**Список використаних джерел:**

1. Дей.О. Словник українських псевдонімів та криптонімів(XVI-XX ст). Київ, Наукова думка, 1969.- с.558.
2. Українка.Л. Волинський скарб. Луцьк, Волинський національний університет Лесі Українки, 2011. – с.551.
3. (Див: https://www.sworld.com.ua/konfer41/237.pdf )

**Прудська А.С.,**
студентка IV курсу кафедри івент-менеджменту та соціальних комунікацій ВП «Миколаївська філія Київського національного університету культури і мистецтв»;
Науковий керівник: Шуляк С. О., кандидат педагогічних наук, доцент, завідувач кафедри івент-менеджменту та соціальних комунікацій ВП «Миколаївська філія Київського національного університету культури і мистецтв», м. Миколаїв, Україна

## КІБЕРБЕЗПЕКА В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

В наш час, диджиталізація, роботизація, інтелектуальна економіка спонукають світ переходити на новий рівень життєдіяльності, коли керівними чинниками виробництва стають інновації та творчі досягнення людей. Суспільство увійшло в еру інновацій, де промислові роботи, 3D-друк, хмарні джерела інформації, 4G- та 5G-зв'язок, геноміка, VR-технології, розумні міста стають звичайною річчю.

Питанням кібербезпеки нашої країни та формуванню механізму міжнародної приділяли увагу численні науковці. Так, наприклад, Д. С. Безуглий обґрунтував необхідність інформаційної безпеки як складової частини національної безпеки країни [5].

Поступовий перехід у розвитку людської формації "інформаційного суспільства" до "високотехнологічного суспільства" обумовлює еволюцію підходів до забезпечення безпеки у нових умовах на різних рівнях.

Відбувається поступова трансформація концепції інформаційної безпеки громадянина, суспільства, держави до необхідності її доповнення новою концепцією – кібербезпека.

За українським законодавством, кібербезпека являє собою захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення,

запобігання та нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [1].

Кібербезпека у широкому розумінні є станом захищеності інформаційного середовища, що гарантує дотримання прав і законних інтересів особистості, суспільства та держави в інформаційній сфері. Сучасне суспільство живе в інформаційному середовищі, де створення, використання та поширення інформації виступає важливою економічною, політичною та культурною діяльністю.

Насамперед інформація виступає об'єктом інформаційного права – правової галузі, яка є сукупністю юридичних норм, що визначають поведінку суб'єктів (громадян, юридичних осіб публічного і приватного права тощо) в інформаційній сфері. Сучасні тенденції розвитку інформаційного права свідчать про динамічний розвиток і видозміну підходів до його правових категорій, появу нових, вдосконалення наявних [2].

Іноді кібербезпеку також визначають крізь призму діяльності, спрямованої на захист систем, мереж і комп'ютерних програм від цифрових атак. Метою таких кібератак зазвичай є отримання доступу до конфіденційної інформації, її зміна або знищення, вимагання грошей у користувачів або порушення нормального бізнес-процесу підприємства.

При побудові ефективної системи кібербезпеки важливо знати перелік тих загроз, яким вона повинна протистояти. При цьому, процес виявлення кіберзагроз вимагає глибокого аналізу їх сутності з подальшою систематизацією набутих знань.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" це визначення має наступне тлумачення.

Кіберзагроза – фактори (події, явища), які мають місце або можуть виникнути в інформаційній, комунікаційній, комп'ютерно-мережній та соціотехнічній складових кіберпростору (або їх комбінації у певному поєднанні), за умови умисного цілеспрямованого або випадкового впливів та створити небезпеку порушення процесів управління і передачі інформації, що відбуваються у кібернетичних системах різних сфер (соціальної, технічної, соціотехнічної), або можуть зашкодити елементам таких систем [4].

Подолання наслідків кіберзлочинності і її профілактика є дуже запитуваною темою для публічних послуг. Сьогодні не всі держави-члени досягли рівня ноухау, необхідного для початку ефективної боротьби з кіберзлочинністю. Європол є спільнотою фахівців в Європі для оперативної підтримки, координації та експертизи в області кіберзлочинності.

Європейський центр кіберзлочинності забезпечує більш широкі спільні заходи у співпраці з державами - членами ЄС, з іншими ключовими зацікавленими сторонами; країн, що не входять в ЄС; з міжнародними організаціями; з керівними органами та постачальниками інтернет-послуг, з компаніями, що займаються інтернет-безпекою фінансового сектора; з академічними експертами; з організаціями громадянського суспільства.

Іншими словами, сучасною тенденцією міжнародної протидії кіберзлочинності є розширення сфери взаємодії держав. Реальністю стає оперативне співробітництво

правоохоронних органів з боротьби з кіберзлочинами (Інтерпол, Європол, Євроюст), створення і використання єдиної бази даних про кіберзлочинців, про вчинені і плановані кіберзлочини (перш за все працює в режимі 24/7) [3].

Отже, проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства. З огляду на сучасні суспільно-політичні та інформаційні виклики визначення політичних, науково-технічних, організаційних та просвітницьких напрямів конструювання ефективної системи кіберзахисту у рамках комплексної протидії кіберзагрозам сприятиме формуванню ефективного механізму протидії загрозам у кібернетичній сфері, випереджальному реагування на динамічні зміни, що відбуваються у кіберпросторі, розробленню та впровадження ефективних засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі.

**Список використаних джерел:**

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII (В редакції Закону України від 24.10.2020 р. № 2163-VIII). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua – Назва з екрану.

2. Сутність кібербезпеки у теорії інформаційного права [Електронний ресурс]. – Режим доступу: http://pdu-journal.kpu.zp.ua/archive/2_2021/6.pdf – Назва з екрану.

3. European Convention on Cybercrime. [Електронний ресурс]. – Режим доступу: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf. – Назва з екрану.

4. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. ISBN 978-617-582-069-8 [Електронний ресурс]. – Режим доступу: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiqxZa9wPf7AhVvlYsKHYDmCD8QFnoECBQQAQ&url=https%3A%2F%2Fmetod.suitt.edu.ua%2Fdownload%2F686&usg=AOvVaw0qHCcdFMp-jJOGSUn6R3h3 – Назва з екрану.

5. Кібербезпека та захист інформації [Електронний ресурс]. – Режим доступу: http://tr.knute.edu.ua/files/2021/05.pdf – Назва з екрану.