Міністерство освіти і науки України
Національний університет водного господарства
та природокористування
Кафедра обчислювальної техніки

04-04-256М

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторних робіт з навчальної дисципліни
«Менеджмент інформаційної безпеки»
для здобувачів вищої освіти другого (магістерського) рівня
галузі знань 12 «Інформаційні технології»
за спеціальністю 123 «Комп'ютерна інженерія»
денної та заочної форм навчання

Рекомендовано науково-
методичною радою
з якості ННІАКОТ
Протокол №7 від 29.05.2023р.

Рівне – 2023

Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни «Менеджмент інформаційної безпеки» для здобувачів вищої освіти другого (магістерського) рівня галузі знань 12 «Інформаційні технології» за спеціальністю 123 «Комп'ютерна інженерія» денної та заочної форм навчання [Електронне видання] / Назарук В. Д. – Рівне : НУВГП. – 32 с.

Укладач: Назарук В. Д., кандидат технічних наук, старший викладач кафедри обчислювальної техніки.

Відповідальний за випуск: Круліковський Б. Б., завідувач кафедри обчислювальної техніки.

Керівник (гарант) освітньої програми «Комп'ютерна інженерія» спеціальності 123 «Комп'ютерна інженерія» Круліковський Б. Б.

ЗМІСТ

Вступ

Навчальна дисципліна «Менеджмент інформаційної безпеки» охоплює питання розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи менеджменту інформаційної безпеки. Значну увагу зосереджено на тому, щоб система менеджменту інформаційної безпеки була частиною та інтегрувалася в процеси організації та загальну структуру управління, щоб інформаційну безпеку розглядали в ході розроблення, інформаційних систем і заходах безпеки для забезпечення збереження конфіденційності, цілісності й доступності інформації.

В процесі опанування теоретичної частини дисципліни «Менеджмент інформаційної безпеки» та виконання завдань лабораторного практикуму здобувачі вищої освіти зможуть освоїти:

- Принципи організації та управління інформаційною безпекою;
- Основні положення безпеки людських ресурсів;
- Управління ресурсами системи менеджменту інформаційної безпеки;
- Управління контролем доступу;
- Порядок придбання, розроблення та впровадження інформаційних систем;
- Управління інцидентами інформаційної безпеки.

Забезпечення інформаційної безпеки розглядається як безперервний процес, основний зміст якого становить управління, яке неможливо забезпечити разовим заходом, оскільки засоби захисту потребують постійного контролю і оновлення.

Говорячи про управління, варто згадати і про такий термін як «менеджмент». Обидва терміни «управління» і «менеджмент» використовуються як синоніми.

На думку окремих дослідників в теорії управління, менеджмент - це цілеспрямований вплив, що погоджує спільну

діяльність, а управління - процес вироблення і здійснення керуючих впливів.

Менеджмент (управління) інформаційною безпекою (далі - УІБ) - це управління персоналом, засобами захисту, ризиками, інцидентами, ресурсами з метою забезпечення ІБ. УІБ є невід'ємним елементом управління підприємством і дозволяє колективно використовувати конфіденційну інформацію, забезпечуючи при цьому її захист, а також захист обчислювальних ресурсів.

Окремими положеннями описано порядок, вимоги та процеси аудиту системи менеджменту інформаційної безпеки.

Процес менеджменту інформаційної безпеки супроводжується положеннями керівних нормативних документів у цій галузі. Переважний обсяг вимог викладено у відповідних стандартах.

Основна увага Методичних вказівок приділена ознайомленню та вивченню положень міжнародних стандартів з інформаційної безпеки.

Вивчення навчальної дисципліни «Менеджмент інформаційної безпеки» має професійно-практичне спрямування і забезпечує здатність розв’язувати складні спеціалізовані організаційні завдання у галузі інформаційної безпеки.

Загальні методичні вказівки

Лабораторні роботи спрямовані на відпрацювання студентами вмінь і навиків використання діючих міжнародних стандартів з інформаційної безпеки.

Тексти стандартів, які розглядаються в ході вивчення, розміщені окремими файлами на ресурсах курсу «Менеджмент інформаційної безпеки в навчальній платформі Moodle.

Кожна лабораторна робота розрахована на 2 години лабораторних занять.

Звіт про кожну лабораторну роботу виконується в текстовому редакторі Word, зберігається окремим документом та надсилається на перевірку викладачу.

Лабораторна робота № 1.
Об'єкти інформаційної безпеки. Основні складові інформаційної безпеки.

1. Загальне завдання

Нижче наведено перелік питань по темі. Із переліку надати письмові відповіді на питання, зазначені в таблиці, згідно номеру за списком студента в групі.

В якості джерела інформації використовувати матеріали лекції № 1 та підручника [1].

Перелік питань

1. Дати визначення інформаційних ресурсів та інформаційних систем.
2. Чому від несанкціонованого впливу необхідно захищати не лише пристрої, а й персонал?
3. Що належить до об’єкта захисту інформації?
4. Дати визначення безпеки інформації в інформаційній системі.
5. Які інформаційні системи називають захищеними?
6. Дати визначення системи захисту інформації в ІС.
7. Назвати три основні підходи до інформаційної безпеки.
8. Назвати основні завдання і складові інформаційної безпеки.
10. Дати визначення доступності інформації.
11. Дати визначення цілісності інформації.
12. Дати визначення конфіденційності інформації.
13. Хто, де і коли вперше описав поняття цілісності, достовірності та конфіденційності інформації?
14. В якому документі і коли в Україні будо офіційно введено поняття цілісності, достовірності та конфіденційності інформації?
15. Дати визначення спостережності інформації.
16. На яких міжнародних документах базуються «Критерії оцінки захищеності інформації в КС від несанкціонованого доступу» (НД ТЗІ 2.5-004-99)?
17. Назвати підсистеми безпеки інформаційної системи.
18. Завдяки чому забезпечується апаратна безпека?
19. Завдяки чому забезпечується безпека програм?
20. Завдяки чому забезпечується безпека даних?
21. Завдяки чому забезпечується безпека комунікацій?

22. Дати визначення менеджменту.
23. Дати визначення менеджменту інформаційної безпеки.
24. Які компоненти включає в себе менеджмент (управління) інформаційною безпекою?
25. Що є кінцевою метою створення управління інформаційною безпекою організації?
26. Які компоненти включає в себе система управління інформаційною безпекою?
27. Які переваги компанії дає впровадження СУІБ і її сертифікація на відповідність міжнародним стандартам?
28. Які переваги для структурних підрозділів компанії надає впровадження СУІБ і її сертифікація на відповідність міжнародним стандартам?
29. Навести приклад шкоди, заподіяної технічними збоями інформаційних систем.
30. Навести приклад шкоди, заподіяної шкідливим програмним забезпеченням.
31. Навести приклад шкоди, заподіяної зломами інформаційних систем.

Таблиця завдань

№ за списком в групі	№№ питань
1.	26, 12, 27, 29
2.	25, 11, 28, 30
3.	24, 10, 27, 31
4.	23, 9, 28, 29
5.	22, 8, 27, 30
6.	21, 7, 28, 31
7.	20, 6, 27, 29
8.	19, 5, 28, 30
9.	18,4, 27, 31
10.	17, 3, 28, 29
11.	16,2, 27, 30
12.	15, 1, 28, 31
13.	14, 26, 27, 29
14.	13, 25, 28, 30

15.	12, 24, 27, 31
16.	11, 23, 28, 29
17.	10, 22, 27, 30
18.	9, 21, 28, 31
19.	8, 20, 27, 29
20.	7, 19, 28, 30

2. Творче завдання

В засобах масової інформації знайти повідомлення про відомі реалізовані загрози інформаційній безпеці. Проаналізувати та класифікувати заподіяну щкоду. Підготувати висновок щодо застосування можливих превентивних заходів захисту для аналогічних інформаційних систем та ресурсів.

Лабораторна робота № 2
Вивчення основних положень «Критеріїв оцінки довірених комп'ютерних систем» (Trusted Computer System Evaluation Criteria, TCSEC). Частина 1

У 1983 році центром був розроблений стандарт «Критерії оцінки довірених комп'ютерних систем» (англ. Trusted Computer System Evaluation Criteria, TCSEC), за кольором своєї обкладинки більш відомий як «Помаранчева книга», який став першим в історії загальнодоступним оцінним стандартом ІБ.

Розробка і публікація «Помаранчевої книги» стали важливою віхою в становленні теорії ІБ. Такі базові поняття, як «політика безпеки», «монітор безпеки звернень» або «адміністратор безпеки» вперше у відкритій літературі з'явилися саме в «Помаранчевої книзі».

Згідно «Помаранчевої книзі» довірена система повинна забезпечити одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу.

Завдання 1. Здійснити переклад та детально опрацювати положення «Критеріїв оцінки довірених комп'ютерних систем»

(Trusted Computer System Evaluation Criteria, TCSEC), які зазначені в таблиці завдання практичної роботи. Занотувати їх в текстовому редакторі Word, розширення .docx., кеглем № 12. Файл прикріпити до Завдання ЛР 2.

Завдання 2. Ознайомитись із повним текстом стандарту та додатками.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	2.1 – 2.1.4.4.
2.	2.2 – 2.2.3.2.1
3.	2.2.4 – 3.1.1.3.1
4.	3.1.1.3.2 – 3.1.1.4
5.	3.1.2 – 3.1.3.2.3
6.	3.1.4 – 3.2.1.2
7.	3.2.1.3 – 3.2.1.3.4
8.	3.2.1.4 – 3.2.2.2
9.	3.2.3 – 3.2.3.2.3
10.	3.2.4 – 3.2.4.4
11.	3.3 – 3.3.1.3.2.2
12.	3.3.1.3.2.3 – 3.3.1.4
13.	3.3.2 – 3.3.3.1.5
14.	3.3.3 – 3.3.3.1.5
15.	3.3.3.2 – 3.3.4.3
16.	4.0 – 4.1.1.2
17.	4.1.1.3 – 4.1.1.3.2
18.	4.1.1.3.3 – 4.1.1.4
19.	4.1.2 – 4.1.2.2
20.	4.1.3 – 4.1.3.1.5

Лабораторна робота № 3
Дослідження положень міжнародного стандарту ДСТУ ISO / IEC 15408-1-2017 «Критерії оцінки безпеки інформаційної технології. Частина 1. Вступ та загальна модель». Частина 1

Цей національний стандарт є перекладом ISO / IEC 15408-1-2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model (Критерії оцінки безпеки інформаційної технології. Частина 1. Вступ та загальна модель)

Цей стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ).

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Здійснити переклад та детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи. Занотувати їх в текстовому редакторі Word, розширення .docx, кеглем № 12. Файл прикріпити до Завдання ЛР3.

Завдання 2. Ознайомитись із повним текстом стандарту та додатками.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	Foreword, Introduction
2.	1 – 3.1.8
3.	3.1.9 – 3.1.22
4.	3.1.23 – 3.1.39
5.	4.1.40 – 3.1.57
6.	3.1.58 – 3.1.74
7.	3.1.75 – 3.2.4

8.	3.2.5 – 3.2.12
9.	3.2.13 – 3.2.24
10.	3.2.25 – 3.4.6
11.	4.4.7 – 4.4.17
12.	3.4.18 – 3.4.22 з рис. 1.
13.	3.5.1 – 3.6.6
14.	4 – 5.2
15.	5.2.1 – 5.3.3
16.	5.3.4 – 5.4
17.	5.5 – 6.1
18.	6.2
19.	6.2.1
20.	6.3 – 7.1

Лабораторна робота № 4
Дослідження положень міжнародного стандарту ISO/IEC 27000-2016. «Інформаційні технології. Система управління інформаційною безпекою. Загальний огляд і термінологія»

Міжнародні стандарти системи управління представляють собою модель для налагодження і функціонування системи управління. Ця модель включає в себе функції, за якими експерти дійшли згоди на підставі міжнародного досвіду, накопиченого в цій області.

При використанні сімейства стандартів СУІБ організації можуть реалізовувати і вдосконалювати СУІБ і підготуватися до її незалежної оцінки, яка застосовується для захисту інформації, такої як фінансова інформація, інтелектуальна власність, інформація про персонал, а також інформація, довірена клієнтами або третіми особами. Ці стандарти можуть використовуватися організацією для підготовки незалежної оцінки своєї СУІБ, застосовуваної для захисту інформації.

Останнє оновлення стандарту ISO / IEC 27000 «ІТ. СУІБ. Загальний огляд і термінологія» відбулося у 2016 році. Проте у відкритому доступі відсутня україномовна версія зазначеного стандарту.

Для здійснення аналізу внесених змін та поправок, студентам, відповідно до завдання, зазначеному у таблиці необхідно перш за все здійснити переклад положень стандарту. За результатами перекладу знайти аналогічні розділи/підрозділи в попередній версії стандарту ISO/IEC 27000-2014 та підготувати висновки про внесені зміни.

Завдання лабораторної роботи

Завдання 1. Здійснити переклад та детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи. Занотувати їх в текстовому редакторі Word, розширення .docx, кеглем № 12. Файл прикріпити до Завдання ЛР 4.

Завдання 2. Ознайомитись із повним текстом стандарту та додатками.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень, підготувати висновки про внесені зміни в останній версії стандарту.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	0.1, 0.2
2.	0.3, 1, 2.1 – 2.10
3.	2.10 – 2.20
4.	2.21 – 2.32
5.	2.33 – 2.44
6.	2.45 – 2.2.56
7.	2.57 – 2.68
8.	2.69 – 2.79
9.	2.80 – 2.89
10.	3.1
11.	3.2.1 – 3.2.3
12.	3.2.4, 3.2.5, 3.3
13.	3.4
14.	3.5.1 – 3.5.3

15.	3.5.4, 3.5.5
16.	3.5.6, 3.5.7
17.	3.6, 3.7
18.	4.1, 4.2
19.	4.3.1, 4.3.2
20.	4.4.1 – 4.4.5

Лабораторна робота № 5
Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27001:2015. «Методи захисту. Системи управління інформаційною безпекою. Вимоги»

Цей національний стандарт є перекладом ISO/IEC 27001:2015 Information technology — Security techniques — Information security management systems — Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги)

Цей стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ).

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Ознайомитись із повним текстом стандарту та додатками.

Завдання 2. Детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи, Занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР 5.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	1 – 5
2.	6
3.	7
4.	8, 9
5.	10
6.	Додаток А 5.1 – А 6.1.5
7.	Додаток А 6.2 – А7.2
8.	Додаток А 7.3 – А8.2
9.	Додаток А 8.3 – А 9.2
10.	Додаток А 9.3 – А 9.4
11.	Додаток А 10 – А 11.1
12.	Додаток А 11.2
13.	Додаток А 12.1 – А 12.4
14.	Додаток А 12.5 – А 13.1
15.	Додаток А 13.2 – А14.1
16.	Додаток А 14.2
17.	Додаток А14.3 – А 15.2
18.	Додаток А 16
19.	Додаток А 17
20.	Додаток А 18

Лабораторна робота № 6
Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27002:2015. «Методи захисту. Звід практик щодо заходів інформаційної безпеки.»

Цей стандарт ідентичний ISO/IEC 27002:2013 Information technology — Code of practice for information security controls (Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки)

Стандарт розроблено для організацій для використання як довідкової інформації щодо вибору заходів безпеки під час впровадження системи управління інформаційною безпекою

(СУІБ) на базі ISO/IEC 27001, або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки.

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Ознайомитись із повним текстом стандарту та додатками.

Завдання 2. Детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи, Занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР 6.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	6
2.	7
3.	8
4.	9.1 – 9.2.3
5.	9.2.4 – 9.4
6.	10
7.	11.1
8.	11.2.1 – 11.2.5
9.	11.2.6 – 11.2.9
10.	12.1
11.	12.2, 12.3
12.	12.4, 12.5
13.	12.6, 12.7
14.	13
15.	14.1 – 14.2.2
16.	14.2.3 – 14.2.8
17.	15.1
18.	15.2
19.	16
20.	17

Лабораторна робота № 7
Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27003:2018. «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанови» (Частина 1)

Цей стандарт ідентичний ISO/IEC 27003:2017 Information technology – Security techniques – Information security management systems – Guidance (Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанови)

Стандарт розроблено для організацій для використання як довідкової інформації щодо вибору методів захисту під час впровадження системи управління інформаційною безпекою (СУІБ) на базі ISO/IEC 27001, або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки.

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Здійснити переклад та детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи, Занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР 7.

Завдання 2. Ознайомитись із повним текстом стандарту та додатками.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	Foreword (Передмова)
2.	Intoduction (Вступ)
3.	1 – 3, 4.1 (Explanation)
4.	4.1 (Guidance – Other information)
5.	4.2
6.	4.3

7.	4.4, 5.1 (a,b)
8.	5.1 (c – h)
9.	5.2
10.	5.3
11.	6.1.1 (Overview – Explanation)
12.	6.1.1 (Guidance) – 6.1.2 (Explanation)
13.	6.1.2 (Guidance) – 6.1.3 (a – c)
14.	6.1.3 (Guidance) – 6.1.3 (d)
15.	6.1.3 (e - f)
16.	6.2 (Explanation)
17.	6.2 (Guidance)
18.	7.1
19.	7.2
20.	7.3

Лабораторна робота № 8
Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27003:2018. «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанови» (Частина 1)

Цей стандарт ідентичний ISO/IEC 27003:2017 Information technology – Security techniques – Information security management systems – Guidance (Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанови)

Стандарт розроблено для організацій для використання як довідкової інформації щодо вибору методів захисту під час впровадження системи управління інформаційною безпекою (СУІБ) на базі ISO/IEC 27001, або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки.

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Здійснити переклад та детально опрацювати положення стандарту, які зазначені в таблиці завдання

практичної роботи, Занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР 8.

Завдання 2. Ознайомитись із повним текстом стандарту та додатками.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	7.4
2.	7.5.1
3.	7.5.2
4.	7.5.3
5.	8.1 (Required activity, Explanation)
6.	8.1 (Guidance)
7.	8.2, 8.3
8.	9.1 (Required activity, Explanation)
9.	9.1 (Guidance)
10.	9.2 (Required activity, Explanation)
11.	9.2 (Guidance. Managing and audit programme)
12.	9.2 (Guidance. Competence and evalution of auditors)
13.	9.2 (Performing the audit)
14.	9.3
15.	10.1 (Required activity, Explanation)
16.	10.11 (Guidance)
17.	10.2
18.	Додаток А (рис. А.1)
19.	7.4
20.	7.5.1

Лабораторна робота № 9
Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27004:2018. «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання»

Цей стандарт ідентичний ISO/IEC 27004:2016 Information technology – Security techniques – Information security management - Monitoring, measurement, analysis and evalution (Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання)

Стандарт розроблено для організацій для використання як довідкової інформації щодо вибору методів захисту під час впровадження системи управління інформаційною безпекою (СУІБ) на базі ISO/IEC 27001, або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки.

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Здійснити переклад та детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи, Занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР 9.

Завдання 2. Ознайомитись із повним текстом стандарту та додатками.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	1 – 4
2.	5
3.	6.1 – 6.3
4.	6.4

5.	7
6.	8.1 – 8.2
7.	8.3.1 – 8.3.3
8.	8.3.4 – 8.5
9.	8.6, 8.7
10.	Додаток А
11.	Додатки В1 – В3
12.	Додатки В4 – В7
13.	Додатки В8 – В10
14.	Додатки В11 – В14
15.	Додатки В15 – В18
16.	Додатки В19 – В22
17.	Додатки В23 – В26
18.	Додатки В27 – В30
19.	Додатки В31 – В34
20.	Додатки В35 – В37

Лабораторна робота № 10
Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27005:2015. «Методи захисту. Управління ризиками інформаційної безпеки»

Цей національний стандарт є ідентичний стандарту ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки.)

Цей стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ).

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Ознайомитись із повним текстом стандарту та додатками.

Завдання 2. Детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи, Занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР 10.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	1 – 3.7
2.	3.8 – 4
3.	5
4.	6
5.	7.1, 7.2
6.	7.3, 7.4
7.	8.1 – 8.2.3
8.	8.2.4 – 8.2.6
9.	8.3 – 8.4
10.	9, 10
11.	11, 12
12.	Додатки А1, А2
13.	Додатки А3, А4
14.	Додаток В1
15.	Додаток В2
16.	Додаток С
17.	Додаток D1
18.	Додаток D2
19.	Додатки Е1 – Е2.1
20.	Додаток Е2.2

Лабораторна робота № 11
Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27006:2015. «Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою»

Цей національний стандарт є ідентичний стандарту ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems. Інформаційні технології. Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою)

Цей стандарт встановлює критерії для організацій, які виконують аудит і сертифікацію систем управління.

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Ознайомитись із повним текстом стандарту та додатками.

Завдання 2. Детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи, Занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР 11.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	1 – 6
2.	7.1 – 7.1.2.1.5
3.	7.1.2.1.6 – 7.2.1.1
4.	7.2.1.2 – 9.1.3.3
5.	9.1.3.4 – 9.1.5
6.	9.1.6 – 9.2.3.3

7.	9.3 – 9.4.3.2
8.	9.5 – 9.6
9.	9.7 – 10
10.	Додаток А
11.	Додатки В1, В2
12.	Додатки В3.1 – В3.3
13.	Додатки В3.4 – В3.5
14.	Додатки В3.6 – В6
15.	Додатки С1, С2
16.	Додаток С3
17.	Додатки D1 – D2.3
18.	Додатки D2.4 – D2.5(A8.3.1)
19.	Додатки D2.5(A5) – D2.5(A9.4.5)
20.	Додатки D2.5(A10.1) – D2.5(A13.1.2)

Лабораторна робота № 12
Дослідження положень міжнародного стандарту ДСТУ ISO/IEC 27007:2018. «Інформаційні технології. Методи захисту. Настанови щодо аудиту систем керування інформаційною безпекою»

Цей стандарт ідентичний ISO/IEC 27007:2017 Information technology – Security techniques – Guidelines for information security management systems auditing (Інформаційні технології. Методи захисту. Настанови щодо аудиту систем керування інформаційною безпекою)

Цей стандарт встановлює критерії для організацій, які виконують аудит і сертифікацію систем управління.

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Здійснити переклад та детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи, Занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР 12.

Завдання 2. Ознайомитись із повним текстом стандарту та додатками.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	арк. 1, 2
2.	арк. 3, 4
3.	арк. 5, 6
4.	арк. 7, 8
5.	арк. 9, 10
6.	арк. 11, 12
7.	арк. 13, 14
8.	арк. 15, 16
9.	арк. 17, 18
10.	арк. 19, 20
11.	арк. 21, 22
12.	арк. 23, 24
13.	арк. 25, 26
14.	арк. 27, 28
15.	арк. 29, 30
16.	арк. 31, 32
17.	арк. 33, 34
18.	арк. 35, 36
19.	арк. 37, 38
20.	арк. 39, 40

Лабораторна робота № 13
Дослідження положень міжнародного стандарту ISO / IEC 27011 МСЕ-Т РЕКОМЕНДАЦІЯ X.1051 Інформаційні технології - Методи безпеки - Настанови щодо управління інформаційною безпекою для телекомунікаційних організацій на основі ISO / IEC 27002

Міжнародний союз електрозв'язку (ITU) - це спеціалізоване агентство ООН у галузі телекомунікацій, інформаційних та комунікаційних технологій (ІКТ). Сектор стандартизації телекомунікаційних засобів МСЕ (ITU-T) є постійним органом МСЕ. МСЕ-Т відповідає за вивчення технічних, експлуатаційних та тарифних питань та надання рекомендацій щодо них з метою стандартизації телекомунікацій на світовій основі. Всесвітня асамблея стандартизації телекомунікацій (WTSA), яка проводиться кожні чотири роки, встановлює теми для вивчення дослідницькими групами МСЕ-Т, які, у свою чергу, готують рекомендації з цих тем. Затвердження Рекомендацій МСЕ-Т поширюється на процедуру, викладену в Резолюції WTSA. У деяких областях інформаційних технологій, які належать до компетенції МСЕ-Т, необхідні стандарти готуються на основі спільної роботи з ISO та IEC. Цей стандарт встановлює критерії для організацій, які виконують аудит і сертифікацію систем управління.

Міжнародний стандарт надає рекомендації щодо тлумачення впровадження та управління управлінням інформаційною безпекою в телекомунікаційних організаціях на основі ISO/IEC 27002 (Кодекс практики управління інформаційною безпекою). Крім застосування цілей безпеки та контролю, описаних в ISO / IEC 27002, телекомунікаційні організації повинні враховувати такі особливості безпеки:

1) Конфіденційність. Інформація, що стосується телекомунікаційних організацій, повинна бути захищена від несанкціонованого розголошення. Це передбачає нерозголошення відомостей з точки зору існування, змісту, джерела, місця призначення та дати та часу переданої інформації. Важливо, щоб телекомунікаційні організації

гарантували, щоб нерозголошення комунікацій, якими вони займаються, не було порушено. Особи, які займаються телекомунікаційною організацією, повинні зберігати конфіденційність будь-якої інформації стосовно інших осіб, яка, можливо, стала відомою під час виконання їхніх робочих обов'язків. ПРИМІТКА - Термін "секретність комунікацій" використовується в деяких країнах у контексті "нерозголошення комунікацій".

2) Цілісність. Установка та використання засобів зв'язку повинні контролюватися, забезпечуючи достовірність, точність та повноту інформації, що передається, ретранслюється або приймається дротом, радіо або будь-якими іншими методами.

3) Доступність. Потрібно надавати лише дозволений доступ до інформації про телекомунікацій та засобів масової інформації, що використовуються для надання послуг зв'язку, незалежно від того, чи це може бути надано за допомогою кабелю, радіо чи будь-якими іншими методами. Як розширення доступності, телекомунікаційні організації повинні надавати пріоритет основним комунікаціям у разі надзвичайних ситуацій та виконувати нормативні вимоги.

Текст стандарту додається.

Завдання лабораторної роботи

Завдання 1. Здійснити переклад та детально опрацювати положення стандарту, які зазначені в таблиці завдання практичної роботи, занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР13.

Завдання 2. Ознайомитись із повним текстом стандарту та додатками.

Завдання 3. На семінарському занятті зробити усну доповідь про результати дослідження розділу/підрозділу стандарту, представити власне розуміння зазначених положень.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	Додаток А9
2.	4.1 – 4.2.3

3.	4.2.4 – 5
4.	6.1
5.	6.2.1 – 6.2.2
6.	6.2.3
7.	6.2.3
8.	8.1
9.	8.2 – 9.1
10.	9.2
11.	10.1
12.	10.2 – 10.6
13.	10.7 – 10.10
14.	11
15.	12
16.	13.1
17.	13.2
18.	14
19.	15
20.	Додаток А10

Лабораторна робота № 14
Дослідження вимог міжнародного стандарту ISO 19011:2011 Настанови щодо здійснення аудитів систем управління

Стандарт ISO19011 можна використати для аудиту системи менеджменту інформаційної безпеки. Він містить інформацію щодо принципів здійснення аудиту, управління програмами аудиту, проведення аудитів СМІБ, а також настанови щодо компетентності аудиторів СМІБ. Його можна застосовувати у всіх організаціях, які потребують внутрішніх чи зовнішніх аудитів СМІБ чи управління програмами аудиту.

Завдання. З метою ознайомлення із вимогами зазначеного стандарту та усвідомлення необхідності їх застосування студентам пропонується:

1. Ознайомитись із структурою та положеннями стандарту.

2. Згідно варіанту (номера за списком в групі) в нижченаведеній таблиці здійснити детальне ознайомлення та витяги із стандарту у вигляді окремих розділів/підрозділів, занотувати їх в текстовому редакторі Word, розширення .docx. Файл прикріпити до Завдання ЛР14.

3. Користуючись отриманими витягами, зробити усну доповідь про зміст занотованих розділів/підрозділів.

Таблиця завдань

№ за списком в групі	Розділи та підрозділи для детального опрацювання
1.	Вступ
2.	3.2 – 3.12
3.	3.13 – 3.20
4.	4
5.	5.1
6.	5.2, 5.3.1, 5.3.2
7.	5.3.3, 5.3.4
8.	5.3.5, 5.3.6
9.	5.4.1 – 5.4.3
10.	5.4.4, 5.4.5
11.	5.4.6, 5.4.7, 5.5
12.	5.6, 6.1, 6.2.1
13.	6.2.2
14.	6.2.3. 6.3.1
15.	6.3.2
16.	6.3.3, 6.3.4
17.	6.4.1, 6.4.2
18.	6.4.3, 6.4.4
19.	6.4.5, 6.4.6
20.	6.4.7, 6.4.8

Лабораторна робота № 15
Підготовка плану впровадження системи менеджменту інформаційної безпеки організації за вимогами стандарту ISO/IEC 27001-2015

Впровадження системи менеджменту інформаційної безпеки в будь-якій організації вимагає чіткого планування передбачуваних заходів на основі вимог міжнародних стандартів. Регламентуючим стандартом з питань впровадження системи менеджменту інформаційної безпеки є ДСТУ ISO/IEC 27001:2015 Information technology — Security techniques — Information security management systems — Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги

Цей стандарт створений для визначення вимог щодо розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Прийняття системи управління інформаційною безпекою є стратегічним рішенням для організації. На проектування та впровадження системи управління інформаційною безпекою організації впливають потреби та цілі організації, вимоги щодо безпеки, застосовувані організаційні процеси, розмір і структура організації.

З метою отримання компетентностей щодо впровадження системи менеджменту інформаційної безпеки студентам в ході практичної роботи пропонується створити «План впровадження системи менеджменту інформаційної безпеки відповідно до видів діяльності» в умовній організації згідно з наступними рекомендаціями.

1. План складається за формою, наведеною нижче (табл.1). В графі «відповідальні» вказується прізвище студента.
2. Характеристики бізнес-процесів та специфіка функціонування інформаційних систем організації визначаються із табл. 2 відповідно до № за списком студента в групі
3. Заходи в плані складаються в довільній формі у відповідності з вимогами розділів 4 – 8 стандарту ДСТУ ISO/IEC 27001:2015.

4. В якості навчального матеріалу доцільно використати рекомендації, викладені в підрозділах 5.1 – 5.6 навчального посібника Ромака В.А. «Системи менеджменту інформаційної безпеки».

5. Роботу необхідно виконати в текстовому редакторі Word та прикріпити до завдання лабораторної роботи

Таблиця 1

План впровадження системи менеджменту інформаційної безпеки відповідно до видів діяльності

№ з/п	Найменування заходів	Пункт розділу стандарту	Відповідальні
1.			

Таблиця 2

Варіанти виконання завдання

№ за списком в групі	Назва умовної організації	Кількість комп'ютерів
1.	Університет	690
2.	Коледж	350
3.	Військова частина	2
4.	Райдержадміністрація	19
5.	Інтернет-магазин	28
6.	Логістичний центр	35
7.	Районний суд	20
8.	Агрофірма	39
9.	Фабрика продуктових товарів	24
10.	Завод по випуску побутової техніки	28
11.	Завод по випуску військової техніки	6
12.	Телекомунікаційна компанія	37
13.	Обласний пенсійний фонд	38
14.	Медичний діагностичний центр	12
15.	Комерційний банк	27

16.	Податкова інспекція	24
17.	Сервісний центр Департаменту Державтоінспекції	45
18.	Сервісний центр надання адміністративних послуг	30
19.	Міський сектор Державної міграційної служби	24
20.	Аеропорт	4

Література

Основна

1. Системи менеджменту інформаційної безпеки : навчальний посібник / В. А. Ромака, В. Б. Дудикевич, Ю. Р. Гарасим, П. І. Гаранюк, І. О. Козлюк, Львів : Видавництво Львівської політехніки, 2012. 232 с.

2. Аудит та управління інцидентами інформаційної безпеки : навчальний посібник / О. Г. Корченко, С. О. Гнатюк, С. В. Казмірчук, В. М. Панченко, С. В. Мельник. Київ, 2014. 189 с.

3. ДСТУ ISO 19011:2011 Настанови щодо здійснення аудитів систем управління. Київ : Мінекономрозвитку України, 2013.

4. ДСТУ ISO/IEC 27000:2015 Методи захисту. Система менеджменту інформаційної безпеки. Огляд і словник. Київ : ДП "УкрНДНЦ", 2016.

5. ДСТУ ISO/IEC 27000:2017 Інформаційні технології Методи захисту. Система менеджменту інформаційної безпеки. Огляд і словник термінів. Київ : ДП "УкрНДНЦ", 2017.

6. ДСТУ ISO/IEC 27001:2015 Методи захисту систем управління інформаційною безпекою. Київ : ДП "УкрНДЦ", 2016.

7. ДСТУ ISO/IEC 27002:2015 Звід практик щодо заходів інформаційної безпеки. Київ : ДП "УкрНДНЦ", 2016.

8. ДСТУ ISO/IEC 27003:2018 Інформаційні технології Методи захисту. Системи керування інформаційною безпекою. Настанови. Київ : ДП "УкрНДНЦ", 2018.

9. ДСТУ ISO/IEC 27004:2018 Інформаційні технології Методи захисту. Системи керування інформаційною безпекою.

Моніторинг, вимірювання, аналізування та оцінювання. Київ : ДП "УкрНДНЦ", 2018.

10. ДСТУ ISO/IEC 27005:2015 Інформаційні технології Методи захисту. Управління ризиками інформаційної безпеки. Київ : ДП "УкрНДНЦ", 2016.

11. ДСТУ ISO/IEC 27006:2015 Інформаційні технології Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем керування інформаційною безпекою. Київ : ДП "УкрНДНЦ", 2016.

12. ДСТУ ISO/IEC 27007:2015 Інформаційні технології Методи захисту. Настанова щодо аудиту керування інформаційною безпекою. Київ : ДП "УкрНДНЦ", 2019. (англ.)

13. ISO/IEC 27007:2015 Інформаційні технології. методи безпеки. Настанови щодо управління інформаційною безпекою для телекомунікаційні організації на базі ISO / IEC 27002. (англ.)

14. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель. Київ : ДП "УкрНДНЦ", 2017. (англ.)

15. ДСТУ ISO/IEC TR 1335-1:2003 Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки ІТ. Київ : Держспоживстандарт України 2005.

16. ДСТУ ISO/IEC TR 1335-4:2005 Настанови з керування безпекою інформаційних технологій. Київ : ДП "УкрНДНЦ", 2005.

17. Критерії безпеки комп'ютерних систем міністерства оборони США. (Помаранчева книга) 1985.

Допоміжна

1. Юдін О. К., Богуш В. М. Інформаційна безпека держави : навчальний посібник. Харків : Консум, 2005. 576 с.

Інформаційні ресурси в Інтернет

1. Стандарти серії ДСТУ/ISO 27000 http://online.budstandart.com/ua/catalog/doc-page.html?id_doc

2. Нормативні документи з технічного захисту інформації https://cip.gov.ua/ua/news/perelik-dokumentiv-normativno-pravovoyi-bazi-sho-zabezpechuye-nadannya-vidpovidnikh-vidiv-poslug-u-galuzi-tekhnichnogo-zakhistu-informaciyi