МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

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

«**ЗАТВЕРДЖУЮ**»
Голова науково-методичної комісії _____
(назва комісії)

_____ _____
(підпис) (ініціали та прізвище)

«_____»_____20_____ року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ БЕЗПЕКИ ІС

(назва навчальної дисципліни)

рівень вищої освіти_____*перший (бакалаврський)*_____
перший (бакалаврський) / другий (магістерський)

галузь знань_____*12 Інформаційні технології*_____
(шифр і назва)

спеціальність ____*126 Інформаційні системи та технології*_____
(шифр і назва)

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

форма навчання _____*денна*_____
(денна / заочна)

Харків – 2017 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни
_____ОСНОВИ БЕЗПЕКИ ІС_____
(назва дисципліни)

Розробники:

__*доцент, к.т.н., доц.*_____	_____	*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)

Протокол від «_31___»__серпня_____2017__ року № __1___

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

ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри	Підпис голови НМК (для дисциплін загальної підготовки та дисциплін професійної підготовки за спеціальністю) або завідувача випускової кафедри (для дисциплін професійної підготовки зі спеціалізації, якщо РПНД розроблена не випусковою кафедрою)

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

Мета навчальної дисципліни "Основи безпеки ІС" є навчання студентів принципам побудови комплексних систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення надання основних послуг безпеки інформації в банківських системах, що засновані на використанні алгоритмів симетричної та несиметричної криптографії в комунікаційних системах, протоколів інфраструктури відкритих ключів (ІВК).

Компетентності:

Загальні компетентності:

- Здатність застосовувати знання у практичних ситуаціях.
- Знання та розуміння предметної області та розуміння професійної діяльності.
- Здатність вчитися і оволодівати сучасними знаннями.
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (фахові) компетентності:

- Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.

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

Класифікація компетентностей за НРК	**Знання**	**Уміння**	**Комунікація**	**Автономія та відповідальність**
ФК 11 Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.	Знання основних положень законодавства в галузі захисту інформації, основні міжнародні та національні стандарти з безпеки даних; принципи побудови профілю захисту інформації для забезпечення послуг з безпеки; механізми та	визначати вимоги політики безпеки та формувати профіль захисту відповідно до забезпечення послуг з безпеки; забезпечувати обґрунтований підбір програмно-апаратних і програмних засобів для забезпечення необхідного рівня захисту	Здатність донесення до фахівців і нефахівців інформації, ідей, проблем, рішень та власного досвіду в галузі професійної діяльності; здатність ефективно формувати комунікаційну стратегію.	Здатність здійснювати захист даних в корпоративних розподілених інформаційних системах, застосовувати системи криптографії в професійній діяльності, вивчати нові технології, методі та прийоми щодо забезпечення захисту інформації;

	протоколи забезпечення ЦКД даних	інформації;		

Структурно-логічна схема вивчення навчальної дисципліни

Попередні дисципліни:	Наступні дисципліни:
“Алгоритмізація та програмування”	Адміністрування ІС ч.1-2
“Комп’ютерна математика ч.2”	
“Мережеві технології”	

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
5	**150 /5**	**72**	**78**	**16**	**32**			**20**		**4**

Співвідношення кількості годин аудиторних занять до загального обсягу складає 48% (%):

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. Принципи безпеки та захисту інформації в ПЗ				
	Л	2	**Тема 1. Огляд безпеки системи**	

№ 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)
	ЛР СР	4 6	Класичні симетричні системи. Дослідження крипостійкості простих симетричних шифрів	
	Л	2	**Тема 2. Механізми і політики розмежування прав доступу. Тема 3. Методи та пристрої забезпечення захисту і безпеки**	
	ЛР	4	Дослідження сучасних блочних симетричних шифрів та режимів шифрування	
	СР	6		
	Л	2	**Тема 4. Захист, доступ та автентифікація** **Тема 5. Моделі захисту.**	
	ЛР	4	Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ ISO\IEC 15948-2	
	СР	9		
	Л	2	**Тема 6. Шифрування даних** **Тема 7. Управління відновленням**	
	ЛР	4	Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ 4145, ECDSA	
	СР	9		
Змістовий модуль 2. Інформаційні технології обробки інформації в операційних системах				
	Л	2	**Тема 8. Основні напрямки розвитку сучасної криптографії**	
	ЛР	4	Стеганографічні методи захисту інформації	
	СР	9		
	Л	2	**Тема 11. Алгоритми з секретним ключем** **Тема 12. Алгоритми з відкритим ключем**	
	ЛР	4	Безпечність персональних конфіденціальних даних на базі секретного диску та захищеної електронної пошти PGP	
	СР	9		
	Л	4	**Тема 9. Механізми та протоколи керування ключами в ІВК**	
	ЛР	2	Статистичні дослідження генераторів випадкових та	
	СР	9	псевдовипадкових послідовностей за методикою	
	Л	2	NIST **Тема 13. Протоколи автентифікації**	
	ЛР	2	**Тема 14. Цифрові підписи**	
	СР	9	Розгортання та управління інфраструктурою	
	Л	2	відкритих ключів **Тема 15. Використання паролів і механізмів**	
	ЛР	2	**контролю за доступом**	

№ 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)
	СР	12	Розгортання та управління інфраструктурою відкритих ключів	
Разом (годин)		150		

САМОСТІЙНА РОБОТА

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацьовування лекційного матеріалу	20
2	Підготовка до практичних(лабораторних, семінарських) занять	20
3	Самостійне вивчення тем та питань, які не викладаються на лекційних заняттях	10
4	Виконання індивідуального завдання:	20
5	Інші види самостійної роботи	8
	Разом	**78**

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Курсовий проект

(вид індивідуального завдання)

Модуль 1. Безпека та захист даних

Аналіз умов функціонування та сучасних загроз інформації в комп'ютерних мережах та системах

Побудова класифікацій криптографічних засобів

Побудова моделі порушника безпеки в КМіС

Побудова моделі реалізації загроз безпеки в КМіС

Побудова математичної моделі пасивних атак у КМіС

Побудова моделі активних атак у КМіС із блокуванням передачі інформації

Побудова моделі активних атак у КМіС із внесенням перешкод

Побудова моделі активних атак "маскарад" у КМіС

Побудова та аналіз моделі оцінки ризику реалізації загроз безпеки комунікаційних систем

Оцінка ризику реалізації загроз у комунікаційних системах

Література: основна [1 – 4]; додаткова [5 – 10].

Модуль 2. Основи побудови систем захисту інформації в ПЗ

Використання Firewall (Брандмауер)

Використання Network Address Translation

Використання демілітаризованої зони

Використання другого firewall-у

Використання Proxy-сервер-у

Використання другого mail-серверу

Антивірусний захист поштової системи

Використання Log-серверу

Література: основна [1 – 4]; додаткова [5 – 10].

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. ОГЛЯД БЕЗПЕКИ СИСТЕМИ	Проблемна лекція "Визначення базових засад захисту інформації в інформаційної системі підприємства"
ТЕМА 13. ПРОТОКОЛИ АВТЕНТИЧНОСТІ **ТЕМА 14. ЦИФРОВІ ПІДПИСИ**	Міні-лекція "Класифікація та огляд національних та міжнародних стандартів захисту інформації. Визначення перспективного напрямку гармонізації міжнародних стандартів"
ТЕМА 6. ШИФРУВАННЯ ДАНИХ	Кейс "Проведення криптоаналізу класичних шифрів". Міні-лекція "Методика визначення крипостійкості та дослідження основних характеристик симетричних та асиметричних криптосистем"

Тема	Практичне застосування навчальних технологій
ТЕМА 12. АЛГОРИТМИ З ВІДКРИТИМ КЛЮЧЕМ	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”

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 курсовий проект і підсумкову контрольну роботу).

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	75			25	100
Макс. проміжні бали	12	7	16		
Кільк. од. обліку у семестрі	*2*	*5*	*1*		
Макс. проміжних балів, всього	24	35	16		100
Коеф.. перерахунку	1				

Макс. кільк.підсумкових балів	24	35	16	25	100

Таблиця 2 – Розподіл балів за виконання курсового проекту

Пояснювальна записка	Ілюстративна частина	Захист роботи	Сума
до 25	до 25	до 50	100

Таблиця 3 – 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

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Євсеєв С.П. Лабораторний практикум з дисципліни “Технології захисту інформації” [Електронний ресурс]. – Режим доступу: ntumoodle.com

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.

2. Кузнецов О. О. Захист інформації в інформаційних систе-мах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

3. Остапов С. Е. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.

4. Хорошко В. А. Методы и средства зашиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

Допоміжна література

5. 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.

6. Мао Венбо Современная криптография: теория и практика.: Пер. с англ. – М.: Издательский дом “Вильямс”, 2005. – 768 с.

7. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. / А. А. Петров– М.: ДМК, 2000. – 448 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.1. – 292 с.

9. 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.

10. Чмора А.Л. Современная прикладная криптография. / А. Л. Чмора. – М.: Гелиос АРВ, 2001. – 256 с.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

11. http://bezopasnost.biz.
12. http://dstszi.gov.ua.
13. http:// securitylab.ru
14. http:// pgpi.org
15. http:// citmgu.ru