МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

19 травня 2023 року

У двох томах

Том 1

Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова.**

Відповідальний за випуск **М. Р. Аракелян.**
Матеріали видано в авторській редакції.

Є24 **Європейські** орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. – Т. 1. – 790 с.

ISBN 978-617-8263-39-3

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У першому томі збірника містяться наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології. Висвітлено питання загроз національній безпеці в їхньому конституційному вимірі, у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-39-3 (т. 1)

СЕКЦІЯ 13
КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Список використаних джерел:

1. Дослідження Check Point: кібератаки зросли на 50 % у порівнянні з минулим роком. URL: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/
2. Барометр ризиків Allianz. 2022. URL: https:// www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
3. Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. URL: https://elibrary.kubg.edu.ua/id/eprint/42325/1/Kraus_Tsyfrova_transformatsiia_kiberbezpeky_2022.pdf
4. Shun-ichi Amari. Information Geometry and Its Applications. Applied Mathematical Sciences, Springer, 2016.
5. Hesham Fouad, Ira S. Moskowitz, Derek Brock, Michael. Scott Integrating Expert Human Decision-Making in Artificial Intelligence Applications, Chapter 13, Human-Machine Shared Contexts, Elsevier, pp. 257–275, June 2020. URL: https://www.sciencedirect.com/science/article/abs/pii/B9780128205433000134?via%3Dihub

Ключові слова: менеджмент, кібербезпека, інформаційна геометрія.
Key words: management, cyber security, information geometry.

ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ

Національний університет «Одеська юридична академія», професор кафедри кібербезпеки, доктор юридичних наук, професор

СЛАТВІНСЬКА ВАЛЕРІЯ МИКОЛАЇВНА

Національний університет «Одеська юридична академія», асистент кафедри кібербезпеки

ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ КІБЕРРОЗВІДКИ

Забезпечення кіберзахисту та кіберрозвідки є важливими аспектами в сфері кібербезпеки. Кіберзахист включає в себе заходи з захисту комп'ютерних мереж, програмного забезпечення та даних від несанкціонованого доступу, витоку інформації, вірусів та інших загроз.

Зокрема, в контексті кібероперацій, на думку Горінова П. В. та Драпушко Р. Г.: «Кіберпростір є новим каналом. Він призначений для створення і поширення різноманітної інформації, яка стала новим двигуном економічного зростання, новою платформою для соціального управління, новим способом міжнародного співробітництва і цілою новою сферою національного суверенітету» [1, с. 267].

Забезпечення кіберзахисту може бути досягнуте за допомогою різних методів, таких як захист мережі за допомогою брандмауера, використання антивірусного програмного забезпечення, регулярні оновлення програмного забезпечення та оперативної системи, використання складних паролів та двофакторної автентифікації, резервне копіювання даних та ін.

Кіберрозвідка включає в себе збір, аналіз та використання інформації про кіберзагрози та кібератаки. Кіберрозвідувачі займаються виявленням та запобіганням кібератак та кібершпигунства. Вони мають у своєму розпорядженні передові технології та програмне забезпечення, що дозволяє виявляти та аналізувати потенційні кіберзагрози та кібератаки. При цьому важливо зазначити, що це відбувається за допомогою інструментів забезпечення кіберрозвідки – програмних та апаратних засобів, які використовуються для збору, аналізу та інтерпретації інформації про потенційні загрози в кіберпросторі. Наведемо деякі з найбільш поширених інструментів кіберрозвідки:

1. Системи виявлення вторгнень (IDS) і системи запобігання вторгнень (IPS): IDS і IPS – це програмні засоби, які дозволяють виявляти та блокувати спроби несанкціонованого доступу до мережі або окремих систем. IDS зазвичай використовується для виявлення несподіваних подій, які можуть вказувати на атаку, тоді як IPS дозволяє заблокувати атаку та запобігти додатковому пошкодженню.
2. Системи управління журналами: ці інструменти дозволяють збирати та аналізувати журнали подій, що стосуються безпеки, щоб виявити підозрілі дії та події, які можуть свідчити про атаку.
3. Системи аналізу вразливостей: ці інструменти використовуються для виявлення вразливостей у програмному забезпеченні, операційних системах та інших компонентах мережі, щоб запобігти атакам.
4. Системи моніторингу мережі: ці інструменти використовуються для відстеження трафіку мережі та виявлення підозрілих активностей, таких як незвичні спроби доступу до ресурсів мережі або незвичні трафікові шаблони.
5. Системи інтелектуального аналізу даних: ці інструменти використовуються для аналізу великих обсягів даних та виявлення підозрілих зразків та поведінки.

Тож кіберрозвідка може допомогти уникнути кібератак та зменшити ризик порушення кібербезпеки. Кіберрозвідка може використовуватися для виявлення вразливостей в мережі та програмному забезпеченні, а також для виявлення кібератак з боку зловмисників.

Отже, для забезпечення ефективного кіберзахисту та кіберрозвідки необхідно розробляти та використовувати різноманітні технології та методики. Наприклад, штучний інтелект може бути використаний для автоматичного виявлення кіберзагроз та захисту мережі від них. Також важливим є постійне навчання та підвищення кваліфікації фахівців з кібербезпеки та кіберрозвідки.

Список використаних джерел:

1. Горінов П. В., Драпушко Р. Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2023. № 1. С. 267–270. DOI: https://doi.org/10.32782/2524-0374/2023-1/63

Ключові слова: кіберрозвідка, кіберзахист, кібератака.
Key words: cyber intelligence, cyber defense, cyber attack.