МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА

НАВЧАЛЬНО-НАУКОВИЙ ЮРИДИЧНИЙ ІНСТИТУТ

Кафедра правоохоронної діяльності

Гуменицька В.В., Яцина М. О.

МЕТОДИЧНІ ВКАЗІВКИ

для підготовки до семінарських (практичних) занять та самостійної роботи з навчальної дисципліни

«ДЕРЖАВНА ПОЛІТИКА В СФЕРІ КІБЕРЗАХИСТУ»

для здобувачів денної форми навчання

першого (бакалаврського) рівня вищої освіти

галузі знань 26 «Цивільна безпека», спеціальності 262 «Правоохоронна діяльність»

(ІІ семестр)

Івано-Франківськ – 2025

Схвалено на засіданні кафедри правоохоронної діяльності Навчально-наукового юридичного інституту (протокол № 5 від 21 січня 2025 року).

Рецензент:

Медицький Ігор Богданович - завідувач кафедри правоохоронної діяльності Навчально-наукового юридичного інституту Прикарпатського національного університету імені Василя Стефаника, доктор юридичних наук, професор

Гуменицька В. В. Яцина М. О. Методичні вказівки для підготовки до практичних занять та самостійної роботи з навчальної дисципліни «Державна політика у сфері кіберзахисту» для здобувачів денної форми навчання першого (бакалаврського) рівня вищої освіти галузі знань 262 «Правоохоронна діяльність», спеціальності 26 «Цивільна безпека», ОПП «Правоохоронна діяльність» (2 семестр). Івано-Франківськ : Навчально-науковий юридичний інститут Прикарпатського національного університету імені Василя Стефаника. Івано-Франківськ, 2024. 25 с.

Методичні вказівки містять в собі основні питання, що виносяться на розгляд семінарських (практичних) занять, вивчення яких є необхідним для набуття знань та умінь у сфері організації та забезпечення кібербезпеки та кіберзахисту.

Методичні вказівки призначені для викладачів та здобувачів вищої освіти Навчально-наукового юридичного інституту Прикарпатського національного університету імені Василя Стефаника при вивченні навчальної дисципліни «Державна політика у сфері кіберзахисту».

,

ЗМІСТ

ВСТУП

Навчальна дисципліна «Державна політика у сфері кіберзахисту» спрямована на формування у здобувачів вищої освіти комплексного розуміння теоретичних та практичних аспектів забезпечення кібербезпеки та кіберзахисту на національному та міжнародному рівнях. У сучасну епоху стрімкого розвитку цифрових технологій та глобальної інформатизації суспільства питання забезпечення кібербезпеки набуває критичного значення для національної безпеки держави, стабільного функціонування її інститутів та захисту прав і свобод громадян. В умовах сьогодення кібератаки перетворилися на потужний інструмент гібридної війни, здатний завдати значної шкоди критичній інфраструктурі, економічній стабільності та суверенітету держави. Ці обставини підкреслюють актуальність навчальної дисципліни, яка зосереджується на питаннях впровадження та вдосконалення ефективного кіберзахисту для забезпечення національної безпеки в умовах цифрової трансформації.

Метою курсу «Державна політика у сфері кіберзахисту» є формування у студентів цілісного розуміння основних принципів, механізмів та інструментів державної політики у сфері кіберррзахисту, аналіз національної та міжнародної нормативно-правової бази, вивчення основних кіберзагроз та стратегій протидії їм.

Цілями навчальної дисципліни є: оволодіння студентами ключовими поняттями, такими як «кіберзахист», «кібербезпека», «кіберпростір», «кіберзлочинність», «кіберзлочин», «кібертероризм» та ін.; формування навичок здійснення комплексного дослідження нормативно-правової бази кібербезпеки України та міжнародного досвіду у цій сфері, включаючи практичні аспекти; оволодіння методикою оцінки сучасних кіберзагроз; проведення детального аналізу структури, повноважень та функцій суб'єктів національної системи кібербезпеки; формування здатності застосовувати отримані знання на практиці.

Досягнення мети та цілей навчальної дисципліни "Державна політика у сфері кіберзахисту" реалізується через виконання таких ключових *завдань*: 1) формування ґрунтовної теоретичної бази знань щодо феномену кіберзлочинності та його сутнісних характеристик; 2) засвоєння практичного інструментарію протидії кіберзлочинам та основних концептуальних засад кібербезпеки; 3) опанування методології оцінювання та аналізу показників кіберзлочинності (включаючи рівень, структуру, динаміку та інші кількісні та якісні індикатори); 4) дослідження практичних аспектів розробки та імплементації державної політики у сфері забезпечення кібербезпеки та боротьби з кіберзлочинністю; 5) набуття знань щодо типологізації кіберзлочинів, їх структурних елементів, послідовності розвитку та етапів реалізації протиправних дій у кіберпросторі; 6) дослідження методів кіберзахисту об’єктів критичної інфраструктури; 7) аналіз особливостей політики кіберзахисту та кібербезпеки провідних країн світу.

Семінарське заняття 1
ТЕМА 1: «ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ» (2 год.)

У сучасному світі інформація є стратегічним ресурсом, а її захист набуває критичного значення для держави, суспільства та кожного громадянина. З розвитком цифрових технологій зростає ризик кібератак, витоку конфіденційних даних, інформаційних маніпуляцій і шкідливого впливу на суспільну свідомість. Тому питання інформаційної безпеки, кібербезпеки та кіберзахисту є важливими складовими національної безпеки України.

Студенти повинні засвоїти зміст та особливості вихідних понять даної навчальної дисципліни, якими є: кіберпростір, кібербезпека, кіберзахист. Також необхідно знати співвідношення таких понять як: національна безпека, інформаційна безпека та кібербезпека. Окремим важливим аспектом даної теми є розуміння місця та ролі кіберзахисту у існуючій системі безпеки суспільства та держави.

Питання до обговорення:

1. Кіберпростір: поняття та особливості.
2. Поняття та сутність національної безпеки України.
3. Інформаційна безпека у системі національної безпеки.
4. Кібербезпека: поняття та зміст.
5. Поняття «кіберзахисту».

Завдання для самостійної роботи:

Підготуйте презентацію на тему «Співвідношення національної безпеки, інформаційної безпеки та кібербезпеки».

Питання для самоконтролю:

1. Дайте визначення поняття "кіберпростір" та розкрийте його основні характеристики.
2. Які основні компоненти включає в себе кіберпростір?
3. Чим відрізняється кіберпростір від інформаційного простору?
4. Назвіть основні особливості кіберпростору як середовища людської діяльності.
5. Як визначається поняття "національна безпека" в законодавстві України?
6. Назвіть основні об'єкти національної безпеки України.
7. Якими нормативно-правовими актами регулюються питання національної безпеки в Україні?
8. Дайте визначення поняття "інформаційна безпека" та розкрийте її сутність.
9. Яке місце займає інформаційна безпека в системі національної безпеки України?
10. Які основні завдання державної політики у сфері інформаційної безпеки?
11. Яким чином інформаційна безпека пов'язана з іншими складовими національної безпеки?
12. Дайте визначення поняття "кібербезпека" та розкрийте його основний зміст.
13. Чим відрізняється поняття "кібербезпека" від поняття "інформаційна безпека"?
14. Які основні принципи забезпечення кібербезпеки визначені законодавством України?
15. Дайте визначення поняття "кіберзахист" та охарактеризуйте його зміст.
16. Як розмежовуються поняття "кібербезпека" та "кіберзахист"?
17. Яка роль державних органів у забезпеченні кіберзахисту об'єктів критичної інфраструктури?

Список рекомендованої літератури:

1. Закон України “Про національну безпеку України”, від 21 червня 2018 року № 2469-VIII // Відомості Верховної Ради. 2018. № 31. Ст. 241.
2. Закон України “Про основні засади забезпечення кібербезпеки України”, прийнятий 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради. 2017. № 45. Ст. 403.
3. Конвенція про кіберзлочинність: Закон України від 07.09.2005. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575#Text
4. Гончаренко В. А. До проблеми визначення та розмежування дефініцій "інформаційна безпека" і "кібербезпека". *Аналітично-порівняльне правознавство.* 2024. №5. С. 466-471. URL: https://doi.org/10.24144/2788-6018.2024.05.73
5. Луценко Ю.В., Тарасюк А.В., Денисенко М.М. Кібербезпека та інформаційна безпека: співвідношення понять. *Юридичний науковий електронний журнал*. 2022. №8. С. 320-323. URL: https://doi.org/10.32782/2524-0374/2022-8/70
6. Свердлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук*. 2022. № 10. С. 175–188. URL: https://doi.org/10.31866/2616-7654.10.2022.269495
7. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року No 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовт-ня 2021 року «Про Стратегію інформаційної безпеки»». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14

Семінарське заняття 2
ТЕМА 2: «ПРАВОВА ОСНОВА ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ УКРАЇНИ» (2 год.)

Тема присвячена комплексному аналізу чинного нормативно-правового забезпечення кібербезпеки України та оцінці його відповідності сучасним викликам. В умовах стрімкої цифровізації всіх сфер життєдіяльності суспільства та зростаючих кіберзагроз, питання нормативно-правового забезпечення кібербезпеки набуває особливого значення для національної безпеки України. Кібератаки на критичну інфраструктуру, інформаційні системи державних органів та приватного сектору становлять реальну загрозу не лише для економічної стабільності, але й для суверенітету та територіальної цілісності держави.

Законодавча база України у сфері кібербезпеки формувалася поетапно, відповідаючи на нові виклики та загрози в кіберпросторі. Особливо інтенсивним цей процес став після 2014 року, коли Україна зіткнулася з безпрецедентними за масштабом кібератаками на об'єкти критичної інфраструктури. Нині правове регулювання кібербезпеки в Україні ґрунтується на системі взаємопов'язаних нормативно-правових актів, які визначають базові принципи, механізми та інституційну структуру забезпечення безпеки в кіберпросторі.

Студенти повинні ознайомитися з ключовими законодавчими актами, стратегічними документами у сфері кібербезпеки, проаналізувати їх взаємозв'язок та ефективність практичної реалізації. Особливу увагу потрібно приділити напрямам та засадам державної політики у сферах національної безпеки та кібербезпеки.

Питання до обговорення:

1. Сучасний стан нормативно-правового забезпечення кібербезпеки.
2. Закон України «Про національну безпеку України».
3. Стратегія національної безпеки України.
4. Закон України «Про основні засади забезпечення кібербезпеки України».
5. Стратегія кібербезпеки України.

Завдання для самостійної роботи:

Проаналізуйте та порівняйте основні нормативно-правові акти України, які регулюють питання інформаційної безпеки, кібербезпеки та кіберзахисту (наприклад, Закон України "Про

основні засади забезпечення кібербезпеки України", Закон України "Про захист персональних даних", а також міжнародні документи, якщо є).

Питання для самоконтролю:

1. Які законодавчі та концептуальні акти входять до Переліку документів, що регулюють питання кібербезпеки України?

2. Які стандарти входять до Переліку документів, що регулюють питання кібербезпеки України?

3. Які галузеві нормативні акти входять до Переліку документів, що регулюють питання кібербезпеки України?

4. Які принципи державної політики у сферах національної безпеки та оборони сформульовані у Законі України «Про національну безпеку України»?

5. Наведіть основні принципи планування у сферах національної безпеки та оборони відповідно до Закону України «Про національну безпеку України».

6. Які основні положення Закону України «Про національну безпеку України» стосуються кібербезпеки?

7. Коли затверджена нова Стратегія національної безпеки України під назвою «Безпека людини – безпека країни» та що вона визначає?

8. Які стратегічні напрями забезпечення кібербезпеки передбачає Стратегія національної безпеки України?

9. Які пріоритети національних інтересів визначає Стратегія національної безпеки України 2020 року?

10. Які принципи та механізми захисту кіберпростору визначені Законом України «Про основні засади забезпечення кібербезпеки України»?

11. Які документи становлять правову основу забезпечення кібербезпеки України за Законом України «Про основні засади забезпечення кібербезпеки України»?

12. Які основні завдання та заходи передбачає Стратегія кібербезпеки України від 2021 року?

13. Хто є основними суб'єктами національної системи кібербезпеки, що безпосередньо здійснюють реалізацію Стратегії кібербезпеки України від 2021 року?

14. Які загрози кібербезпеці визначено в Стратегії кібербезпеки України від 2021 року?

15. Які перспективи та виклики стоять перед Україною у сфері кібербезпеки?

Список рекомендованої літератури:

1. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. Київ : Преса України, 1997. 80 с.

2. Закон України "Про національну безпеку України", від 21 червня 2018 року № 2469-VIII // Відомості Верховної Ради. 2018. № 31. Ст. 241.

3. Закон України "Про основні засади забезпечення кібербезпеки України", прийнятий 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради. 2017. № 45. Ст. 403.

4. Указ Президента України від 14 вересня 2020 року №392/2020 "Про Стратегію національної безпеки України" // [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/3922020-35037 .

5. Указ Президента України від 14 травня 2021 року № №447/2021 "Про Стратегію кібербезпеки України" // [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/4472021-40013 .

6. Конвенція про кіберзлочинність: Закон України від 07.09.2005. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575#Text

Семінарське заняття 3-4

ТЕМА 3: «ВИКЛИКИ ТА ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ» (4 год.)

Сучасний світ дедалі більше залежить від інформаційних технологій, що робить питання кібербезпеки надзвичайно актуальним. Україна, як і багато інших країн, стикається з численними викликами у сфері захисту національних інтересів в інформаційному просторі. Постійне зростання кількості кібератак, розвиток комп'ютерної злочинності та зростаюча загроза кібертероризму вимагають системного аналізу та вироблення ефективних механізмів протидії.

Тема присвячена основним загрозам національним інтересам України у сферах інформаційної безпеки та кібербезпеки. При підготовці до семінарського заняття здобувачі повинні проаналізувати глобальні та національні виклики в інформаційній сфері, визначити ключові поняття та види загроз у кіберпросторі. Окрему увагу слід приділити дослідженню об'єктів, що потребують особливого захисту, зокрема об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів.

При опрацюванні питання кіберзлочинності як серйозної загрози сучасному суспільству потрібно проаналізувати основні поняття та ознаки комп'ютерної злочинності, що відрізняють кіберзлочини від традиційних форм протиправної діяльності, розглянути видову характеристику кіберзлочинності та її структуру. Протягом останніх років наша країна неодноразово ставала об'єктом масштабних кібератак, спрямованих на дестабілізацію суспільно-політичної ситуації, порушення роботи державних установ та об'єктів критичної інфраструктури. Обговорення цих питань дозволить краще зрозуміти механізми захисту інформаційного простору, а також виробити ефективні стратегії протидії сучасним кіберзагрозам.

Питання до обговорення:

І частина

1. Актуальні загрози національним інтересам України у сфері кібербезпеки.

1.1. Глобальні виклики та загрози інформаційній безпеці.

1.2. Національні виклики та загрози інформаційній безпеці.

2. Поняття та види загроз безпеці держави у кіберпросторі.

2.1. Виклики для України у сфері кібербезпеки.

2.2. Загрози кібербезпеці України: поняття та види.

2.3. Чинники та передумови формування загроз кібербезпеці.

3. Основні об'єкти кіберзахисту України.

3.1. Об'єкти критичної інфраструктури.

3.2. Об'єкти критичної інформаційної інфраструктури.

3.3. Державні інформаційні ресурси як особливий об'єкт кіберзахисту.

ІІ частина

1. Комп'ютерна злочинність (кіберзлочинність): поняття, ознаки та тенденції розвитку.
2. Детермінанти кіберзлочинності.
3. Видова характеристика кіберзлочинності та її структура.
4. Місце кіберзлочинності у структурі системи злочинності, її показники.
5. Способи здійснення комп'ютерних злочинів у кіберпросторі.

Завдання для самостійної роботи:

Здійсніть аналіз сучасних кіберзагроз, які можуть становити небезпеку для національної безпеки України. Розгляньте основні типи кіберзагроз (кібератаки, шкідливе програмне забезпечення, фішинг, інсайдерські загрози) і визначте їхній вплив на стратегічні сфери (енергетика, телекомунікації, фінансовий сектор).

Проаналізуйте реальний або гіпотетичний кіберінцидент, що стався в Україні (наприклад, кібератака на енергетичну інфраструктуру чи державні органи). Оцініть його вплив на національну безпеку України та можливі юридичні наслідки для держави та організацій, які постраждали.

Оцініть правові аспекти кіберзахисту інфраструктури критичного значення (енергетика, водопостачання, транспорт), яка є важливою для національної безпеки України. Розгляньте питання забезпечення її захисту від кіберзагроз, відповідальності держави та приватних компаній.

Питання для самоконтролю:

1. Які основні причини зростання загроз в інформаційній сфері на теперішній час?

2. Проаналізуйте глобальні виклики та загрози інформаційній безпеці України, визначені Стратегією інформаційної безпеки України від 2021 р.

3. Розкрийте національні виклики та загрози інформаційній безпеці України, визначені Стратегією інформаційної безпеки України від 2021 р..

4. Назвіть причини виникнення нових ризиків і загроз у кіберпросторі.

5. Проаналізуйте основні виклики для України у сфері кібербезпеки, визначені Стратегією кібербезпеки України від 2021 р.

6. Розкрийте основні загрози кібербезпеці України, визначені Стратегією кібербезпеки України від 2021 р.

7. Які передумови та чинники формують загрози кібербербезпеці України, визначені Стратегією кібербезпеки України від 2021 р.?

8. Назвіть основні об'єкти кібербезпеки, визначені Законом України «Про основні засади забезпечення кібербезпеки України» від 2017 р.

9. Назвіть основні об'єкти кіберзахисту, визначені Законом «Про основні засади забезпечення кібербезпеки України» від 2017 р.

10. За яким правовим документом відносяться об'єкти до ***критичної*** *інфраструктури та здійснюється формування Реєстру об'єктів критичної інфраструктури?*

11. Назвіть критерії, за якими відносяться об'єкти до Критичної інфраструктури відповідно до Закону України "Про інфраструктуру" від 2021 р.

12. Поясніть, які об'єкти критичної інфраструктури протягом року підлягають відчуженню відповідно до Закону України «Про критичну інфраструктуру" від 2021 р.

13. Які об'єкти відносяться до об'єктів критичної інфраструктури відповідно до Закону України «Про критичну інфраструктуру" від 2021 р.

14. Поясніть порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

15. На кого покладається відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури?

16. Коли та ким було вперше сформульовано поняття "комп'ютерна злочинність" та яким було його визначення?

17. У чому різняться розуміння комп'ютерного злочину вчених вітчизняної науки?

18. Дайте визначення поняттю комп'ютерний злочин відповідно до Кримінального Кодексу України.

19. З яким терміном ототожнюють термін «комп'ютерний злочин» в Україні та яке визначення його дає Закон України «Про основні засади забезпечення кібербезпеки України» від 2017р.?

20. Назвіть основні напрямки діяльності держави щодо забезпечення її інформаційних інтересів і безпеки в кібернетичній та інформаційній сферах, які визначені у Стратегії національної безпеки України 2020 р.

21. Перелічіть основні детермінанти кіберзлочинності.

22. Яке місце займає кіберзлочинність у структурі системи злочинності?

Список рекомендованої літератури:

1. Закон України «Про національну безпеку України» // Відомості Верховної Ради (ВВР). 2018. №31. Ст. 241.

2. Указ Президента України від 14 вересня 2020 року №329/2020 «Про Стратегію національної безпеки України» // [Електронний ресурс]. Режим доступу:

https://www.president.gov.ua.
3. Указ Президента України від 14 травня 2021 року №447/2021 «Про Стратегію кібербезпеки України» // [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/4472021-40013.
4. Указ Президента України від 28 грудня 2021 року №685/2021 «Про стратегію інформаційної безпеки» // [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/6852021-41069.
5. Закон України «Про основні засади забезпечення кібербезпеки України». Затверджений Указом Президента України від 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403.
6. Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
7. Указ Президента України «Про Концепцію забезпечення національної системи стійкості» від 27 вересня 2021 року №479/2021. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/n0065525-21#Text.
8. Закон України від 16.12.2020 № 1089-IX «Про електронні комунікації» // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20#n2246.
9. Закон України від 22 травня 2003 року № 851-IV «Про електронні документи та електронний документообіг» // [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15#Text .
10. Закон України від 21 січня 1994 року № 3855-XII «Про державну таємницю» // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text.
11. Постанова КМ України «Деякі питання об'єктів критичної інфраструктури» від 09.10.2020 № 1109. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.
12. Горбулін В. П, Качинський А. Б. Засади національної безпеки України: підручник для студ. вищих навч. закл. / Інститут проблем національної безпеки. Київ: Інтертехнологія, 2009. 270 с.
13. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект підручник / [В. Л. Бурячок, Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора Б. Толубка. Київ : ДУТ, 2015. 288 с.
14. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. / [кол. авторів: О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.; за заг. ред. В. В. Коваленка]. Київ : Вид. дім "Скіф", 2012. 728 с.
15. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навч. посіб. для вищих навч. закладів / Українська Академія держ. управління при Президентові України; Академія держ. податкової служби України. Київ : Преса України, 2000. 304 с.
16. Науково-практичний коментар Розділу XVI КК України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" (статті 362 - 363, висновки, словник) / [О.О. Климчук, Р.В. Макуха, Д.С. Мельник; за заг. ред. О.О. Климчука]. Київ : Центр навч.-наук. та наук.-практ. НА СБУ, 2014. 88 с.
17. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України"; станом на 01.01.2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.
18. Мельник Д. С. Комп'ютерні злочини: проблеми виділення та кваліфікації. *Міжнародний науковий журнал «Інтернаука»*. Київ, 2021, вип. 4 (104), С. 59-62. URL: https//doi.org/10.25313/2520-2057-2021-4-7055.
19. Мельник Д. С. Захист національної критичної інформаційної інфраструктури: актуальні проблеми та шляхи вирішення. «*Адміністративне право і процес»:* науково-практичний журнал. Київ, 2022. №3(38)/2022. С. 5-16.
20. Бабанін С. В. Кіберзлочинність. *Вісник Асоціації кримінального права України*.

2016. Т. 1, № 5. С. 468–470. URL: http://vakp.nlu.edu.ua/article/view/173523

21. Русецький А. А., Куцолабський Д. А. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74–78. URL: file:///C:/Users/Admin/Downloads/Pib_2017_1_15.pdf

22. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»:стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1–2 (10–11). С. 276–282.

23. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / [Бутузов В. М., Гавловський В. Д., Скалозуб Л. П. та ін.; за ред. Є. Д. Скулиша]. Київ, 2011. 404 с.

24. Злочини у сфері використання комп'ютерної техніки: навч. посіб. / Карчевський В. М. Київ, 2010. 168 с.

Семінарське заняття 5
ТЕМА 4: «КІБЕРТЕРОРИЗМ У СУЧАСНОМУ СВІТІ: ПОНЯТТЯ, ВИДИ ТА ШЛЯХИ ПРОТИДІЇ» (2 год.)

У XXI столітті кіберпростір став невід'ємною частиною життя суспільства, державного управління та функціонування критичної інфраструктури. Однак разом із розвитком інформаційних технологій з'явилися нові форми протиправної діяльності, серед яких особливе місце посідає кібертероризм. Кібератаки на об'єкти критичної інфраструктури, фінансові установи, державні інформаційні системи можуть призвести до катастрофічних наслідків, прирівняних до наслідків від вчинення тероризму.

При підготовці до семінарського заняття необхідно розглянути ключові аспекти кібертероризму, починаючи від історії його виникнення до сучасних механізмів протидії, простежити еволюцію комп'ютерного тероризму від перших хакерських атак до новітніх високоорганізованих операцій, що здійснюються терористичними організаціями та навіть окремими державами.

Особливу увагу слід приділити понятійному апарату, а саме: знати зміст понять «кібертероризм», «кібератака», «кібер-терористичний акт» тощо. Знати види кібертероризму та його співвідношення з тероризмом. Розглянути юридичний склад даного злочину, що дозволить зрозуміти, які саме дії підпадають під правове визначення кібертероризму та які елементи повинні бути наявними для кваліфікації діяння як кібертерористичного акту. Необхідно проаналізувати міжнародно-правовий досвід протидії кібертероризму, що дозволить сформувати комплексне уявлення про шляхи запобігання кібертерористичним загрозам у майбутньому.

Питання до обговорення:

1. Феномен «кібертероризму» та історія його виникнення.
2. Кібертероризм: поняття та ознаки.
3. Основні форми кібертероризму.
4. Співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне).
5. Юридичний склад кібертероризму.
6. Міжнародно-правовий досвід запобігання та протидії кібертероризму.

Завдання для самостійної роботи:

Здійсніть аналіз поняття кібертероризму в контексті сучасної правової теорії та практики. Як це поняття визначається в міжнародному праві і національному законодавстві України? Розгляньте основні характеристики кібертероризму.

Дослідження видів кібертероризму та їх вплив на державну безпеку. Розгляньте такі форми кібертероризму, як кібератаки на інфраструктуру критичного значення, поширення пропаганди та дезінформації через Інтернет, кібернапади на державні органи влади.

Дослідження міжнародних зусиль у боротьбі з кібертероризмом, зокрема через Організацію Об'єднаних Націй (ООН), Європейський Союз та інші міжнародні організації. Як міжнародні правові механізми можуть бути використані для протидії кібертероризму?

Проаналізуйте національне законодавство України щодо боротьби з кібертероризмом. Як Україна реагує на кібертероризм на рівні державних органів, правозахисних структур та міжнародної співпраці? Які кроки можна зробити для посилення законодавчої та практичної боротьби з кібертероризмом?

Питання для самоконтролю:

1. *Коли вперше з'явився термін "кібертероризм"?*
2. *Які історичні передумови виникнення кібертероризму?*
3. *Назвіть ключові етапи еволюції кібертероризму.*
4. *Як вплинув розвиток інтернет-технологій на трансформацію кібертероризму?*
5. *Дайте визначення поняття "кібертероризм".*
6. *Які основні ознаки кібертероризму дозволяють відмежувати його від інших видів кіберзлочинів?*
7. *Які суб'єктивні та об'єктивні ознаки кібертероризму?*
8. *У чому полягає суспільна небезпека кібертероризму порівняно з іншими видами кіберзлочинності?*
9. *Перелічіть основні форми кібертероризму.*
10. *Які спільні риси мають кібертероризм і традиційний тероризм?*
11. *Назвіть ключові відмінності між кібертероризмом і традиційним тероризмом.*
12. *Які елементи входять до об'єктивної сторони кібертероризму?*
13. *Дайте характеристику суб'єкту кібертероризму.*
14. *У чому полягає суб'єктивна сторона кібертероризму?*
15. *Які основні міжнародні нормативно-правові акти регулюють питання протидії кібертероризму?*
16. *Назвіть міжнародні організації, що займаються боротьбою з кібертероризмом.*
17. *Які є перспективні напрями міжнародного співробітництва у сфері боротьби з кібертероризмом?*

Список рекомендованої літератури:

1. Закон України «Про основні засади забезпечення кібербезпеки України». Затверджений Указом Президента України від 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403.
2. Закон України «Про боротьбу з тероризмом» від 20 березня 2003 року № 638-IV. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/638-15#Text.
3. Закон України «Про національну безпеку України» // Відомості Верховної Ради (ВВР). 2018. №31. Ст. 241.
4. Указ Президента України від 14 вересня 2020 року №329/2020 «Про Стратегію національної безпеки України» // [Електронний ресурс]. Режим доступу: https://www.president.gov.ua.
5. Указ Президента України від 14 травня 2021 року №447/2021 «Про Стратегію кібербезпеки України» // [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/4472021-40013.
6. Науково-практичний коментар Закону України “Про основні засади забезпечення кібербезпеки України”; станом на 01.01.2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.
7. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / [Бутузов В. М., Гавловський В. Д., Скалозуб Л. П. та ін.; за ред. Є. Д. Скулиша]. Київ, 2011. 404 с.
8. Білан І. А. Кібертероризм: інформаційно-правовий аспект. Інформація і право. 2023. № 4(47) С. 64-71. DOI: https://doi.org/10.37750/2616-6798.2023.4(47).291584 Режим

доступу: http://il.ippi.org.ua/article/view/291584
9. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. Безпека інформації. 2013. № 2. С. 118-129.
10. Котляров В. Кібертероризм як загроза міжнародній безпеці. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2023. Випуск 5 (71). С. 46-54.
11. Гавва С. К., Головко С. Г. Сучасний кібертероризм як загроза національній безпеці. Національний авіаційний університет. 2023. Ст. 54-56.
12. Зінченко О. І. Європейська регіональна система протидії кібертероризму: політичні, інституційні та правові механізми. Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Питання політології». Вип. 39. 2021. С. 118-122. URL: https://periodicals.karazin.ua/politology/article/view/17813
13. Рульов І. Співвідношення кібертероризму та кіберзлочину. Юридичний вісник. 2021. № 3. С. 178–185. URL: https://dspace.onua.edu.ua/items/f7f84fc6-620d-4f9c-ae6b-dcd46b208485
14. Conway Maura. Cyberterrorism: the story so far. Journal of Information Warfare. 2003. Vol. 2. No. 2. P. 33-42.
15. Lee Jarvis, Stuart Macdonald. What Is Cyberterrorism? Findings From a Survey of Researchers. Terrorism and Political Violence. 2015. Volume 27. Isuue 4. P. 657-678. URL: https://sci-hub.se/10.1080/09546553.2013.847827
16. Stuart Macdonald, Lee Jarvis, Simon M. Lavis. Cyberterrorism Today? Findings From a Follow-on Survey of Researchers. Studies in Conflict & Terrorism. 2019. Volume 5. Issue 8. P. 727-752. URL: https://sci-hub.se/10.1080/1057610X.2019.1696444

Семінарське заняття 6-7
ТЕМА 5: «ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ» (4 год.)

Вивчення даної теми має на меті розкриття концептуальних засад державної політики у сфері кібербезпеки, аналіз основних принципів та завдань національної системи кібербезпеки, а також ознайомлення з сучасними міжнародними стандартами безпеки інформаційних систем.

При підготовці до семінарського заняття необхідно проаналізувати державну політику кібербезпеки, функціонування організаційно-технічної моделі кіберзахисту, його організаційно-керуючу та технічну інфраструктури, розглянути структуру, функції, завдання та принципи національної системи кібербезпеки. Особливу увагу слід приділити підходам до забезпечення безпеки інформаційних систем відповідно до міжнародних стандартів ISO та питанням інтеграції України до міжнародно-правового регулювання кіберпростору.

На сьогодні в Україні функціонує Національна система кібербезпеки, що об’єднує державні органи, приватний сектор і громадські організації, які разом працюють над захистом інформаційних ресурсів країни. Необхідно проаналізувати діяльність Державної служби спеціального зв'язку та захисту інформації України, Національного координаційного центру кібербезпеки при РНБО, Кіберполіції, Міністерства оборони України та Генерального штабу ЗСУ, Національного банку України як державних суб’єктів забезпечення кібербезпеки України. Важливо дослідити роль розвідувальних органів у протидії кіберзагрозам, забезпеченні кіберконтррозвідки та захисті державних ресурсів від атак. Також слід розглянути, як приватний сектор сприяє підвищенню кіберзахисту України, які форми державно-приватного партнерства існують у цій сфері.

Питання до обговорення:

І частина:

1. Державна політика кібербезпеки України.
2. Національна система кібербезпеки України.

2.1. Функції та завдання національної системи кібербезпеки.

2.2. Принципи національної системи кібербезпеки.

3. Сучасні заходи забезпечення безпеки інформаційних систем на базі міжнародних стандартів ISO.

4. Інтеграція України до міжнародно-правового регулювання кіберпростору.

ІІ частина:

1. Державні суб'єкти забезпечення кібербезпеки України.

1.1. Державна служба спеціального зв'язку та захисту інформації України.

1.2. Національний координаційний центр кібербезпеки при РНБО.

1.3. Національна поліція України (Кіберполіція).

1.4. Міністерство оборони України та Генеральний штаб ЗСУ.

1.5. Національний банк України.

2. Роль розвідувальних органів у забезпеченні кібербезпеки України.

3. Приватний сектор як суб'єкт забезпечення кібербезпеки України.

Завдання для самостійної роботи:

Розробіть основні положення політики кібербезпеки для державних органів України, спрямованої на забезпечення національної безпеки. Визначте роль юриста в розробці та впровадженні такої політики.

Оцініть роль міжнародних організацій (наприклад, ЄС, ООН, НАТО) у забезпеченні кібербезпеки України. Як міжнародні зобов'язання можуть сприяти підвищенню національної безпеки в кіберпросторі? Розгляньте юридичні аспекти співпраці України з міжнародними організаціями в цій сфері.

Проаналізуйте організаційну структуру забезпечення кібербезпеки в Україні. Розгляньте роль державних органів, таких як Державна служба спеціального зв'язку та захисту інформації України, Національний координаційний центр кібербезпеки, а також інших органів у сфері забезпечення кіберзахисту.

Проаналізуйте механізми взаємодії державних органів і приватних компаній у сфері кібербезпеки. Як органи влади координують свою діяльність із приватним сектором для забезпечення національної кібербезпеки? Які правові інструменти застосовуються для співпраці?

Питання для самоконтролю:

1. Які основні напрями державної політики кібербезпеки України?

2. Які нормативно-правові акти регулюють кібербезпеку в Україні?

3. Які стратегічні документи визначають політику кібербезпеки України?

4. Як реалізується державна політика у сфері кібербезпеки на рівні державних органів?

5. У чому полягають завдання національної системи кібербезпеки України?

6. Які принципи покладено в основу функціонування національної системи кібербезпеки?

7. У чому полягає принцип координації та співпраці в сфері кібербезпеки?

8. Які міжнародні стандарти ISO використовуються для забезпечення кібербезпеки?

9. Які переваги має застосування стандарту ISO/IEC 27001 у сфері інформаційної безпеки?

10. Як стандарти ISO допомагають підприємствам та державним установам захищати інформаційні системи?

11. Які міжнародні організації займаються регулюванням кіберпростору?

12. Як Україна співпрацює з НАТО та ЄС у сфері кібербезпеки?

13. Які угоди та договори підписала Україна у межах міжнародного регулювання кіберпростору?

14. У чому полягає значення Будапештської конвенції для України?

15. Розкрийте загальну структуру системи суб'єктів забезпечення кібербезпеки України.

16. Які повноваження має Державна служба спеціального зв'язку та захисту інформації України у сфері кібербезпеки?

17. Яку роль відіграє CERT-UA в системі забезпечення кібербезпеки та як він взаємодіє з іншими суб'єктами?

18. Які завдання покладені на Національний координаційний центр кібербезпеки?

19. Які основні завдання та повноваження Департаменту кіберполіції Національної поліції України?

20. Охарактеризуйте основні напрями протидії кіберзлочинності, які здійснює кіберполіція.

21. Які повноваження має Служба безпеки України у сфері забезпечення кібербезпеки держави?

22. Розкрийте роль СБУ у захисті державних інформаційних ресурсів та критичної інформаційної інфраструктури.

23. Які завдання покладено на Міністерство оборони України та Генеральний штаб ЗСУ у сфері кібербезпеки?

24. Які повноваження має Національний банк України як суб'єкт забезпечення кібербезпеки?

25. Які розвідувальні органи України беруть участь у забезпеченні кібербезпеки?

26. Які основні функції виконує Служба зовнішньої розвідки України (СЗР) у сфері кібербезпеки?

27. Як Головне управління розвідки Міністерства оборони України (ГУР МО) забезпечує кіберзахист військової сфери?

28. Чому приватний сектор відіграє важливу роль у забезпеченні кібербезпеки України?

29. Які основні заходи кіберзахисту впроваджуються приватними компаніями?

30. Які форми державно-приватного партнерства використовуються для підвищення кіберзахисту?

Список рекомендованої літератури:

1. Указ Президента України від 14 вересня 2020 року №329/2020 «Про Стратегію національної безпеки України» // [Електронний ресурс]. Режим доступу: https://www.president.gov.ua.
2. Указ Президента України від 14 травня 2021 року №447/2021 «Про Стратегію кібербезпеки України» // [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/4472021-40013.
3. Постанова Кабінету міністрів України від 19 червня 2019 року №518 "Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури" // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
4. Закон України від 5 липня 1994 року № 80/94-ВР "Про захист інформації в інформаційно-телекомунікаційних системах" // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
5. Гуцалюк М. Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю // Інформація і право. № 4(39)/2021. С. 141-147.
6. Правова база української кібербезпеки: загальний огляд і аналіз. Міжнародна фундація виборчих систем в Україні. 2019. 35 с.
7. Марущак А. І. Методи правового регулювання безпеки особи, суспільства, держави в інформаційній сфері. // Вісник Національної академії правових наук України. 2019. № 3. С. 75-89.
8. Марущак А. І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. // Інформація і право. 2018. № 3.С. 104-110.
9. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016

року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

10. Дубов. Д. В. Стратегічні аспекти кібербезпеки України. // Стратегічні пріоритети. 2013. №4. С. 119-127.

Семінарське заняття 8
ТЕМА 6: «ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРЗЛОЧИНИ»
(2 год.)

Кіберзлочинність стала однією з найбільш динамічних форм транснаціональної злочинності, що завдає значних збитків як окремим громадянам, так і державним та приватним установам, підриває національну безпеку держав. Ефективна протидія кіберзлочинності потребує комплексного підходу, важливою складовою якого є чітко визначена система юридичної відповідальності. Правові механізми притягнення до відповідальності за кіберзлочини мають свою специфіку, зумовлену характером протиправних діянь, особливостями їх виявлення, фіксації та доказування.

При підготовці до семінарського заняття необхідно розглянути поняття та види юридичної відповідальності за правопорушення у кіберпросторі, особливості кримінальної, адміністративної та цивільно-правової відповідальності, а також міжнародно-правові механізми регулювання відповідальності за кіберзлочини.

Особливу увагу слід приділити проблемним аспектам правозастосування, що виникають у процесі притягнення до відповідальності за кіберзлочини, зокрема питанням збору та оцінки цифрових доказів, визначення юрисдикції при транскордонних кіберзлочинах, а також механізмам відшкодування шкоди, заподіяної кіберзлочинами.

Питання до обговорення:

1. Поняття, види та особливості юридичної відповідальності за кіберзлочини.
2. Кримінальна відповідальність за кіберзлочини: загальна характеристика та основні положення.
3. Адміністративна відповідальність за правопорушення у сфері кібербезпеки.
4. Цивільно-правова відповідальність за кіберзлочини: механізми відшкодування завданої шкоди.
5. Міжнародно-правове регулювання відповідальності за кіберзлочини.

Завдання для самостійної роботи:

Розгляньте реальний кейс (або вигадану ситуацію), коли юридична особа або фізична особа стали жертвами кіберзлочинів (фішинг, крадіжка даних, кібератака). Оцініть правові наслідки цього інциденту для постраждалої сторони та можливу відповідальність за порушення норм кібербезпеки.

Підготуйте реферат на тему «Кримінологічний портрет кіберзлочинця» або «Типи кіберзлочинців».

Підготуйте презентацію на тему «Види кіберзлочинів».

Оцініть міжнародні правові норми щодо боротьби з кіберзлочинами, такі як Будапештська конвенція. Як Україна взаємодіє з іншими державами в боротьбі з кіберзлочинами? Яка відповідальність існує на міжнародному рівні за кіберзлочини, що охоплюють декілька юрисдикцій?

Питання для самоконтролю:

1. Які особливості має юридична відповідальність у сфері кіберзлочинності?

2. Яка специфіка юрисдикції при притягненні до відповідальності за кіберзлочини?

3. Як співвідносяться різні види юридичної відповідальності за кіберправопорушення?

4. *Які склади кіберзлочинів передбачені Кримінальним кодексом?*

5. *Які покарання передбачені за кіберзлочини та які фактори впливають на їх призначення?*

6. *Які проблеми існують при доказуванні кіберзлочинів?*

7. *Які адміністративні правопорушення передбачені в інформаційній сфері?*

8. *Які адміністративні стягнення застосовуються за кіберправопорушення?*

9. *Як розмежувати адміністративну та кримінальну відповідальність за правопорушення в інформаційній сфері?*

10. *Які підстави виникнення цивільно-правової відповідальності за кіберправопорушення?*

11. *Як визначається розмір шкоди, завданої кіберзлочином?*

12. *Які особливості має процедура відшкодування шкоди, заподіяної кіберзлочином?*

13. *Яка практика судів щодо компенсації моральної шкоди за кіберзлочини?*

14. *Як вирішуються юрисдикційні питання при транскордонних кіберзлочинах?*

15. *Які механізми міжнародного співробітництва існують у сфері боротьби з кіберзлочинністю?*

16. *Які проблеми гармонізації національного законодавства з міжнародними стандартами відповідальності за кіберзлочини?*

Список рекомендованої літератури:

1. Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змінами та доповненнями).

URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

2. Кодекс України про адміністративні правопорушення від 07.12.1984 р. №8073-X (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text

3. Цивільний кодекс України від 16.01.2003 р. №435-IV (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

4. Закон України «Про основні засади забезпечення кібербезпеки України». Затверджений Указом Президента України від 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403.

5. Бутузов В.М., Василинчук В.І. Протидія комп'ютерній злочинності в Україні: системно-структурний аналіз: монографія. Київ: КНТ, 2021. 408 с.

6. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. 2022. DOI https://doi.org/10.32782/2524-0374/2022-12/96

URL: http://www.lsej.org.ua/12_2022/96.pdf

7. Алієв Р., Панасевич, Л. Юридична відповідальність у контексті національної безпеки та оборони України. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи: IV міжнар. наук.-практ. конф.* 2023. С. 144-147. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/18540/1/2_5300948988634084300.pdf#page=145

8. Лугівська Л., Яцишин О, Любавіна В. Тенденції розвитку кримінальної відповідальності за кіберзлочини в умовах цифровізації суспільства. *Dictum factum*, 2024, 2 (16): С. 258—264. DOI: https://doi.org/10.32703/2663-6352/2024-2-16-258-264 URL: https://df.duit.in.ua/index.php/dictum/article/view/363/326

9. Гудман Д. Міжнародна співпраця у протидії кіберзлочинності. Лондон: Academic Press, 2018. 320 с.

10. Клімов В. Правові основи боротьби з кіберзлочинами у країнах ЄС. Прага: EU Law, 2019. 200 с.

11. Шевченко О. Вдосконалення кримінального законодавства України у сфері кіберзлочинності. Харків: Основа, 2021. 210 с.

12. Філіпова Т. Проблеми протидії кіберзлочинності в Україн. Київ: Генеза, 2020. 280 с.

13. Кондратьєв В. Перспективи притягнення до відповідальності за скоєння воєнних кіберзлочнів. *Актуальні проблеми міжнародного та європейського права. погляд молодих вчених*, С. 139-142. URL: https://intrel.lnu.edu.ua/wp-content/uploads/2023/11/Materialy-konferentsii-19-zhovtnia-2023.pdf#page=139

14. Лупай А., Павлюх О, Павлюх А. Актуальність питання боротьби з кіберзлочинністю як складова загальнокримінальної злочинності. *Ірпінський юридичний часопис*. 2023. С. 211-218. DOI: https://doi.org/10.33244/2617-4154-3(12)-2023-211-218
URL: https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/137

Семінарське заняття 9
ТЕМА 7: «ОСОБЛИВОСТІ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КРАЇНАХ СВІТУ»
(2 год.)

Тема присвячена комплексному аналізу особливостей нормативно-правового забезпечення кібербезпеки в провідних країнах світу та міжнародних організаціях. У фокусі уваги правові системи США та Великобританії як держав, що демонструють передові підходи до регулювання кібербезпеки, а також нормативна база НАТО та Європейського Союзу, що відображає колективні зусилля з протидії кіберзагрозам.

Актуальність вивчення міжнародного досвіду нормативно-правового забезпечення кібербезпеки зумовлена низкою факторів. По-перше, транскордонний характер кіберзагроз вимагає узгоджених підходів до їх подолання на міжнародному рівні. По-друге, провідні країни світу та міжнародні організації накопичили значний досвід у сфері правового регулювання кібербезпеки, вивчення якого дозволяє виявити найбільш ефективні практики та адаптувати їх до національних умов. По-третє, в умовах глобалізації та інтеграції інформаційних систем зростає потреба в гармонізації національних законодавств у сфері кібербезпеки.

Студентам необхідно приділити особливу увагу компаративному аналізу різних моделей правового регулювання кібербезпеки, виявленню їхніх спільних рис та відмінностей, а також оцінці ефективності правових механізмів захисту національних інтересів у кіберпросторі. Такий підхід дозволяє не лише систематизувати знання про зарубіжний досвід правового забезпечення кібербезпеки, але й виявити найбільш перспективні практики, що можуть бути адаптовані до національних умов.

Питання до обговорення:

1. Нормативно-правове регулювання кібербезпеки США.
2. Правові норми забезпечення кібербезпеки Великобританії.
3. Законодавче регулювання кібербезпеки НАТО.
4. Правові засади забезпечення кібербезпеки ЄС.

Завдання для самостійної роботи:

Проаналізуйте нормативно-правове забезпечення кібербезпеки в декількох країнах світу (наприклад, США, Європейський Союз, Китай, Індія, Україна). Визначте основні відмінності в підходах до регулювання кібербезпеки.

Розгляньте роль міжнародних організацій (таких як ООН, ЄС, НАТО, АСЕАН, Інтерпол) у розробці нормативно-правових актів і стандартів для забезпечення кібербезпеки. Оцініть їх вплив на національне законодавство різних країн.

Вивчіть Європейські регламенти та директиви щодо кібербезпеки (наприклад, Директива NIS, Регламент ЄС про кібербезпеку). Проаналізуйте, як ці документи впливають на національне законодавство країн-членів ЄС.

Питання для самоконтролю:

1. Які основні нормативні акти визначають нормативно-правове регулювання забезпечення кібербезпеки США?

2. Які державні органи та установи, організації входять до структури національної системи забезпечення інформаційної безпеки США?

3. Які спеціальні служби та правоохоронні органи США приймають участь у забезпеченні кібербезпеки держави?

4. Охарактеризуйте загальні положення нормативно-правового регулювання забезпечення кібербезпеки США.

5. Розкрийте структуру загальнодержавної 2455 США (основні суб'єкти, їх завдання і функції, консультативно-дорадчі структури).

6. Розкрийте особливості діяльності спеціальних служб та правоохоронних органів США у сфері забезпечення кібербезпеки держави.

7. Які основні нормативні акти визначають нормативно-правове регулювання забезпечення кібербезпеки ЄС?

8. Які органи та установи, організації входять до структури системи забезпечення кібербезпеки ЄС?

9. *Розкрийте структуру системи забезпечення кібербезпеки ЄС (основні суб'єкти, їх завдання і функції, консультативно-дорадчі структури*).

10. Охарактеризуйте загальні положення нормативно-правового регулювання забезпечення кібербезпеки ЄС.

11. Які основні нормативні акти визначають нормативно-правове регулювання забезпечення кібербезпеки НАТО?

12. Які органи та установи, організації входять до структури системи забезпечення кібербезпеки НАТО?

13. Розкрийте зміст основних нормативно-правових актів Великобританії, які встановлюють порядок захисту інформації.

14. Які державні органи та установи входять до структури загальнодержавної системи забезпечення кібербезпеки Британії?

15. Які спеціальні служби та органи сектору безпеки і оборони Великобританії приймають участь у забезпеченні кібербезпеки Британії?

16. Охарактеризуйте загальні положення нормативно-правового регулювання забезпечення кібербезпеки Великобританії.

17. Розкрийте структуру загальнодержавної системи забезпечення кібербезпеки Великобританії (основні суб'єкти, їх завдання і функції тощо).

18. Розкрийте роль парламенту Великобританії та його структурних елементів у забезпеченні кібербезпеки країни.

19. Яку роль відіграє уряд Великобританії у загальнодержавній системі забезпечення кібербезпеки.

20. Значення державно-приватного партнерства у забезпеченні кібербезпеки Великобританії.

21. Розкрийте особливості діяльності спеціальних служб та правоохоронних органів Великобританії у сфері забезпечення кібербезпеки держави.

Список рекомендованої літератури:

1. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній: практичний посібник. Київ : Консалтингова компанія «СІДКОН», 2021. 372 с.

2. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. Київ : Вид-во "Ліра-К", 2021. 412 с.

3. Присяжнюк М. М., Остроухов В. В. «Інформаційні загрози державній безпеці України у гібридній війні». Інформаційна безпека людини, суспільства, держави: Науково-практичний журнал. Київ : НА СБ України, №1-3 (31-33) 2022. С. 28-39.

4. Калініченко О. НАТО на кіберзахисті: як Альянс допомагає Україні вберегтися від хакерських атак РФ // [Електронний ресурс]. Режим доступу: https://www.eurointegration.com.ua/articles/2022/07/6/7142651/

5. Остроухов В. В., Присяжнюк М. М. Соціально-орієнтовані та загальнодоступні

ресурси мережі Інтернет в інформаційній війні проти України. Інформаційна безпека людини, суспільства, держави: Науково-практичний журнал. Київ : НА СБ України, №.1-3 (28-30). 2021. С.56-64.

6. Шпачук В. Суб'єкти державного управління кібербезпекою країни: зарубіжний досвід. Державне управління: удосконалення та розвиток. 2019. №2. // [Електронний ресурс]. URL: http://www.dy.nayka.com.ua/pdf/2_2019/7.pdf

7. Кращі практики управління кібербезпекою: оглядовий звіт. Проект ЄС - ПРООН з парламентської реформи. 2019. 129 с.

8. Інформаційно-психологічне протиборство: підручник. Видання третє доповнене та перероблене / [В.М. Петрик, В.В. Бедь, М.М. Присяжнюк та ін.]; за заг. ред. В. В. Бедя. Київ : ПАТ "ВІПОЛ", 2018. 388 с.

9. Кібербезпека: світові тенденції та виклики для України аналітична доповідь / Д. В. Дубов, М. А. Ожеван. Київ : НІСД, 2017. 30 с.

10. Забезпечення інформаційної безпеки у провідних країнах світу: навч. посіб. / [В. М. Петрик, Д. С. Мельник, О. О. Бакалинський та ін.; за заг. ред. Петрика В. М.]. Київ : Вид-во ІСЗЗІ НТУУ «КПІ», 2014. 260 с.

11. Кіберпростір як новий вимір геополітичного суперництва: монографія / Дубов Д. В. Київ : НІСД, 2014. 328с.

12. Законодавство та стратегії у сфері кібербезпеки країн Європейського союзу США, Канади та інших. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром. 2014. 37 с. // [Електронний ресурс]. Режим доступу: https://infocenter.rada.gov.ua/uploads/documents/28982.pdf

13. Грицун О. О. Безпека в кіберпросторі: міжнародно-правові аспекти. // Науковий вісник Херсонського державного університету. Серія "Юридичні науки", 2014. Т. 4. Секція "Міжнародне право". С. 197-202.

ОСОБЛИВОСТІ ОЦІНЮВАННЯ

Визначається Порядком організації та проведення оцінювання успішності здобувачів вищої освіти Прикарпатського національного університету імені Василя Стефаника, введеним в дію наказом ректора Прикарпатського національного університету імені Василя Стефаника від 19 травня 2023 р. № 309. URL: https://efund.pnu.edu.ua/wp-content/uploads/sites/172/2023/09/poriadok-orhanizatsii-ta-provedennia-otsiniuvannia-uspishnosti-zdobuvachiv-vyshchoi-osvity.pdf, а також Методичними рекомендаціями до порядку оцінювання успішності здобувачів вищої освіти у навчально-науковому юридичному інституті (далі - МРПОУ), затвердженими Вченою радою навчально-наукового юридичного інституту Прикарпатського національного університету імені Василя Стефаника, протокол №13 від 27 червня 2024 року) https://law.pnu.edu.ua/wp-content/uploads/sites/100/2024/11/metodychni-rekomendatsii-pro-poriadok-otsiniuvannia-uspishnosti.pdf

Вивчення дисципліни передбачає обов'язкове виконання всіма студентами письмової контрольної роботи, яка виконується на 9-му семінарському занятті. На контрольну виноситься 1 описове завдання, яке оцінюється в 6 балів, 1 коротке завдання нормативного змісту, яке оцінюється в 6 балів та 8 тестових запитань, кожне з яких оцінюється в 1 бал. Максимальний бал за контрольну становить 50.

Система оцінювання семінарських занять визначена п.п. 4.4.3.2, 4.4.3.3 Положення про порядок організації навчального процесу та оцінювання успішності студентів у навчально-науковому юридичному інституті Прикарпатського національного університету імені Василя Стефаника.

,

ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Алієв Р., Панасевич, Л. Юридична відповідальність у контексті національної безпеки та оборони України. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи: IV міжнар. наук.-практ. конф.* 2023. С. 144-147. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/18540/1/2_5300948988634084300.pdf#page=145

2. Бабанін С. В. Кіберзлочинність. *Вісник Асоціації кримінального права України*. 2016. Т. 1, № 5. С. 468–470. URL: http://vakp.nlu.edu.ua/article/view/173523

3. Білан І. А. Кібертероризм: інформаційно-правовий аспект. Інформація і право. 2023. № 4(47) С. 64-71. DOI: https://doi.org/10.37750/2616-6798.2023.4(47).291584 Режим доступу: http://il.ippi.org.ua/article/view/291584

4. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / [В. Л. Бурячок, Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора Б. Толубка. Київ : ДУТ, 2015. 288 с.

5. Бутузов В.М., Василинчук В.І. Протидія комп'ютерній злочинності в Україні: системно-структурний аналіз: монографія. Київ: КНТ, 2021. 408 с.

6. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»:стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1–2 (10–11). С. 276–282.

7. Гавва С. К., Головко С. Г. Сучасний кібертероризм як загроза національній безпеці. Національний авіаційний університет. 2023. Ст. 54-56.

8. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації.* 2013. № 2. С. 118-129.

9. Гончаренко В. А. До проблеми визначення та розмежування дефініцій "інформаційна безпека" і "кібербезпека". *Аналітично-порівняльне правознавство.* 2024. №5. С. 466-471. URL: https://doi.org/10.24144/2788-6018.2024.05.73

10. Горбулін В. П, Качинський А. Б. Засади національної безпеки України: підручник для студ. вищих навч. закл. / Інститут проблем національної безпеки. Київ: Інтертехнологія, 2009. 270 с.

11. Грицун О. О. Безпека в кіберпросторі: міжнародно-правові аспекти. // Науковий вісник Херсонського державного університету. Серія “Юридичні науки”, 2014. Т. 4. Секція “Міжнародне право”. С. 197-202.

12. Гудман Д. Міжнародна співпраця у протидії кіберзлочинності. Лондон: Academic Press, 2018. 320 с.

13. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

14. Дубов. Д. В. Стратегічні аспекти кібербезпеки України. // Стратегічні пріоритети. 2013. №4. С. 119-127.

15. Забезпечення інформаційної безпеки у провідних країнах світу: навч. посіб. / [В. М. Петрик, Д. С. Мельник, О. О. Бакалинський та ін.; за заг. ред. Петрика В. М.]. Київ : Вид-во ІСЗЗІ НТУУ «КПІ», 2014. 260 с.

16. Закон України “Про національну безпеку України”, від 21 червня 2018 року № 2469-VIII // Відомості Верховної Ради. 2018. № 31. Ст. 241.

17. Закон України “Про основні засади забезпечення кібербезпеки України”, прийнятий 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради. 2017. № 45. Ст. 403.

18. Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-

20#Text.

19. Закон України від 16.12.2020 № 1089-IX «Про електронні комунікації» // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20#n2246.

20. Закон України від 22 травня 2003 року № 851-IV «Про електронні документи та електронний документообіг» // [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15#Text .

21. Закон України від 21 січня 1994 року № 3855-XII «Про державну таємницю» // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text

22. Законодавство та стратегії у сфері кібербезпеки країн Європейського союзу США, Канади та інших. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром. 2014. 37 с. // [Електронний ресурс]. Режим доступу: https://infocenter.rada.gov.ua/uploads/documents/28982.pdf

23. Зінченко О. І. Європейська регіональна система протидії кібертероризму: політичні, інституційні та правові механізми. Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Питання політології». Вип. 39. 2021. С. 118-122. URL: https://periodicals.karazin.ua/politology/article/view/17813

24. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. Київ : Вид-во “Ліра-К”, 2021. 412 с.

25. Інформаційно-психологічне протиборство: підручник. Видання третє доповнене та перероблене / [В.М. Петрик, В.В. Бедь, М.М. Присяжнюк та ін.]; за заг. ред. В. В. Бедя. Київ : ПАТ “ВІПОЛ”, 2018. 388 с.

26. Калініченко О. НАТО на кіберзахисті: як Альянс допомагає Україні вберегтися від хакерських атак РФ // [Електронний ресурс]. Режим доступу: https://www.eurointegration.com.ua/articles/2022/07/6/7142651/

27. Кібербезпека: світові тенденції та виклики для України аналітична доповідь / Д. В. Дубов, М. А. Ожеван. Київ : НІСД, 2017. 30 с.

28. Кіберпростір як новий вимір геополітичного суперництва: монографія / Дубов Д. В. Київ : НІСД, 2014. 328 с.

29. Клімов В. Правові основи боротьби з кіберзлочинами у країнах ЄС. Прага: EU Law, 2019. 200 с.

30. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній: практичний посібник. Київ : Консалтингова компанія «СІДКОН», 2021. 372 с.

31. Конвенція про кіберзлочинність: Закон України від 07.09.2005. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575#Text

32. Кондратьєв В. Перспективи притягнення до відповідальності за скоєння воєнних кіберзлочнів. *Актуальні проблеми міжнародного та європейського права. погляд молодих вчених*, С. 139-142. URL: https://intrel.lnu.edu.ua/wp-content/uploads/2023/11/Materialy-konferentsii-19-zhovtnia-2023.pdf#page=139

33. Конституція України : прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. Київ : Преса України, 1997. 80 с.

34. Котляров В. Кібертероризм як загроза міжнародній безпеці. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2023. Випуск 5 (71). С. 46-54.

35. Кращі практики управління кібербезпекою: оглядовий звіт. Проект ЄС - ПРООН з парламентської реформи. 2019. 129 с.

36. Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

37. Лугівська Л., Яцишин О, Любавіна В. Тенденції розвитку кримінальної відповідальності за кіберзлочини в умовах цифровізації суспільства. Dictum factum, 2024, 2 (16): С. 258—264. DOI:https://doi.org/10.32703/2663-6352/2024-2-16-258-

264URL:https://df.duit.in.ua/index.php/dictum/article/view/363/326

38. Лупай А., Павлюх О, Павлюх А Актуальність питання боротьби з кіберзлочинністю як складова загальнокримінальної злочинності. Ірпінський юридичний часопис. 2023. С. 211-218. DOI: https://doi.org/10.33244/2617-4154-3(12)-2023-211-218 URL:https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/137

39. Луценко Ю.В., Тарасюк А.В., Денисенко М.М. Кібербезпека та інформаційна безпека: співвідношення понять. Юридичний науковий електронний журнал. 2022. №8. С. 320-323. URL: https://doi.org/10.32782/2524-0374/2022-8/70

40. Марущак А. І. Методи правового регулювання безпеки особи, суспільства, держави в інформаційній сфері. // Вісник Національної академії правових наук України. 2019. № 3. С. 75-89.

41. Марущак А. І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. // Інформація і право. 2018. № 3.С. 104-110.

42. Мельник Д. С. Комп'ютерні злочини: проблеми виділення та кваліфікації. *Міжнародний науковий журнал «Інтернаука»*. Київ, 2021, вип. 4 (104), С. 59-62. URL: https//doi.org/10.25313/2520-2057-2021-4-7055.

43. Мельник Д. С. Захист національної критичної інформаційної інфраструктури: актуальні проблеми та шляхи вирішення. «*Адміністративне право і процес»:* науково-практичний журнал. Київ, 2022. №3(38)/2022. С. 5-16.

44. Науково-практичний коментар Розділу XVI КК України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" (статті 362 - 363, висновки, словник) / [О.О. Климчук, Р.В. Макуха, Д.С. Мельник; за заг. ред. О.О. Климчука]. Київ : Центр навч.-наук. та наук.-практ. НА СБУ, 2014. 88 с.

45. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України"; станом на 01.01.2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

46. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навч. посіб. для вищих навч. закладів / Українська Академія держ. управління при Президентові України; Академія держ. податкової служби України. Київ : Преса України, 2000. 304 с.

47. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / [Бутузов В. М., Гавловський В. Д., Скалозуб Л. П. та ін.; за ред. Є. Д. Скулиша]. Київ, 2011. 404 с.

48. Остроухов В. В., Присяжнюк М. М. Соціально-орієнтовані та загальнодоступні ресурси мережі Інтернет в інформаційній війні проти України. Інформаційна безпека людини, суспільства, держави: Науково-практичний журнал. Київ : НА СБ України, №.1-3 (28-30). 2021. С.56-64.

49. Постанова КМ України «Деякі питання об'єктів критичної інфраструктури» від 09.10.2020 № 1109. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

50. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. / [кол. авторів: О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.; за заг. ред. В. В. Коваленка]. Київ : Вид. дім "Скіф", 2012. 728 с.

51. Рульов І. Співвідношення кібертероризму та кіберзлочину. Юридичний вісник. 2021. № 3. С. 178–185. URL: https://dspace.onua.edu.ua/items/f7f84fc6-620d-4f9c-ae6b-dcd46b208485

52. Русецький А. А., Куцолабський Д. А. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74–78. URL: file:///C:/Users/Admin/Downloads/Pib_2017_1_15.pdf

53. Свердлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук*.

2022. № 10. С. 175–188. URL: https://doi.org/10.31866/2616-7654.10.2022.269495

54. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року No 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовт-ня 2021 року «Про Стратегію інформаційної безпеки»». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14

55. Указ Президента України від 14 травня 2021 року № №447/2021 "Про Стратегію кібербезпеки України" // [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/4472021-40013 .

56. Указ Президента України «Про Концепцію забезпечення національної системи стійкості» від 27 вересня 2021 року №479/2021. // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/n0065525-21#Text.

57. Філіпова Т. Проблеми протидії кіберзлочинності в Україн. Київ: Генеза, 2020. 280 с.

58. Шевченко О. Вдосконалення кримінального законодавства України у сфері кіберзлочинності. Харків: Основа, 2021. 210 с.

59. Шпачук В. Суб'єкти державного управління кібербезпекою країни: зарубіжний досвід. Державне управління: удосконалення та розвиток. 2019. №2. // [Електронний ресурс]. URL: http://www.dy.nayka.com.ua/pdf/2_2019/7.pdf

60. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. 2022. DOI https://doi.org/10.32782/2524-0374/2022-12/96

URL: http://www.lsej.org.ua/12_2022/96.pdf

61. Conway Maura. Cyberterrorism: the story so far. Journal of Information Warfare. 2003. Vol. 2. No. 2. P. 33-42.

62. Lee Jarvis, Stuart Macdonald. What Is Cyberterrorism? Findings From a Survey of Researchers. Terrorism and Political Violence. 2015. Volume 27. Isuue 4. P. 657-678. URL: https://sci-hub.se/10.1080/09546553.2013.847827

63. Stuart Macdonald, Lee Jarvis, Simon M. Lavis. Cyberterrorism Today? Findings From a Follow-on Survey of Researchers. Studies in Conflict & Terrorism. 2019. Volume 5. Issue 8. P. 727-752. URL: https://sci-hub.se/10.1080/1057610X.2019.1696444