ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
Кафедра інформаційних технологій та систем

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Юрій УТКІН
«_30_» серпня 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(обов'язкова навчальна дисципліна 120 кредитів**)**

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітньо–професійна програма Інформаційні управляючі системи

Спеціальність 126 Інформаційні системи та технології

Галузь знань 12 Інформаційні технології

Освітній ступінь Бакалавр

Навчально-науковий інститут економіки, управління, права та інформаційних технологій

Полтава 2021/2022 н.р.

Робоча програма навчальної дисципліни «Безпека інформаційних систем» для здобувачів вищої освіти за освітньо-професійною програмою Інформаційні управляючі системи спеціальності 126 Інформаційні системи та технології (120 кредитів)

Мова викладання державна

Розробник: Лариса Дегтярьова, доцент кафедри інформаційних систем та технологій, к.т.н., доцент

« 30 » серпня 2021 року

Розробник _____ Лариса ДЕГТЯРЬОВА

Схвалено на засіданні кафедри інформаційних систем та технологій
Протокол від 30 серпня 2021 р. №1

Затверджено завідувачем кафедри
« 30 » серпня 2021 року _____ Юрій УТКІН

Погоджено гарантом освітньої програми Інформаційні управляючі системи

« 30 » серпня 2021 року _____ Олена КОПІШИНСЬКА

Схвалено головою НМР спеціальності «Інформаційні системи та технології»
_____ Олена КОПІШИНСЬКА

1. Опис навчальної дисципліни

Елементи характеристики	Денна форма навчання: 126ІСТ_бд_2020[1] (стн)
Загальна кількість годин	90
Кількість кредитів	3
Місце в індивідуальному навчальному плані студента	Обов’язкова
Рік навчання (курс)	2
Семестр	4
Лекції (годин)	14
Лабораторні роботи (годин)	16
Самостійна робота (годин)	60
в т. ч. індивідуальні завдання (контрольна робота) (годин)	-
Вид підсумкового контролю	екзамен

2. Передумови для вивчення навчальної дисципліни

Дисципліна базується на окремих темах дисциплін «Комп'ютерні мережі», «Інформаційні системи», «Проектування інформаційних систем».

3. Заплановані результати навчання

Мета навчальної дисципліни «Безпека інформаційних систем» розкриття сучасних методів захисту інформації в інформаційних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

Основними завданнями вивчення дисципліни «Безпека інформаційних систем» є формування у майбутніх фахівців знань, навичок і умінь, що забезпечують реалізацію захисту конфіденційності інформації; здійснення захисту цілісності інформації; сприяння доступності необхідної інформації.

Компетентності:

Загальні:

- КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу.
- КЗ 2. Здатність застосовувати знання у практичних ситуаціях.
- КЗ 3. Здатність до розуміння предметної області та професійної діяльності.

Спеціальні (фахові):

- КС 3. Здатність до проектування, розробки, налагодження та вдосконалення системного, комунікаційного та програмно-апаратного забезпечення інформаційних систем та технологій, Інтернету речей (IoT), комп’ютерно-інтегрованих систем та системної мережної структури, управління ними.

– КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов’язків.

– КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

Програмні результати навчання:

– ПР 3. **Використовувати** базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп’ютерних програм мовами високого рівня із застосуванням об’єктно-орієнтованого програмування для розв’язання задач проектування і використання інформаційних систем та технологій.

– ПР 5. **Аргументувати** вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.

– ПР 6. **Демонструвати** знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп’ютерних систем та середовищ з метою їх запровадження у професійній діяльності.

Методи навчання:

усні та методи стимулювання і мотивації: роз’яснення мети вивчення предмета; висування вимог; заохочення;

словесні: пояснення, лекція, інструктаж;

наочні: демонстрація, ілюстрування;

практичні: лабораторна робота;

за логікою: індуктивний, аналітичний, синтетичний, порівняння;

за мисленням: дослідницький, репродуктивний;

інноваційні методи навчання: мультимедійна презентація; дистанційне навчання;

методи самостійної роботи вдома: самостійна робота без керівництва викладача (усні та письмові домашні завдання, завдання самостійної роботи).

4. Програма навчальної дисципліни

Тема 1. Проблеми безпеки в Інтернет.

Електронний бізнес і проблеми безпеки. Основні моделі електронної комерції. Здійснення електронних платежів через Інтернет. Потенційні загрози для електронного бізнесу. Шляхи розв`язання проблем безпеки електронного бізнесу.

Тема 2. Проблеми безпеки корпоративних інформаційних систем.

Основні поняття інформаційної безпеки. Проблеми безпеки IP-мереж. IP версія 4. IP версія 6. Аналіз загроз безпеки інформаційних систем та мереж. Модель загроз безпеки.

Тема 3. Побудова підсистеми інформаційної безпеки.

Експертиза захищеності комп`ютерної системи. Розробка концепції і політики інформаційної безпеки. Проектування комп`ютерної системи в захищеному виконанні. Варіанти реалізації основних функцій підсистеми інформаційної безпеки комп`ютерної системи. Експертиза та сертифікат ЗЗІ.

Тема 4. Принципи інформаційної безпеки.

Протидія несанкціонованому міжмережевому доступу. Фільтрація трафіку. Виконання функцій посередництва. Особливості міжмережевого екранування на різних рівнях моделі OSI. Екранний маршрутизатор. Шлюз сеансового рівня. Прикладний шлюз.

Тема 5. Встановлення і конфігурування систем FireWall.

Розробка політики міжмережевої взаємодії. Визначення схеми підключення міжмережевого екрану. Настройка параметрів функціонування брандмауера. Критерії оцінки міжмережевих екранів. Сучасні системи FireWall. Переваги і недоліки. Підтримка різних платформ і режимів роботи. Ефективність управління. Підтримка функцій захисту.

Тема 6. Побудова захищених віртуальних мереж VPN.

Способи створення захищених віртуальних каналів. Захищені віртуальні канали. Тунелювання на канальному рівні. Протокол PPTP. Протокол L2F. Протокол L2TP. Захист віртуальних каналів на мережевому рівні. Архітектура засобів безпеки IPSec. Протокол заголовку аутентифікації. Протокол інкапсульованого захисту. Управління захищеним тунелем. Захищені віртуальні канали на сеансовому рівні. Протокол SSL. Протокол Socks.

Тема 7. Розподіл криптографічних ключів.

Узгодження параметрів захищеного каналу. Протокол SKIP. Розподіл криптографічних ключів. Протокол ISAKMP. Узгодження параметрів кожного захищеного з`єднання.

5. Структура (тематичний план) навчальної дисципліни

Назви тем	Кількість годин			
	Денна форма навчання: 126ІСТ_бд_2020[1] (стн)			
	усього	у тому числі		
		л	лр	с.р.
Тема 1. Проблеми безпеки в Інтернет	12	2	2	8
Тема 2. Проблеми безпеки корпоративних інформаційних систем.	14	2	4	8
Тема 3. Побудова підсистеми інформаційної безпеки.	12	2	2	8
Тема 4. Принципи інформаційної безпеки.	13	2	2	9
Тема 5. Встановлення і конфігурування систем FireWall.	13	2	2	9
Тема 6. Побудова захищених віртуальних мереж VPN.	13	2	2	9
Тема 7. Розподіл криптографічних ключів	13	2	2	9
Усього годин	**90**	**14**	**16**	**60**
Екзамен	**27**			

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання: 126ІСТ_бд_2020[1](стн)
1	**Л/р №1:** Робота з обліковими записами користувачів і груп ОС Windows Server. Встановлення правил доступу до об’єктів файлової системи	2
2	**Л/р №2:** Використання теорії чисел для захисту інформації	2
3	**Л/р №3:** Організація безпеки локальної мережі при використанні утиліт, що реалізують моніторинг трафіка	2
4	**Л/р №4:** Організація безпеки механізму аутентифікації при перехопленні парольних хешей і їхньої розшифровки	2
5	**Л/р №5:** Налаштовування та адміністрування міжмережних екранів	2
6	**Л/р №6:** Методика побудови захищеної телекомунікаційної мережі із використанням VPN	2
7	**Л/р №7:** Криптографічні методи захисту даних: проста перестановка по ключу, подвійна перестановка, магічні квадрати	4
	Разом	**16**

7. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
		Денна форма навчання: 126ІСТ_бд_2020[1] (стн)
1	**Тема 1.** Проблеми безпеки в Інтернет	8
2	**Тема 2.** Проблеми безпеки корпоративних інформаційних систем.	8
3	**Тема 3.** Побудова підсистеми інформаційної безпеки.	8
4	**Тема 4.** Принципи інформаційної безпеки.	9
5	**Тема 5.** Встановлення і конфігурування систем FireWall.	9
6	**Тема 6**. Побудова захищених віртуальних мереж VPN.	9
7	**Тема 7.** Розподіл криптографічних ключів	9
	Разом	**60**

8. Оцінювання результатів навчання

Програмні результати навчання	Форми контролю
ПРН 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп’ютерних програм мовами високого рівня із застосуванням об’єктно-орієнтованого програмування для розв’язання задач проектування і використання інформаційних систем та технологій.	усний контроль: робота на лекціях (участь в обговоренні висування гіпотез, пропозицій тощо); письмовий контроль: перевірка звітів про виконання лабораторних робіт і їх захист; перевірка самостійної роботи; лабораторно-практичний контроль: виконання лаб. робіт; Екзамен (виконання теоретичних та практичних завдань)
ПРН 5. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.	усний контроль: робота на лекціях (участь в обговоренні висування гіпотез, пропозицій тощо); письмовий контроль: перевірка звітів про виконання лабораторних робіт і їх захист; перевірка самостійної роботи; лабораторно-практичний контроль: виконання лаб. робіт; Екзамен (виконання теоретичних та практичних завдань)
ПРН 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп’ютерних систем та середовищ з метою їх запровадження у професійній діяльності.	усний контроль: робота на лекціях (участь в обговоренні висування гіпотез, пропозицій тощо); письмовий контроль: перевірка звітів про виконання лабораторних робіт і їх захист; перевірка самостійної роботи; лабораторно-практичний контроль: виконання лаб. робіт; Екзамен (виконання теоретичних та практичних завдань)

Забезпечення тематикою дисципліни успішного опанування програмних результатів навчання для здобувачів вищої освіти (126ІСТ_бд_2020[1](стн))

Теми занять	Програмні результати навчання			**Разом**
	ПРН3	ПРН5	ПРН6	
Тема 1. Проблеми безпеки в Інтернет	+	+	+	3
Тема 2. Проблеми безпеки корпоративних інформаційних систем.	+	+	+	3
Тема 3. Побудова підсистеми інформаційної безпеки.	+	+	+	3
Тема 4. Принципи інформаційної безпеки.	+	+	+	3
Тема 5. Встановлення і конфігурування систем FireWall.	+	+	+	3
Тема 6. Побудова захищених віртуальних мереж VPN.			+	1
Тема 7. Розподіл криптографічних ключів		+	+	2
Разом	**5**	**6**	**7**	**18**
максимальний відсоток у підсумковій оцінці з навчальної дисципліни, %	28	28	44	**100**
мінімальний відсоток у підсумковій оцінці з навчальної дисципліни, %	17	17	26	**60**

Критерієм успішного навчання є досягнення здобувачем вищої освіти мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання.

Критерії успішного опанування програмних результатів навчання

студентами денної форми навчання

Програмні результати навчання	Відсоток у підсумковій оцінці з навчальної дисципліни, %	Пороговий рівень оцінок, балів	
		максимальний	мінімальний
ПРН3	29	28	17
ПРН5	29	28	17
ПРН6	42	44	26
Разом	100	100	60

Одним із обов’язкових елементів освітнього процесу є систематичний поточний контроль оволодіння компетентностями та підсумкова оцінка рівня досягнення програмних результатів навчання.

Форми, шкала та критерії оцінювання результатів навчання при проведенні поточного контролю успішності здобувачів вищої освіти:

Програмні результати навчання	Форма оцінювання (денна форма навчання)														**Разом**	
	Робота на лекціях		Підготовка до лабораторних занять		Виконання завдань на лабораторних заняттях		Оформлення звітів і їх захист		Самостійна робота		Екзамен		Контроль-на робота з теорії			
	Мінімальна к-ть балів	Максимальна к-ть балів	Мінімальна к-ть балів	Максимальна к-ть балів	Мінімальна к-ть балів	Максимальна к-ть балів	Мінімальна к-ть балів	Максимальна к-ть балів	Мінімальна к-ть балів	Максимальна к-ть балів	Мінімальна к-ть балів	Максимальна к-ть балів	Мінімальна к-ть балів	Максимальна к-ть балів	Мінімальна к-ть балів	Максимальна к-ть балів
ПРН3	3	4	1	2	4	9	1	2	3	4	4	6	1	1	17	28
ПРН5	3	4	1	2	4	9	1	2	3	4	4	6	1	1	17	28
ПРН6	4	6	2	4	8	14	2	4	4	6	5	8	1	2	26	44
Разом	**10**	**14**	**4**	**8**	**16**	**32**	**4**	**8**	**10**	**14**	**13**	**20**	**3**	**4**	**60**	**100**

Критерієм успішного проходження здобувачем вищої освіти підсумкового оцінювання є досягнення ним рівня вище межі незадовільного навчання.

Одним із обов'язкових елементів навчального процесу є систематичний поточний контроль засвоєння знань та підсумкова оцінка рівня засвоєння навчального матеріалу і вміння використовувати ці знання на практиці.

Засоби оцінювання та методи демонстрування результатів навчання для поточного контролю успішності здобувача вищої освіти здійснюється за видами навчальної роботи:

- робота на лекціях (0-2 бали);
- підготовка до лабораторних занять (0-1 бал);
- виконання завдань на лабораторних заняттях (0-4 бали);
- оформлення звітів і їх захист (0-1 балів);
- самостійна робота (0-2 бали);
- контрольна робота з теорії (0-4 бали)

Семестровий підсумковий контроль – оцінювання рівня засвоєння здобувачем вищої освіти всього обсягу навчальної дисципліни проводиться у формі **екзамен**.

Критерії оцінювання окремих видів навчальної роботи здобувачів вищої освіти денної форми навчання[1]

Вид роботи, кількість балів	Критерії оцінювання кожного виду роботи в межах зазначеної кількості балів
Робота на лекціях (0-2бали)	0 балів – студент не був присутній на лекції та не опрацював матеріал; 1 бал – студент є присутнім на лекції, веде конспект лекції. 2 бали – студент є присутнім на лекції, веде активну участь в обговоренні проблемних питань, веде конспект лекції.
Підготовка до лабораторних занять (0-1 бал)	0 балів – студент не підготувався до лабораторного заняття; 1 бал – студент знає тему заняття та базовий теоретичний матеріал для роботи над виконанням завдань.

[1] Додаткові бали можуть нараховуватись за окремі додаткові види робіт (написання тез доповіді, виступ на конференції в межах 5 балів)

Виконання завдань на лабораторних заняттях (0-4 бали)	0 -1 бал – студент не виконав жодної вправи лабораторної роботи або всі завдання виконано невірно; 2 бали – правильне виконання 1 вправи (або двох частин по 0,5 балів) лабораторної роботи з відповідями на контрольні питання; 3 бали – правильне виконання всіх вправ лабораторної роботи без відповідей на контрольні питання; 4 бали - правильне виконання всіх вправ лабораторної роботи та відповідь на всі контрольні питання.
Оформлення звітів і їх захист (0-2 балів)	0 балів – студент не оформив звіт; 1 бал – звіт оформлено в електронному виді, але він не включає в себе відповіді на контрольні питання; 2 бали - звіт оформлено в електронному виді та роздрукованому вигляді, він включає в себе відповіді на контрольні питання. Для лабораторних робіт, розрахованих на 4 години та тих, що мають два або більше завдань, передбачено 2 звіти
Самостійна робота (0-2 бали)	Самостійна робота з тем 6-8 передбачає максимальну кількість балів 3: 0 балів – студент не представив виконане завдання самостійної роботи, або виконано до 20% обсягу завдань; 1 бал – від 20 % до 75 % правильного виконання роботи; 2 бали – від 75 % до 100 % правильного виконання завдання.
контрольна робота з теорії (0-4 бали)	0 -1 бал – студент відповів на жодне питання вірно, або неточна відповідь тільки на одне питання; 2 бали – правильна відповідь на 1 питання (або неточна відповідь на 2 питання); 3 бали – правильна відповідь на половину питань опитування; 4 бали - правильна відповідь на всі питання опитування.

9. Схема нарахування балів з навчальної дисципліни

Денна форма навчання

Теми	Види навчальної роботи здобувачів вищої освіти							
	Робота на лекціях	Підготовка до лаб. занять	Виконання завдань на лабораторних заняттях	оформлення звітів і їх захист	самостійна робота	Екзамен	Контрольна робота з теорії	всього
Тема 1. Проблеми безпеки в Інтернет	2	1	4	1	2			10
Тема 2. Проблеми безпеки корпоративних інформаційних систем.	2	1	4	1	2			10
Тема 3. Побудова підсистеми інформаційної безпеки.	2	1	4	1	2			10
Тема 4. Принципи інформаційної безпеки.	2	1	4	1	2			10
Тема 5. Встановлення і конфігурування систем FireWall.	2	1	4	1	2			10
Тема 6. Побудова захищених віртуальних мереж VPN.	2	1	4	1	2			10
Тема 7. Розподіл криптографічних ключів	2	2	8	2	2			16

Теоретичне опитування (контр. Робота)							4	4
Екзамен						20		20
Разом балів за темами	**14**	**8**	**32**	**8**	**14**	**20**	**4**	**100**

Шкала та критерії оцінювання знань здобувачів вищої освіти (126ІСТ_бд_2020 (стн)) на екзамені*

Вид завдання, кількість балів	Критерії оцінювання
Відповідь на теоретичне питання 1, 0-5 балів	5 балів – більше 90 % правильних відповідей 4 бали - більше 50 % правильних відповідей 3 бали – більше 39 % правильних відповідей 2 бали – до 39 % правильних відповідей 1 бал – до 25 % правильних відповідей 0 балів – відсутність відповіді на теоретичне питання, що не дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти
Відповідь на теоретичне питання 2 (0 – 5 балів)	5 балів – більше 90 % правильних відповідей 4 бали - більше 50 % правильних відповідей 3 бали – більше 39 % правильних відповідей 2 бали – до 39 % правильних відповідей 1 бал – до 25 % правильних відповідей 0 балів – відсутність відповіді на теоретичне питання, що не дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти
Практичне завдання (0 – 10 балів)	0 балів – відсутність розрахунку практичної ситуації, що не дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти 2 балів: студент вміє проводити аналіз вхідних даних та розуміє засоби та методи, які треба використати для розрахунків; 4 балів: студент виконав частину завдання, яка складає 25% від загальної кількості обробленої інформації; 6 балів – студент виконав частину завдання, яка складає 50% від загальної кількості обробленої інформації; 8 балів – студент виконав частину завдання, яка складає 75% від загальної кількості обробленої інформації; 10 балів – розрахунки практичного завдання виконані правильно, сформовані повні висновки, що свідчать про формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти
Разом за виконання екзаменаційних завдань	20 балів

10. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна (за потреби)

Інструменти, обладнання та програмне забезпечення, необхідне для навчальної дисципліни, забезпечує спеціалізована комп'ютерна лабораторія 202, 213.

11. Рекомендовані джерела інформації

Основні

1. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах. навч. посіб. Х.: НТУ «ХПІ», 2015. 251 с.
2. Хорошко В. О. Проєктування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.
3. Петренко В.И., Мандрица И.В. Защита персональних даннях в информационных системах. Практикум. Издательство: Лань, 2019. 687 с.
4. Кузнецов О.О. Захист інформації в інформаційних системах. Вид. ХНЕУ, 2017. 286 с.

Допоміжні

1. Яковенко Є., Журавель І, Горбатий І. Інформаційна безпека. Львів: Львівська політехніка, 2019. 580 с.
2. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Вид-во SIDCON, 2021. 372 с.
3. Лисенко С. Теорія адміністративно-правового забезпечення інформаційної безпеки підприємництва: монографія. Видавничий дім "Персонал", 2017. 404 с.

Інформаційні ресурси

1. Сайт ПДАА. Режим доступу: http://www.pdaa.edu.ua/Сайт ПДАА.
2. Дегтярьова Л.М. Система захисту інформації, як функціональна підсистема об'єкту інформатизації. Проблеми інфокомунікацій : матеріали 2-ої Всеукр. наук.-техн. конф., 5 груд. 2018 р. / ПолтНТУ; НТУ; НТУ«ХПІ»; ДУТ; УкрДУЗТ; БНТУ; ВКСС ВІТІ. – Полтава : ПолтНТУ, 2018. – С. 17-18 http://dspace.pdaa.edu.ua:8080/handle/123456789/8528
3. Одарущенко О.М., Одарущенко О.Б., Дегтярьова Л.М. Метод оцінювання та забезпечення функціональної безпеки при розроблені та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмованих логічних інтегральних схемах// Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали десятої міжнародної науково-технічної конференції. – Баку : ВА ЗС АР; Харків : НТУ

"ХПІ"; Харків : ДП "ПДПРОНДІАВІАПРОМ"; Жиліна : УмЖ, 2020 - С. 20. http://dspace.pdaa.edu.ua:8080/handle/123456789/8469

4. Дегтярьова Л.М., Мірошникова М.В., Волошко С.В. Аналіз структури системи захисту інформації. Системи управління, навігації та зв'язку. – Полтава: ПолтНТУ, 2019 – № 2 (54). – С. 78-83. http://dspace.pdaa.edu.ua:8080/handle/123456789/7478
5. Безпека інформаційних систем – Режим доступу: https://pidruchniki.com/74227/informatika/bezpeka_informatsiynih_sistem