7МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра кібербезпеки та DATA-технологій, факультет № 6

МЕТОДИЧНІ МАТЕРІАЛИ ДО ПРАКТИЧНИХ ЗАНЯТЬ

з навчальної дисципліни
«Управління кібербезпекою об'єктів критичної інфраструктури»
обов’язкових компонент
освітньої програми другого (магістерського) рівня вищої освіти

125 "Кібербезпека" (Безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 27.11.2023 № 10

СХВАЛЕНО
Вченою радою
факультету № 6
Протокол від 15.11.2023 №10

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 24.11.2023 № 10

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 (протокол від 14.11.2023 № 11/1).

Розробник:
Доцент кафедри кібербезпеки та DATA-технологій факультету № 6, кандидат наук з державного управління, доцент Онищенко Ю.М.

Рецензенти:
1. Завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, доктор технічних наук, професор Петров К.Е.
2. Доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент Світличний В.А.

1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		Лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2						
Тема № 1. Теоретичні засади запобігання і протидії проявам кіберзлочинності	28	4	4		20	**екзамен**
Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	32	6	6		20	
Тема № 3. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану	32	6	6		20	
Тема № 4 Організаційно-правові аспекти забезпечення кібербезпеки об’єктів критичної інфраструктури України	32	6	6		20	
Тема № 5. Вимоги до кіберзахисту об’єктів критичної інфраструктури	32	6	6		20	
Тема № 6. Зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури	24	2	2		20	
Всього за семестр № 2	**180**	**30**	**30**		**120**	

2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		Лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2						
Тема № 1. Теоретичні засади запобігання і протидії проявам кіберзлочинності	29	1	1		27	**екзамен**
Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	30	2	1		27	
Тема № 3. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану	30	2	1		27	
Тема № 4 Організаційно-правові аспекти забезпечення кібербезпеки об’єктів критичної інфраструктури України	31	2	2		27	
Тема № 5. Вимоги до кіберзахисту об’єктів критичної інфраструктури	31	2	2		27	
Тема № 6. Зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури	29	1	1		27	
Всього за семестр № 2	**180**	**10**	**8**		**162**	

3. Методичні вказівки до практичних занять

Тема № 1.Теоретичні засади запобігання і протидії проявам кіберзлочинності

Навчальна мета заняття: отримати знання про взаємозв'язок злочинності та інформаційних технологій та поняття глобального кіберпростору.

Кількість годин: 4 год.

Навчальні питання

1. Взаємозв'язок злочинності та інформаційних технологій
2. Поняття глобального кіберпростору

Література:

Основна:

1. Текст лекції № 1 з навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури».
2. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України»/Верховна Рада України. URL:http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 26.10.2022).
3. Про кіберзлочинність: конвенція Ради Європи від 07.09.2005 ратифікована Верховною Радою України 07.09.2005 URL:http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 26.10.2022).
4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016. – URL:http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 26.10.2022).
5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021. – URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 26.10.2022).
6. Онищенко Ю.М. Державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації. дис. канд. наук з держ. управ: 25.00.02. Харків, 2015. 200 с.
7. Кравцова М.О. Запобігання кіберзлочинності в Україні: монографія / М.О. Кравцова, О.М. Литвинов / [За загальною редакцією д-ра юрид. наук, проф. О.М. Литвинова]. – Харків: Панов, 2016. – 212 с.
8. Орлов О.В. Удосконалення механізмів реалізації державної політики у сфері боротьби з кіберзлочинністю в Україні / О.В. Орлов, Ю.М. Онищенко // Публічне управління: науковий журнал Академії державного управління Республіки Арменія. – 2014. – № 1-2/2014. – 42 с.
9. Гуцалюк М. Сучасні тенденції організованої кіберзлочинності. Інформація і право. № 1(28)/2019. С. 118-128.

Додаткова:

10. Про національну безпеку України: Закон України від 21.06.2018 № 2469. Відомості Верховної Ради. 2018. № 31. Ст. 241.
11. Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року “Про організацію планування в секторі безпеки і оборони України”: Указ Президента України від 16.05.2019 № 225/2019. URL: https://zakon.rada.gov.ua/laws/show/225/2019#n2 (дата звернення:

26.10.2022).
12. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”: Указ Президента України від 14.09.2020 №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 26.10.2022).
13. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: Постанова Кабінету Міністрів України від 11.11.2020 № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text (дата звернення: 26.10.2022).
14. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85: від 10.11.2015. К.: Національна поліція України, 2015. 9 с.
15. Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво: Закон України від 12.07.2017 № 2129. URL: https://zakon.rada.gov.ua/laws/show/2129-19#n2 (дата звернення: 26.10.2022).
16. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/ activities-services/main-reports/internet-organised-crime-threat-assessment (дата звернення: 26.10.2022).

Інформаційні ресурси в інтернеті:

17. http://www.niss.gov.ua/
18. https://cyberpolice.gov.ua/
19. https://cip.gov.ua/ua
20. https://cert.gov.ua/
21. https://ssu.gov.ua/
22. https://www.president.gov.ua/

Матеріально-технічне забезпечення: комп’ютерна мережа з підключенням до Internet.

План проведення заняття

І. Порядок проведення вступу до заняття.

Ознайомитися з текстом лекції № 1 з навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури», Законом України «Про основні засади забезпечення кібербезпеки України», Конвенцією Ради Європи «Про кіберзлочинність», «Стратегію кібербезпеки України».

ІІ. Порядок проведення основної частини заняття.

Опрацювати текст лекції № 1, створивши стислий конспект лекції в електронному виді.

Користуючись текстом лекції, літературою до лекції (зі списку літератури) сформулювати розгорнуті відповіді на загальні запитання:

1. Аспекти взаємозв'язку злочинності та інформаційних технологій.

2. Співвідношення глобалізації інформаційних процесів та кіберзлочинності.
3. Позитивні та негативні наслідки поширення комп'ютерних технологій.
4. Темпи розвитку всесвітньої мережі Інтернет.
5. Превентивні можливості глобальних інформаційних мереж.
6. Транснаціональна злочинність: визначення, причини виникнення, тенденції.
7. Що належить до комп'ютерних злочинів згідно з міжнародними класифікаторами
8. Напрями використання кібертерористами глобальної мережі Інтернет.
9. Соціально-психологічний аспект глобальної мережі Інтернет.
10. Незаконний контент у глобальній мережі Інтернет: види, способи розповсюдження.
11. Напрями використання інформаційних технологій органами державної влади.
12. Напрями використання інформаційних технологій правоохоронними органами США.
13. Напрями використання інформаційних технологій правоохоронними органами України.
14. Наведіть характеристику дефініції кіберпростір.
15. Ознаки кіберпростору.
16. Шляхи вирішення питання щодо регулювання мережі Інтернет і, відповідно, визначення повноважень держави в цій сфері.
17. Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини».
18. Як Конвенція Ради Європи «Про кіберзлочинність» визначає види комп'ютерних злочинів “у чистому вигляді”?
19. Як Конвенція Ради Європи «Про кіберзлочинність» визначає скоювані за допомогою комп'ютера (computer-facilitated) злочини?
20. Характеристика дефініції кіберзлочинність.
21. Наведіть визначення поняття кіберпростір.
22. Наведіть визначення поняття кіберзлочин.
23. Наведіть визначення поняття кіберзлочинність.

III. Порядок проведення заключної частини заняття.

Здобувачі освіти після опрацювання тексту лекції № 1 та виконання завдань самостійної роботи зобов’язані пройти контрольне тестування за темою.

Викладач перевіряє у здобувачів результати виконання поставлених задач, виставляє відповідні оцінки; зазначає перелік задач для самостійної роботи, вказує час і спосіб перевірки результатів самостійної роботи; оголошує тему наступного заняття.

Тема № 2. Засади забезпечення кібербезпеки України

Навчальна мета заняття: отримати знання про поняття кібербезпеки і кіберзахисту, суб'єктів забезпечення кібербезпеки в Україні, національну систему кібербезпеки, нормативно-правову базу протидії кіберзлочинності.

Кількість годин: 6 год.

Навчальні питання

1. Поняття кібербезпеки і кіберзахисту.
2. Суб'єкти забезпечення кібербезпеки в Україні.
3. Національна система кібербезпеки.
4. Нормативно-правова база протидії кіберзлочинності.

Література:

Основна:

1. Текст лекції № 2 з навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури».
2. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України»/Верховна Рада України. URL:http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 26.10.2022).
3. Про кіберзлочинність: конвенція Ради Європи від 07.09.2005 ратифікована Верховною Радою України 07.09.2005 URL:http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 26.10.2022).
4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016. – URL:http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 26.10.2022).
5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021. – URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 26.10.2022).
6. Онищенко Ю.М. Державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації. дис. канд. наук з держ. управ: 25.00.02. Харків, 2015. 200 с.
7. Кравцова М.О. Запобігання кіберзлочинності в Україні: монографія / М.О. Кравцова, О.М. Литвинов / [За загальною редакцією д-ра юрид. наук, проф. О.М. Литвинова]. – Харків: Панов, 2016. – 212 с.
8. Орлов О.В. Совершенствование механизмов реализации государственной политики в сфере борьбы с киберпреступностью в Украине / О.В. Орлов, Ю.М. Онищенко // Публічне управління: науковий журнал Академії державного управління Республіки Арменія. – 2014. – № 1-2/2014. – 42 с.
9. Гуцалюк М. Сучасні тенденції організованої кіберзлочинності. Інформація і право. № 1(28)/2019. С. 118-128.

Додаткова:

10. Про національну безпеку України: Закон України від 21.06.2018 № 2469. Відомості Верховної Ради. 2018. № 31. Ст. 241.
11. Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року “Про організацію планування в секторі безпеки і оборони України”: Указ Президента України від 16.05.2019 № 225/2019. URL: https://zakon.rada.gov.ua/laws/show/225/2019#n2 (дата звернення: 26.10.2022).
12. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”: Указ Президента України від 14.09.2020 №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 26.10.2022).
13. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: Постанова Кабінету Міністрів України від 11.11.2020 № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text (дата звернення: 26.10.2022).
14. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85: від 10.11.2015. К.: Національна поліція України, 2015. 9 с.
15. Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво: Закон України від 12.07.2017 № 2129. URL: https://zakon.rada.gov.ua/laws/show/2129-19#n2 (дата звернення: 26.10.2022).
16. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/ activities-services/main-reports/internet-organised-crime-threat-assessment (дата звернення: 26.10.2022).

Інформаційні ресурси в інтернеті:

17. http://www.niss.gov.ua/
18. https://cyberpolice.gov.ua/
19. https://cip.gov.ua/ua
20. https://cert.gov.ua/
21. https://ssu.gov.ua/
22. https://www.president.gov.ua/

Матеріально-технічне забезпечення: комп’ютерна мережа з підключенням до Internet.

План проведення заняття

І. Порядок проведення вступу до заняття.

Ознайомитися з текстом лекції № 2 з навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури», Законом України «Про основні засади забезпечення кібербезпеки України», Конвенцією Ради Європи

«Про кіберзлочинність», «Стратегію кібербезпеки України», Положенням про Департамент кіберполіції Національної поліції України.

ІІ. Порядок проведення основної частини заняття.

Опрацювати текст лекції 2, створивши стислий конспект лекції в електронному виді.

Користуючись текстом лекції, літературою до лекції (зі списку літератури) сформулювати розгорнуті відповіді на загальні запитання:

1. Що складає правову основу забезпечення кібербезпеки України?
2. Який Закон України визначає засади забезпечення кібербезпеки України?
3. Наведіть визначення поняття кібербезпеки.
4. Що належить до об’єктів кібербезпеки?
5. Наведіть визначення поняття кіберзахисту.
6. Що належить до об’єктів кіберзахисту?
7. Визначення терміну об’єкт критичної інформаційної інфраструктури.
8. Визначення терміну система управління технологічними процесами.
9. Які об’єкти можуть бути віднесені до критичної інфраструктури?
10. Надайте визначення та характеристику поняття кіберпростір.
11. Надайте визначення та характеристику поняття інцидент кібербезпеки (кіберінцидент).
12. Надайте визначення та характеристику поняття кібератака.
13. Надайте визначення та характеристику поняття кіберзагроза.
14. Надайте визначення та характеристику поняття кібероборона.
15. Надайте визначення та характеристику поняття кіберзагроз.
16. Визначення терміну кіберрозвідка.
17. Визначення терміну кібершпигунство.
18. Визначення терміну кібертероризм.
19. Хто здійснює координацію діяльності у сфері кібербезпеки в Україні?
20. Хто забезпечує формування та реалізацію державної політики у сфері кібербезпеки в Україні?
21. Суб’єкти забезпечення кібербезпеки.
22. Завдання суб’єктів національної системи кібербезпеки.
23. Надайте визначення та характеристику поняття Національна телекомунікаційна мережа.
24. Надайте визначення та характеристику поняття Національні електронні інформаційні ресурси.
25. Надайте визначення та характеристику поняття системи електронних комунікацій.
26. Наведіть основні завдання Департаменту кіберполіції.
27. Наведіть основні функції Департаменту кіберполіції.
28. Надайте визначення та характеристику поняття національна система кібербезпеки.
29. Наведіть основні завдання у сфері забезпечення кібербезпеки Державної служби спеціального зв’язку та захисту інформації України.

30. Наведіть основні завдання у сфері забезпечення кібербезпеки Національної поліції України.
31. Наведіть основні завдання у сфері забезпечення кібербезпеки Служби безпеки України.
32. Наведіть основні завдання у сфері забезпечення кібербезпеки Міністерства оборони України, Генерального штабу Збройних Сил України.
33. Наведіть основні завдання у сфері забезпечення кібербезпеки розвідувальних органів України.
34. Наведіть основні завдання у сфері забезпечення кібербезпеки Національного банку України.
35. Проведенням яких заходів забезпечується функціонування національної системи кібербезпеки?
36. У чому полягають застереження, з якими Україна ратифікувала Конвенцію «Про кіберзлочинність»?
37. Наведіть юрисдикцію щодо кіберзлочинів згідно Конвенції «Про кіберзлочинність».
38. Яким чином у Конвенції «Про кіберзлочинність» висвітлено принципи міжнародного співробітництва країн-учасниць у сфері протидії кіберзлочинності?
39. У чому полягає процедура екстрадиції?
40. Наведіть визначення OSINT та ставлення Конвенції «Про кіберзлочинність» до даного методу збору інформації.

ІІІ. Порядок проведення заключної частини заняття.

Здобувачі освіти після опрацювання тексту лекції № 2 та виконання завдань самостійної роботи зобов'язані пройти контрольне тестування за темою.

Викладач перевіряє у здобувачів результати виконання поставлених задач, виставляє відповідні оцінки; зазначає перелік задач для самостійної роботи, вказує час і спосіб перевірки результатів самостійної роботи; оголошує тему наступного заняття.

Тема № 3. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану

Навчальна мета заняття: отримати знання про поняття кібербезпеки і кіберзахисту, суб'єктів забезпечення кібербезпеки в Україні, національну систему кібербезпеки, нормативно-правову базу протидії кіберзлочинності.

Кількість годин: 10 год.

Навчальні питання

1. Можливі державні механізми боротьби з кіберзлочинністю
2. Проблеми захисту інформації від несанкціонованого доступу
3. Можлива структура державного механізму взаємодії у сфері боротьби з кіберзлочинністю

4. Напрями розвитку системи запобігання кіберзлочинності в Україні

Література:

Основна:

1. Текст лекції № 3 з навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури».
2. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України»/Верховна Рада України. URL:http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 26.10.2022).
3. Про кіберзлочинність: конвенція Ради Європи від 07.09.2005 ратифікована Верховною Радою України 07.09.2005 URL:http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 26.10.2022).
4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016. – URL:http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 26.10.2022).
5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021. – URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 26.10.2022).
6. Онищенко Ю.М. Державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації. дис. канд. наук з держ. управ: 25.00.02. Харків, 2015. 200 с.
7. Кравцова М.О. Запобігання кіберзлочинності в Україні: монографія / М.О. Кравцова, О.М. Литвинов / [За загальною редакцією д-ра юрид. наук, проф. О.М. Литвинова]. – Харків: Панов, 2016. – 212 с.
8. Орлов О.В. Удосконалення механізмів реалізації державної політики у сфері боротьби з кіберзлочинністю в Україні / О.В. Орлов, Ю.М. Онищенко // Публічне управління: науковий журнал Академії державного управління Республіки Арменія. – 2014. – № 1-2/2014. – 42 с.
9. Гуцалюк М. Сучасні тенденції організованої кіберзлочинності. Інформація і право. № 1(28)/2019. С. 118-128.

Додаткова:

10. Про національну безпеку України: Закон України від 21.06.2018 № 2469. Відомості Верховної Ради. 2018. № 31. Ст. 241.
11. Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року “Про організацію планування в секторі безпеки і оборони України”: Указ Президента України від 16.05.2019 № 225/2019. URL: https://zakon.rada.gov.ua/laws/show/225/2019#n2 (дата звернення: 26.10.2022).
12. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”: Указ Президента

України від 14.09.2020 №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 26.10.2022).
13. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: Постанова Кабінету Міністрів України від 11.11.2020 № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text (дата звернення: 26.10.2022).
14. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85: від 10.11.2015. К.: Національна поліція України, 2015. 9 с.
15. Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво: Закон України від 12.07.2017 № 2129. URL: https://zakon.rada.gov.ua/laws/show/2129-19#n2 (дата звернення: 26.10.2022).
16. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/ activities-services/main-reports/internet-organised-crime-threat-assessment (дата звернення: 26.10.2022).

Інформаційні ресурси в інтернеті:

17. http://www.niss.gov.ua/
18. https://cyberpolice.gov.ua/
19. https://cip.gov.ua/ua
20. https://cert.gov.ua/
21. https://ssu.gov.ua/
22. https://www.president.gov.ua/

Матеріально-технічне забезпечення: комп’ютерна мережа з підключенням до Internet.

План проведення заняття

І. Порядок проведення вступу до заняття.

Ознайомитися з текстом лекції № 3 з навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури», Законом України «Про основні засади забезпечення кібербезпеки України», Конвенцією Ради Європи «Про кіберзлочинність», «Стратегію кібербезпеки України», Положенням про Департамент кіберполіції Національної поліції України.

ІІ. Порядок проведення основної частини заняття.

Опрацювати текст лекції 3, створивши стислий конспект лекції в електронному виді.

Користуючись текстом лекції, літературою до лекції (зі списку літератури) сформулювати розгорнуті відповіді на загальні запитання:

1. Наведіть основні умови для забезпечення функціонування вільної та безпечної глобальної мережі Інтернет.

2. Наведіть основні пропозиції вирішення проблеми національної кібербезпеки.
3. Наведіть першочергові кроки України на шляху забезпечення кібербезпеки.
4. Наведіть основні складові кібербезпеки та надайте їх характеристику.
5. Що має визначати типова політика кібербезпеки держави?
6. Наведіть основні вимоги до національної політики кібербезпеки держави.
7. Які положення має містити стратегія кібербезпеки держави?
8. Значення CERT у забезпеченні кібербезпеки держави?
9. Завдання CERT-UA.
10. Державно-приватне партнерство у сфері забезпечення кібербезпеки держави: визначення, принципи, першочергові завдання.
11. Співпраця між органами державно влади, які опікуються питаннями кібербезпеки держави: визначення, принципи, першочергові завдання.
12. Що вимагає створення національного потенціалу держави для усунення кіберінцидентів?
13. У чому полягає реалізація механізму координації в системі державного управління ?
14. У чому полягає реалізація практики обміну інформацією у сфері забезпечення кібербезпеки між приватним сектором і урядовими органами?
15. Принципи застосування законодавства у сфері кібербезпеки.
16. Принципи забезпечення кібербезпеки.
17. Міжнародне співробітництво у сфері кібербезпеки.
18. Контроль за законністю заходів із забезпечення кібербезпеки України.
19. Запобігання та протидія кіберзлочинності як об’єкт державного управління в умовах глобалізації.
20. Зарубіжний досвід щодо реалізації державних механізмів у галузі запобігання та боротьби з кіберзлочинністю.
21. Особливості організаційних та нормативно-правових засад боротьби з кіберзлочинністю.
22. Проблеми державного управління у сфері запобігання проявам кіберзлочинності.
23. Напрями розв'язання проблеми проявів кіберзлочинності.
24. Моделі державних механізмів боротьби з кіберзлочинністю.
25. Напрями впорядкування правового підґрунтя діяльності та взаємовідносин в організаційно-функціональній структурі суб’єктів протидії кіберзлочинності.
26. Система запобігання кіберзлочинності в Україні.

ІІІ. Порядок проведення заключної частини заняття.

Здобувачі освіти після опрацювання тексту лекції 3 та виконання завдань самостійної роботи зобов’язані пройти контрольне тестування за темою.

Викладач перевіряє у здобувачів результати виконання поставлених задач, виставляє відповідні оцінки; зазначає перелік задач для самостійної роботи, вказує час і спосіб перевірки результатів самостійної роботи; оголошує тему наступного заняття.

Тема № 4. Організаційно-правові аспекти забезпечення кібербезпеки об’єктів критичної інфраструктури України

Навчальна мета заняття: отримати знання про основні поняття, цілі, напрями, принципи, правові основи та суб’єктів державної політики у сфері захисту об'єктів критичної інфраструктури.

Кількість годин: 6 год.

Навчальні питання

1. Поняття та визначення у сфері захисту критичної інфраструктури України.
2. Основні цілі, напрями та принципи державної політики у сфері захисту об'єктів критичної інфраструктури.
3. Правові основи забезпечення безпеки об'єктів критичної інфраструктури.
4. Суб’єкти забезпечення безпеки об’єктів критичної інфраструктури.
5. Організаційні засади національної системи захисту критичної інфраструктури.

Література:

Основна:

1. Закон України «Про критичну інфраструктуру»: сподівання та реалії URL: https://uifuture.org/publications/zakon-ukrayiny-pro-krytychnu-infrastrukturu-spodivannya-ta-realiyi/

2. Закон України про критичну інфраструктуру: Закон України від 05.12.2022: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

3. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К.: НІСД, 2019. – 224 с. URL: http://zakon3.rada.gov.ua/laws/show/1009-2017-%D1%80 121.

4. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4 (37). С. 83–93.

5. Бобро Д.Г. Методологія оцінки рівня критичності об’єктів інфраструктури. Стратегічні пріоритети. 2016. № 3 (40). С. 77–86. URL: http://www.niss.gov.ua/public/File/Str_prioritetu/SP_3_40_16.pdf.

6. Бобро Д.Г. Удосконалення методології ранжування об’єктів критичної інфраструктури та їх віднесення до критичної інфраструктури: аналітична записка 2016. URL: http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf

7. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко та ін.; за заг. ред. д-ра

техн. наук, професора В.Б. Толубка. − К.: ДУТ, 2015. URL: https://duikt.edu.ua/uploads/l_1209_69915296.pdf

8. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: розпорядження Кабінету Міністрів України від 6 груд. 2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

9. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4 (37). С. 83-93.

10. Бобро Д.Г. Методологія оцінки рівня критичності об'єктів інфраструктури. Стратегічні пріоритети. 2016. № 3 (40). С. 77-86. URL: http://www.niss.gov.ua/public/File/Str_prioritetu/SP_3_40_16.pdf.

Додаткова:

11. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України (№2684-IX від 18.10.2022): URL: https://zakon.rada.gov.ua/laws/show/2684-20#n8.\

12. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики / Д. Бірюков // Наукові записки. – К.: Інститут політичних і етнонаціональних досліджень імені І.Ф. Кураса НАН України, 2013. – № 6 (68). – С. 106-115.

13. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4 (37). С. 83–93.

14. Домарацький М.Б. Нормативне й адміністративне забезпечення державного регулювання критичної інфраструктури в Україні: аналіз і оцінка / М.Б. Домарацький // Вісник Національного університету цивільного захисту України. – 2020. – Вип. 1(12). – С. 470–475. URL: https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disDomarackij.pdf

Матеріально-технічне забезпечення: комп'ютерна мережа з підключенням до Internet.

План проведення заняття

І. Порядок проведення вступу до заняття.

Ознайомитися з текстом лекції № 4 з навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури», Законом України «Про критичну інфраструктуру».

ІІ. Порядок проведення основної частини заняття.

Опрацювати текст лекції № 4, створивши стислий конспект лекції в електронному виді.

Користуючись текстом лекції, літературою до лекції (зі списку літератури) сформулювати розгорнуті відповіді на загальні запитання:

1. Чим фрагментарний підхід відрізняється від застосування цілісного підходу під час розбудови системи захисту ОКІ?
2. Що розуміється під терміном «критична інфраструктура»?
3. Що розуміється під терміном «безпека критичної інфраструктури»?
4. Що розуміється під терміном «життєво важливі функції та/або послуги»?
5. Що розуміється під терміном «захист критичної інфраструктури»?
6. Що розуміється під терміном «ідентифікація об’єкта критичної інфраструктури»?
7. Що розуміється під терміном «інцидент безпеки критичної інфраструктури»?
8. Що розуміється під терміном «категоризація об’єктів інфраструктури»?
9. Що розуміється під терміном «категорія критичності (критерії) об’єкта критичної інфраструктури»?
10. Що розуміється під терміном «кризова ситуація»?
11. Що розуміється під терміном «критична технологічна інформація»?
12. Що розуміється під терміном «національна система захисту критичної інфраструктури»?
13. Що розуміється під терміном «несанкціоноване втручання»?
14. Що розуміється під терміном «об’єкти критичної інфраструктури»?
15. Що розуміється під терміном «оператор критичної інфраструктури»?
16. Що розуміється під терміном «охорона об’єктів критичної інфраструктури»?
17. Що розуміється під терміном «паспорт безпеки»?
18. Що розуміється під терміном «проектна загроза об’єкту критичної інфраструктури»?
19. Що розуміється під терміном «реєстр об’єктів критичної інфраструктури»?
20. Що розуміється під терміном «режим функціонування критичної інфраструктури»?
21. Що розуміється під терміном «рівень критичності об’єкта критичної інфраструктури»?
22. Що розуміється під терміном «сектор критичної інфраструктури»?
23. Що розуміється під терміном «стійкість критичної інфраструктури»?
24. Що розуміється під терміном «стійкість критичної інфраструктури»?
25. Які види об'єктів вважаються критичною інфраструктурою в Україні?
26. Які загрози можуть ставитися перед об'єктами критичної інфраструктури?
27. За сукупністю яких критеріїв відбувається віднесення об’єктів до критичної інфраструктури?
28. З якою метою здійснюється категоризація об’єктів критичної інфраструктури?
29. Наведіть категорії критичності об’єктів критичної інфраструктури.
30. Ким здійснюється категоризація об’єктів критичної інфраструктури?

31. Наведіть які об'єкти можуть вважатися частинами критичної інфраструктури в Україні.
32. Наведіть основні засади державної політики у сфері захисту критичної інфраструктури.
33. Наведіть основні принципи формування захисту критичної інфраструктури в Україні.
34. Що є метою державної політики у сфері захисту критичної інфраструктури?
35. Що належить до основних завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури?
36. У яких режимах функціонування здійснюється забезпечення захисту та стійкості критичної інфраструктури?
37. Ким приймається Рішення про оголошення режимів функціонування критичної інфраструктури?
38. Хто належить до основних суб'єктів забезпечення безпеки об'єктів критичної інфраструктури?
39. Який підзаконний акт регламентує порядок визнання об’єкта критичною інфраструктурою?
40. Окресліть повноваження Верховної Ради України у сфері забезпечення захисту критичної інфраструктури суб’єкти державної системи захисту критичної інфраструктури.
41. Окресліть повноваження Президента України у сфері забезпечення захисту критичної інфраструктури суб’єкти державної системи захисту критичної інфраструктури.
42. Окресліть повноваження Кабінету Міністрів України у сфері забезпечення захисту критичної інфраструктури суб’єкти державної системи захисту критичної інфраструктури.
43. Окресліть повноваження Ради національної безпеки і оборони України у сфері забезпечення захисту критичної інфраструктури суб’єкти державної системи захисту критичної інфраструктури.
44. Хто забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури, координацію діяльності суб’єктів національної системи захисту критичної інфраструктури?
45. Наведіть основні завдання функціональних органів у сфері захисту критичної інфраструктури.
46. Наведіть основні завдання секторальних органів у сфері захисту критичної інфраструктури.
47. Наведіть основні завдання місцевих органів виконавчої влади та військово-цивільні адміністрації у сфері захисту критичної інфраструктури.
48. Наведіть основні права, обов’язки та завдання операторів критичної інфраструктури.
49. Які заходи захисту можуть бути вжиті для об'єктів критичної інфраструктури?

50. Які організації відповідають за захист об'єктів критичної інфраструктури в Україні?
51. Правові основи захисту об'єктів критичної інфраструктури в Україні.
52. Які основні принципи безпеки повинні бути враховані при захисті об'єктів критичної інфраструктури?
53. Які види кіберзагроз можуть становити небезпеку для об'єктів критичної інфраструктури?
54. Які стратегії реагування на інциденти пов'язані з захистом об'єктів критичної інфраструктури?
55. Які основні кроки потрібно здійснити для відновлення роботи об'єкта критичної інфраструктури після інциденту?
56. Які міжнародні стандарти і рекомендації визначають принципи захисту об'єктів критичної інфраструктури?
57. Які основні функції центрів керування кризових ситуацій, пов'язаних з захистом об'єктів критичної інфраструктури?
58. Які вимоги ставляться до персоналу, який займається захистом об'єктів критичної інфраструктури?
59. Які основні принципи фізичного захисту об'єктів критичної інфраструктури?
60. Які види контролю та моніторингу можуть застосовуватися для забезпечення безпеки об'єктів критичної інфраструктури?
61. Які юридичні наслідки проведення моніторингу рівня безпеки ОКІ?
62. Яким шляхом здійснюється взаємодія національної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки?
63. Яким шляхом здійснюється державно-приватне партнерство у сфері захисту критичної інфраструктури?
64. Хто і як часто здійснює зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України?
65. Яким чином здійснюється Громадський нагляд у сфері захисту критичної інфраструктури?

ІІІ. Порядок проведення заключної частини заняття.

Здобувачі освіти після опрацювання тексту лекції № 4 та виконання завдань самостійної роботи зобов’язані пройти контрольне тестування за темою.

Викладач перевіряє у здобувачів результати виконання поставлених задач, виставляє відповідні оцінки; зазначає перелік задач для самостійної роботи, вказує час і спосіб перевірки результатів самостійної роботи; оголошує тему наступного заняття.

Тема № 5. Вимоги до кіберзахисту об’єктів критичної інфраструктури

Навчальна мета заняття: отримати знання про загальні та базові вимоги до кіберзахисту об’єктів критичної інфраструктури.

Кількість годин: 6 год.

Навчальні питання

1. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури.
2. Базові вимоги із забезпечення кіберзахисту об’єктів критичної інфраструктури.

Література:

Основна:

1. Закон України про критичну інфраструктуру: Закон України від 05.12.2022: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
2. Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р Про схвалення Концепції створення державної системи захисту критичної інфраструктури URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text
3. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
4. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К.: НІСД, 2019. – 224 с. URL: http://zakon3.rada.gov.ua/laws/show/1009-2017-%D1%80 121.
5. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4 (37). С. 83–93.
6. Бобро Д.Г. Методологія оцінки рівня критичності об’єктів інфраструктури. Стратегічні пріоритети. 2016. № 3 (40). С. 77–86. URL: http://www.niss.gov.ua/public/File/Str_prioritetu/SP_3_40_16.pdf.
7. Бобро Д.Г. Удосконалення методології ранжування об’єктів критичної інфраструктури та їх віднесення до критичної інфраструктури: аналітична записка 2016. URL: http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf
8. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко та ін.; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. − К.: ДУТ, 2015. URL: https://duikt.edu.ua/uploads/l_1209_69915296.pdf
9. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4 (37). С. 83-93.
10. Бобро Д.Г. Методологія оцінки рівня критичності об’єктів інфраструктури. Стратегічні пріоритети. 2016. № 3 (40). С. 77-86. URL: http://www.niss.gov.ua/public/File/Str_prioritetu/SP_3_40_16.pdf.

Додаткова:

11. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України (№2684-IX від 18.10.2022): URL: https://zakon.rada.gov.ua/laws/show/2684-20#n8.\

12. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики / Д. Бірюков // Наукові записки. – К.: Інститут політичних і етнонаціональних досліджень імені І.Ф. Кураса НАН України, 2013. – № 6 (68). – С. 106-115.

13. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4 (37). С. 83–93.

14. Домарацький М.Б. Нормативне й адміністративне забезпечення державного регулювання критичної інфраструктури в Україні: аналіз і оцінка / М.Б. Домарацький // Вісник Національного університету цивільного захисту України. – 2020. – Вип. 1(12). – С. 470–475. URL: https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disDomarackij.pdf

Матеріально-технічне забезпечення: комп’ютерна мережа з підключенням до Internet.

План проведення заняття

І. Порядок проведення вступу до заняття.

Ознайомитися з текстом лекції № 5 з навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури», розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р «Про схвалення Концепції створення державної системи захисту критичної інфраструктури», Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури».

ІІ. Порядок проведення основної частини заняття.

Опрацювати текст лекції № 5, створивши стислий конспект лекції в електронному виді.

Користуючись текстом лекції, літературою до лекції (зі списку літератури) сформулювати розгорнуті відповіді на загальні запитання:

1. Окресліть основні проблеми у створенні системи захисту критичної інфраструктури, які потребують розв’язання.
2. Надайте визначення терміна критичні бізнес/операційні процеси об’єктів критичної інфраструктури.
3. Надайте визначення терміна система інформаційної безпеки.
4. Мета проведення незалежного аудиту інформаційної безпеки на ОКІ.
5. Хто має організовувати проведення незалежного аудиту інформаційної безпеки на ОКІ згідно з вимогами законодавства в сфері захисту інформації та кібербезпеки?

6. На чому ґрунтується технічне завдання на створення системи інформаційної безпеки?
7. Кого має невідкладно інформувати власник та/або керівник ОКІ у випадку настання комп'ютерної надзвичайної події?
8. Розшифруйте та надайте характеристику КСЗІ.
9. Хто забезпечує створення резервних копій інформаційних ресурсів ОКІІ ОКІ та критичних бізнес/операційних процесів ОКІ?
10. Що повинні забезпечувати організаційні та технічні заходи з кіберзахисту, які впроваджуються на ОКІІ ОКІ?
11. З урахуванням чого розробник КСЗІ ОКІІ ОКІ здійснює формування додаткових заходів із забезпечення кіберзахисту ОКІ?
12. Наведіть основні базові вимоги із забезпечення кіберзахисту об'єктів критичної інфраструктури
13. Основні вимоги до формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки.
14. Як на ОКІ оформлюються права та обов'язки всіх категорій користувачів та адміністраторів ОКІІ ОКІ, обов'язки адміністраторів з обслуговування компонентів ОКІІ ОКІ та забезпечення її інформаційної безпеки?
15. Як часто Власник/керівник ОКІ зобов'язаний організовувати та проводити обстеження своїх ОКІІ ОКІ з метою оновлення даних щодо програмно-апаратного складу ОКІІ ОКІ, технології обробки інформації на ОКІІ ОКІ, переліку критичних інформаційних ресурсів та компонентів ОКІІ ОКІ, які підлягають захисту?
16. Що має відбутися, якщо за результатами обстеження ОКІІ ОКІ виявлено, що на ОКІІ ОКІ змінено технологію обробки інформації, впроваджено нові програмні або апаратні компоненти, змінено перелік критичних інформаційних ресурсів та компонентів об'єкта, які підлягають захисту?
17. Що має здійснюватися у випадку виявлення нових загроз та/або ризиків? здійснюється оновлення технічного завдання на створення КСЗІ (системи інформаційної безпеки) ОКІІ ОКІ, іншої документації та впровадження оновлених вимог на ОКІІ ОКІ.
18. Наведіть приклади інформації, яка розкриває параметри та особливості функціонування компонентів ОКІІ ОКІ, і які в інтересах національної безпеки відносять до інформації з обмеженим доступом.
19. Що визначає політика інформаційної безпеки ОКІ?
20. Наведіть вимоги до провадження програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки на ОКІ.
21. Наведіть вимоги до переліку програмного та апаратного забезпечення, що використовується на ОКІІ ОКІ.
22. Наведіть вимоги до управління доступом користувачів та адміністраторів до об'єктів захисту ОКІІ ОКІ.
23. Що передбачає механізм розподілу прав доступу до ОКІІ ОКІ?
24. Наведіть вимоги до ідентифікації та автентифікації користувачів та адміністраторів ОКІІ ОКІ.

25. Наведіть вимоги до використання багатофакторної автентифікації користувачів та адміністраторів на ОКІ.
26. Наведіть вимоги до використання паролів, зокрема паролів за замовчуванням.
27. Які вимоги висуваються до обладнання, яке підключається до системи управління технологічними процесами ОКІ?
28. Наведіть вимоги до реєстрації подій компонентами ОКІІ ОКІ та їх періодичного аудиту.
29. Яку інформацію мають містити журнали реєстрації подій компонентів об’єкта?
30. Які вимоги до зберігання журналів реєстрації подій?
31. Наведіть вимоги до забезпечення мережевого захисту компонентів та інформаційних ресурсів ОКІІ ОКІ.
32. Наведіть вимоги до засобів мережевого захисту, які повинні бути встановлені у разі неможливості фізичного розділення зовнішньої мережі та ОКІІ ОКІ на межі (периметрі) між зовнішніми мережами, іншими інформаційно-комунікаційними системами, що обслуговують ОКІ.
33. Хто і як часто зобов’язаний проводити перевірку ефективності заходів щодо захисту ОКІІ ОКІ від зовнішнього проникнення шляхом виконання періодичних тестів на проникнення (Penetration test)?
34. Які є обмеження щодо використання на ОКІІ ОКІ технологій Wi-Fi та Bluetooth?
35. Наведіть вимоги до забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів ОКІІ ОКІ.
36. Наведіть вимоги до визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ ОКІ.
37. Наведіть вимоги до визначення умов використання програмного та апаратного забезпечення ОКІІ ОКІ.
38. Хто має право на встановлення або видалення програмного забезпечення на ОКІ?
39. Наведіть вимоги до визначення умов розміщення компонентів ОКІІ ОКІ
40. Наведіть вимоги до зберігання схем розміщення та підключення обладнання.

ІІІ. Порядок проведення заключної частини заняття.

Здобувачі освіти після опрацювання тексту лекції № 5 та виконання завдань самостійної роботи зобов’язані пройти контрольне тестування за темою.

Викладач перевіряє у здобувачів результати виконання поставлених задач, виставляє відповідні оцінки; зазначає перелік задач для самостійної роботи, вказує час і спосіб перевірки результатів самостійної роботи; оголошує тему наступного заняття.

Тема № 6. Зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури

Навчальна мета заняття: отримати знання про зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури.

Кількість годин: 2 год.

Навчальні питання

1. Передовий зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури.
2. Система забезпечення безпеки та стійкості критичної інфраструктури в США.
3. Система забезпечення безпеки та стійкості критичної інфраструктури у Великій Британії.
4. Система забезпечення безпеки та стійкості критичної інфраструктури у Польщі.
5. Висновки для України з огляду на зарубіжний досвід щодо державної системи забезпечення безпеки та стійкості критичної інфраструктури.
6. Організація підготовки кадрів і населення на державному рівні та в межах секторів критичної інфраструктури.
7. Особливості Національної системи планування США.

Література:

Основна:

1. Орлов О. В. Узагальнення міжнародного досвіду створення державної системи попередження та запобігання злочинам в мережі Інтернет / О.В. Орлов, Ю.М. Онищенко // Теорія та практика державного управління № 2(45) / 2014. – С. 212-219.
2. Мельников О.Ф. Реформування державних механізмів боротьби з кіберзлочинністю / О.Ф. Мельников, Ю.М. Онищенко // Теорія та практика державного управління: зб. наук. пр. – Х.: Вид-во ХарРІ НАДУ «Магістр», 2015. – Вип. 3(50). – С. 18-24.
3. Орлов О. В. Узагальнення міжнародного досвіду створення державної системи попередження та запобігання злочинам в мережі Інтернет / О.В. Орлов, Ю.М. Онищенко // Теорія та практика державного управління № 2(45) / 2014. – С. 212-219.
4. Онищенко Ю.М. Державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації. дис. канд. наук з держ. управ: 25.00.02. Харків, 2015. 200 с.
5. Бірюков Д.С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. Науково-інформаційний вісник Академії національної безпеки. 2015. № 3-4. С. 155-170.
6. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4 (37). С. 83–93.

7. Бобро Д.Г. Методологія оцінки рівня критичності об’єктів інфраструктури. Стратегічні пріоритети. 2016. № 3 (40). С. 77–86. URL: http://www.niss.gov.ua/public/File/Str_prioritetu/SP_3_40_16.pdf.
8. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко та ін.; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. − К.: ДУТ, 2015.
9. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз. 2018. URL: https://scholar.google.com.ua/citations?user=187UaFYAAAAJ&hl=uk
10. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк // Безпека інформації. − 2013. − Т. 19. − № 2. − С. 120. URL: http://nbuv.gov.ua/UJRN/bezin_2013_19_2_8
11. Гнатюк, С.О., Рябий, М.О., & Лядовська, В.М. (2014). Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. Зв’язок, № 4, С. 3-7. URL: http://nbuv.gov.ua/UJRN/Zvjazok_2014_4_3
12. Гнатюк, С. О., Сидоренко, В. М., & Дуксенко, О. П. (2015). Сучасні підходи до виявлення та ідентифікації найбільш важливих об’єктів критичної інфраструктури. Безпека інформації, 21(3), 269–275. doi: 10.18372/2225-5036.21.9690/
13. Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. Теоретико-методологічний аспект забезпечення інформаційної безпеки об’єктів критичної інфраструктури. Вісник Національного університету «Львівська політехніка». Комп’ютерні системи та мережі, 2014. № 806. С. 34-39: вебсайт. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_8
14. Реалізація політики США щодо безпеки та стійкості КІ відбувається на основі положень чинного Плану захисту критичної інфраструктури (2013): Партнерство для безпеки і стійкості критичної інфраструктури. URL: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.
15. Office of National Infrastructure Protection. URL: https://www.dhs.gov/office-infrastructure-protection

Додаткова:

16. Управління захисту інфраструктури (США). URL: https://www.dhs.gov/office-infrastructureprotection
17. Національна політика безперервності. Сайт U.S. FEMA. URL: https://www.fema.gov/medialibrary-data/1384886826028-729844d3fd23ff85d94d52186c85748f/NCPIP.pdf).
18. Національна стратегія внутрішньої безпеки. (США) URL: https://www.dhs.gov/xlibrary/assets/ nat_strat_homelandsecurity_2007.pdf
19. Національна стратегія фізичного захисту критичної інфраструктури та ключових активів. URL: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

20. Національна стратегія безпеки кіберпростору. URL: https://www.energy.gov/sites/prod/ files/National%20Strategy%20to%20Secure%20Cyberspace.pdf
21. Закон про національну безпеку 2002 року. (США) URL: https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf
22. Президентська політична директива 21 (PPD-21) Безпека та стійкість критичної інфраструктури.(США) URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policydirective-critical-infrastructure-security-and-resil
23. Виконавчий наказ 13636: Покращення кібербезпеки критичної інфраструктури (США) URL: https:// www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurityincentives-study.pdf

Ресурси в Інтернеті

24. Europol. – https://www.europol.europa.eu/content/memberpage/austria-791.
25. Online Investigative Principles for Federal Law Enforcement Agents. – https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf .
26. Canadian Cyber Incident Response Centre (CCIRC). – http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx .
27. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
28. Action Plan 2010-2015 for Canada's Cyber Security Strategy. – http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx
29. Information security. Finnish communication regulatory authority. – https://www.viestintavirasto.fi/en/informationsecurity.html
30. Le secrétariat général de la défense et de la sécurité nationale (SGDSN). – Organisation http://www.sgdsn.gouv.fr/site_rubrique88.html
31. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. – http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire
32. Cyber Security Strategy for Germany. – https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile
33. Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary. – http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf
34. Discussion draft on National Cyber Security Policy. Department of Information Technology Ministry of Communications and Information Technology Government of India Electronics Niketan, Lodhi Road New Delhi – 110003. – http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf
35. Cyber Security Policies. – http://www.space-cyber.jp/cyber/
36. National Cyber Security Center. – http://service1.nis.go.kr/eng/intro/NCSCInfo.jsp

37. Government ICT Security Command Centre. – http://www.mampu.gov.my/web/en/prisma
38. National risk analysis – Direktoratet for samfunnssikkerhet. – www.dsb.no/Global/Publikasjoner/2013/Tema/NRB_2013_english.pdf
39. Ellyne Phneah /Singapore to open Cyber Security Lab to train law enforcers // Phneah Ellyne. – http://www.zdnet.com/sg/singapore-to-open-cyber-security-lab-to-train-law-enforcers-7000012392/
40. Sweden's Information Security. – https://msb.se/RibData/Filer/pdf/26419. pdf.

Матеріально-технічне забезпечення: комп'ютерна мережа з підключенням до Internet.

План проведення заняття

І. Порядок проведення вступу до заняття.

Ознайомитися з текстом лекції № 6 з навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури», основною та додатковою літературою.

ІІ. Порядок проведення основної частини заняття.

Опрацювати текст лекції № 6, створивши стислий конспект лекції в електронному виді.

Користуючись текстом лекції, літературою до лекції (зі списку літератури) сформулювати розгорнуті відповіді на загальні запитання:

1. Які основні принципи забезпечення конфіденційності, цілісності та доступності інформації в системах критичної інфраструктури?
2. Які види аварій можуть стати загрозою для об'єктів критичної інфраструктури?
3. Які можливі наслідки для суспільства при недостатньому захисті об'єктів критичної інфраструктури?
4. Які стратегії резервування та відновлення даних використовуються для забезпечення безпеки об'єктів критичної інфраструктури?
5. Основні принципи географічного розташування об'єктів критичної інфраструктури для забезпечення безпеки?
6. Що таке "стійкість до впливу стихійних лих" і як вона враховується при захисті об'єктів критичної інфраструктури?
7. Які основні види тренувань та навчання використовуються для підвищення готовності персоналу до реагування на інциденти?
8. Які методи шифрування використовуються для захисту інформації в системах критичної інфраструктури?
9. Які технології шифрування використовуються для захисту інформації в системах критичної інфраструктури?
10. Основні принципи забезпечення фізичної безпеки персоналу, що працює на об'єктах критичної інфраструктури.
11. Які загрози можуть становити інсайдери (внутрішні працівники) для об'єктів критичної інфраструктури?

12. Наведіть ланцюг п’яти взаємопов’язаних місій, визначених Національною системою готовності США.
13. Які основні етапи розробки та реалізації планів захисту об'єктів критичної інфраструктури?
14. Згідно з прийнятим у США підходом виконання яких етапів передбачає процес планування?
15. З яких елементів складається Національна система планування США?
16. Наведіть, які рівні планування включає Національна система планування США.
17. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Австралії.
18. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Австрії.
19. Охарактеризуйте організаційну структуру забезпечення кібербезпеки. Бельгії.
20. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Бразилії.
21. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Канаді.
22. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Естонії.
23. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Фінляндії.
24. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Франції.
25. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Німеччині.
26. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Угорщині.
27. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Індії.
28. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Італії.
29. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Японії.
30. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Республіки Корея.
31. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Малайзії.
32. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Нідерландах.
33. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Нової Зеландії.

34. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Норвегії.
35. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Польщі.
36. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Сінгапуру.
37. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Іспанії.
38. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Швеції.
39. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Швейцарії.
40. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Великобританії.

ІІІ. Порядок проведення заключної частини заняття.

Здобувачі освіти після опрацювання тексту лекції № 6 та виконання завдань самостійної роботи зобов'язані пройти контрольне тестування за темою.

Викладач перевіряє у здобувачів результати виконання поставлених задач, виставляє відповідні оцінки; зазначає перелік задач для самостійної роботи, вказує час і спосіб перевірки результатів самостійної роботи; оголошує тему наступного заняття.