МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

МЕТОДИЧНІ ВКАЗІВКИ

до самостійної роботи
для здобувачів першого (бакалаврського) рівня вищої освіти
спеціальності 262 – Правоохоронна діяльність

Обговорено і рекомендовано
на засіданні кафедри кібербезпеки
та математичного моделювання
протокол № 8
від 21.01.2022 р.

Чернігів – 2022

Інформаційна безпека держави. Методичні вказівки до самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 262 – Правоохоронна діяльність // Укл.: Ю.М.Ткач, С.М.Семендяй – Чернігів: НУ «Чернігівська політехніка», 2022. – 19 с.

Укладачі: Ткач Юлія Миколаївна
доктор педагогічних наук, завідувач кафедри кібербезпеки та математичного моделювання, професор

Семендяй Сергій Матвійович
старший викладач кафедри кібербезпеки та математичногомоделювання

Відповідальний за випуск: Петренко Тарас Анатолійович
кандидат технічних наук, доцент кафедри кібербезпеки та математичного моделювання

Рецензент: Мехед Дмитро Борисович
кандидат педагогічних наук, доцент кафедри кібербезпеки та математичного моделювання

Вказівки підготовлено відповідно до навчального плану підготовки бакалаврів спеціальності 262 – Правоохоронна діяльність. Методичні рекомендації містять загальні положення щодо організації самостійної роботи студентів, теоретичний матеріал та завдання на роботу. Є керівним документом для здобувачів вищої освіти освітнього ступеню «бакалавр», спеціальності 262 – Правоохоронна діяльність.

ЗМІСТ

ВСТУП

Самостійна робота передбачена навчальним планом освітньо-кваліфікаційного рівня «бакалавр» спеціальності 262 – «Правоохоронна діяльність». Самостійна робота є основним засобом оволодіння навчальним матеріалом у час, вільний від аудиторних навчальних занять без посередньої участі науково-педагогічного працівника. Зміст самостійної роботи здобувача вищої освіти визначається робочою навчальною програмою дисципліни, методичними рекомендаціями до самостійної роботи та завданнями (вказівками) викладача.

Самостійна робота здобувача вищої освіти забезпечується системою навчально-методичних засобів, передбачених для вивчення навчальної дисципліни: підручник, навчальні та методичні посібники, конспект лекцій НПП. Методичні матеріали для самостійної роботи здобувачів вищої освіти передбачають можливість проведення самоконтролю з боку здобувача вищої освіти. Для самостійної роботи здобувачу вищої освіти також рекомендується відповідна наукова та фахова монографічна і періодична література.

Самостійна робота здобувача вищої освіти над засвоєнням навчального матеріалу з дисципліни може виконуватися в бібліотеці Університету, навчальних кабінетах, комп'ютерних класах (лабораторіях), а також у домашніх умовах.

Обсяг часу, відведений для самостійної роботи здобувача вищої освіти, відображений у навчальному плані й складає 90 годин.

Робота здобувача вищої освіти включає: опрацювання навчального матеріалу, виконання індивідуальних завдань, підготовку до практичних занять, контрольних заходів, написання реферату.

Навчальний матеріал, передбачений робочою навчальною програмою дисципліни для засвоєння здобувачем вищої освіти в процесі самостійної роботи, виноситься на підсумковий (семестровий) контроль поряд з навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

ТЕМАТИЧНИЙ ПЛАН САМОСТІЙНОЇ РОБОТИ

Тема 1. Поняття інформаційної безпеки держави, суспільства та особи

Підтеми:

1. Інформаційна безпека (поняття і визначення).
2. Підходи до визначення поняття «інформаційна безпека».
3. Поняття та загальні властивості інформації.
4. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері.
5. Об'єкти, суб'єкти та види інформаційної безпеки.
6. Співвідношення понять інформаційної та кібербезпеки.

Основні поняття:

- Інформація;
- Інформаційні відносини;
- Інформаційний суверенітет;
- Інформаційний простір;
- Інформаційна інфраструктура;
- Інформаційні ресурси;
- Інформаційні технології;
- Інформаційна система;
- Інформаційне середовище;
- Інформаційний ринок;
- Інформаційний продукт;
- Інформаційне забезпечення;
- Інформаційне поле;
- Інформаційне суспільство;
- Інформатизація;
- Інформатика;
- Інформаційна зброя;
- Інформаційна сфера;
- Інформаційна безпека;
- Державна таємниця;
- Матеріальні носії секретної інформації;
- Система захисту державної таємниці;
- Допуск до державної таємниці;
- Гриф секретності;
- Ступінь секретності;
- Інформаційна безпека держави.

Запитання для самоконтролю та самоперевірки:

1. Які основні підходи до визначення поняття «інформаційна безпека» ви

знаєте?
2. Назвіть основні ознаки інформаційної безпеки.
3. Назвіть основні визначення поняття «інформаційна безпека».
4. Назвіть об'єкти, суб'єкти та види інформаційної безпеки.
5. Що таке інформація?
6. Що таке джерело інформації?
7. Які є носії інформації?
8. Що розуміють під інформаційними ресурсами?
9. Що таке загроза інформації ?
10. Дайте визначення документованої інформації.
11. Назвіть перелік конфіденційної інформації.
12. Як класифікуються види інформації?
13. Які є основні властивості інформації ?
14. Які класи (види) загроз розрізняються в інформаційній сфері?
15. Які загрози відносяться до рівня порушення конфіденційності ?
16. Які загрози відносяться до рівня порушення цілісності ?
17. Які існують категорії джерел конфіденційної інформації?
18. Що таке кіберборотьба? Які основні особливості їй притаманні?
19. Дайте визначення поняття «кібернетична безпека».
20. Назвіть істотні ознаки, які його характеризують.

Тема 2. Небезпеки для інформаційної безпеки держави, суспільства та особи

Підтеми:

1. Поняття загроз інформаційній безпеці.
2. Види загроз інформаційній безпеці.
3. Дестабілізуючі фактори загроз.
4. Фактори загроз інформаційній безпеці.
5. Джерела загроз інформаційній безпеці.
6. Етапи розвитку засобів інформаційних комунікацій.

Основні поняття:

- Загрози інформаційній безпеці;
- Дестабілізуючі фактори загроз;
- Джерела загроз інформаційній безпеці.

Запитання для самоконтролю та самоперевірки:

1. Яким чином розрізняються групи загроз інформації?
2. Назвіть основні характеристики загроз інформаційній безпеці України.
3. Які основні підходи до визначення дестабілізуючих факторів ви знаєте?
4. Дайте визначення поняттям «загроза», «небезпека».
5. Як співвідносяться категорії «небезпека» та «загроза»?
6. Визначте види загроз за певними критеріями.
7. Визначте фактори загроз за певними критеріями.

8. Назвіть джерела загроз інформаційній безпеці.
9. Назвіть базові загрози інформаційній безпеці держави.
10. Назвіть базові загрози інформаційній безпеці суспільству.
11. Назвіть базові загрози інформаційній безпеці людині, громадянину.
12. Які існують етапи розвитку засобів інформаційних комунікацій?
13. Які завдання можуть вирішуватися за допомогою сучасної інформаційної зброї?

Тема 3. Методи та засоби забезпечення інформаційної безпеки держави

Підтеми:

1. Основні принципи забезпечення інформаційної безпеки держави.
2. Система забезпечення інформаційної безпеки держави.
3. Основні форми забезпечення інформаційної безпеки держави.
4. Методи забезпечення інформаційної безпеки.

Основні поняття:

- Превентивність;
- Адекватна інформованість;
- Забезпечення інформаційної безпеки держави;
- Інформаційний патронат;
- Інформаційний захист;
- Інформаційна кооперація;
- Інформаційне протиборство;
- Методи забезпечення інформаційної безпеки.

Запитання для самоконтролю та самоперевірки:

1. Поняття системи забезпечення інформаційної безпеки держави.
2. У чому полягає відмінність системи інформаційної безпеки від системи забезпечення інформаційної безпеки?
3. Що таке превентивність?
4. Дати визначення інформаційного протиборства.
5. Що таке інформаційна кооперація?
6. Що таке інформаційний патронат?
7. Як можна тлумачити поняття адекватної інформованості?

Тема 4. Поняття та зміст інформаційного протиборства.

Підтеми:

1. Основні форми інформаційного протиборства.
2. Основні форми інформаційної війни.
3. Інформаційна зброя в інформаційній війні.

Основні поняття:

- Інформаційне протиборство;
- Інформаційна експансія;
- Інформаційна агресія;
- Інформаційна війна;
- Концепція інформаційної війни;
- Органи інформаційної війни;
- Наступальна інформаційна операція;
- Оборонна інформаційна операція;
- Радіоелектронна війна;
- Радіоелектронне забезпечення;
- Радіоелектронна атака;
- Радіоелектронна контрпротидія;
- Інформаційна зброя атаки;
- Інформаційна зброя забезпечення;
- Інформаційна алгоритмічна (математична) зброя;
- Програми з потенційно небезпечними наслідками;
- Комп'ютерні віруси;
- Засоби несанкціонованого доступу;
- Програмні закладки.

Запитання для самоконтролю та самоперевірки:

1. Дайте визначення поняття «інформаційне протиборство».
2. Назвіть рівні проведення інформаційного протиборства.
3. Назвіть основні ступені інформаційного протиборства.
4. Дайте визначення поняттям «інформаційна експансія», «інформаційна агресія» та «інформаційна війна».
5. Що відноситься до органів інформаційної війни?
6. Назвіть основні форми інформаційної війни.
7. Що являє собою оперативна безпека?
8. Яким чином відрізняється інформаційна зброя від звичайних засобів ураження?
9. Назвіть сферу застосування інформаційної зброї.
10. Назвіть основні об’єкти застосування інформаційної зброї.
11. Яким чином розрізняються засоби ураження інформаційних комп'ютерних систем?
12. Які функції мають спроможність виконувати програми з потенційно небезпечними наслідками?
13. Що таке комп’ютерні віруси?
14. Які існують види програмних закладок?

Тема 5. Основи теорії інформаційної боротьби

Підтеми:

1. Зміст теорії інформаційної боротьби.

2. Закони та закономірності інформаційної боротьби.
3. Принципи інформаційної боротьби.
4. Заходи інформаційної боротьби.
5. Способи інформаційної боротьби.
6. Форми ведення інформаційної боротьби.
7. Методологія оцінки ефективності інформаційної боротьби.

Основні поняття:

- Інформаційна боротьба;
- Мета інформаційної боротьби;
- Політичний фактор;
- Економічний фактор;
- Воєнний фактор;
- Інформаційний фактор;
- Теорія ураження інформації;
- Теорія сил і засобів ураження інформації;
- Теорія захисту інформації;
- Категорії інформаційної боротьби;
- Принципи інформаційної боротьби;
- Заходи інформаційної боротьби;
- Способи інформаційної боротьби;
- Форми ведення інформаційної боротьби ;
- Оцінка ефективності інформаційної боротьби;
- Критерій ефективності інформаційної боротьби.

Запитання для самоконтролю та самоперевірки:

1. Дати визначення інформаційної боротьби.
2. Яка мета інформаційної боротьби?
3. Які фактори впливають на зміст інформаційної боротьби?
4. Які існують заходи інформаційної боротьби?
5. Охарактеризувати принципи інформаційної боротьби**.**
6. Дати визначення метода оцінки ефективності інформаційної боротьби.
7. Які існують форми ведення інформаційної боротьби?
8. Які існують способи інформаційної боротьби?
9. Що таке радіоелектронно-вогневий удар
10. Формула для обчислення числового значення критерію ефективності інформаційної боротьби

Тема 6. Основи безпеки інформаційних ресурсів

Підтеми:

1. Загрози безпеці інформації та інформаційних ресурсів.
2. Джерела загроз безпеці інформації.

3. Класифікація вразливостей безпеки.
4. Моделі порушень інформаційних ресурсів.
5. Побудова моделі порушника.

Основні поняття:

- Джерело загрози;
- Загроза (дія);
- Фактор (вразливість);
- Наслідки (атака);
- Крадіжка;
- Копіювання комп'ютерної інформації;
- Знищення комп'ютерної інформації;
- Пошкодження;
- Модифікація комп'ютерної інформації;
- Блокування комп'ютерної інформації;
- Обман;
- Об'єктивні вразливості
- Суб'єктивні вразливості;
- Випадкові вразливості;
- Кваліфікація порушника;
- Ступінь ризику.

Запитання для самоконтролю та самоперевірки:

1. Що є джерелом та фактором загрози інформації?
2. Що розуміють під збитками?
3. Які є види загроз комп'ютерної інформації?
4. Які є групи джерел загроз безпеці інформації?
5. Наведіть класифікацію уразливостей безпеці інформації?
6. Які є моделі порушень інформаційних ресурсів?
7. Яка мета і цілі порушника об’єктів інформаційної діяльності?
8. Класифікація порушника за характером дій.

Тема 7. Забезпечення безпеки інформації та інформаційних ресурсів.

Підтеми:

1. Основні напрями забезпечення безпеки інформації.
2. Правовий захист. Організаційний захист.
3. Інженерно-технічний захист.

Основні поняття:

- Правовий захист;
- Конституційне законодавство;
- Загальні закони;
- Закони про організацію управління;

- Спеціальні закони;
- Підзаконні нормативні акти;
- Правоохоронне законодавство України;
- Спеціальне законодавство;
- Ліцензія;
- Комерційна таємниця;
- Організаційний захист;
- Інженерно-технічний захист;
- Фізичні засоби захисту;
- Програмні засоби захисту;
- Криптографічні та стеганографічні засоби захисту;
- Зони безпеки.

Запитання для самоконтролю та самоперевірки:

1. Які напрями захисту інформації ви знаєте?
2. Сформулюйте поняття права.
3. Яка структура правових актів, які орієнтовані на правовий захист інформації?
4. Дати означення ліцензії.
5. Що таке комерційна таємниця?
6. Що забезпечує організаційний захист?
7. Назвіть основні організаційні заходи.
8. Функції служби безпеки підприємства (фірми, організації).
9. Завдання служби безпеки підприємства (фірми, організації).
10. Що таке інженерно-технічний захист? Його завдання.
11. Фізичні засоби захисту та їх завдання.
12. Які апаратні засоби захисту інформації ви знаєте?
13. Що таке криптографія та стеганографія?

Тема 8. Захист інформаційних систем

Підтеми:

1. Джерела конфіденційної інформації.
2. Інформаційна система як об’єкт захисту інформації.
3. Рівні захисту інформаційних систем.
4. Аналіз вразливостей корпоративних інформаційних систем.
5. Основні принципи захисту інформації.

Основні поняття:

- Джерела конфіденційної інформації;
- Технічні носії;
- Технічні засоби обробки інформації;
- Промислові та виробничі відходи;
- Інформаційна система;

- Конфіденційність;
- Доступність;
- Цілісність;
- Захищена інформаційна система;
- Рівні захисту інформаційних систем;
- Корпоративна інформаційна система;
- Принципи захисту інформації.

Запитання для самоконтролю та самоперевірки:

1. Що таке джерело інформації?
2. Які існують категорії джерел конфіденційної інформації?
3. Дайте визначення інформаційної системи.
4. Які складові має інформаційна система?
5. Що є об'єктом та предметом захисту інформації?
6. Розкрийте поняття «цілісність».
7. Розкрийте поняття «доступність».
8. Розкрийте поняття конфіденційності інформації.
9. Назвіть основні напрями забезпечення безпеки інформації.
10. Назвіть основні характеристики інформаційної системи.
11. Розкрийте зміст моделі системи захисту інформації.
12. Якими показниками може бути оцінено якість розподілу доступу?
13. Назвіть основні принципи та рівні захисту інформаційних систем.
14. Які існують основні принципи захисту інформації?

Тема 9. Інформаційно-комунікаційні системи та комп'ютерні мережі

Підтеми:

1. Визначення інформаційно-комунікаційних систем.
2. Захист інформації в комп'ютерних мережах.
3. Безпека інформаційних ресурсів у ІКСМ на базі ISO/IEC.
4. Задачі організації безпеки інформації та інформаційних ресурсів.

Основні поняття:

- Багаторівнева модель інформаційно-комунікаційної системи;
- Захист інформації в комп'ютерних мережах;
- Мережева взаємодія;
- Стандарт ISO/IEC 17799;
- Безпека обміну інформацією й програмним забезпеченням.

Запитання для самоконтролю та самоперевірки:

1. Розкрийте поняття інформаційно-комунікаційної системи.
2. Назвіть рівні інформаційно-комунікаційних мереж.
3. Сутність випадкового методу доступу до ресурсів системи.
5. Які основні типи протоколів використовуються в моделі ISO/OSI?

6. Перерахуйте основні функції рівнів моделі ISO/OSI.
7. Дайте визначення поняттю «IP адреса»?
8. Назвіть основні вимоги для проектування більшості мережних проектів.
9. Основні завдання захисту інформації в мережі?
10. Різновиди побудови комп'ютерних мереж?
11. Що повинні включати угоди обміну програмним забезпеченням?
12. Назвіть заходи управління обробкою й зберіганням інформації.

Тема 10. Основи управління інформаційною безпекою

Підтеми:

1. Політика інформаційної безпеки організації.
2. Основні правила інформаційної безпеки організації.
3. Заходи управління інформаційною безпекою.

Основні поняття:

- Політика інформаційної безпеки організації;
- Об'єкт інформаційної безпеки організації;
- Система забезпечення інформаційної безпеки організації;
- Методологія розробки політики безпеки;
- Концепція інформаційної безпеки;
- Аналіз ризиків;
- Основні правила інформаційної безпеки організації;
- Заходи управління інформаційною безпекою.

Запитання для самоконтролю та самоперевірки:

1. Що розуміється під "політикою інформаційної безпеки"?
2. Що представляє собою система забезпечення інформаційної безпеки організації?
3. Які є основні принципи політики безпеки організації?
4. Що передбачає аналіз ризиків інформаційної сфери?
5. Наведіть основні правила інформаційної безпеки організації.
6. Які є варіанти побудови системи забезпечення інформаційної безпеки?
7. Наведіть комплекс заходів із забезпечення безпеки інформації.
8. Які повинні бути вироблені підходи забезпечення безпеки інформації на правовому рівні?
9. Які повинні бути вироблені підходи забезпечення безпеки інформації на організаційному рівні?
10. Які повинні бути вироблені підходи забезпечення безпеки інформації на технічному рівні?
11. Які є правила розмежування доступу користувачів?
12. Що містити в собі документальне оформлення політики безпеки?

Тема 11. Забезпечення інформаційної безпеки України

Підтеми:

1. Інформаційна безпека і її місце в системі національної безпеки України.
2. Основні реальні та потенційні загрози інформаційній безпеці України.
3. Стан та перспективи розвитку інформаційної безпеки України.

Основні поняття:

- Система національних інтересів;
- Військова безпека;
- Екологічна безпека;
- Інформаційна безпека;
- Сили забезпечення безпеки;
- Основні реальні та потенційні загрози.

Запитання для самоконтролю та самоперевірки:

1. Що розуміється під "інформаційною безпекою України"?
2. Яке її місце в системі національної безпеки України?
3. Основні напрями політики інформаційної безпеки України?
4. Найважливіші завдання в області інформаційної безпеки?
5. Які відомства регулюють правові стосунки в області захисту інформації?
6. У яких сферах проявляються основні реальні та потенційні загрози безпеці України?
7. Охарактеризуйте загрози інформаційній безпеці України у воєнній сфері.
8. Охарактеризуйте загрози інформаційній безпеці України в економічній сфері.
9. Охарактеризуйте загрози інформаційній безпеці України у в екологічній сфері.

Тема 12. Система та політика забезпечення інформаційної безпеки України.

Підтеми:

1. Основні функції системи забезпечення інформаційної безпеки України.
2. Мета функціонування, завдання системи забезпечення інформаційної безпеки.
3. Політика інформаційної безпеки і її реалізація в Законодавстві України.
4. Органи забезпечення інформаційної безпеки і захисту інформації.
5. Методи забезпечення інформаційної безпеки України.
6. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя.

Основні поняття:

- політика інформаційної безпеки;
- законодавство в області захисту інформації;
- відомства, що регулюють відносини в області захисту інформації;

- Державна служба спеціального зв’язку та захисту інформації України;
- Державна система урядового зв’язку;
- Національна система конфіденційного зв’язку;
- урядовий фельд’єгерський зв’язок;
- поштовий зв'язок спеціального призначення;
- радіочастотний ресурс;
- План використання радіочастотного ресурсу України;
- Концепція реформування Державної служби спеціального зв'язку та захисту інформації України.

Запитання для самоконтролю та самоперевірки:

1. Поняття системи забезпечення інформаційної безпеки.
2. У чому полягає відмінність системи інформаційної безпеки від системи забезпечення інформаційної безпеки?
3. Визначте мету формування системи забезпечення інформаційної безпеки.
4. Окресліть методи забезпечення інформаційної безпеки.
5. Охарактеризуйте забезпечення інформаційної безпеки України в сфері економіки.
6. Охарактеризуйте забезпечення інформаційної безпеки України в сфері внутрішньої та зовнішньої політики.
7. Як тлумачиться забезпечення інформаційної безпеки України у галузі науки та техніки?
8. Як можна охарактеризувати забезпечення інформаційної безпеки України у загальнодержавних інформаційних і телекомунікаційних системах?
9. Який державний орган призначений для забезпечення функціонування і розвитку Національної системи конфіденційного зв’язку?
10. Які заходи передбачає Концепція реформування Державної служби спеціального зв'язку та захисту інформації України?
11. На що саме спрямовуватиметься, згідно з Концепцією реформування Державної служби спеціального зв'язку та захисту інформації України, розвиток Національної системи конфіденційного зв'язку?
12. Що являє собою Державна система урядового зв'язку?
13. Якими нормативними документами визначається можливість забезпечення урядовим зв'язком конкретних посадових осіб державних органів, місцевого самоврядування, підприємств, установ та організацій?
14. Що являє собою Національна система конфіденційного зв'язку?
15. Дайте визначення фельд’єгерському зв’язку.
16. Які основні завдання підрозділів урядового фельд’єгерського зв’язку Державної служби спеціального зв’язку та захисту інформації України?
17. Яке має призначення Поштовий зв'язок спеціального призначення?
18. Дайте визначення радіочастотного ресурсу.
19. Ким саме розробляється План використання радіочастотного ресурсу України?

Тема 13. Інформаційна безпека України у сфері прав і свобод людини

Підтеми:

1. Поняття права на інформацію.
2. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина.
3. Структура конституційного права на інформацію.
4. Нормативно-правове забезпечення інформаційної безпеки України.

Основні поняття:

- Види інформаційних прав і свобод;
- Структура конституційного права на інформацію;
- Інформаційний суверенітет України;
- Основні напрями державної політики у сфері ТЗІ.

Запитання для самоконтролю та самоперевірки:

1. Дайте визначення поняття «право на інформацію».
2. Як співвідносяться поняття «право на інформацію», «інформаційні права» ?
3. Яка структура конституційного права на інформацію?
4. Назвіть основні права та свободи в інформаційній сфері, що закріплюються Конституцією України.
5. Що Ви вважаєте слід зробити для створення надійної системи забезпечення інформаційної безпеки і захисту інформаційної сфери суспільства?
6. Які базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України?
7. Які правові основи інформаційної діяльності закладено у Закон України «Про інформацію»?
8. Надайте визначення інформації згідно зі ст. 1 Закону України «Про інформацію».
9. Які основні види інформації визначаються у Законі України «Про інформацію»?
10. Як поділяється інформація за режимом доступу до неї?
11. Як здійснюється контроль за режимом доступу до інформації?
12. Як поділяється за своїм правовим режимом інформація з обмеженим доступом?
13. Яка інформація відноситься до конфіденційної?
14. Яка інформація не може бути конфіденційною?
15. Яка інформація відноситься до таємної інформації?
16. Чим та як визначається інформація, що складає державну таємницю?
17. Чим визначається ступень таємності інформації?
18. Які грифи таємності можуть надаватися інформації та який їх терміни дії?
19. Яка інформація входить до інформаційних ресурсів України?
20. Чим забезпечується інформаційний суверенітет України?

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аналіз вразливостей корпоративних інформаційних систем / Д.Б. Мехед, Ю.М. Ткач, В.М. Базилевич, В.І. Гур'єв, Я.Ю. Усов // Захист інформації Ukrainian Information Security Research Journal. – 2018. – №1. – С. 61–66.
2. Андріяш В. І. Державна політика: концептуальні аспекти визначення. Електронний ресурс. – Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=626
3. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,;// Гол. ред. Ю. О. Шпак. - К.: "МК-Прес", 2015. - 432 с.
4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
5. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015.— 288 с.
6. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.
7. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD) [Електронний ресурс] – Режим доступу: http://www.cbz.com.ua/
8. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD) [Електронний ресурс] – Режим доступу: https://web.archive.org/web/20160304091010/http:/www.cbz.com.ua/resources/files/8510076024d22f2d964df2.pdf
9. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/47/2017#Text
10. Забезпечення інформаційної безпеки держави: Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.
11. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/3855-12#Text
12. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
13. Закон України «Про інформацію» від 02.10.1992 № 2657-XII [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
14. Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є.Забезпечення інформаційної безпеки держави Є.В. Іванченко [та ін.] ; за

ред. проф. В.О. Хорошка ; Вид-во Нац. авіац. ун-ту, 2016. 254 с.

15. Інформаційна безпека держави: підручник / [В.М. Петрик. М.М. Присяжнюк., Д.С. Мельник та ін.]; в 2 т. Т. 1. / за заг. ред. В.В. Остроухова - К.: ДНУ «Книжкова палата України». 2016. 264 с.

16. Інформаційна безпека України в умовах євроінтеграції: конспект лекцій. Електронний ресурс. – Режим доступу: http://pidruchniki.com/1584072028356/politologiya/informatsiyna_bezpeka_ukrayini_v_umovah_yevrointegratsiyi

17. Карпенко В. Інформаційна політика та безпека: підручник. – Київ, 2006. -Електронний ресурс. Режим доступу: http://ukrlife.org/main/karp/bezpeka15.htm

18. Климчук О. О. Забезпечення інформаційної безпеки держави : підручник / [О. О. Климчук, В. М. Петрик, М. М. Присяжнюк та ін.] ; за заг. ред. О. А. Семченка та В. М. Петрика. – К. : ДНУ «Книжкова палата України», 2015. – 672 с.

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

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

21. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1020

22. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/uploads/l_1023_75718671.pdf

23. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1032

24. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1030

25. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1031

26. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1050

27. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу:

http://www.dut.edu.ua/ua/lib/1/category/919/view/1036

28. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1037

29. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/uploads/l_1057_37661772.pdf

30. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%EF#Text

31. Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736[1] [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF-%EF

32. Про Стратегію інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://ips.ligazakon.net/document/U685_21?an=4&ed=2021_12_28

33. Технічне завдання на створення автоматизованої системи. ГОСТ 34.602-89 [Електронний ресурс] – Режим доступу: https://www.rts.ua/rus/forpro/613/0/17/