протидії їм, що сприятиме ефективному вирішенню задач міжнародної інформаційної безпеки.

**Аналіз останніх досліджень і публікацій.** Актуальні проблеми міжнародної інформаційної безпеки розглядалися в ряді робіт дослідників, аналітиків та профільних фахівців. Зокрема, в роботі [1] розглянуто питання підвищення ефективності корпоративної інформаційної безпеки організацій шляхом розробки універсальної консолідованої стратегії взаємодії служб IT та інформаційної безпеки, яка ґрунтується на вивченні та глибокому аналізі статистичних даних щодо існуючої ситуації з такою взаємодією в різних компаніях різних галузей і регіонів світу, зокрема на прикладі регіону EMEA. У ряді робіт аналізуються останні гучні конкретні кібератаки, що продовжують і надалі становити суттєву загрозу інформаційній безпеці в усьому світі. Так, в роботі [6] розкриті та задокументовані особливості відомої китайської кібератаки «Hafnium», спрямованої на локальні сервери Exchange. У статті [2] авторами побудована теоретична модель управління інформаційною безпекою на основі стратегічної узгодженості, з урахуванням основних факторів ефективного управління IT безпекою. При цьому розглядаються проблеми узгодженості стратегічних цінностей компанії для ефективного управління інформаційною безпекою.

Однак важливими є питання ефективного забезпечення міжнародної інформаційної безпеки, яке б ґрунтувалося не лише на висновках окремих дослідників, аналітиків, профільних фахівців чи досвіді організацій за певний період часу, але й на вивченні та глибокому аналізі останніх інтегрованих матеріалів, що стосуються сучасних глобальних та різносторонніх питань міжнародної інформаційної безпеки. Зокрема, на найбільш актуальних дослідницьких та звітних матеріалах профільних міжнародних компаній, які спеціалізуються на проблематиці міжнародної інформаційної безпеки та розробці відповідних комплексних інструментів її забезпечення.

**Мета статті, завдання дослідження.** Метою роботи є аналіз сучасного стану та актуальних проблем міжнародної інформаційної безпеки для забезпечення ефективного управління нею на державному та корпоративному рівнях у різних країнах та регіонах світу.

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

- обробити і проаналізувати останню звітність та висновки, що стосуються сучасного стану міжнародної інформаційної безпеки в різних країнах і регіонах світу;
- дослідити основні інформаційні загрози, їх типи, актуальні напрямки та джерела;
- проаналізувати існуючі та перспективні напрямки і засоби протидії інформаційним загрозам для забезпечення ефективної міжнародної інформаційної безпеки.

Для вирішення поставлених завдань у даній роботі був проведений аналіз опублікованих результатів та висновків, що стосуються сучасного стану міжнародної інформаційної безпеки, викладених у щорічному звіті Microsoft Digital Defense Report [5], який охоплює період протягом 2022 року.

**Основні результати дослідження.** За даними звітності Microsoft, за останні півтора року близько 60% усіх кібератак, що спостерігаються з національних держав, було здійснено з Російської Федерації. При цьому атаки з боку російських національних державних суб'єктів стають дедалі ефективнішими: рівень успішних компрометацій 2021 року становив 21%, а 2022 року – 32%. Російські національні державні суб'єкти дедалі частіше націлені на урядові агенції для збору розвідувальних даних, які зросли з 3% від усіх цілей у 2021 році до 53%. В основному це агентства, які займаються зовнішньою політикою, національною безпекою чи обороною.

До першої трійки країн, на які націлені російські кібератаки, увійшли США, Україна та Великобританія. Що стосується України, з початком повномасштабного воєнного вторгнення РФ їх кібератаки здійснюються практично на всі ті ж об'єкти інфраструктури держави, що й ракетні атаки: військові, енергетичні, логістичні, промислові тощо. За два місяці до повномасштабного вторгнення уряд США направив в Україну групу кіберспеціалістів з Агенції нацбезпеки США для зміцнення кіберзахисту нашої країни. Перебування експертів на місці позитивно вплинуло на рівень кіберзахисту, при цьому успіш-

ний захист Україною більшості своєї кіберінфраструктури від досвідчених російських хакерів є одним із ключових елементів успіху на полі бою.

США планує й надалі допомагати українським військовим у кібербезпеці та кібероборони. Так, Міністерство оборони України і Фонд цивільних досліджень та розвитку США (CRDF Global) домовились про взаємодію у сфері кібербезпеки та підтримки реалізації заходів кібероборони. Співпраця передбачає обмін ідеями, інформацією та досвідом у сфері кібербезпеки, а також сприяння у вдосконаленні освітніх, науково-технічних і технологічних можливостей Міністерства оборони України та ЗСУ.

Однак Росія – не єдина держава, яка розвиває свої підходи в галузі кіберзлочинності, а шпигунство – не єдина мета атак на національні держави протягом досліджуваного періоду. Після цієї країни найбільша кількість атак, які спостерігалися в даний період з боку країн, що фігурують у звітності Microsoft, була з боку Північної Кореї, Ірану та Китаю. Південна Корея, Туреччина та В'єтнам також були активними, але створювали набагато меншу кількість кібератак.

Хоча шпигунство є найбільш поширеною метою атак на національні держави, деякі дії зловмисників розкривають інші цілі, зокрема:

– Іран, який у чотири рази збільшив націлювання на Ізраїль за останні два роки, виконує руйнівні атаки на тлі загострення напруженості у відносинах між двома країнами;

– Північна Корея, яка націлена на криптовалютні компанії з метою отримання прибутку, оскільки її економіка була підірвана санкціями та Covid 19;

– 21% атак, які спостерігалися серед суб'єктів національних держав, були націлені на споживачів, а 79% атак – на підприємства, причому найбільш цільовими секторами були уряд (48%), науково-виробничі об'єднання та аналітичні центри (31%), освіта (3%), міжурядові організації (3%), IT-сфера (2%), енергетика (1%) та медіа (1%).

У цьому контексті окремо слід виділити Китай. Хоча ця країна не вирізняється унікальністю у своїй меті збору інформації, слід зазначити, що кілька китайських суб'єктів використовували низку раніше не ідентифікованих вразливостей. Так, Microsoft виявила та оприлюднила застосований китайськими хакерами так званий Pulse Secure VPN Zero-Day [3].

Китай також використовує свої розвіддані для різних цілей. Наприклад, китайський суб'єкт Chromium націлювався на організації в Індії, Малайзії, Монголії, Пакистані та Таїланді, щоб зібрати соціальну, економічну та політичну інформацію про ці сусідні країни. Інший китайський суб'єкт Nickel націлювався на урядові міністерства закордонних справ Центральної та Південної Америки і Європи. При цьому очікується, що в міру зміни впливу Китаю у зв'язку з ініціативою країни «Один пояс, один шлях» ці учасники продовжуватимуть використовувати збір даних кіберрозвідки для аналізу інвестицій, для переговорів та впливу.

Зрештою, слід зазначити, що китайські хакери досить наполегливі: навіть після того, як у Microsoft розкрили спроби Китаю провести збір розвідданих щодо осіб, причетних до виборів у США в 2020 році, його суб'єкт Zirconium продовжив свою діяльність у день цих виборів.

Загалом за останні три роки Microsoft близько 20500 разів повідомив своїх клієнтів про спроби різних державних суб'єктів з різних країн світу зламати їхні системи. При цьому слід розуміти, що Microsoft не відслідковує кожної глобальної кібератаки. Наприклад, у них обмежена видимість атак, націлених на локальні системи, якими організації управляють самі. Те ж саме стосується кібератаки Exchange Server [6] на початку 2021 року, а також атак, націлених на клієнтів інших постачальників технологій.

У Microsoft вважають, що спільне використання наявних у них даних про ці загрози корисне для клієнтів, політиків та більш широкої міжнародної спільноти фахівців з безпеки, і вони запрошують інших ділитися такими ж даними. При цьому позитивним є те, що їхня видимість міжнародних кіберзагроз і здатність допомогти зупинити ці загрози продовжуватимуть зростати в міру того, як все більше урядів та організацій у світі переходять на хмарні технології.

Ще однією серйозною і зростаючою світовою проблемою, про що свідчить звіт Microsoft Digital Defense, є кіберзлочинність, особливо програми вимагачі. Але в той час, як суб'єкти кібератак на національні держави здебільшого націлені на жертв з метою отримання корисної інформації, кіберзлочинці націлені на жертв для отримання грошей. Як результат, цілі кіберзлочинних атак часто мають інший профіль, а самі атаки націлені на критично важливу інфраструктуру, часто з використанням програм вимагачів. При цьому група Microsoft з виявлення та реагування (DART) [5] виділяє п'ять основних галузей, на які були націлені кібератаки із застосуванням програм вимагачів (рис. 1): роздрібна торгівля (13%), страхування та фінансові послуги (12%), виробництво та сільське господарство (12%), уряд (11%) та охорона здоров'я (9%). При цьому Сполучені Штати є найбільш цільовою країною, на яку припадає більш ніж утричі більше атак з використанням програм вимагачів, ніж наступна за чисельністю цільова країна – Китай.

Взагалі, за останні два роки економіка «кіберзлочинності як послуги» перетворилася із зароджуваної, але швидкозростаючої галузі на зрілу злочинну діяльність. Сьогодні практично будь-хто, незалежно від технічних знань, може отримати доступ до надійного онлайн ринку, щоб придбати низку послуг, необхідних для проведення кібератак з будь-якою метою. При цьому торговий майданчик складається із трьох компонентів.


*Рис. 1. Галузі, на які націлені кібератаки із застосуванням програм вимагачів**

**Розроблено авторами за матеріалами: [5]*

*Fig. 1. Industries targeted by cyberattacks using ransomware**

**Developed by the authors based on the materials: [5]*

По перше, зі зростанням попиту злочинці дедалі більше зосереджуються на диференційованих готових наборах інформаційного зараження і розширюють використання автоматизації, знижуючи свої витрати і збільшуючи масштаби. Існують комплекти, які продаються лише за кілька десятків доларів. По друге, окремі постачальники надають скомпрометовані облікові дані, необхідні для доступу до особистих облікових даних потенційних жертв кіберзлочинців та розгортання комплектів. Спостерігаються випадки, коли облікові дані продаються від 1 до 50 доларів кожна, залежно від цінності мети.

По третє, послуги умовного депонування криптовалюти є посередниками між покупцями і продавцями, щоб гарантувати, що комплекти та облікові дані працюють як слід. Останнім часом почали виявлятися складні комплекти, які не лише надають злочинцеві дані про жертву, який придбав і розгорнув комплект, але й таємно надають дані організації, яка створила комплект.

Програми вимагачі залишаються однією з найбільших загроз кіберзлочинності, і останнім часом вони продовжують розвиватися, стаючи все більш руйнівними. Замість того, щоб зосереджуватися на автоматичних атаках, які покладаються на кількість і характеризуються низьким рівнем вимог для отримання прибутку, програма вимагач, керована людиною, використовує інформацію, отриману з онлайн джерел, краде і вивчає фінансові та страхові документи жертви й досліджує скомпрометовані мережі, щоб вибрати цілі та встановити значно вищі вимоги викупу.

Проведені в роботі дослідження показали, що в міру збільшення кількості, витонченості та впливу сітьових загроз, для протидії їм міжнародні організації, компанії та окремі особи повинні вжити заходи для зміцнення так званої першої лінії захисту. Забезпечення фундаментальної гігієни кібербезпеки – як і елементарних норм гігієни у побуті – є основними кроками, які повинні бути зроблені.

Однак, лише не більше 20% клієнтів Microsoft використовують функції строгої автентифікації, наприклад, таку як багатофакторна автентифікація (MFA). Хоча Microsoft пропонує це безкоштовно, і міжнародні організації можуть розміщувати такий захист для своїх користувачів за замовчуванням. Фактично, якби організації просто застосовували MFA, використовували захист від шкідливих програм і постійно оновлювали свої системи, вони були б захищені від більш ніж 99% кібератак, які спостерігаються сьогодні.

Звичайно, технологічні компанії, що пропонують ті чи інші засоби та інструменти інформаційної безпеки, можуть відіграти важливу роль у розробці

безпечного програмного забезпечення, передових продуктів та послуг кібербезпеки для тих клієнтів, які хочуть їх розгорнути, а також у виявленні та зупиненні інформаційних загроз. Проте базові кроки для самозахисту, що вживаються міжнародними організаціями, можуть забезпечити більше, ніж найвитонченіші заходи, які технологічні компанії та уряди могли б вжити для їхнього захисту. Позитивним є те, що за останні два роки спостерігається зростання використання строгої автентифікації на 220%, оскільки міжнародні компанії замислилися над підвищенням рівня безпеки у віддаленому робочому середовищі. Однак у цьому плані ще доведеться пройти довгий шлях, який буде вимагати додаткових досліджень та глибокого аналізу. Зокрема, ефективним рішенням може стати підвищення кваліфікації професіоналів у галузі кібербезпеки, які зможуть допомогти міжнародним організаціям будь-якого типу залишатись у безпеці.

Висновки та перспективи подальших розробок. Проведені дослідження показали, що на даний момент існують три основні тенденції, які додатково вселяють надію на підвищення рівня кіберзахисту та інформаційної безпеки у світі.

*По перше*, уряд США зробив безпрецедентні кроки для вирішення проблеми кібербезпеки, використовуючи вже існуючі закони та повноваження. Зокрема, у 2021 році було опубліковано Виконавче розпорядження [4], спрямоване на те, щоб забезпечити федеральному уряду США та тим, з ким він працює, більш високий рівень інформаційної безпеки. Крім того, керівництвом Білого дому у партнерстві з приватними організаціями розроблено новий стандарт співпраці у разі виникнення кіберінцидентів.

*По друге,* уряди по всьому світу приймають і вводять нові закони, які вимагають від організацій обов'язкової звітності щодо виявлення кібератак, щоб відповідні державні органи розуміли масштаб проблеми та могли розслідувати інциденти, використовуючи свої ресурси.

*По третє*, уряди і компанії добровільно інформують громадськість, коли стають жертвами атак. Така прозорість допомагає кожному краще зрозуміти проблему та сприяє більш активній взаємодії з боку урядів та служб швидкого реагування.

Щодо *подальших тенденцій*, слід констатувати, що національні держави все частіше використовують і продовжуватимуть використовувати кібератаки для будь яких своїх політичних цілей, чи то шпигунства, підриву чи руйнації. Очікується, що все більше країн приєднуватимуться до списку тих, хто бере участь у наступальних кібероперація х, і що ці операції стануть більш зухвалими, наполегливими та руйнівними, з більш серйозними наслідками. При цьому ринок кіберзлочинності продовжуватиме ставати все більш витонченим і спеціалізованим, якщо у світі не вживатимуть заходів, щоб зупинити їх. У даний час урядами та компаніями прикладається більше, ніж будь-коли, зусиль щодо протидії цим небезпекам. Однак потрібно прагнути до того, щоб вони залишалися в центрі уваги національних та міжнародних порядків найближчими роками.

Таким чином, висновки даної статті, засновані на аналізі проблематики інформаційної безпеки на основі щорічної звітності Microsoft Digital Defense Report щодо актуального стану у світі кіберзагроз та кіберзлочинності, покликані сприяти підвищенню ефективності управління й пошуку дієвих інструменті та практичних підходів у забезпеченні міжнародної інформаційної безпеки.

*Основними напрямками подальших досліджень* розглянутої проблематики можуть бути розробки більш детальних, конкретних та універсальних підходів і рекомендацій, що стосуються:

– попередження кібератак та захисту від них;

– розробки ефективних підходів та інструментів для боротьби з кіберзлочинністю;

– питань неперервного підвищення кваліфікації та обміну досвідом професіоналів у галузі міжнародної інформаційної безпеки;

– ефективного поєднання зусиль урядів провідних країн світу, міжнародних організацій та транснаціональних компаній у забезпеченні міжнародної інформаційної безпеки.

## СПИСОК ЛІТЕРАТУРИ

1. Лубенець С.В., Харченко І.М., Новікова Л.В. Проблеми побудови консолідованих стратегій управління корпоративною інформаційною безпекою в регіоні ЕМЕА. Вісник Харківського національного університету імені В.Н. Каразіна. Сер. «Міжнародні відносини. Економіка. Країнознавство. Туризм». Вип. 14. С. 24 34. https://doi.org/10.26565/2310-9513-2021-14-03

2. Cindy Zhiling Tu, Yufei Yuan, Norm Archer, Catherine E. Connelly. Strategic value alignment for information security management: a critical success factor analysis. Information and Computer Security. 2018. Vol. 26, № 2. P. 150-170.

3. Dan Perez, Sarah Jones, Greg Wood, Stephen Eckels. Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day : web site. URL: https://www.mandiant.com/resources/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day (date of the application: 13.02.2023).

4. Joseph R., Biden Jr. Executive Order on Improving the Nation's Cybersecurity : web site. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (date of the application: 13.02.2023).
5. Microsoft Digital Defense Report 2022 : web site. URL: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1 (date of the application: 13.02.2023).
6. Tom Burt. New nation-state cyberattacks : web site. URL: https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/ (date of the application: 13.02.2023).

*Стаття надійшла до редакції 13.02.2023*
*Стаття рекомендована до друку 16.03.2023*

# CURRENT PROBLEMS OF INTERNATIONAL INFORMATION SECURITY

**Serhii Lubenets**, Ph.D (Technical Sciences), Associate Professor, Department of International Relations, International Information and Security, V.N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, Ukraine, 61022, e-mail: s.lubenec@karazin.ua, ORCID: https://orcid.org/0000-0003-1061-8763

**Igor Harchenko,** Ph.D (Technical Sciences), Associate Professor, Department of International Relations, International Information and Security, V.N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, Ukraine, 61022, e-mail: kharchenko@karazin.ua, ORCID: https://orcid.org/0000-0002-1372-0408

**Yevhen Pavlenko**, Ph.D (Technical Sciences), Associate Professor, Department of the Specialized Computer Systems, Ukrainian State University of Railway Transport, Feuerbach Square, 7, Kharkiv city, Ukraine, 61050, e-mail: evgenijpavlenko821@gmail.com, ORCID: https://orcid.org/0000-0003-0699-6294

The problems and areas of ensuring effective international information security are considered, which are based on the analysis of the current state of global cybercrime, the existing main directions of global cyberattacks and the development of possible methods and means of countering them, with the use of current research and reporting materials of specialized international companies specializing in the problems of international information security security and the development of appropriate comprehensive tools for its provision. The subject of research in the article is the issue of ensuring international information security, cyber protection and combating cybercrime. The goal is to analyze the current state and current problems of international information security to ensure its effective management at the state and corporate levels in various countries and regions of the world. Tasks: processing and analysis of the latest reports and conclusions concerning the current state of international information security in various countries and regions of the world; research of the main information threats, their types, current directions and sources; analysis of existing and promising directions and means of countering information threats to ensure effective international information security. The general scientific method of system analysis is used - to identify existing information and cyber threats and analyze their features, as well as to research existing and promising ways of combating them. The following results were obtained: based on the results of processing reports and the conclusions of the Microsoft Digital Defense Report concerning the current state of international information security in various countries and regions of the world, the main information threats, their types, current directions, goals and sources were investigated. Current issues of international cybercrime based on the use of ransomware, as well as the main target areas of relevant cyberattacks, have been determined. Existing and promising directions and means of countering information threats to ensure effective international information security are analyzed. The main trends in increasing the level of cyber protection and information security in the world have been determined. Conclusions: It is shown that as the number, sophistication and impact of online threats increase, to counter them, international organizations, companies and individuals must take measures to strengthen the so-called first line of defense, in particular, use strong multi-factor authentication. It was determined that at the moment there are three main trends in increasing the level of cyber protection and information security in the world: the implementation of unprecedented steps by the leading countries of the world to solve the problem of cyber security using already existing laws and powers; the adoption and introduction by governments around the world of new laws that require organizations to report on the detection of cyber attacks; voluntary notification by governments and international companies to the public when they become victims of attacks. The trend is also a further increase in the number and scope of cyber-attacks for any political purpose, be it espionage, subversion or destruction. At the same time, it is expected that more countries will join the list of those participating in offensive cyber operations, and that these operations will become more daring, persistent and disruptive, with more serious consequences. At the same time, in order to counter this, governments and international companies are making more and more efforts to counter these informational dangers.

**Keywords**: *information security, cyber security, cyber protection, cyber crime, ransomware.*

## REFERENCES

1. Lubenets S., Harchenko I., Novikova L. (2021) Problemy pobudovy konsolidovanyh strategij upravlinnja korporatyvnoju informacijnoju bezpekoju v regioni EMEA [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, vol. 14, pp. 24 34. (in Ukrainian). https://doi.org/10.26565/2310-9513-2021-14-03

2. Cindy Zhiling Tu, Yufei Yuan, Norm Archer, Catherine E. Connelly (2018) Strategic value alignment for information security management: a critical success factor analysis. Information and Computer Security, vol. 26, no. 2. pp. 150-170.

3. Dan Perez, Sarah Jones, Greg Wood, Stephen Eckels. Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day. Available at: https://www.mandiant.com/resources/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day (accessed 13.02.2023).

4. Joseph R., Biden Jr. Executive Order on Improving the Nation's Cybersecurity. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed 13.02.2023).

5. Microsoft Digital Defense Report 2022. Available at: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1 (accessed 13.02.2023).

6. Tom Burt. New nation-state cyberattacks. Available at: https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/ (accessed 13.02.2023).

*The article was received by the editors 13.02.2023*
*The article is recommended for printing 16.03.2023*