МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Методичні вказівки
до семінарських занять та виконання самостійних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека»
галузі знань F Інформаційні технології
спеціальності F5 Кібербезпека та захист інформації
денної та заочної форм навчання

Луцьк 2025

УДК 349:004.056
Г 72

Електронна копія друкованого видання передана для внесення в репозиторій ЛНТУ
Директор бібліотеки _____ Н.П. Поліщук

Рекомендовано до видання вченою радою факультету бізнесу та права ЛНТУ, протокол № ____ від «___»_____2025 року.

Голова вченої ради факультету бізнесу та права _____ Л.Л. Ковальська

Розглянуто і схвалено на засіданні кафедри права ЛНТУ, протокол № ___ від «___»_____ 2025 року

Завідувач кафедри права _____ В.В. Аніщук

Укладач: _____ С.Г. Зицик, кандидат юридичних наук, доцент кафедри права ЛНТУ

Рецензент: _____Н.В. Рябих, кандидат юридичних наук, доцент кафедри права ЛНТУ

Відповідальний за випуск: _____ С.Г. Зицик, кандидат юридичних наук, доцент кафедри права ЛНТУ.

Г 72 Нормативно-правове забезпечення кібербезпеки. [Текст]: методичні вказівки до семінарських занять та виконання самостійних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузі знань F Інформаційні технології спеціальності F5 Кібербезпека та захист інформації денної та заочної форм навчання / уклад. С.Г. Зицик. Луцьк. ЛНТУ, 2025 с. 38.

Видання містить методичні вказівки до семінарських занять та виконання самостійних робіт з дисципліни «Нормативно-правове забезпечення кібербезпеки», перелік літератури для підготовки здобувачів. В основу методичних вказівок покладені підручники кращих українських науковців з інформаційного права та кібербезпеки.

ЗМІСТ

ПЕРЕДМОВА

Питання нормативно-правового регулювання сфери кібербезпеки зберігають значну актуальність в умовах правового режиму воєнного стану та необхідності поглиблення євроінтеграційних процесів.

Україна під час широкомасштабної агресії зустрічається з різними видами кібератак та кіберзлочинів, країна-агресор прагне заблокувати надання електронних послуг наслідком чого є непоодинокі випадки порушення прав громадян, порушуються цілісність та конфіденційність персональних відомостей, здійснюються фішингові атаки, провокується інформаційно-психологічний натиск на людей. Тож, захист кіберпростору в умовах зазначених викликів виступає стратегічно важливим пріоритетом у системі національної безпеки України.

Тож, для відвернення кіберзагроз та захисту території й інформаційного простору держави наразі потрібна концентрація всіх видів ресурсів та впорядкування повноважень відповідних суб'єктів забезпечення кібербезпеки у поєднанні з дієвою державною політикою та ефективним нормативно-правовим забезпеченням зазначеної сфери.

Формування та реалізація державної політики у сфері кібербезпеки, захист прав і свобод людини та громадянина, національних інтересів України у кіберпросторі, боротьба з кіберзлочинністю забезпечується Кабінетом Міністрів України, Уряд України також організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

Суб'єктами забезпечення кібербезпеки є державні органи (Держспецзв'язку, СБУ, Нацполіція, Міноборони, НБУ та інші центральні органи виконавчої влади), органи місцевого самоврядування, підприємства, установи та організації, що належать до критичної інфраструктури або надають послуги у сфері інформаційних технологій, а також громадяни України, які зобов'язані сприяти кібербезпеці.

1. ТЕМАТИКА ЗАВДАНЬ

ТЕМА 1. Стратегія кібербезпеки України

План

1. Стан реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96.
2. Національний кіберпростір: виклики та кіберзагрози.
3. Національна система кібербезпеки: засади розбудови.
4. Пріоритети забезпечення кібербезпеки України та стратегічні цілі.
5. Стратегічні завдання.
6. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки.

Питання для самоперевірки

1. Визначте механізми реалізації стратегії та забезпечення відкритості.
2. Охарактеризуйте виміри успіху (метрики).
3. Охарактеризуйте виклики для України у сфері кібербезпеки.
4. Назвіть загрози кібербезпеці України.
5. Назвіть напрямки зовнішньополітичної діяльності України у сфері кібербезпеки.
6. Надайте визначення понять: кібербезпека, кіберпростір, кіберзагроза, кіберзахист, кіберінцидент, кіберзлочин, кібератака, кібергігієна, індикатори кіберзагроз, критична інформаційна інфраструктура, Національна електронна комунікаційна мережа, національні електронні інформаційні ресурси, Національний центр резервування державних інформаційних ресурсів, об’єкт критичної інформаційної інфраструктури, система управління технологічними процесами, системи електронних комунікацій, реагування на кіберінциденти, система активної протидії агресії у кіберпросторі.

ТЕМА 2. Суб’єкти забезпечення кібербезпеки

План

1. Рада національної безпеки та оборони України.

2. Міністерства та інші центральні органи виконавчої влади.

3. Місцеві державні адміністрації.

4. Органи місцевого самоврядування.

5. Правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності.

6. Збройні Сили України, інші військові формування.

7. Національний банк України.

8. Підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури.

9. Суб'єкти господарювання, громадяни України та об'єднання громадян як суб'єкти забезпечення кібербезпеки.

Питання для самоперевірки

1. Назвіть склад Ради національної безпеки та оборони України.

2. Які повноваження Національного координаційного центру кібербезпеки?

3. Що визначають положення Директиви Європейського Союзу щодо мережевої та інформаційної безпеки?

4. Яким чином здійснюється планування проведення кібероперацій стратегічного рівня?

5. Які повноваження Державної служби спеціального зв'язку та захисту інформації України?

ТЕМА 3. Національна система кібербезпеки

План

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

2. Національна поліція України.

3. Служба безпеки України.

4. Міністерство оборони України, Генеральний штаб Збройних Сил України.

5. Розвідувальні органи України.

6. Національний центр резервування державних інформаційних ресурсів.

7. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.

Питання для самоперевірки

1. Яким чином здійснюється координація суб'єктів забезпечення кібербезпеки?
2. У чому полягає стандартизація у сферах криптографічного та технічного захисту інформації?
3. Охарактеризуйте діяльність національної команди реагування на кіберінциденти.
4. Охарактеризуйте діяльність CERT-UA.
5. Назвіть функції правоохоронних органів у сфері забезпечення кібербезпеки.

ТЕМА 4. Правове регулювання інформаційної діяльності

План

1. Право на інформацію. Види інформації.
2. Правовий режим використання відкритої інформації
3. Публічна інформація. Звернення громадян. Запит на отримання публічної інформації.
4. Створення, поширення, використання та застосування інформації.
5. Конфіденційна інформація. Персональні дані та їх захист.
6. Службова інформація.
7. Державна таємниця.
8. Електронні довірчі послуги.

Питання для самоперевірки

1. Як співвідносяться поняття «конфіденційна інформація» та персональні дані»?
2. Охарактеризуйте відкриті бази даних.
3. Яка відповідальність інформації з обмежених доступом.
4. Що таке таємниця слідства?
5. Яка інформація може бути віднесена до державної таємниці?

ТЕМА 5. Критична інфраструктура України

План

1. Реєстр об'єктів критичної інформаційної інфраструктури.

2. Реєстр об’єктів критичної інфраструктури.

3. Інцидент безпеки критичної інфраструктури.

4. Критерії віднесення об’єктів до критичної інфраструктури.

5. Суб’єкти національної системи захисту критичної інфраструктури.

6. Режими функціонування національної системи захисту критичної інфраструктури.

Питання для самоперевірки

1. Хто є розпорядником інформаційно-комунікаційної системи реєстру та володільцем інформації (відомостей), що міститься у реєстрі об’єктів критичної інформаційної інфраструктури?

2. Хто здійснює ідентифікацію об’єктів критичної інформаційної інфраструктури та оцінку критичності об’єкта інформаційної інфраструктури?

3. Назвіть секторальні органи у сфері захисту критичної інфраструктури.

4. Визначте сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам.

5. Кому подається на затвердження зведений перелік об’єктів критичної інфраструктури секторальними органами у сфері захисту критичної інфраструктури?

ТЕМА 6. Кіберзлочинність

План

1. Конвенція про кіберзлочинність.

2. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем.

3. Правопорушення, пов'язані з комп'ютерами.

4. Правопорушення, пов'язані зі змістом.

5. Правопорушення, пов'язані з порушенням авторських та суміжних прав.

6. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

7. Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки.

Питання для самоперевірки

1. Охарактеризуйте шахрайство з використанням електронно-обчислювальної техніки, несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

2. Яка відповідальність настає за несанкціоновані збут або розповсюдження інформації з обмеженим доступом?

3. Охарактеризуйте правопорушення проти конфіденційності згідно з Конвенцією про кіберзлочинність.

4. Які злочини вчиняються з використанням електронних довірчих послуг?

5. Охарактеризуйте правопорушення, пов’язані з порушенням авторських та суміжних прав згідно з Конвенцією про кіберзлочинність.

ТЕМА 7. Організаційно-технічна модель кіберзахисту

План

1. Команди реагування на комп’ютерні надзвичайні події.

2. Забезпечення функціонування організаційно-технічної моделі кіберзахисту.

3. Сектори організаційно-керуючої інфраструктури кіберзахисту.

4. Заходи сил кіберзахисту під час функціонування технологічної інфраструктури кіберзахисту.

5. Ідентифікація, захист, виявлення, реагування та відновлення як заходи з кіберзахисту системами кіберзахисту.

Питання для самоперевірки

1. Що передбачає здійснення заходів з кіберзахисту системами кіберзахисту?

2. Охарактеризуйте сили і засоби кіберзахисту, спрямовані на оперативне (кризове) реагування на кібератаки та кіберінцидент.

3. Хто вживає першочергових заходів із захисту об'єкта критичної інформаційної інфраструктури від кібератак?

4. Визначте базові вимоги із забезпечення кіберзахисту об'єктів критичної інфраструктури.

5. Охарактеризуйте доступність та відмовостійкість компонентів.

ТЕМА 8. Забезпечення функціонування Національної телекомунікаційної мережі

План

1. Національна телекомунікаційна мережа.
2. Об'єкти Національної телекомунікаційної мережі.
3. Ресурс Національної телекомунікаційної мережі.
4. Структура Національної телекомунікаційної мережі.
5. Центр управління мережею.

Питання для самоперевірки

1. У якій черговості надається ресурс Національної телекомунікаційної мережі?

2. Яким чином державні органи отримують доступ до Інтернету?

3. Для чого призначена мультисервісна платформа Національної телекомунікаційної мережі?

4. Охарактеризуйте структуру Національної телекомунікаційної мережі.

5. Яким чином здійснюється забезпечення захищених електронних комунікацій?

ТЕМА 9. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури

План

1. Формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки.

2. Управління доступом користувачів та адміністраторів.

3. Ідентифікація та автентифікація користувачів та адміністраторів.

4. Реєстрація подій компонентами об’єкта критичної інформаційної інфраструктури та їх періодичний аудит.

5. Мережевий захист компонентів та інформаційних ресурсів.

6. Доступність та відмовостійкість компонентів та інформаційних ресурсів.

7. Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації.

8. Визначення умов використання програмного та апаратного забезпечення.

9. Визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури.

Питання для самоперевірки

1. Яка відмінність ідентифікації від автентифікації?
2. Визначте базові заходи з кіберзахисту.
3. Опишіть процедуру оцінювання ризиків кібербезпеки.
4. Які умови використання змінних (зовнішніх) пристроїв та носіїв інформації можуть бути на об’єкті критичної інфраструктури?
5. Які параметри визначають доступність та відмовостійкість компонентів та інформаційних ресурсів?

ТЕМА 10. Забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах

План

1. Забезпечення технічного та криптографічного захисту інформації з обмеженим доступом, а також відкритої інформації, вимога щодо захисту якої встановлена законом.
2. Криптографічний захист в системі таємної інформації.
3. Вимоги до захисту в системі інформації від несанкціонованого блокування.
4. Реєстрація подій.
5. Організаційні засади забезпечення захисту інформації.

Питання для самоперевірки

1. Надайте визначення понять: авторизація з безпеки, авторизована система з безпеки, блокування інформації в системі, виток інформації, володілець інформації, власник системи, доступ до інформації в системі, комплекс технічного захисту інформації, криптографічний захист інформації.

2. Охарактеризуйте перелік авторизованих систем з безпеки.

3. Визначте порядок доступу до інформації в системі.

4. Охарактеризуйте процедуру резервування державних інформаційних ресурсів та систем.

5. Визначте умови обробки інформації в системі.

2. ПРАКТИЧНІ ЗАВДАННЯ

Завдання 1. Визначте основні функції, критичні бізнес/операційні процеси об'єкта критичної інфраструктури згідно наданого переліку. На їх основі необхідно встановити вимоги до кіберзахисту.

Луцька міська рада, Волинська обласна державна адміністрація, СБУ у Волинській області Волинський обласний територіальний центр комплектування та соціальної підтримки, Автостанція «Луцьк», Київський метрополітен, Луцькводоканал, Рівненська АЕС, Головне управління поліції у Волинській області, Волинська обласна державна адміністрація, Vodafone Україна, Суспільне телебачення, Волинський прикордонний загін, Національний банк України.

Завдання 2. Вам довірено організувати систему захисту комерційної таємниці фірми. 1. Зазначте ваш підхід до вирішення вищезазначеного завдання. 2. Як впливає вихід інформації, яка складає комерційну таємницю на фінансово-економічне становище підприємства? 3. Надайте характеристику механізму захисту комерційної таємниці. 4. Які основні нормативно-правові акти України регулюють питання захисту комерційної таємниці підприємства?

Завдання 3. Порушуючи інструкцію щодо зберігання державної таємниці, конструктор заводу Т. брав документи, що містили державну таємницю, для роботи з ними вдома. Одного разу, перебуваючи в стані сп'яніння, він загубив папку з такими документами. Громадянин С. підібрав папку і показала своєму синові. Ознайомившись зі змістом документів, останній відніс знахідку до міського управління СБУ. Кваліфікуйте дії Т.

Завдання 4. Проти журналістки Паньків, яка не пройшла процедуру допуску до відомостей, що становлять державну таємницю, було порушено кримінальну справу за ознаками злочину, передбаченим ст. 328 КК України. Обставини справи зводилися до наступного. Журналістка Паньків оприлюднила (опублікувала в газеті) закриті відомості про обсяги запасів у надрах стратегічного виду корисних копалин в Україні, отримані нею в ході інтерв'ю з високопоставленою особою з Мінекономрозвитку. 1. Чи є журналістка суб'єктом розголошення державної таємниці? 2. Чи є суб'єктом розголошення відомостей,

що становлять державну таємницю посадова особа з Мінекономрозвитку, у функціональні обов'язки якого входить робота з такими відомостями? 3. Чи може журналістка бути притягнута до кримінальної відповідальності, якщо в ході інтерв'ю була попереджена з боку інтерв'юйованого, що відомості якими він ділиться не підлягають розповсюдженню в силу їх таємності? 4. Чи може журналістка бути притягнута до кримінальної відповідальності як співучасник злочину?

Завдання 5. Група осіб створила сайт, що імітує відомий онлайн-магазин. Завдяки розсиланню фішингових листів вони отримали дані банківських карток покупців, після чого зняли з рахунків значні суми. Частину коштів вони перевели на криптовалютні гаманці. Які об’єкт і предмет посягання в цій ситуації? Чим відрізняється шахрайство в кіберпросторі від класичного шахрайства?

Завдання 6. Працівник ІТ-відділу великої компанії встановив на офісних комп’ютерах програму для майнінгу криптовалюти. Отримані монети перераховував на власний гаманець. Компанія виявила втрату продуктивності та зростання рахунків за електроенергію. Чи є вчинене посяганням на власність? У чому його особливість? Як кваліфікувати дії працівника? Який склад злочину підходить найточніше: крадіжка чи зловживання службовим становищем?

Завдання 7. Особа зламала акаунт користувача в ігровій платформі Web3 і незаконно переоформила цифрові об’єкти (NFT, токени), що мали ринкову цінність, на інший обліковий запис. Власник звернувся до поліції з вимогою повернення цифрового майна. Чи можна вважати NFT предметом злочину проти власності? Як впливають на кваліфікацію технічні аспекти власності на токени? Чи підпадає таке діяння під дію чинного Кримінального кодексу України?

Завдання 8. Олександр, студент-фахівець із кібербезпеки, виявив уразливість у мобільному додатку банку, яка дозволяла без авторизації отримати доступ до облікових записів клієнтів. Замість повідомлення банку він використав цю прогалину для переказу коштів із декількох рахунків на свій електронний гаманець, завдавши збитків на понад 200 тисяч гривень. Чи є в цьому випадку ознаки незаконного заволодіння майном? Якщо так, у якій формі?

Чи змінюється кримінальна оцінка, якщо Олександр спершу тестував уразливість із «науковим інтересом»?

Завдання 9. Громадянин А звернувся до банку зі скаргою: з його рахунка було здійснено кілька переказів на сторонні картки без його згоди. Розслідування з'ясувало, що до мобільного застосунку банку було здійснено доступ з нового пристрою після отримання шкідливого посилання в месенджері. Банк вважає, що клієнт сам передав доступ. До якого виду кіберзлочинів належить описане діяння? Яка форма вини притаманна особі, що здійснила несанкціонований доступ?

Завдання 10. Бухгалтер підприємства Б під час формування платіжного доручення отримав електронного листа з «уточненим» рахунком постачальника. Він змінив IBAN у системі інтернет-банкінгу, і кошти були перераховані на рахунок шахрая. Постачальник не отримав оплату, а банк відмовився компенсувати втрати. Чи можна вважати такі дії кіберзлочином проти власності або у сфері банківської діяльності? Яка роль фішингу в цій ситуації?

Завдання 11. Група осіб із використанням спеціального ПЗ отримала доступ до системи внутрішньої авторизації банку та змінила ліміти на зняття коштів із банкоматів. Протягом години було виведено значні суми готівки. Який склад кримінального правопорушення вбачається у цій ситуації? Чи є предметом посягання інформаційна система чи грошові кошти?

Завдання 12. Платформа Z надає послуги онлайн кредитування. Виявилося, що верифікація користувачів була підробною, а дані клієнтів незаконно передавались третім особам. У процесі перевірки виявлено, що платформа не зареєстрована в Нацбанку як фінансова установа. Які правові порушення має така платформа? Чи можна дії організаторів кваліфікувати як кіберзлочини у фінансовій сфері?

Завдання 13. Під час кібератаки на систему дистанційного банкінгу «SmartPay» було вивантажено дані про рахунки клієнтів, паролі та історію операцій. Частина даних з'явилася на хакерських форумах. НБУ рекомендував банку тимчасово зупинити обслуговування. До яких наслідків для кібербезпеки банку призвів злам? Яка відповідальність може настати за зберігання або розповсюдження викрадених даних?

Завдання 14. Під час перевірки діяльності територіального управління кіберполіції було виявлено, що значна частина працівників не має спеціалізованої ІТ-освіти, а підвищення кваліфікації не проводилося понад 3 роки. У цей час на території регіону зросла кількість інцидентів, пов'язаних із фішинговими атаками на державні установи. У чому полягає загроза неналежного кадрового забезпечення в розслідуванні кіберзлочинів? Які шляхи кадрового вдосконалення повинні бути реалізовані?

Завдання 15. Під час розслідування шахрайства з банківськими картками було встановлено, що зловмисник діє з території іншої країни, а сервер, на якому розміщено фішинговий сайт – у третій державі. Українські правоохоронці ініціювали запит до Єдиного центрального органу з міжнародного співробітництва. Яка установа в Україні виконує функції центрального органу з міжнародного співробітництва у сфері кіберзлочинів? Які міжнародні правові механізми можуть бути використані для отримання доказів?

Завдання 16. У результаті хакерської атаки було виведено з ладу електронну систему управління енергетичного об'єкта в одному з регіонів України. Атака координувалася з-за кордону, мала ознаки спрямованості проти державної безпеки й викликала дестабілізацію в регіоні. Чи належить така атака до категорії кіберзлочинів, що становлять загрозу національній безпеці? Які правоохоронні та безпекові органи мають бути залучені до реагування?

Завдання 17. До кіберполіції надійшла інформація про масове поширення шкідливого програмного забезпечення через VPNканали. З метою отримання відомостей про користувачів певного сервера був запущений оперативно-розшуковий захід за місцем розміщення інтернет-провайдера. Які умови проведення оперативно-розшукових заходів регламентує закон? Чи може поліція отримати доступ до логів провайдера без ухвали суду?

Завдання 18. Під час розслідування витоку інформації з медичного реєстру слідчий сформував кілька версій: службова недбалість, втручання працівника з доступом до адміністрування, зовнішня кібератака. Проте експерт указав на зміну параметрів доступу вручну з IP-адреси медичної установи. Як слід перевірити кожну з версій? Які заходи можна застосувати для підтвердження внутрішньої причетності?

Завдання 19. Під час розслідування злочину, пов’язаного з розповсюдженням дитячої порнографії, було виявлено, що всі докази зберігаються не локально, а в хмарному сервісі за кордоном. Підозрюваний використовує двофакторну автентифікацію та шифрування. Які особливості проведення обшуку в таких випадках? Чи може слідчий вилучити логіни та паролі? Як діяти, якщо доступ заблоковано підозрюваним? Який процесуальний порядок отримання даних із хмарного сервісу за кордоном?

Завдання 20. Слідство встановило факт вимагання коштів у криптовалюті Bitcoin. Потерпілий отримав електронного листа з загрозами та адресою для переказу. Транзакція була здійснена. Слідчі мають доступ до blockchain-запису та ідентифікували IPадресу відправника через лог-файли поштового сервісу, однак адреса належить пулу хостинг-провайдера з США. Які електронні інформаційні системи можуть надати додаткову інформацію про криптогаманець зловмисника? Як установити ймовірне географічне положення зловмисника через мережеві ідентифікатори?

3. ТРЕНІНГИ

Порядок проведення тренінгу:

1. Вступна частина проводиться з метою ознайомлення здобувачів з темою тренінгового заняття.

2. Організаційна частина полягає у створенні робочого настрою у колективі здобувачів, визначенні правил проведення тренінгового заняття. Можлива наявність роздаткового матеріалу у вигляді таблиць, бланків документів та презентації.

3. Практична частина реалізовується шляхом виконання завдань самостійно та у групах здобувачів у кількості 3-5 осіб з певних проблемних питань теми тренінгового заняття.

4. Підведення підсумків. Обговорюється результати виконаних завдань у групах. Обмін думками з питань, які виносилися на тренінгові заняття.

Тематика тренінгів:

Тренінг № 1. Тематика: судовий розгляд справи про вчинення кіберзлочину.

Тренінг № 2. Тематика: захист об'єктів критичної інформаційної інфраструктури.

4. ТЕСТОВІ ЗАВДАННЯ ДЛЯ ПЕРЕВІРКИ ЗНАНЬ

1. Національний координаційний центр кібербезпеки - це
а) робочий орган Держспецзв'язку
б) робочий орган Ради національної безпеки і оборони України
в) робочий орган кіберполіції
г) підрозділ Служби безпеки України
2. Раду національної безпеки і оборони України очолює
а) Міністр оборони
б) Міністр закордонних справ
в) Президент України
г) Прем'єр-міністр України
3. Стратегія кібербезпеки України передбачає:
а) створення MIL.CERT-UA
б) створення MISP
в) імплементацію Конвенції про кіберзлочинність
г) приєднання до НАТО
4. Стратегія кібербезпеки України передбачає:
а) утворення кібервійськ
б) створення національної системи управління інцидентами
в) управління військами
г) управління суб'єктами забезпечення кібербезпеки
5. Запровадження планування видатків на кібербезпеку за окремими бюджетними програмами - це напрям діяльності
а) Президента України
б) Кабінету міністрів України
в) Верховної ради України
г) Ради національної безпеки та оборони України
6. Стратегія кібербезпеки України передбачає:
а) впровадження електронного документообігу між державними органами
б) розвиток систем технічного і криптографічного захисту інформації
в) розвиток Національного центру резервування державних інформаційних ресурсів
г) розвиток об'єктів критичної інформаційної інфраструктури
7. Стратегія кібербезпеки України передбачає:
а) впровадження цифрових послуг для населення
б) підвищення ефективності системи захисту персональних даних
в) провадження індикаторів стану кібербезпеки

8. Види інформації з обмеженим доступом
а) конфіденційна
б) таємна
в) службова
9. Інформації про особу (персональні дані) є
а) конфіденційною
б) таємною
в) службовою
10. Публічна інформація - це інформація
а) оголошена публічно
б) про діяльність суб'єктів владних повноважень
в) є завжди відкритою незалежно від змісту
г) є інформацією з обмеженим доступом
11. Інформація в документах суб'єктів владних повноважень про діяльність, яка передує прийняттю рішень є
а) конфіденційною
б) таємною
в) службовою
12. Інформація про зміст мобілізаційних планів державних органів є
а) конфіденційною
б) таємною
в) службовою
13. Ознаки кіберзлочину
а) передбачений Кримінальним кодексом України
б) вчинений з використанням кіберпростору
в) стосується реалізації комп'ютерної техніки
г) вчинений невідомими особами
14. Елементи кіберпростору
а) мережа Інтернет
б) кіберзлочинець
в) кіберполіція
г) комунікайційні системи
15. Спрямовані (навмисні) дії в кіберпросторі
а) кібератака
б) кіберінцидент
в) кіберзагроза
г) кіберзахист

16. Наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі
а) кібератака
б) кіберінцидент
в) кіберзагроза
г) кіберзахист
17. Подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора)
а) кібератака
б) кіберінцидент
в) кіберзагроза
г) кіберзахист
18. Сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам
а) кібератака
б) кіберінцидент
в) кіберзагроза
г) кіберзахист
19. Правопорушення проти конфіденційності згідно з Конвенцією про кіберзлочинність
а) незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями
б) порушення захисту прав виконавців, виробників фонограм і організацій мовлення
в) правопорушення, пов'язані з дитячою порнографією
г) підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами
20. Правопорушення, пов'язані з комп'ютерами згідно з Конвенцією про кіберзлочинність
а) підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами
б) порушення захисту прав виконавців, виробників фонограм і організацій мовлення
в) правопорушення, пов'язані з дитячою порнографією
г) незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями

21. Правопорушення, пов'язані зі змістом згідно з Конвенцією про кіберзлочинність
а) правопорушення, пов'язані з дитячою порнографією
б) порушення захисту прав виконавців, виробників фонограм і організацій мовлення
в) підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами
г) незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями
22. Правопорушення, пов'язані з порушенням авторських та суміжних прав згідно з Конвенцією про кіберзлочинність
а) порушення захисту прав виконавців, виробників фонограм і організацій мовлення
б) правопорушення, пов'язані з дитячою порнографією
в) підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами
г) незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями
23. Кіберзлочини згідно з Кримінальним кодексом України
а) шахрайство з використанням електронно-обчислювальної техніки
б) Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж
в) Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації
г) Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї
д) Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється
е) Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи

мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку
24. Об’єкти кібербезпеки
а) конституційні права і свободи людини і громадянина;
б) суспільство, держава, національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави
в) об’єкти критичної інфраструктури
г) громадяни, юридичні особи
25. Суб’єкти забезпечення кібербезпеки
а) правоохоронні органи, Держспецзв'язку
б) президент України, міністерства, органи місцевого самоврядування
в) підприємства, установи та організації, які не віднесені до об’єктів критичної інфраструктури
26. Основними суб’єктами національної системи кібербезпеки є
а) Держспецзв'язку, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України
б) президент України, міністерства, органи місцевого самоврядування
підприємства, установи та організації, які не віднесені до об’єктів критичної інфраструктури
27. Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA
а) збирає, накопичує та аналізує інформацію про кіберінциденти, веде державний реєстр кіберінцидентів
б) надає практичну допомогу з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об’єктів
в) здійснює розкриття кіберзлочинів, веде реєстр злочинів проти основ управління
г) має у прямому підпорядкуванні правоохоронні підрозділи та надає їм вказівки по усуненню негативних наслідків кіберінцидентів
28. Розпорядником інформаційно-комунікаційної системи реєстру та володільцем інформації (відомостей), що міститься у реєстрі об’єктів критичної інформаційної інфраструктури є
а) Адміністрація Держспецзв’язку
б) Кабінет Міністрів України

в) Офіс Президента України
г) Рада національної безпеки та оборони України
29. Хто здійснює ідентифікацію об’єктів критичної інформаційної інфраструктури та оцінку критичності об’єкта інформаційної інфраструктури
а) оператор основних послуг
б) уповноважений орган, який формує секторальний перелік об’єктів критичної інформаційної інфраструктури
в) Адміністрація Держспецзв’язку
30. На підставі відомостей із секторальних переліків об’єктів критичної інформаційної інфраструктури, отриманих від уповноважених органів за сектори (підсектори) критичної інфраструктури держави, формує та веде національний перелік об’єктів критичної інформаційної інфраструктури
а) оператор основних послуг
б) уповноважений орган, який формує секторальний перелік об’єктів критичної інформаційної інфраструктури
в) Адміністрація Держспецзв’язку
31. Першочергових заходів із захисту об’єкта критичної інформаційної інфраструктури від кібератак вживає
а) оператор основних послуг
б) уповноважений орган, який формує секторальний перелік об’єктів критичної інформаційної інфраструктури
в) Адміністрація Держспецзв’язку
г) Власник об’єкта критичної інформаційної інфраструктури, що внесений до національного переліку
32. Хто здійснює ідентифікацію об’єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури
а) оператор основних послуг
б) уповноважений орган, який формує секторальний перелік об’єктів критичної інформаційної інфраструктури
в) Секторальний орган у сфері захисту критичної інфраструктури
г) Адміністрація Держспецзв’язку
д) Власник об’єкта критичної інформаційної інфраструктури, що внесений до національного переліку
33. Зведений перелік об’єктів критичної інфраструктури секторальними органами у сфері захисту критичної інфраструктури подаються на затвердження
а) Кабінету Міністрів України

б) Президенту України
в) Адміністрації Держспецзв'язку
г) Раді національної безпеки та оборони України
34. Визначити секторальні органи у сфері захисту критичної інфраструктури
а) Міненерго, Мінцифри, Держспецзв'язку, Мінрегіон, Мінагрополітики, Мінекономіки
б) МОЗ, НКЦПФР, Мінфін, Мінінфраструктури, Мінстратегпром, МВС, Міндовкілля
в) Міноборони, СБУ, ДСА, Мін'юст, МОН, Національний банк, Центральна виборча комісія
г) Мінсоцполітики, МКІП, Держспецзв'язку.
35. Повноваження Держспецзв'язку
а) реалізація державної політики у сферах криптографічного і технічного захисту інформації
б) реалізація державної політики у сфері електронного документообігу
в) організовує забезпечення урядовим фельд'єгерським зв'язком та урядовим зв'язком
г) здійснює державний контроль за станом захисту у кіберпросторі державних інформаційних ресурсів та інформації
д) виконує функції Адміністрації зв'язку та радіочастот України
36. Електронна процедура, яка дає змогу підтвердити електронну ідентифікацію
а) автентифікація
б) реєстрація
в) ратифікація
37. Процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи
а) автентифікація
б) реєстрація
в) ратифікація
г) електронна ідентифікація
38. Користувачі електронних довірчих послуг
а) нотаріуси, особи, які надають електронну довіреність
б) суб'єкти забезпечення кібербезпеки, що надають послуги за наявності електронної довіреності

в) підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних.

38. Адміністрація Держспецзв'язку як суб'єкт Національної телекомунікаційної мережі:

а) здійснює контроль за наданням послуг Національної телекомунікаційної мережі за допомогою радіосегмента у смугах радіочастот спеціального користування

б) розробляє та затверджує схеми організації зв'язку в Національній телекомунікаційної мережі

в) розробляє та реалізує технічну політику з питань формування номерного ресурсу Національної телекомунікаційної мережі, його структуру і простір нумерації в інтересах забезпечення достатньої ємності такого ресурсу та його відповідність міжнародним вимогам

39. Здійснення заходів з кіберзахисту системами кіберзахисту передбачає:

а) автентифікацію, попередження, виявлення, застосування, реагування

б) автентифікацію, попередження, виявлення, реагування, відновлення

в) ідентифікацію, захист, виявлення, реагування, відновлення

40. Визначте секторальні органи у сфері захисту критичної інфраструктури

а) Міноборони, СБУ, ДСА, Мін'юст, МОН, Національний банк, Центральна виборча комісія

б) Мінсоцполітики, МКІП, Держспецзв'язку

в) МОЗ, НКЦПФР, Мінфін, Мінінфраструктури, Мінстратегпром, МВС, Міндовкілля

г) Усі відповіді правильні

д) Міненерго, Мінцифри, Держспецзв'язку, Мінрегіон, Мінагрополітики, Мінекономіки

41. Ідентифікація об'єктів критичної інформаційної інфраструктури проводиться у такому порядку:

а) - уповноважений орган визначає об'єкти, проводить оцінку їх критичності та надає інформацію уповноваженому органу

- Адміністрація Держспецзв'язку формує секторальний перелік об'єктів критичної інформаційної інфраструктури

- оператор основних послуг формує та веде національний перелік об'єктів критичної інформаційної інфраструктури

б) - оператор основних послуг визначає об'єкти, проводить оцінку їх критичності та надає інформацію уповноваженому органу
- уповноважений орган формує секторальний перелік об'єктів критичної інформаційної інфраструктури
- Адміністрація Держспецзв'язку формує та веде національний перелік об'єктів критичної інформаційної інфраструктури
в) - Адміністрація Держспецзв'язку визначає об'єкти, проводить оцінку їх критичності та надає інформацію уповноваженому органу
- уповноважений орган формує секторальний перелік об'єктів критичної інформаційної інфраструктури
- оператор основних послуг формує та веде національний перелік об'єктів критичної інформаційної інфраструктури

42. Організаційно-технічна модель кіберзахисту є:
а) комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем
б) комплексом заходів, сил і засобів кіберзахисту, спрямованих на ідентифікацію об'єктів критичної інфраструктури, критичної інформаційної інфраструктури та визначення технічних параметрів їх обслуговування

43. Першочергових заходів із захисту об'єкта критичної інформаційної інфраструктури від кібератак вживає
а) уповноважений орган, який формує секторальний перелік об'єктів критичної інформаційної інфраструктури
б) власник об'єкта критичної інформаційної інфраструктури, що внесений до національного переліку
в) Адміністрація Держспецзв'язку
г) оператор основних послуг

44. Кіберзахист об'єкта критичної інфраструктури забезпечується:
а) оператором основних послуг та/або Адміністрацією Держспецзв'язку
б) власником та/або керівником об'єкта критичної інфраструктури
в) уповноваженим органом, який формує секторальний перелік об'єктів критичної інформаційної інфраструктури

45. Базові вимоги із забезпечення кіберзахисту об'єктів критичної інфраструктури включають наявність
а) підрозділу або посадової особи з інфраструктурної безпеки; визначення прав та обов'язків користувачів

б) підрозділу або посадової особи з інформаційної безпеки;
в) визначення прав та обов'язків всіх категорій користувачів та адміністраторів
46. Транспортна платформа Національної телекомунікаційної мережі формує ресурс Національної телекомунікаційної мережі із таких складових:
а) фізичний сегмент, супутниковий сегмент, аудіосегмент
б) оптичний сегмент, супутниковий сегмент, радіосегмент
в) класичний сегмент, космічний сегмент, аудіосегмент
47. Формування загальної політики інформаційної безпеки; управління доступом користувачів; ідентифікація та автентифікація; реєстрація подій; мережевий захист; доступність та відмовостійкість компонентів; визначення умов використання змінних (зовнішніх) пристроїв; визначення умов використання програмного та апаратного забезпечення; визначення умов розміщення компонентів це –
а) технічні заходи
б) правові заходи
г) організаційні заходи
д) організаційні і технічні заходи
48. Кібергігієна -
а) уміння, навички користування інформаційними технологіями
б) критерії, що визначають порядок використання антивірусних програм в інформаційних системах
в) параметри допуску певних категорій осіб до роботи з інформаційними системами
49. Категоризація об'єктів критичної інфраструктури здійснюється за критеріями
а) рівень негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури
б) суспільну значущість об'єкта критичної інфраструктури
г) економічну значущість об'єкта критичної інфраструктури
д) Усі відповіді правильні
е) наявність взаємозв'язків між об'єктами критичної інфраструктури
є) соціальну значущість об'єкта критичної інфраструктури
ж) значущість об'єкта критичної інфраструктури для забезпечення національної безпеки та обороноздатності країни

50. Державні органи з метою здійснення захищеного інформаційного обміну, зберігання резервних копій інформаційних ресурсів, підключення до системи захищеного доступу державних органів до Інтернету Державного центру кіберзахисту використовують:
а) ресурси Національної телекомунікаційної мережі
б) резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту
в) інформаційні ресурси об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури
51. Базові вимоги із забезпечення кіберзахисту об'єктів критичної інфраструктури включають наявність:
а) визначення переліку інформаційних, програмних та апаратних ресурсів об'єкта критичної інформаційної інфраструктури; політики управління ризиками інформаційної безпеки і методики їх оцінювання та оброблення
б) правової оцінки ризиків виникнення кіберзагроз
в) розроблення та підтримання в актуальному стані технічної, проектної та іншої документації на комплексну систему захисту інформації
52. Життєво важливі послуги та функції -
а) послуги, які надаються, та функції, що виконуються, операторами основних послуг, збої та переривання у наданні (виконанні) яких призводять до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України
б) послуги, які надаються, та функції, що виконуються, операторами основних послуг, збої та переривання у наданні (виконанні) яких не призводять до позитивних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України
в) послуги, які надаються, та функції, що виконуються, операторами основних послуг, збої та переривання у наданні (виконанні) яких призводять до позитивних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки і оборони України
53. Власник об'єкта критичної інфраструктури

а) державний орган, підприємство, установа, організація будь-якої форми власності, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належить об’єкт критичної інфраструктури
б) державний орган якому на правах власності належить об’єкт критичної інфраструктури, який відповідає за його поточне функціонування
в) державний орган, підприємство, установа, організація будь-якої форми власності, юридична та/або фізична особа, якому/якій на правах власності, належить об’єкт критичної інфраструктури
г) підприємство, установа, організація будь-якої форми власності, юридична та/або фізична особа, якому/якій на правах оренди належить об’єкт критичної інфраструктури
54. Ідентифікація об’єкта критичної інформаційної інфраструктури - це
а) процедура інвентаризації об’єкта інформаційної інфраструктури до об’єктів критичної інформаційної інфраструктури
б) процедура віднесення об’єкта інформаційної інфраструктури до об’єктів критичної інформаційної інфраструктури
в) процедура автентифікації об’єкта інформаційної інфраструктури
55. Кіберзахист об’єкта критичної інфраструктури забезпечується шляхом:
а) впровадження на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю
б) організаційно-технічної моделі кіберзахисту
в) впровадження процесів організації функціонування об’єктів критичної інфраструктури, реалізації загроз, на які призводить до виведення з ладу або порушення функціонування самого об’єкта критичної інфраструктури та відповідно справляє негативний вплив на стан національної безпеки
56. Ресурс Національної телекомунікаційної мережі надається у такій черговості:
а) в інтересах функціонування державної системи урядового зв’язку, спецкористувачам, операторам НСКЗ, користувачам бюджетної сфери, власникам об’єктів критичної інформаційної інфраструктури
б) власникам об’єктів критичної інформаційної інфраструктури, в

інтересах функціонування державної системи урядового зв'язку, операторам НСКЗ, спецкористувачам, користувачам бюджетної сфери
57. Державні органи отримують доступ до Інтернету через:
а) Усі відповіді правильні
б) систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту
в) через власні системи захищеного доступу до Інтернету із створеними комплексними системами захисту інформації з підтвердженою відповідністю
г) через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю
58. Мультисервісна платформа Національної телекомунікаційної мережі призначена для забезпечення користувачів:
а) аналітичними послугами, послугами спеціального зв'язку та послугами з відновлення роботи об'єктів критичної інформаційної інфраструктури
б) мультимедійними послугами, послугами спеціального зв'язку та послугами з кіберзахисту
в) комерційними послугами, послугами спеціального зв'язку та послугами з кібербезпеки
59. Механізм віднесення об'єктів до критичної інфраструктури:
а) - оператори основних послуг ідентифікують об'єкти, разом з Держспецзв'язку здійснюють категоризацію; - секторальні органи складають та ведуть секторальні переліки об'єктів критичної інфраструктури і передають для формування зведеного переліку Кабінету Міністрів України; - Держспецзв'язку затверджує зведений перелік об'єктів критичної інфраструктури
б) - оператори основних послуг ідентифікують об'єкти, разом з Держспецзв'язку здійснюють категоризацію; - секторальні органи складають та ведуть секторальні переліки об'єктів критичної інфраструктури і передають Держспецзв'язку для формування зведеного переліку; - Кабінет Міністрів України затверджує зведений перелік об'єктів критичної інфраструктури
в) - секторальні органи у сфері захисту критичної інфраструктури ідентифікують об'єкти, разом з оператором здійснюють категоризацію

- секторальні органи складають та ведуть секторальні переліки об’єктів критичної інфраструктури і передають Держспецзв’язку для формування зведеного переліку; - Кабінет Міністрів України затверджує зведений перелік об’єктів критичної інфраструктури

60. Сектор (підсектор) критичної інфраструктури - це

а) державні підприємства, яким Держспецзв’язку надає спеціальні повноваження у сфері кібербезпеки

б) сукупність об’єктів критичної інфраструктури, які належать до одного сектору (підсектору) економіки та/або мають спільну функціональну спрямованість

в) сукупність об’єктів критичної інфраструктури, які визначені Держспецзв’язку та/або мають спільну функціональну спрямованість

61. Структура Національної телекомунікаційної мережі поділяється на:

а) структурну платформу, інформаційну платформу, Центр управління мережею

б) транспортну платформу, мультисервісну платформу, Центр управління мережею

в) транспортну платформу, інформаційну платформу, Центр управління мережею

62. Заходами з кіберзахисту, які здійснюються у процесі впровадження організаційно-технічної моделі кіберзахисту, є:

а) організаційні, нормотворчі, інформаційно-методичні, заходи з використання електронних довірчих послуг

б) організаційні, правові, інженерно-технічні заходи, заходи з криптографічного та технічного захисту інформації

в) організаційні, адміністративні, науково-технічні заходи, заходи з аналітичного та технічного захисту інформації

5. РЕКОМЕНДОВАНІ ТЕМИ РЕФЕРАТІВ

1. Інформація з обмеженим доступом.
2. Конфіденційна інформація юридичних осіб.
3. Види персональних даних.
4. Державна таємниця.
5. Правове регулювання доступу до службової інформації.
6. Реалізація Стратегії кібербезпеки в Україні.
7. Кіберзлочин в українському законодавстві.
8. Міжнародна співпраця в розкритті кіберзлочинів.
9. Заходи забезпечення кібербезпеки на об'єкті критичної інформаційної інфраструктури.
10. Кібербезпека в банківській системі.
11. Національний Центр резервування даних.
12. Потужності Національної телекомунікаційної мережі.
13. Впровадження комплексної системи захисту інформації.
14. Формування загальної політики інформаційної безпеки.
15. Недостатній рівень IT-освіти в суспільстві.
16. Завдання кіберполіції.
17. Повноваження Держспецзв'язку.
18. Діяльність CERT-UA.
19. Цифрові докази в судовому процесі.
20. Кіберзлочинність у фінансовій сфері України.
21. Розслідування кіберзлочинів, вчинених з використання віртуальних активів.
22. Захист інформаційної системи.
23. Кризове реагування на кібератаки та кіберінцидент.
24. Криптографічний захист в системі таємної інформації.
25. Правопорушення проти конфіденційності згідно з Конвенцією про кіберзлочинність

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Бачинський Т. Основи ІТ-права. Посібник. Київ. Юрінком Інтер, 2020. 244 с.
2. Висоцький В. М., Хатнюк Ю. А. Судові та правоохоронні органи України. Навчальний посібник. Львів. Львів. держ. ун-т внутр. справ, 2022. 219 с.
3. Гусаров С. М. Судові, правоохоронні, контрольно-наглядові та правозахисні органи України. Підручник. Харків. Нац. ун-т внутр. справ, 2020. 507 с.
4. Дараган В. В. Судові та правоохоронні органи України. Дніпро. ДДУВС, 2021. 399 с.
5. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів круглого столу (09 грудня 2020 р., м. Харків). Харків. ХНУВС, 2020. 132 с.
6. Макаров М. А., Симчук А. С., Кулик М. Й., Терещенко Ю. В., Харченко С. В. Судові та правоохоронні органи України. Навчальний посібник. Київ. Нац. акад. внутр. справ, 2022. 656 с.
7. Ткачук Н. А. Стан та проблемні питання реалізації Стратегії кібербезпеки України. Інформація і право. 2019. № 1. С. 129-134.
8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26 серпня 2021 року № 447/2021 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.06.2023).
9. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України": Указ Президента України від 01 лютого 2022 року № 37/2022 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text (дата звернення: 10.06.2023).
10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури»: Указ Президента України від 16 січня 2017 року № 8/2017 / Президент України. URL:

https://zakon.rada.gov.ua/laws/show/8/2017#Text (дата звернення: 10.12.2025).

11. Про рішення Ради національної безпеки і оборони України від 16 лютого 2017 року «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури»: Указ Президента України від 16 лютого 2017 року № 37/2017 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/37/2017#Text (дата звернення: 10.12.2025).

12. Про Національний координаційний центр кібербезпеки: Указ Президента України від 7 червня 2016 року № 242/2016 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 10.12.2025).

13. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (дата звернення: 10.12.2025).

14. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 10.12.2025).

15. Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29 грудня 2021 р. № 1426/ Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text (дата звернення: 10.12.2025).

16. Деякі питання функціонування Національної телекомунікаційної мережі: Постанова Кабінету Міністрів України від 16 грудня 2020 р. № 1358 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text (дата звернення: 10.12.2025).

17. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 10.12.2025).

18. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 08 лютого 2021 р. № 92 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text (дата звернення: 10.12.2025).

19. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.12.2025).

20. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 10.12.2025).

21. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення: 10.12.2025).

22. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 10.12.2025).

23. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 10.12.2025).

24. Про інформацію: Закон України від 02 жовтня 1992 року № 2657-XII / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 10.12.2025).

25. Про електронні довірчі послуги: Закон України від 05 жовтня 2017 року № 2155-VIII / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 10.12.2025).

26. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 року № 851-IVI / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 10.12.2025).

27. Котух Є.В. Кібербезпека у публічному секторі [Текст] : монографія / Є. В. Ковтух ; Нац. акад. держ. упр. при Президентові України, Харків. регіон. ін-т держ. упр. - Харків : Колегіум, 2021. - 271 с.

28. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. – Київ: ВАІТЕ, 2021. – 106 с.

29. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

30. Колб О., Дучимінська Л. Інформаційна безпека як об'єкт правового захисту в Україні. Освітньо-наукове забезпечення діяльності складових сектору безпеки й оборони України : тези XII Всеукр. наук.-практ. конфер. (Хмельницький, 26 листопада 2020 року). Хмельницький : Вид-во НАДПСУ, 2020. С. 291-292.

31. Колб О. Г., Дучимінська Л. М., Колб Р. О. Національна безпека України: поняття, зміст, проблеми забезпечення та шляхи їх вирішення. Деліктологія: монографія. Під заг.ред. І. М. Копотуна, С. В. Пєткова. Куновіце: Академія ГУСПОЛ: 2020, Т. 2 с. 38-57.

32. Кримінальна відповідальність за несанкціоноване втручання в роботу ЕОМ: монографія / Ю. А. Бельський, П. А. Воробей, А. В. Савченко, О. Г. Колб. Київ: Юрінком Інтер, 2019. 264 с.

33. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2021. № 6 (червень). 261с.

34. Лисеюк А. М., Свінцицька Т. В. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції. Право та інновації. № 4 (48). 2024. С. 32-38.

35. Зайцева-Калаур І. В. Інформаційне право. Практикум: навчально-методичні матеріали. Тернопіль, 2017. 55 с.

36. Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан. Кіберзлочинність та електронні докази : навч. посібник. Львів. ЛНТУ ім. Івана Франка, 2022. 298 с.

37. М. О. Думчиков. Методичні вказівки до проведення практичних (семінарських), індивідуальних занять та самостійної роботи з дисципліни «Протидія кіберзлочинності». Суми: Сумський державний університет, 2025. 80 с.

Нормативно-правове забезпечення кібербезпеки. [Текст]: методичні вказівки до семінарських занять та виконання самостійних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузі знань F Інформаційні технології спеціальності F5 Кібербезпека та захист інформації денної та заочної форм навчання / уклад. С.Г. Зицик. Луцьк. ЛНТУ, 2025 с. 38.

Комп'ютерний набір С.Г. Зицик
Редактор С.Г. Зицик

Підп. до друку «__»_____2025 р.
Формат 60х84/16. Папір офс.
Гарн. Таймс. Ум. друк. арк. __
Тираж 50 прим.

Відділ іміджу та промоцій
Луцького національного технічного університету
43018, м. Луцьк, вул. Львівська, 75
Друк – ВІП ЛНТУ