КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4(20), 2023
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2023.20.9399
УДК 004.056

**Черниш Юлія Олександрівна**
Старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-6626-5656
*yuliia.chernysch@viti.edu.ua*

**Мальцева Ірина Робертівна**
Старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-6073-4637
*iryna.maltseva@viti.edu.ua*

**Штонда Роман Михайлович**
Начальник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-5986-0847
*roman.shtonda@viti.edu.ua*

**Кузнецов Віктор Миколайович**
Слухач
Національний університет оборони України імені Івана Черняховського, Київ, Україна
ORCID ID: 0009-0009-6824-9308
*vikvik3@i.ua*

**Гоменюк Віктор Миколайович**
Слухач
Національний університет оборони України імені Івана Черняховського, Київ, Україна
ORCID ID: 0009-0007-2286-6832
*gomenuk.vik@gmail.com*

**Підкова Олександр Іванович**
Слухач
Національний університет оборони України імені Івана Черняховського, Київ, Україна
ORCID ID: 0009-0009-0387-7100
*pidkovaoleksandr2@gmail.com*

# ПІДХОДИ ЩОДО ДОСЯГНЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЯХ РІЗНИХ СФЕР ДІЯЛЬНОСТІ ПІД ЧАС НАДЗВИЧАЙНОГО (ВОЄННОГО) СТАНУ

**Анотація.** Кількість випадків кібератак зростає. У сучасних організаціях різних сфер діяльності вся інформація, все частіше, зберігається в цифровій або електронній формі, будь то на окремих комп'ютерах чи пристроях зберігання даних, на серверах організацій чи службах зберігання даних, або за допомогою веб-«хмарних» технологій.

Метою даної статті є розуміння захисту інформації та аналіз вирішення проблеми, а також виявлення загроз, які можуть серйозно вплинути на організації будь-якого розміру.

У даній статті досліджені найпопулярніші методи щодо захисту інформації під час війни. Розберемося детально, чим саме, той чи інший метод, зможе вам допомогти.

Зараз усі підприємства мають важливу для бізнесу інформацію та дані, що зберігаються в електронному вигляді, тому підтримка безпеки даних є надзвичайно важливою. Зростання використання веб-сервісів, таких як хмара, створює додаткові проблеми цифрового захисту.

Недостатній кіберзахист може поставити під загрозу системи та служби, завдати шкоди людям і, в крайніх випадках, поставити під загрозу життя.

Хоча організація не може гарантувати стовідсоткову безпеку своїх цифрових активів, у цій статті наведено поради щодо того, як оцінити загрози системам і розробити режим безпеки, який гарантує постійний захист конфіденційних цифрових активів.

**Ключові слова:** кібератаки, кіберзагрози, кіберзахист, кіберпростір

## ВСТУП

У сучасному гіперз'єднаному світі організації мають усвідомлювати, що для забезпечення захисту від різного виду кіберзагроз, потрібна співпраця на багатьох рівнях. Потрібно ширше впроваджувати та використовувати безпечні технології та процедури.

Оскільки конфлікт в Україні вступає в черговий важкий період, організації України та всього світу в цілому, стикаються з підвищеною загрозою кібератак. Спонсоровані державою агресором, російські суб'єкти поки, що не здійснювали явних нападів на установи за межами України, але в минулому продемонстрували спроможність і готовність атакувати державну та приватну інфраструктуру в сусідніх державах. В Україні ж було скоєну незліченну кількість спроб атакувати ті чи інші об'єкти, установи, ресурси, і багато атак, все ж були успішними. Незліченна кількість кіберзлочинців та інших опортуністів намагатимуться й надалі використовувати цю складну ситуацію для здійснення зловмисних атак заради власної матеріальної вигоди.

**Постановка проблеми**. Кількість випадків кібератак зростає. У сучасних організаціях різних сфер діяльності вся інформація, все частіше, зберігається в цифровій або електронній формі, будь то на окремих комп'ютерах чи пристроях зберігання даних, на серверах організацій чи службах зберігання даних, або за допомогою веб-«хмарних» технологій.

**Аналіз останніх досліджень і публікацій.** Дані зараз здебільшого зберігаються в електронному або цифровому форматі, тому найбільше уваги приділяється кібербезпеці. Так звані кібератаки від комп'ютерних вірусів і хакерства стали серйозною загрозою для комп'ютерних систем і мереж у всьому світі. Сучасні організації повинні надсерйозно сприймати ці загрози та інвестувати час і ресурси, необхідні для захисту своїх цифрових активів, в кібербезпеку, або ризикувати потенційно шкідливими системними зломами та збоями.

**Мета статті.** Метою даної статті є розуміння захисту інформації, та аналіз вирішення проблеми, а також виявлення загроз, які можуть серйозно вплинути на організації будь-якого розміру.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для нашої держави ризик кібератак точно зростатиме, оскільки санкції Заходу, які президент росії назвав «схожими на оголошення війни», й надалі будуть сильно шкодити російській економіці. З іншого боку, вони мають значний потенціал для того, щоб завдати шкоди майже в більшості сфер.

Зловмисне програмне забезпечення NotPetya, яке Росія запустила в Україні в 2017 році, поширилося серед великих організацій по всьому світу, завдавши збитків приблизно на 10 мільярдів доларів [1]. Корпораціям, які вирішили скоротити чи призупинити діяльність у росії, у відповідь на вторгнення, потрібно добре усвідомлювати те, що кіберризики дуже зросли.

Уряди та організації повинні бути пильними, щоб протистояти цим загрозам постійно посилювати свої протоколи кібербезпеки та захист інформації. На щастя, організації не починають з нуля. Останніми роками вони інвестували значні кошти в кібернетифікацію та, адаптуючись до віддаленої роботи під час пандемії, переглянули засоби контролю безпеки. Ці зусилля були підкріплені більш пильним регулятивним

контролем у зв'язку з нещодавніми атаками та новими вимогами страховиків, які прагнуть запобігти атакам програм-вимагачів. В 2020 році США виділили для України 38 млн на посилення кібербезпеки, що стало не менш потужним кроком для підтримки в майбутньому [2]. Тепер організаціям необхідно розвивати цей прогрес і ширше впроваджувати безпечні технології та процедури.

Можемо виділити основні кроки для досягнення результатів, а саме:

**1. Співпрацюйте з аналогами, постачальниками та конкурентами**

У сучасному гіперз'єднаному світі жодна організація не може сподіватися знайти потрібні рішення, ховаючись на самоті за власними стінами. Безпека в цифрах. Одна з атак, яку уряд України приписує російським спецслужбам, скомпрометувала комп'ютерні мережі багатьох державних установ в Україні та Європі та десятків організацій [3]. Ось чому організаціям необхідно співпрацювати з аналогами, постачальниками та конкурентами. Приватному сектору необхідно підтримувати насичений, відповідний та активний діалог із державним сектором, щоб обмінюватися інформацією про загрози, вразливі місця та підозрілу поведінку, формулювати рішучі практичні плани протидії будь-якій атаці.

Закон України «Про основні засади забезпечення кібербезпеки України» (зі змінами) від 28 липня 2022 року, має на меті збільшення обміну розвідданими в критично важливих секторах інфраструктури України. Він вимагає спільних та активних зусиль для протидії агресії у кіберпросторі [4].

Також сектор фінансових послуг створив культуру співпраці через Центр обміну інформацією та аналізу фінансових послуг. Ця співпраця посилилася після того, як Сполучені Штати, Європейський Союз та інші уряди оголосили про широкі економічні та фінансові санкції проти росії, включаючи заморожування значної частини валютних резервів країни та видалення великих російських банків із платіжної мережі SWIFT [5]. Банки визнають, що в нинішніх умовах кіберзахист є важливим для підтримки стабільності фінансової системи. Інші галузі, багато з яких мають власні інформаційно-аналітичні центри, повинні наслідувати цей приклад.

**2. Використовуйте всі інструменти в арсеналі кіберзахисту**

В останні роки організації інвестували значні кошти в кібербезпеку, і знову фінансові установи були в авангарді. За останні п'ять років витрати на інформаційну безпеку в банківському секторі України зросли в середньому на понад 15% у рік. Під час пандемії організації переглянули та оновили засоби контролю безпеки, щоб враховувати різні шаблони доступу до мережі за допомогою інфраструктури віртуального робочого столу, розширеної багатофакторної автентифікації та можливостей запобігання втраті даних. Компанії з управління активами стали ініціаторами впровадження біометричних методів доступу, що значно знижує ризик злому через зламані паролі.

Організації повинні зосередити свої зусилля на максимальному використанні цих інструментів, забезпечивши їх ефективну інтеграцію та налаштованість для оптимального захисту. Наприклад, тут виступає каталізатором страхова галузь. У відповідь на сплеск атак програм-вимагачів в останні роки страховики підштовхують компанії до впровадження таких інструментів, як багатофакторна автентифікація, інструменти виявлення кінцевих точок і реагування, фільтрація електронної пошти, а також покращене навчання з питань кібербезпеки та тестування реагування на інциденти. Усе частіше це ставки для отримання кіберстрахового покриття.

Примітно, що організації не можуть ігнорувати базове блокування. Це передбачає такі основні принципи, як забезпечення актуальності бази даних керування конфігураціями, інвентаризації всіх IT-служб, програмного та апаратного забезпечення,

а також того, що ваші команди встановили найновіші програмні виправлення для усунення вразливостей. Хоча боротьба з вичерпаними системами аж ніяк не є короткостроковим рішенням, поточні обставини ще раз підкреслюють необхідність продовжувати замінювати технології, які недостатньо кіберстійкі проти сучасних зловмисних загроз.

**3. Подивіться вниз по ланцюжку**

Недавня атака, яка була спрямована на українські банки, була названа найпотужнішою в історії України. Вона показала, що вразливі місця можуть існувати глибоко в цифрових ланцюжках поставок [6]. Організаціям необхідно активно взаємодіяти з постачальниками, щоб переконатися, що вони серйозно сприймають кіберзагрозу та впроваджують однакові засоби контролю автентифікації, доступу, контролю керування виправленнями та іншими джерелами ризику.

Залежність від сторонніх технологій, даних і цифрових рішень зростає, оскільки організації звертаються до передових можливостей, для створення яких у них немає таланту, часу чи бажання. Враховуючи цю підвищену залежність, правила взаємодії змінюються. Це означає наявність більш складних вимог до третіх сторін. Типовий набір вимог стає дедалі жорсткішим охоплюючи різні сфери, починаючи від політики захисту від шкідливих програм і даних та закінчуючи класифікацією інформації та процедурами управління інцидентами.

**4. Розглянемо потік робочої сили**

Організації також повинні бути пильними у питаннях щодо внутрішнього ризику. Велика відставка вплинула на кібербезпеку та IT-персонал, а також на інші сфери робочої сили. Плинність кадрів зростає, і багато працівників можуть бути новими та майже невідомими їхнім колегам. Це може створити ризик ключових осіб, коли плани передбачають присутність здібних осіб або команд, яких може більше не бути. Тому важливо перевірити, чи достатньо працівників та пов’язаних з ними процедур з огляду на поточні загрози, а також чи потрібні люди на місці та в підготуванні.

Потік робочої сили також дає можливість для незадоволених працівників або поганих акторів. Щоб захиститися від цього ризику, організаціям слід переглянути та, за необхідності, посилити свою політику щодо перевірки репутації, вимагати скидання пароля, переконатися, що доступ і привілеї співробітників відповідають їхнім ролям, і бути готовими активно стежити за підозрілою поведінкою.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Жоден крок не може гарантувати захист від кіберзагроз, але за останні роки організації багато чого дізналися про загрози, придбали та освоїли безліч інструментів та створили команди експертів для зміцнення свого захисту. Оскільки геополітична напруженість зростає, організації повинні бути повністю готові до нових викликів та переконатися, що вони ефективно використовують ці інструменти та співпрацюють між колегами, постачальниками та владою. Державні органи, урядові організації разом з українськими компаніями з кібербезпеки і найголовнішими світовими виробниками рішень запровадили ешелонований кіберзахист для нашої рідної держави та бізнесу в цілому [7].

У такі критичні часи, як цей, історичні інвестиції в управління кіберризиками та кібербезпеку показують свою реальну цінність. Як нещодавно зауважив один фінансовий директор підприємства, «комерційне обгрунтування кіберінвестицій полягає в тому, що ми можемо залишатися в бізнесі, коли станеться найгірше».

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Економічна правда. (2017). *Україну атакував масовий інтернет-вірус*. http://epravda.com.ua/news/2017/06/27/626501/

2 Шеремета, Д. (2020). *США виділять Україні $38 млн на посилення кібербезпеки*. Главком | Glavcom. https://glavcom.ua/economics/finances/ssha-vidilyat-ukrajini-38-mln-na-posilennya-kiberbezpeki-663356.html

3 *Кібератака на Україну: як "зламували" урядові сайти? - BBC News Україна*. BBC News Україна. https://www.bbc.com/ukrainian/news-60050149

4 Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2022) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text

5 Шейко, Ю. (2022). *ЄС відключив сім російських банків від SWIFT: як це працює – DW – 02.03.2022*. dw.com. https://www.dw.com/uk/yes-vidkliuchyv-sim-rosiiskykh-bankiv-vid-swift-yak-tse-pratsiuie/a-60990268

6 Кузнецова, К. (2022, 17 лютого). *Найпотужніша кібератака за всю історію України: ціль хакерів, кого підозрюють і які наслідки для держави*. ТСН.ua. https://tsn.ua/ukrayina/naypotuzhnisha-kiberataka-za-vsyu-istoriyu-ukrayini-cil-hakeriv-kogo-pidozryuyut-i-yaki-naslidki-dlya-derzhavi-1979239.html

7 Мальцева, І., Черниш, Ю., Штонда, Р. (2022). Аналіз деяких кіберзагроз в умовах війни. : *Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка, 4*(16), 37-44. https://csecurity.kubg.edu.ua/index.php/journal/article/view/362.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023

**Yuliya O. Chernish**
Senior Researcher
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-6626-5656
*yuliia.chernysch@viti.edu.ua*

**Irina R. Maltseva**
Senior Researcher
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-6073-4637
*iryna.maltseva@viti.edu.ua*

**Roman M. Shtonda**
Head of Research Department
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-5986-0847
*roman.shtonda@viti.edu.ua*

**Victor M. Kuznetsov**
Listener
National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID ID: 0009-0009-6824-9308
*vikvik3@i.ua*

**Viktor M. Homeniuk**
Listener
National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID ID: 0009-0007-2286-6832
*gomenuk.vik@gmail.com*

**Oleksandr I. Pidkova**
Listener
National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID ID: 0009-0009-0387-7100
*pidkovaoleksandr2@gmail.com*

# APPROACHES TO ACHIEVING INFORMATION PROTECTION IN ORGANIZATIONS OF DIFFERENT FIELDS OF ACTIVITIES DURING A STATE OF EMERGENCY (MARTIAL WAR)

**Abstract.** The number of cyber attacks is increasing. In modern organizations of various fields of activity, all information is increasingly stored in digital or electronic form, be it on individual computers or data storage devices, on the organization's servers or data storage services, or with the help of web-based "cloud" technologies.

The purpose of this article is to provide an understanding of information security and analysis of the solution to the problem, as well as to identify threats that can seriously affect organizations of all sizes.

This article examines the most popular methods of protecting information during wartime. Let's take a closer look at how this or that method can help you.

All businesses now have business-critical information and data stored electronically, so maintaining data security is critical. The growing use of web-based services such as the cloud creates additional digital security challenges.

Inadequate cyber security can compromise systems and services, harm people and, in extreme cases, endanger lives.

While an organization cannot guarantee that its digital assets are 100 percent secure, this article provides advice on how to assess threats to systems and develop a security regime that ensures that sensitive digital assets are always protected.

**Keywords:** cyber attacks, cyber threats, cyber defense, cyberspace.

## REFERENCES

1 Ekonomichna pravda. (2017). Ukrainu atakuvav masovyi internet-virus. http://epravda.com.ua/news/2017/06/27/626501/
2 Sheremeta, D. (2020). SShA vydiliat Ukraini $38 mln na posylennia kiberbezpeky. Hlavkom | Glavcom. https://glavcom.ua/economics/finances/ssha-vidilyat-ukrajini-38-mln-na-posilennya-kiberbezpeki-663356.html
3 Kiberataka na Ukrainu: yak "zlamuvaly" uriadovi saity? - BBC News Ukraina. BBC News Ukraina. https://www.bbc.com/ukrainian/news-60050149
4 Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy, Zakon Ukrainy № 2163-VIII (2022) (Ukraina). https://zakon.rada.gov.ua/laws/show/2163-19#Text
5 Sheiko, Yu. (2022). YeS vidkliuchyv sim rosiiskykh bankiv vid SWIFT: yak tse pratsiuie – DW – 02.03.2022. dw.com. https://www.dw.com/uk/yes-vidkliuchyv-sim-rosiiskykh-bankiv-vid-swift-yak-tse-pratsiuie/a-60990268
6 Kuznetsova, K. (2022, 17 liutoho). Naipotuzhnisha kiberataka za vsiu istoriiu Ukrainy: tsil khakeriv, koho pidozriuiut i yaki naslidky dlia derzhavy. TSN.ua. https://tsn.ua/ukrayina/naypotuzhnisha-kiberataka-za-vsyu-istoriyu-ukrayini-cil-hakeriv-kogo-pidozryuyut-i-yaki-naslidki-dlya-derzhavi-1979239.html
7 Maltseva, I., Chernysh, Yu., Shtonda, R. (2022). Analiz deiakykh kiberzahroz v umovakh viiny. : Elektronne fakhove naukove vydannia Kiberbezpeka: osvita, nauka, tekhnika, 4(16), 37-44. https://csecurity.kubg.edu.ua/index.php/journal/article/view/362.