

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

**Харківський національний
університет внутрішніх справ**

**Кафедра інформаційних технологій та кібербезпеки
факультету № 4**

МЕТОДИЧНІ МАТЕРІАЛИ

**до семінарських занять
з навчальної дисципліни**

**«Державне управління у сфері кібербезпеки»
вибіркових компонент освітньої програми
другого (магістерського) рівня вищої освіти**

**125 «Кібербезпека» (Безпека інформаційних та
комунікаційних систем)**

Харків 2020

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО

Вченою радою
факультету № 4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки факультету № 4 (протокол від 15.09.2020 № 16).

Розробники:

Професор кафедри інформаційних технологій та кібербезпеки факультету № 4, кандидат технічних наук, доцент Носов В.В.
Доцент кафедри інформаційних технологій та кібербезпеки факультету № 4, кандидат наук з державного управління, доцент Онищенко Ю.М.

Рецензенти:

Доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент Тулупов В.В.
Завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, доктор технічних наук, професор Петров К.Е.

1. Розподіл часу навчальної дисципліни за темами

2.1. 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	Семінарські заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2						
Тема № 1. Теоретичні засади запобігання і протидії проявам кіберзлочинності	24	4	4		16	
Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	36	6	6		24	
Тема № 3. Державні механізми запобігання і протидії кіберзлочинності	60	10	10		40	
Всього за семестр	120	20	20		80	залік

2.2. 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	Семінарські заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2						
Тема № 1. Теоретичні засади запобігання і протидії проявам кіберзлочинності	29	1	2		26	
Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	37	1	2		34	
Тема № 3. Державні механізми запобігання і протидії кіберзлочинності	54	2	2		50	
Всього за семестр	120	4	6		110	залік

2. Методичні вказівки до семінарських занять

Тема №1. Теоретичні засади запобігання і протидії проявам кіберзлочинності

Семінарське заняття 1. Взаємозв'язок злочинності та інформаційних технологій

Навчальна мета заняття: опанувати взаємозв'язок злочинності та інформаційних технологій

Час проведення:

- денна форма навчання - 2 год.
- заочна форма навчання - 1 год.

Навчальні питання

Вступ

1. Глобальні інформаційні технології
2. Глобалізації злочинності

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на загальні принципи побудови мережі Інтернет, сервісів хмарних обчислень, розподілених технологій P2P. Засвоїти поняття DarkNet.

Під час вивчення 2-го питання визначити види і склади злочинів, що використовують локальні і глобальні інформаційні технології.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 1. Нагадати основні визначення. Детально розглянути матеріал лекції 1. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).

3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
 - повнота та аргументованість відповідей;
 - робота в команді;
 - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Питання цільових виступів.

1. Архітектура Інтернет.
2. TOR.

Тема реферату.

1. Склади злочинів за КК України, в яких можливо використання інформаційних технологій.

Література

1. Текст лекції № 1.
2. 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.
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: 08.09.2020).
4. 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: 08.09.2020).
5. 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: 08.09.2020).
6. Носов В. В. Організація та забезпечення інформаційної безпеки: навчальний посібник / В.В. Носов, О.В. Манжай. – Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2007. – 216 с.

Семінарське заняття 2. Зарубіжний досвід реалізації державних механізмів у галузі запобігання та боротьби з кіберзлочинністю

Навчальна мета заняття: обговорити зарубіжний досвід реалізації державних механізмів у галузі запобігання та боротьби з кіберзлочинністю

Час проведення:

- денна форма навчання - 2 год.
- заочна форма навчання - 1 год.

Навчальні питання

Вступ

1. Механізми ЄС у запобіганні та боротьби з кіберзлочинністю
2. Механізми США у запобіганні та боротьби з кіберзлочинністю

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на загальні механізми ЄС у запобіганні та боротьби з кіберзлочинністю та особливості їх реалізації в окремих країнах ЄС.

Під час вивчення 2-го питання оглянути федеральні структури і нормативно-правову базу США з питань запобігання та боротьби з кіберзлочинністю.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 1. Нагадати основні визначення. Детально розглянути матеріал лекції 1. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей

- час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
 6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
 7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
 8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
 9. Полеміка між командами протягом 5-ти хвилин.
 10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
 11. Викладач оцінює якість роботи кожної з команд.
 12. Критерії оцінювання (за п'ятибальною шкалою кожний):
 13. повнота та аргументованість відповідей;
 14. робота в команді;
 15. дотримання правил етикету.
 16. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
 17. По закінченні гри підбиваються підсумки.
 18. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Питання цільових виступів.

1. Структури ЄС у запобіганні та боротьби з кіберзлочинністю.

2. Структури США у запобіганні та боротьби з кіберзлочинністю.

Тема реферату.

1. Зарубіжні статистичні дані щодо розкриття кіберзлочинів.

Література

1. Текст лекції № 1.
2. 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.
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: 08.09.2020).
4. 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: 08.09.2020).
5. 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: 08.09.2020).
6. Носов В.В. Організація та забезпечення інформаційної безпеки: навчальний посібник / В.В. Носов, О.В. Манжай. – Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2007. – 216 с.

Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні

Семінарське заняття 3. Поняття кібербезпеки і кіберзахисту

Навчальна мета заняття: опрацювати суть понять кібербезпеки і кіберзахисту

Час проведення:

- денна форма навчання - 2 год.
- заочна форма навчання - 1 год.

Навчальні питання

Вступ

1. Кібербезпека держави
2. Кіберзахист держави

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на правову основу забезпечення кібербезпеки держави і об'єкти захисту.

Під час вивчення 2-го питання розібрати заходи кіберзахисту і поняття об'єкти критичної інфраструктури.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 2. Нагадати основні визначення. Детально розглянути матеріал лекції 2. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.

6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
13. повнота та аргументованість відповідей;
14. робота в команді;
15. дотримання правил етикету.
16. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
17. По закінченні гри підбиваються підсумки.
18. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Питання цільових виступів.

1. Правова основа забезпечення кібербезпеки держави.
2. Об'єкти критичної інфраструктури України.

Тема реферату.

1. Принципи забезпечення кібербезпеки.

Література

1. Текст лекції № 2.
2. 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.

3. Орлов О.В. Совершенствование механизмов реализации государственной политики в сфере борьбы с киберпреступностью в Украине / О.В. Орлов, Ю.М. Онищенко // Публичное управление: научный журнал Академии государственного управления Республики Армения. – 2014. – № 1-2/2014. – 42 с.
4. 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: 08.09.2020).
5. 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: 08.09.2020).
6. 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: 08.09.2020).
7. Носов В.В. Організація та забезпечення інформаційної безпеки: навчальний посібник / В.В. Носов, О.В. Манжай. – Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2007. – 216 с.

Семінарське заняття 4. Національна система кібербезпеки

Навчальна мета заняття: усвідомити порядок функціонування національної системи кібербезпеки

Час проведення:

- денна форма навчання - 2 год.
- заочна форма навчання – 0,5 год.

Навчальні питання

Вступ

1. Суб'єкти забезпечення кібербезпеки в Україні
2. Шляхи функціонування національної системи кібербезпеки

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на заходи національної системи кібербезпеки.

Під час вивчення 2-го питання розібрати шляхи функціонування національної системи кібербезпеки.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 2. Нагадати основні визначення. Детально розглянути матеріал лекції 2. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.

7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
13. повнота та аргументованість відповідей;
14. робота в команді;
15. дотримання правил етикету.
16. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
17. По закінченні гри підбиваються підсумки.
18. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Питання цільових виступів.

1. Основні завдання Національної поліції України у національній системі кібербезпеки.

2. Індикатори кіберзагроз.

Тема реферату.

1. Міжнародні стандарти з питань кібербезпеки та кіберзахисту.

Література

1. Текст лекції № 2.

2. 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: 08.09.2020).

3. 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: 08.09.2020).
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.

Семінарське заняття 5. Урядова команда реагування на комп'ютерні надзвичайні події України

Навчальна мета заняття: обговорити задачі і результати діяльності CERT-UA

Час проведення:

- денна форма навчання - 2 год.
- заочна форма навчання – 0,5 год.

Навчальні питання

Вступ

1. Завдання CERT-UA
2. Поточна діяльність CERT-UA

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на порядок взаємодії CERT-UA з НПУ, забезпечення своєчасного інформування про кібератаки.

Під час вивчення 2-го питання розібрати поточну діяльність CERT-UA.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 2. Нагадати основні визначення. Детально розглянути матеріал лекції 2. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.

2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
13. повнота та аргументованість відповідей;
14. робота в команді;
15. дотримання правил етикету.
16. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.

17. По закінченні гри підбиваються підсумки.

18. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Питання цільових виступів.

1. Накопичення та проведення аналізу даних про кіберінциденти.
2. Рекомендації щодо протидії сучасним видам кібератак та кіберзагроз.

Тема реферату.

1. Зарубіжні урядові команди реагування на комп'ютерні надзвичайні події.

Література

1. Текст лекції № 2.
2. 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: 08.09.2020).
3. 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: 08.09.2020).

Тема №3. Державні механізми запобігання і протидії кіберзлочинності
Семінарське заняття 6. Запобігання і протидія кіберзлочинності: норми права, приватний сектор

Навчальна мета заняття: окреслити застосування норм права до кібернетичного простору і роль приватного сектору у запобіганні і протидії кіберзлочинності

Час проведення:

- денна форма навчання – 2 год.

- заочна форма навчання – 0,5 год.

Навчальні питання

Вступ

1. Застосування норм права до кібернетичного простору
2. Роль приватного сектору у запобіганні і протидії кіберзлочинності

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на розуміння норм права реального світу та можливість їх перенесення до кібернетичного простору.

Під час вивчення 2-го питання розібрати можливу роль приватного сектору у запобіганні і протидії кіберзлочинності.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 3. Нагадати основні визначення. Детально розглянути матеріал лекції 3. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для

команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.

5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
13. повнота та аргументованість відповідей;
14. робота в команді;
15. дотримання правил етикету.
16. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
17. По закінченні гри підбиваються підсумки.
18. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Питання цільових виступів.

1. Норми права і кібернетичний простір в Україні.

2. Роль приватного сектору у запобіганні і протидії кіберзлочинності.

Тема реферату.

1. Норми права і кібернетичний простір в ЄС.

Література

1. Текст лекції № 3.
2. 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: 08.09.2020).
3. 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: 08.09.2020).

Семінарське заняття 7. Організаційно-технічні заходи забезпечення кібербезпеки в Україні

Навчальна мета заняття: обговорити існуючі і перспективні організаційно-технічні заходи забезпечення кібербезпеки в Україні

Час проведення:

- денна форма навчання - 2 год.
- заочна форма навчання – 0,5 год.

Навчальні питання

Вступ

1. Технічні заходи
2. Організаційні заходи

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на розуміння норм права реального світу та можливість їх перенесення до кібернетичного простору.

Під час вивчення 2-го питання розібрати можливу роль приватного сектору у запобіганні і протидії кіберзлочинності.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 3. Нагадати основні визначення. Детально розглянути матеріал лекції 3. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.

10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
13. повнота та аргументованість відповідей;
14. робота в команді;
15. дотримання правил етикету.
16. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
17. По закінченні гри підбиваються підсумки.
18. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Питання цільових виступів.

1. Технічні заходи забезпечення кібербезпеки в Україні.
2. Організаційні заходи забезпечення кібербезпеки в Україні.

Тема реферату.

1. Організаційно-технічні заходи забезпечення кібербезпеки в США.

Література

1. Текст лекції № 3.
2. 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: 08.09.2020).
3. 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: 08.09.2020).

Семінарське заняття 8. Кібернетичні командування та системи безпеки, як органи державного управління

Навчальна мета заняття: розкрити задачі кібернетичного командування та систем безпеки, як органів державного управління

Час проведення:

- денна форма навчання - 2 год.
- заочна форма навчання – 0,5 год.

Навчальні питання

Вступ

1. Зарубіжний досвід створення кібернетичного командування
2. Можлива структура кібернетичного командування в Україні

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на досвід США і НАТО у створенні кібернетичного командування.

Під час вивчення 2-го питання розібрати можливу структуру кібернетичного командування в Україні.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 3. Нагадати основні визначення. Детально розглянути матеріал лекції 3. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не

приймає то вона має право ще на одну спробу вибору питання.

4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обох командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
13. повнота та аргументованість відповідей;
14. робота в команді;
15. дотримання правил етикету.
16. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
17. По закінченні гри підбиваються підсумки.
18. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Питання цільових виступів.

1. Кібернетичне командування НАТО.
2. Структура кібернетичного командування в Україні.

Тема реферату.

1. Задачі підрозділів радіоелектронної боротьби і радіотехнічної розвідки.

Література

1. Текст лекції № 3.
2. 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.
3. Носов В.В. Організація та забезпечення інформаційної безпеки: навчальний посібник / В.В. Носов, О.В. Манжай. – Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2007. – 216 с.

Семінарське заняття 9. Національна стратегія кібербезпеки

Навчальна мета заняття: оглянути основні положення національної стратегії кібербезпеки та заходи з її реалізації

Час проведення:

- денна форма навчання - 2 год.
- заочна форма навчання – 0,25 год.

Навчальні питання

Вступ

1. Національна стратегія кібербезпеки
2. Заходи з реалізації Стратегії кібербезпеки України

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на розділи і зміст Стратегії кібербезпеки України.

Під час вивчення 2-го питання розібрати, які заходи було реалізовано із Стратегії кібербезпеки України.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 3. Нагадати основні визначення. Детально розглянути матеріал лекції 3. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.

8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
13. повнота та аргументованість відповідей;
14. робота в команді;
15. дотримання правил етикету.
16. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
17. По закінченні гри підбиваються підсумки.
18. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Питання цільових виступів.

1. Структура Стратегії кібербезпеки України.
2. План заходів на 2017 рік з реалізації Стратегії кібербезпеки України.

Тема реферату.

1. Стратегія кібербезпеки США.

Література:

1. Текст лекції № 3.
2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".
3. 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: 08.09.2020).

Семінарське заняття 10. Взаємодія у сфері боротьби з кіберзлочинністю

Навчальна мета заняття: обговорити можливу структуру державного механізму взаємодії у сфері боротьби з кіберзлочинністю

Час проведення:

- денна форма навчання - 2 год.
- заочна форма навчання – 0,25 год.

Навчальні питання

Вступ

1. Структура взаємодії державних органів
2. Напрями розвитку системи запобігання кіберзлочинності в Україні

Висновки

Методичні вказівки

Під час вивчення 1-го питання звернути увагу на структуру державного механізму взаємодії у сфері боротьби з кіберзлочинністю.

Під час вивчення 2-го питання розібрати напрями розвитку системи запобігання кіберзлочинності в Україні.

План проведення заняття

I. Порядок проведення вступу до заняття.

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

II. Порядок проведення основної частини заняття.

Провести опитування за контрольними питаннями до лекції 3. Нагадати основні визначення. Детально розглянути матеріал лекції 3. Обговорити питання, розібрати матеріал лекції, що викликає складність у засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.

4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
13. повнота та аргументованість відповідей;
14. робота в команді;
15. дотримання правил етикету.
16. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
17. По закінченні гри підбиваються підсумки.
18. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

III. Порядок проведення заключної частини заняття.

Перевірити у здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для

самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи. Оголосити тему наступного заняття.

Питання цільових виступів.

1. Система раннього попередження та сповіщення про кіберінциденти.
2. Напрями розвитку системи запобігання кіберзлочинності в Україні.

Тема реферату.

1. Структура взаємодії федеральних органів США у боротьби з кіберзлочинністю.

Література:

1. Текст лекції № 3.
2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".
3. 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: 08.09.2020).
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.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

3.1 Основна:

1. 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: 08.09.2020).
2. 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: 08.09.2020).
3. 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: 08.09.2020).

4. Носов В.В. Організація та забезпечення інформаційної безпеки: навчальний посібник / В.В. Носов, О.В. Манжай. – Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2007. – 216 с.

3.2 Допоміжна:

5. Орлов О.В. Совершенствование механизмов реализации государственной политики в сфере борьбы с киберпреступностью в Украине / О.В. Орлов, Ю.М. Онищенко // Публичное управление: научный журнал Академии государственного управления Республики Армения. – 2014. – № 1-2/2014. – 42 с.
6. 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.
7. 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.

3.3 Інформаційні ресурси:

8. <http://www.niss.gov.ua/articles/454/>
9. <https://cyberpolice.gov.ua/strategy-2020/>