МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра *програмної інженерії та інформаційних технологій управління*
(назва)

«**ЗАТВЕРДЖУЮ**»
Голова групи забезпечення
спеціальності _____
(назва групи)

_____ _____
(підпис) (ініціали та прізвище

«02» вересня 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ КІБЕРБЕЗПЕКИ
(назва навчальної дисципліни)

рівень вищої освіти *перший (бакалаврський)*
перший (бакалаврський) / другий (магістерський)

галузь знань *12 Інформаційні технології*
(шифр і назва)

спеціальність *126 Програмне забезпечення інформаційних систем*
(шифр і назва)

спеціалізація _____
(шифр і назва)

вид дисципліни *професійна підготовка*
(загальна підготовка / професійна підготовка)

форма навчання *денна*
(денна / заочна)

Харків – 2021 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни
ОСНОВИ КІБЕРБЕЗПЕКИ
(назва дисципліни)

Розробники:

проф, д.т.н., проф.		*Євсеєв С.П.*
(посада, науковий ступінь та вчене звання)	(підпис)	(ініціали та прізвище)
(посада, науковий ступінь та вчене звання)	(підпис)	(ініціали та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри

програмної інженерії та інформаційних технологій управління
(назва кафедри)

«27» серпня 2021 року № 1

Завідувач кафедри _____ Годлевський М.Д.
(назва кафедри) (підпис) (ініціали та прізвище)

2. ЛИСТ ПОГОДЖЕННЯ

Шифр та назва освітньої програми	ПІБ Гаранта ОП	Підпис, дата
126 “ Інформаційні системи та технології ”	Орловський Д.Л.	

3. ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри	Підпис Гаранта освітньої програми

4. МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

4.1 Мета навчальної дисципліни "Основи кібербезпеки" є навчання студентів принципам побудови систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення надання основних послуг безпеки інформації в кіберпросторі, проведення аудиту поточного стану інформаційної безпеки.

4.2 Завдання дисципліни:

– ознайомлення студентів з принципами побудови систем захисту інформації;
– ознайомлення студентів з основними механізмами послуг безпеки;
– вивчення студентами менеджменту інформаційної безпеки;
– навчання студентів основам аудиту інформаційної безпеки;
– вивчення студентами спеціальних механізмів кіберзахисту.

4.3 Перелік компетентностей

Після вивчення дисциплін студент набуває:

Загальні компетентності:

К05. Здатність вчитися і оволодівати сучасними знаннями.
К06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (фахові) компетентності:

К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання

Класифікація компетентностей за НРК	**Знання** **Зн1** Концептуальні знання, набуті у процесі навчання та професійної діяльності, включаючи певні знання сучасних досягнень **Зн2** Критичне осмислення основних теорій, принципів, методів і понять у навчанні та професійній діяльності	**Уміння** **Ум1** Розв'язання складних непередбачуваних задач і проблем у спеціалізованих сферах професійної діяльності та/або навчання, що передбачає збирання та інтерпретацію інформації (даних), вибір методів та інструментальних засобів, застосування інноваційних підходів	**Комунікація** **К1** Донесення до фахівців і нефахівців інформації, ідей, проблем, рішень та власного досвіду в галузі професійної діяльності **К2** Здатність ефективно формувати комунікаційну стратегію	**Автономія та відповідальність** **АВ1** Управління комплексними діями або проектами, відповідальність за прийняття рішень у непередбачуваних умовах **АВ2** Відповідальність за професійний розвиток окремих осіб та/або груп осіб **АВ3** Здатність до подальшого навчання з високим рівнем автономності
Загальні компетентності				
К05. Здатність вчитися і оволодівати сучасними знаннями		**Ум1 АВ3**		**АВ3**
К06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел		**Ум1**		
Спеціальні (фахові) компетентності				
К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки)	**Зн2**	**Ум1Ум1**		

Структурно-логічна схема вивчення навчальної дисципліни

Попередні дисципліни:	Наступні дисципліни:
“Вища математика”	“Архітектура та проектування програмного забезпечення”
“Основи архітектури ЕОМ та операційні системи”	
“Моделі та структури даних”	
“Основи комп'ютерних мереж”	
“Основи веб-розробки”	

5. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Загальний обсяг (годин) / кредитів ECTS	З них		За видами аудиторних занять (годин)			Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ)	Поточний контроль	Семестровий контроль	
		Аудиторні заняття (годин)	Самостійна робота (годин)	Лекції	Лабораторні заняття	Практичні заняття, семінари		Контрольні роботи (кількість робіт)	Залік	Екзамен
1	2	3	4	5	6	7	8	9	10	11
6	**90/3**	**48**	**42**	**16**	**32**			**2**		**іспит**

Співвідношення кількості годин аудиторних занять до загального обсягу складає 53 (%):

6. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Назви змістових модулів. Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
1	2	3	4	5
Змістовий модуль 1. Базові структури даних та основні обчислювальні алгоритми				
1	ЛК	2	**Тема 1. Поняття кібербезпеки держави та складових національних інтересів України в кібербезпеки** Основні поняття у галузі кібербезпеки, принципи та складові національних інтересів у сфері кібербезпека. Нормативні документи. Основні об’єкти критичної інфраструктури.	**5, 9–14**
2	ЛР СР	2 6	**Лабораторна робота № 1.** Розгортання операційної системи для проведення аудиту інформаційної безпеки комп’ютерних мереж та інформаційних систем	**5, 10–14**
3	ЛК	2	**Тема 2. Аналіз ризиків в області кібербезпеки. Класифікація кіберзагроз. Практичні моделі розмежування прав доступу**	**5, 9–14**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Назви змістових модулів. Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
			Еволюція кіберзагроз, класифікація загроз. Основні питання аудиту інформаційної та кібербезпеки.	
4	ЛР СР	2 6	**Лабораторна робота № 2.** Інструменти прихованого збору технічної інформації з інформаційної системи або комп'ютерної мережі	**5, 10–14**
5	ЛК	4	**Тема 3. Механізми забезпечення конфіденційності та цілісності даних**. Принципи побудови сучасних симетричних та несиметричних криптосистем. Основні алгоритми традиційної та криптографії з відкритим ключом. Основні режими блокових шифрів. Протоколи використання несиметричних алгоритмів	**1–4, 6–9**
6	ЛР СР	4 6	**Лабораторна робота № 3.** Дослідження сучасних блочних симетричних шифрів та режимів шифрування. Дослідження сучасних асиметричних криптосистем шифрування	**1–4, 6–9**
7	ЛК	2	**Тема 4. Механізми забезпечення автентифікації.** Основні принципи побудови MDC, MAC-кодів, класифікація спеціалізованих геш-функцій. Принципи формування цифрового підпису. Стандарти цифрового підпису	**1–4, 6–9**
8	ЛР СР	4 6	**Лабораторна робота № 4.** Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ 4145, ECDSA. Дослідження вразливостей системи або мережі за допомогою спеціалізованого сканера вразливостей – Nessus	**1–4, 6–9**
Змістовий модуль 2. Системи захисту інформації у кіберпросторі				
9	ЛК	2	**Тема 5. Основні напрямки розвитку сучасної криптографії.** Основні принципи побудови крипто-кодових конструкцій, цифровій стеганографії. Моделі стеганографічних протоколів.	**1-4**
10	ЛК СР	4 6	**Лабораторна робота № 5.** Стеганографічні методи захисту інформації	**1**
11	ЛК	2	**Тема 6. Механізми та протоколи керування ключами в ІВК** Основні принципи побудови архітектури з відкритим	**1–4, 6–9**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Назви змістових модулів. Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
			ключом. Протоколи використання ІВК. Основні функції центра сертифікації ключів, криптоперіод ключів. Стандарти протоколів ISO/IEC 11770-2, 3.	
12	ЛР СР	2 6	**Лабораторна робота № 6.** Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NIST	**1**
13	ЛК	2	**Тема 7. Технології аналізу ризиків** Основні принципи аудиту інформаційної безпеки. Етапи проведення аудиту інформаційної безпеки. Основи практичного ризик-менеджменту.	**5, 10–14**
14	ЛР СР	4 6	**Лабораторна робота № 7.** Визначення вразливостей веб ресурсів та веб додатків. Сканер вразливостей – Vega	**5, 10–14**
15	ЛК	2	**Тема 8. Аналіз ризиків в управлінні інформаційною безпекою** Політика системи менеджменту інформаційної безпеки. Основні документи системи менеджменту інформаційної безпеки, принципи формування політики безпеки. Стандарт 27001:2013.	**5, 10–14**
16	ЛР	10	**Лабораторна робота № 8.** Збір технічної та чуттєвої інформації за допомогою ПЗ класу – сніфери. Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng	**5, 10–14**
Разом (годин)		**90**		

7. САМОСТІЙНА РОБОТА

Важливою умовою покращення якості підготовки студентів є раціональна організація їх самостійної роботи, що включає самостійне опрацювання студентами певного кола питань, роботу із літературними джерелами та виконання індивідуального розрахункового завдання. Це пробуджує у них інтерес до предмета, розвиває здатність самостійно аналізувати прочитане, сприяє ґрунтовному засвоєнню матеріалу дисципліни.

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацьовування лекційного матеріалу	15
2	Підготовка до практичних(лабораторних, семінарських) занять	10
3	Самостійне вивчення тем та питань, які не викладаються на лекційних заняттях	15
4	Інші види самостійної роботи	2
	Разом	**42**

8. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Не передбачено навчальним планом

9. МЕТОДИ НАВЧАННЯ

При викладанні навчальної дисципліни для активізації навчального процесу передбачено застосування сучасних навчальних технологій, таких, як: проблемні лекції; робота в малих групах; семінари-дискусії; кейс-метод; ділові ігри.

Проблемні лекції спрямовані на розвиток логічного мислення студентів. Коло питань теми лекції обмежується двома-трьома ключовими моментами, увага студентів концентрується на матеріалі, що не знайшов широкого відображення в підручниках, використовується досвід закордонних навчальних закладів з роздаванням студентам під час лекцій друкованого матеріалу та виділенням головних висновків з питань, що розглядаються. При викладанні лекційного матеріалу студентам пропонуються питання для самостійного розмірковування. При цьому лектор задає запитання, які спонукають студента шукати розв'язання проблемної ситуації. Така система примушує студентів сконцентруватися і почати активно мислити в пошуках правильної відповіді.

На початку проведення проблемної лекції необхідно чітко сформулювати проблему, яку необхідно вирішити студентам. При викладанні лекційного

матеріалу слід уникати прямої відповіді на поставлені запитання, а висвітлювати лекційний матеріал таким чином, щоб отриману інформацію студент міг використовувати при розв'язанні проблеми.

Міні-лекції передбачають викладення навчального матеріалу за короткий проміжок часу й характеризуються значною ємністю, складністю логічних побудов, образів, доказів та узагальнень. Міні-лекції проводяться, як правило, як частина заняття-дослідження. На початку проведення міні-лекції за вказаними темами лектор акцентує увагу студентів на необхідності представити викладений лекційний матеріал у так званому структурно-логічному вигляді. На розгляд виносяться питання, які зафіксовані у плані лекцій, але викладаються вони стисло. Лекційне заняття, проведене у такий спосіб, пробуджує у студента активність та увагу при сприйнятті матеріалу, а також спрямовує його на використання системного підходу при відтворенні інформації, яку він одержав від викладача. Проблемні лекції та міні-лекції доцільно поєднувати з такою формою активізації навчального процесу, як робота в малих групах.

Робота в малих групах дає змогу структурувати лекційні або лабораторні заняття за формою і змістом, створює можливості для участі кожного студента в роботі за темою заняття, забезпечує формування особистісних якостей та досвіду соціального спілкування. Після висвітлення проблеми (при використанні проблемних лекцій) або стислого викладання матеріалу (при використанні міні-лекцій) студентам пропонується об'єднуватися у групи по 5-6 осіб та презентувати наприкінці заняття своє бачення та сприйняття матеріалу.

Презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань. Однією з позитивних рис презентації та її переваг при використанні в навчальному процесі є обмін досвідом, який здобули студенти при роботі у певній малій групі.

Лабораторні заняття (з елементами семінарської дискусії) дозволяють формувати у студентів навички особистого експериментального дослідження фізичних процесів що відбуваються під час роботи компонентів операційної системи, проводити аналіз умов її функціонування, а також розробляти нові елементи та системні компоненти відповідно до вимог, що пред'являються до них, узагальнювати отримані результати, формулювати висновки та думки, вести подальший обмін думками та поглядами з іншими учасниками щодо отриманих результатів досліджень з даної теми, а також розвивають творче мислення, допомагають формувати погляди і переконання, вчать об'єктивно оцінювати результати і пропозиції опонентів, критично підходити до власних результатів та поглядів.

Ділові та рольові ігри – форма активізації студентів, за якої вони задіяні в процесі інсценізації певної виробничої ситуації у ролі безпосередніх

учасників подій. Наприклад, при проведенні лабораторного заняття за темою “ Безпечність персональних конфіденціальних даних на базі секретного диску та захищеної електронної пошти PGP ” слід поділити аудиторію на групи, кожній з яких дати завдання використовуючи поштові протоколи.

Кейс-метод – метод аналізу конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності спеціалістів і передбачає розгляд виробничих, управлінських та інших ситуацій, складних конфліктних випадків, проблемних ситуацій, інцидентів у процесі вивчення навчального матеріалу.

Розподіл форм та методів активізації процесу навчання за темами навчальної дисципліни

Тема	Практичне застосування навчальних технологій
ТЕМА 1. ПОНЯТТЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ ТА СКЛАДОВИХ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ УКРАЇНИ В КІБЕРБЕЗПЕКИ	Проблемна лекція “Вплив кібербезпеки на складові національних інтересів України”
ТЕМА 4. МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ АВТЕНТИФІКАЦІЇ	Міні-лекція “Класифікація та огляд національних та міжнародних стандартів забезпечення автентичності та цифрового підпису”
ТЕМА 3. МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ДАНИХ.	Кейс “Проведення криптоаналізу класичних шифрів”. Міні-лекція “Методика визначення крипостійкості та дослідження основних характеристик симетричних та асиметричних криптосистем”
ТЕМА 6. МЕХАНІЗМИ ТА ПРОТОКОЛИ КЕРУВАННЯ КЛЮЧАМИ В ІВК	Проблемна лекція “Визначення засобів захисту від НСД в інформаційної системі підприємства. Розгортання інфраструктури відкритих ключів”. Ділова гра “Обґрунтування вибору механізмів захисту для забезпечення ефективного використання інформації на підприємстві”

10. МЕТОДИ КОНТРОЛЮ

Система оцінювання знань, вмінь та навичок студентів передбачає виставлення оцінок за усіма формами проведення занять. Перевірка та оцінювання знань студентів може проводитись у таких
формах:

1. Оцінювання роботи студентів у процесі лабораторних занять.
2. Проведення проміжного контролю.
3. Проведення модульного контролю.

Загальна модульна оцінка складається з поточної оцінки, яку студент отримує під час лабораторних занять та оцінки за виконання модульної контрольної роботи.

Загальна оцінка з дисципліни визначається як середнє арифметичне модульних оцінок.

Порядок поточного оцінювання знань студентів

Поточне оцінювання здійснюється під час проведення лабораторних занять і має на меті перевірку рівня підготовленості студента до виконання конкретної роботи. Об'єктами поточного контролю є:

1) активність та результативність роботи студента протягом семестру над вивченням програмного матеріалу дисципліни; відвідування занять;

2) виконання проміжного контролю;

3) виконання модульного контрольного завдання.

Контроль систематичного виконання самостійної роботи та активності на лабораторних заняттях

Оцінювання проводиться за 5-бальною шкалою за такими критеріями:

1) розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються;

2) ступінь засвоєння матеріалу дисципліни;

3) ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються;

4) уміння поєднувати теорію з практикою при розгляді виробничих ситуацій, розв'язанні задач, проведенні розрахунків при виконанні завдань, винесених для самостійного опрацювання, та завдань, винесених на розгляд в аудиторії;

5) логіка, структура, стиль викладу матеріалу в письмових роботах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки.

Оцінка "відмінно" ставиться за умови відповідності виконаного завдання студента або його усної відповіді до всіх п'яти зазначених критеріїв.

Відсутність тієї чи іншої складової знижує оцінку на відповідну кількість балів.

При оцінюванні практичних завдань увага приділяється також їх якості та самостійності, своєчасності здачі виконаних завдань викладачу (згідно з графіком навчального процесу). Якщо якась із вимог не буде виконана, то оцінка буде знижена.

Проміжний модульний контроль

Проміжний модульний контроль рівня знань передбачає виявлення опанування студентом матеріалу лекційного модуля та вміння застосовувати

його для вирішення практичної ситуації і проводиться у вигляді контрольної роботи за темами 1-го або 2-го модулю.

Проведення модульного контролю

Модульний контроль здійснюється та оцінюється за допомогою проведення контрольної роботи за всіма темами дисципліни.

Підсумкова оцінка з дисципліни розраховується як середня з кількох складових, що враховує оцінки кожного виду контролю (дві оцінки за результатами поточного модульного контролю, оцінку за лабораторні заняття, розрахункове завдання і підсумкову контрольну роботу).

11. РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1 – Розподіл балів

	Поточний контроль			Семестровий контроль	Всього за семестр
	КР	лр	ІНДЗ		
Підсумкові бали	64			36	100
Макс. проміжні бали	12	8	–		
Кільк. од. обліку у семестрі	*2*	5	–		
Макс. проміжних балів, всього	24	40	–		100
Коеф. перерахунку	1				
Макс. кільк.підсумкових балів	24	35	–	36	100

Критерії та система оцінювання знань та вмінь студентів.

Згідно основних положень ЄКТС, під системою оцінювання слід розуміти сукупність методів (письмові, усні і практичні тести, екзамени, проекти, тощо), що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними критеріями оцінювання для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

Критерії оцінювання – це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.
Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів протягом навчального семестру, встановлення постійного зворотного зв’язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.

2. Підвищення об’єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100 бальної шкали (табл. 2). Оцінки обов’язково переводять у національну шкалу (з виставленням державної семестрової оцінки „відмінно”, „добре”, „задовільно” чи „незадовільно”) та у шкалу ECTS (A, B, C, D, E, FX, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
90 ... 100	A	відмінно
82 … 89	B	добре
74 … 81	C	
64 … 73	D	задовільно
60 … 63	E	
35 … 59	FX	незадовільно з можливістю повторного складання
0 … 34	F	незадовільно з обов'язковим повторним вивченням дисципліни

12. НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Стандарт вищої освіти першого (бакалаврського) рівня за спеціальністю 121 "Інженерія програмного забезпечення", який затверджено наказом Міністерства освіти і науки України від 29.10.2018 р. № 1166.
2. Робоча програма навчальної дисципліни.
3. Силабус навчальної дисципліни
4. Євсеєв С.П. Лабораторний практикум з дисципліни "Технології захисту інформації" [Електронний ресурс]. – Режим доступу: ntumoodle.com

13. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Євсеєв С.П, Остапов С.Е., Король О.Г. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678.

2. Р. В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016..

3. Ленков С.В. Методы и средства защиты информации. В 2-х томах/ С. В. Ленков, Д. А. Перегудов, В. А. Хорошко.– К.: Арий, 2008. – Т.II. Информационная безопасность. – 344 с.

Допоміжна література

4. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання. Том І. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.

5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.

6. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. – Харьків, Видавництво: Форт, 2012. – 878.

7. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМИТ”, 2006. – Т.1. – 292 с.

8. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМИТ”, 2006. – Т.2. – 252 с.

9. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016).

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

10. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11423.

11. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Електронний ресурс]. Доступно: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii.

12. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Електронний ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11425

13. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Електронний ресурс]. Доступно: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005

14. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Електронний ресурс]. доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11427

15. http://dstszi.gov.ua.