МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

М. В. Афанасьєв

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**121 "ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**"ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ"**

Вид дисципліни	**базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 1 від 26.08.2019 р.

Розробник(-и):
Євсеєв С.П, д.т.н., с.н.с., завідувач кафедри КІТ
Король О.Г., к.т.н., доц. кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Анотація навчальної дисципліни:

Подано тематичний план навчальної дисципліни й її змістовність за модулями та темами, вміщено плани лекцій і лабораторних занять, матеріал щодо закріплення знань (завдання для самостійної роботи, контрольні запитання), методичні рекомендації та оцінювання знань студентів. Революційні зміни останнього десятиліття, що відбулися в Інтернет-ресурсах, зумовили до об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір, що спонукало до створення інформаційно-корпоративних мереж на основі Інтернет-технологій, які істотно розширили спектр електронних послуг суспільства в цілому та людині окремо. Як на-слідок, суттєво трансформувалися і загрози такому інформаційному ресурсу, як Інтернет-ресурс (ІР). Загрози безпеці ІР набули ознак гібридності. Прояви ознак гібридності унаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці (КБ) та безпеці інформації (БІ) на ІР призвели до виникнення явища синергізму, негативні прояви від якого потребують кардинального перегляду концепцій побудови діючих систем безпеки.

Розповсюдження Інтернет-технологій також, безперечно, вимагає добре поставленого захисту інформації яка циркулює і в кіберпросторі. Тому вивчення основних механізмів забезпечення безпеки, захисту програмного забезпечення на всьому циклі його існування приділяється багато уваги.

Мета навчальної дисципліни:

Метою викладання дисципліни "Безпека програм та даних" є навчання студентів принципам захисту програмного забезпечення на всьому циклі його існування, дослідженню та використанню сучасних процедур забезпечення основних услуг безпеки інформації в інформаційно-комунікаційних ресурсах Інтернет-технологій та кіберпросторі, що засновані на використанні алгоритмів симетричної та несиметричної криптографії, цифровому підписі та протоколів інфраструктури відкритих ключів (ІВК).

Курс	**4**	
Семестр	**1**	
Кількість кредитів ECTS	**4**	
Аудиторні навчальні заняття	**лекції**	**30**
	семінарські, практичні	**–**
	лабораторні	**30**
Самостійна робота		**60**
Форма підсумкового контролю	**залік**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Дискретна математика	Інженерія програмного забезпечення
Комп'ютерні системи та архітектура комп'ютерів	Програмування Інтернет
Комп'ютерні мережі	Архітектура та проектування програмного забезпечення

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Аналіз основ теорії захисту інформації щодо системного підходу до організації комплексних систем захисту даних на основі застосування криптографічних методів	Знати основні положення законодавства в галузі захисту інформації, основні міжнародні та національні стандарти з безпеки даних; основні терміни та визначення політики безпеки, принципи побудови профілю захисту інформації для забезпечення послуг безпеки
Здатність приймати участь у проектуванні програмного забезпечення, включаючи проведення моделювання (формальний опис) його структури, поведінки та процесів функціонування	Знати та вміти використовувати механізми та протоколи забезпечення конфіденційності, забезпечення автентичності (доступності) та цілісності даних
Знання і розуміння специфікацій, стандартів, правил і рекомендацій в професійній галузі, уміння оцінювати ступінь обґрунтованості їх застосування, здатність дотримуватися їх при реалізації процесів життєвого циклу	Знати моделі порушника, основні види атак, принципи лінійного та диференційного криптоаналізу. Методи та процедури захисту в банківських системах. Забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій в програмному забезпечені IoT
дослідження формування цифрового підпису за допомогою протоколів інфраструктури відкритих ключів (ІВК)	Знати та вміти використовувати механізми та протоколи керування ключами в ІВК інформаційної системи

3. Програма навчальної дисципліни

Змістовий модуль 1. Безпека і захист даних

Тема 1. Механізми і політики розподіл прав доступу

Основні поняття та визначення безпеки. Роль захисту інформації в ІС, умови функціонування підсистеми безпеки в комп'ютерних мережах і системах. Вимоги щодо безпеки системи, риски безпеки. Послуги з безпеки: конфіденційність, цілісність, доступність, причетність, спостережність. Розподіл послуг безпеки за рівнями моделі *ISO/OSI*. Критерії захищеності комп'ютерних систем. Розроблення профілю захисту. Механізми реалізації послуг з безпеки. Стандарт *ISO*-7498-2. Побудування та впровадження систем захисту інформації. Засоби забезпечення захисту інформації в СУБД. Засоби ідентифікації й автентифікації об'єктів баз даних, управління доступом. Засоби контролю цілісності інформації, організація аудита. Скасування прав доступу. Видача прав доступу до об'єктів баз даних

Тема 2. Механізми шифрування. Симетричні та несиметричні криптосистеми

Математичні основи сучасної теорії захисту інформації. Методи булевої алгебри, елементи кореляційного та спектрального аналізів. Прості шифри. Симетричне шифрування даних. Криптографічні примітиви та типи структур симетричного шифрування. Блочні симетричні шифри, алгоритми блокового симетричного шифрування *DES*, ГОСТ-28147, Rijndael, Калина-256. Архітектура блочних симетричних шифрів. Типові режими роботи криптосистеми: “Електронна кодова книга”, “Зчеплення блоків шифру”, “Зворотний зв’язок з шифру”, “Зворотний зв’язок з виходу”. Потокові шифри. Регістри зсуву зі зворотнім зв’язком. Асиметричне шифрування даних. Математичні положення теорії скінченних полів і систем класів лишків. Математичні положення теорії чисел. Асиметричні алгоритми шифрування даних *RSA* й Ель Гамаля.

Тема 3. Протоколи автентифікації. Цифрові підписи

Захист інформації на мережевому рівні. Протоколи захисту та цілісності *IPSec*, *SSL*, *TLS*, їх сутність. Класифікація механізмів автентифікації. *MDC*-коди, основні алгоритми. *MAC*-коди, основні способи формування. Методи побудови універсальних геш-функцій. Класифікація стандартів електронних цифрових підписів. Моделі цифрових підписів. Основні стандарти цифрового підпису.

Тема 4. Комплексні системи захисту даних

Системи захисту PGP і CS MIME. Криптографічні функції. Сумісність на рівні електронної пошти. Захищена електронна пошта.

Тема 5. Основні види атак на програмне забезпечення. Основи криптоаналізу

Формальне математичне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, рисків і вразливих елементів інформаційних систем. Класифікація криптоаналітичних атак. Диференціальний криптоаналіз, диференціальний криптоаналіз на основі відмов пристрою. Лінійний криптоаналіз. Силова атака на основі розподілених розв’язань.

Тема 6. Основи цифровій стеганографії

Основні принципи приховування повідомлення на основі методів стеганографії. Класифікація и принципи приховування алгоритмів цифровій стеганографії.

Змістовий модуль 2. Безпека в програмному забезпеченні

Тема 7. Основи технології відкритих ключів (PKI).

Компоненти та сервіси інфраструктури відкритих ключів. Архітектура та топологія PKI. Стандарти в галузі PKI. Сертифікати відкритих ключів X.509, управління сертифікатами. Системи PKI. Документ із політики захисту інформації, його сутність і структура, управління ключами. Профілі безпеки автоматизованих систем. Основні вимоги до політики PKI.

Тема 8. Захист програмного забезпеченні в Інтернет-технологіях

Основні принципи захисту інформації під час підключення до мережі Інтернет. Використання паролів і механізмів контролю.

Тема 9. Захист персональних даних

Основні принципи захисту персональних даних на основі програмного коду. Моделі захисту персональних даних.

Тема 10. Основні принципи захисту програмного забезпечення

Принципи забезпечення програмного забезпечення на кожному етапі життєвого циклу ПЗ.

Теми лабораторних робіт

Лабораторна робота 1. Класичні симетричні системи. Дослідження крипостійкості простих симетричних шифрів;

Лабораторна робота 2. Дослідження сучасних блочних симетричних шифрів і режимів шифрування;

Лабораторна робота 3. Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ *ISO\IEC* 15948-2;

Лабораторна робота 4. Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ-4145, *ECDSA*;

Лабораторна робота 5. Стеганографічні методи захисту інформації;

Лабораторна робота 6. Безпечність персональних конфіденційних даних на базі секретного диску та захищеної електронної пошти *PGP*;

Лабораторна робота 7. Статистичні дослідження генераторів випадкових і псевдовипадкових послідовностей за методикою *NIST*.

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних і лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі колоквіуму як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лекційних і лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються; ступінь засвоєння фактичного матеріалу навчальної дисципліни; ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються; вміння поєднувати теорію з практикою при розгляді виробничих ситуацій, розв'язанні задач, проведенні розрахунків у процесі виконання індивідуальних завдань та завдань, винесених на розгляд в аудиторії; логіка, структура, стиль викладу матеріалу в письмових роботах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки; арифметична правильність виконання індивідуального та комплексного розрахункового завдання; здатність проводити критичну та незалежну оцінку певних проблемних питань; вміння пояснювати альтернативні погляди та наявність власної точки зору, позиції на певне проблемне питання; застосування аналітичних підходів; якість і чіткість викладення міркувань; логіка, структуризація та обґрунтованість висновків щодо

конкретної проблеми; самостійність виконання роботи; грамотність подачі матеріалу; використання методів порівняння, узагальнення понять та явищ; оформлення роботи.

Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є: глибина і міцність знань, рівень мислення, вміння систематизувати знання за окремими темами, вміння робити обґрунтовані висновки, володіння категорійним апаратом, навички і прийоми виконання практичних завдань, вміння знаходити необхідну інформацію, здійснювати її систематизацію та обробку, самореалізація на практичних та семінарських заняттях.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі заліку, який вважається зданим успішно, якщо студент упродовж семестру набрав 60 і більше балів.

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – “зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову “Відомість обліку успішності” навчальної дисципліни.

Розподіл балів за тижнями

(вказати засоби оцінювання згідно з технологічною картою)

Теми змістового модуля			Лекційні заняття	Захист лабораторних робіт	Експрес-опитування	Поточні КР	Усього
Змістовий модуль 1	**Тема 1**	1 тиждень	1	–	–	–	1
	Тема 2	2 тиждень	1	5	3	–	9
	Тема 2	3 тиждень	1	–	–	–	1
	Тема 3	4 тиждень	1	5	3	–	9
	Тема 3	5 тиждень	1	–	–	–	1
	Тема 4	6 тиждень	1	5	3	–	9
	Тема 5	7 тиждень	1	–	–	12	13
	Тема 5	8 тиждень	1	5	3	–	9
	Тема 6	9 тиждень	1	–	–	–	1
Змістовий модуль 2	**Тема 7**	10 тиждень	1	5	3	–	9
	Тема 7	11 тиждень	1	–	–	–	1
	Тема 8	12 тиждень	1	5	3	–	9
	Тема 9	13 тиждень	1	–	–	12	13
	Тема 10	14 тиждень	1	5	3	–	9
	Тема 10	15 тиждень	1	5	–	–	6
		16 тиждень	–	–	–	–	–
		17 тиждень	–	–	–	–	
		18 тиждень	–	–	–	–	–
Усього			15	40	21	24	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

5. Рекомендована література

Основна

1. *Технології захисту інформації*. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов

С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6

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

3. 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.

Додаткова

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

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

Інформаційні ресурси в Інтернеті

6. http://bezopasnost.biz

7. http://dstszi.gov.ua