МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____ М. В. Афанасьєв

ЗАХИСТ ІНФОРМАЦІЇ
робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**122 "КОМП`ЮТЕРНІ НАУКИ"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**"КОМП`ЮТЕРНІ НАУКИ"**

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
Коц Г. П., к.е.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. Захист інформації перетворюється сьогодні на одну з найактуальніших задач внаслідок надзвичайно широкого розповсюдження як власне різноманітних систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення з нею сторонніх осіб. Проблема набуває особливої гостроти після прийняття урядом України закону про захист персональних даних, який зобов'язує зберігати та передавати персональні дані працівників лише у захищеному вигляді в інформаційних системах (ІС).

Не менш важливим завданням вважається широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, майбутнє введення електронних паспортів та медичних карт, студентських квитків та залікових книжок; зрештою все більше державних установ та приватних підприємств переходять на електронний документообіг, який до того ж, вимагає юридичної чинності підпису фізичної або юридичної особи. Розповсюдження таких технологій також, безперечно, вимагає добре поставленого захисту інформації.

Мета навчальної дисципліни:

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

Курс	**4**	
Семестр	**1**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**лекції**	**16**
	семінарські, практичні	**–**
	лабораторні	**48**
Самостійна робота		**86**
Форма підсумкового контролю	**екзамен**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Дискретна математика	Технології тестування ПЗ
Комп'ютерні системи	Кросплатформене програмування
Комп'ютерні мережі	Функціональне програмування

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
дослідження сучасних протоколів і процедур щодо забезпечення основних послуг безпеки у відповідності до стандартів ISO-7498-2, ISO/IEC 10181	Знати та вміти використовувати механізми та протоколи забезпечення конфіденційності, забезпечення автентичності (доступності) та цілісності даних
дослідження основних протоколів захисту інформації в банківських системах відповідно до стандартів СОУ Н НБУ 65.1 СУІБ 1.0:2010, СОУ Н НБУ 65.1 СУІБ 2.0:2010, методів двофакторній автентифікації, дослідження відповідних атак на системи банківських транзакцій та вивчення методів протидії	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 АБС
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. Огляд безпеки системи

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

Тема 2. Механізми і політики розмежування прав доступу

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 3. Методи та пристрої забезпечення захисту і безпеки

Компоненти криптосистеми й їх функціональні характеристики. Побудова класифікацій криптографічних засобів. Захист інформації за допомогою міжмережевих екранів.

Тема 4. Захист, доступ та автентифікація

Загальні механізми забезпечення безпеки. Взаємозв'язок послуг і механізмів безпеки, взаємозв'язок послуг і рівнів моделі взаємодії відкритих систем. Автентифікація даних, механізми забезпечення та методи автентифікації

Тема 5. Моделі захисту. Захист пам'яті

Побудова моделі порушника безпеки. Організація захисту, захист окремих чарунок пам'яті. Основні засоби захисту пам'яті у процесі управління, у тому числі з привілеями. Моделі безпеки. які застосовують для побудови захисту в СУБД. Захист БД у системах з видаленим доступом. Інтерфейси *CGI*, *API* та *FastCGI*

Тема 6. Шифрування даних

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 7. Управління відновленням

Захист і відновлення даних. Формування служб резервного копіювання та відновлення даних для критично-важливих серверів. Кластерізація серверів. Етапи управління формуванням плану резервного відновлення. Типи та топології резервного копіювання.

Тема 8. Основні напрямки розвитку сучасної криптографії

Основні криптографічні примітиви. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри. Основні напрями розвитку асиметричних криптоалгоритмів. Криптографія на еліптичних кривих. Теоретико-числові задачі, складність арифметики точок ЕК у різних формах і поданні. Цифрова стеганографія з відкритим ключем.

Тема 9. Механізми та протоколи керування ключами в ІВК

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.

Змістовий модуль 2. Мережева безпека

Тема 10. Основні види атак, принципи криптоаналізу.

Формальне математичне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, ризиків 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 11. Алгоритми з секретним ключем

Захист інформації на мережевому рівні. Протоколи захисту та цілісності *IPSec*, *SSL*, *TLS*, їх сутність

Тема 12. Алгоритми з відкритим ключем

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

Тема 13. Протоколи автентифікації

Класифікація механізмів автентифікації. *MDC*-коди, основні алгоритми. *MAC*-коди, основні способи формування. Методи побудови універсальних геш-функцій.

Тема 14. Цифрові підписи

Класифікація стандартів електронних цифрових підписів. Моделі цифрових підписів. Основні стандарти цифрового підпису.

Тема 15. Використання паролів і механізмів контролю за доступом

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

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, практичних, семінарських, 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 семестрового екзамену, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час семінарських, практичних 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 проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних завдань та одне теоретичне завдання, які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю 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	3	–	–	4
	Тема 3	3 тиждень	1	–	3	–	4
	Тема 4	4 тиждень	1	3	–	–	4
	Тема 5	5 тиждень	1	–	–	–	1
	Тема 6,	6 тиждень	1	3	3	–	7
	Тема 7	7 тиждень	1	–	–	6	7
	Тема 8	8 тиждень	1	–	–	–	1
	Тема 11	9 тиждень	1	3	3	–	7
Змістовий модуль 2	**Тема 12**	10 тиждень	1	–	–	–	1
	Тема 9	11 тиждень	1	3	–	–	4
	Тема 13	12 тиждень	1	–	3	6	9
	Тема 14	13 тиждень	1	3	–	–	4
	Тема 10	14 тиждень	1	–	–	–	1
	Тема 15	15 тиждень	1	3	–	–	4
		16 тиждень	–	–	–	–	–
		17 тиждень	–	–	–	–	–
		18 тиждень	–	–	–	–	–
Екзамен			–	–	–	–	40
Усього			15	21	12	12	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

5.1 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.

5.2 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

5.3 Інформаційні ресурси в мережі Інтернет

6. http://bezopasnost.biz

7. http://dstszi.gov.ua