МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"

Заступник керівника
(проректор з науково-педагогічної роботи)

_____

"_____"_____ 20___року

БЕЗПЕКА БАНКІВСЬКИХ СИСТЕМ

робоча програма для студентів

Галузь знань	**12 “ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ”**
Спеціальність	**125 “КІБЕРБЕЗПЕКА”**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**…**

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 № 12 від 05.03.2019 р.

Розробник(-и):
Євсеєв С.П, д.т.н., с.н.с., завідувач кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри
2018/2019			

1. Вступ

Анотація навчальної дисципліни:

У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки (ІБ) держави в банківському секторі (БнС). Ключову роль при побудові систем безпеки банківських інформаційних ресурсів (БІР) як складових національних інформаційних ресурсів держави, відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення ІБ держави на усіх рівнях.

Революційні зміни останнього десятиліття, що відбулися в банківському секторі, зумовили до об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір, що спонукало до створення автоматизованих банківських систем (АБС), які істотно розширили спектр електронних послуг державних і комерційних банків світу та України. Як наслідок, суттєво трансформувалися і загрози такому національному інформаційному ресурсу держави, як БІР під якими в роботі розуміється банківська інформація (БІн). Загрози безпеці БІР набули ознак гібридності. Прояви ознак гібридності внаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці (КБ) та безпеці інформації (БІ) на БІР призвели до виникнення явища синергізму, негативні прояви якого потребують кардинального перегляду концепцій побудови діючих систем безпеки.

Мета вивчення дисципліни "Безпека банківських систем"

1. Оволодіння студентами комплексом знань в області захисту банківських інформаційних ресурсів, системами й методами визначення захищеності програмних продуктів в автоматизованих банківських системах, набуття на основі цих знань практичних навичок і теоретичних знань, необхідних для творчого підходу в питанні сучасного та в майбутньому оперативного захисту контуру бізнес-процесів в організаціях банківського сектору.
2. Формування професійної компетентності майбутніх фахівців з кібербезпеки, достатньої для роботи на посаді адміністратора інформаційної безпеки банку та необхідної для розвитку кар'єри.

Завдання дисципліни

У результаті вивчення дисципліни студенти повинні:

- знати про джерела і способи дії загроз на об'єкти інформаційної безпеки банківських установ, про правові і нормативні акти, які визначають систему захисту інформації в автоматизованих банківських системах (АБС); про документи, що визначають ступінь захищеності комп'ютерних систем; методи аналізу надійності системи захисту інформації в АБС; основні методи, технологію, принципи і правила захисту транзакцій в АБС, у тому числі від сучасних загроз гібридного характеру;
- мати достатньо повне уявлення про методи і технології захисту банківських інформаційних ресурсів, принципами формування системи управління інформаційної безпекою, механізми технічного захисту від сучасних загроз, основі регулятори та їх вимоги щодо побудови комплексної системи безпеки банківських інформаційних ресурсів;
- набути практичних навичок роботи з програмними засобами забезпечення безпеки банківських інформаційних ресурсів в АБС за складовими безпеки: ІБ, КБ, та БІ, проводити комплексну оцінки дотримання вимог регуляторів щодо забезпечення інформаційної безпеки, налаштування програмних застосунків щодо електронного цифрового підпису, механізмів PKI. Забезпечення

Курс	**1**	
Семестр	**2**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**лекції**	**32**
	семінарські, практичні	
	лабораторні	**32**
Самостійна робота		**86**
Форма підсумкового контролю	**екзамен**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Основи криптографічного захисту	Організаційне забезпечення захисту інформації
Основи побудови та захисту сучасних операційних систем	Основи технічного захисту інформації
Комплексні системи захисту інформації	Безпека інформаційних служб Інтернет

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності	Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки
Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах
Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки; на основі політики захисту організації розробляти нормативні документи для її реалізації

3. Програма навчальної дисципліни

Змістовий модуль 1. Захист інформації у банківських системах електронних платежів

Тема 1. методи та задачі забезпечення банківської безпеки
Тема 2. Правове забезпечення банківської безпеки
Тема 3. Доступ до банківської інформації
Тема 4. Ризики у банківській діяльності
Тема 5. Оцінка ризиків у банківській діяльності
Тема 6. Злочини у банківській діяльності
Тема 7. Забезпечення банківської безпеки

Тема 8. Структура автоматизованої банківської системи, системи масових електронних платежів

Змістовий модуль 2. Захист внутрішньобанківської інформації

Тема 9. Послуги і механізмів криптографічного захисту банківських інформаційних ресурсів.

Тема 10. Ключі для захисту банківської інформації

Тема 11. Технологія захисту міжбанківських платежів

Тема 12. Безпека електронних банківських документів

Тема 13. Менеджмент інформаційної безпеки в АБС

Тема 14. Інструментальні засоби моніторингу та реєстрації інцидентів ІБ

Тема 15. Інструменти контролю каналів зв'язку та веб-ресурсів

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, семінарські, практичні 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 5 практичних ситуацій (два стереотипних, два діагностичних та одне евристичне 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	Практичні заняття	Лабораторні заняття	Семінарські заняття	Перевірка есе	Презентація	Експрес-опитування	Тестування	Письмова контрольна робота	Колоквіум	Усього
Змістовий модуль 1.	**Тема 1**	1 тиждень	2										2
	Тема 2	2 тиждень	2										2
	Тема 3	3 тиждень	2		3								5
	Тема 4	4 тиждень	2										2
	Тема 5	5 тиждень	2		3								5
	Тема 6	6 тиждень	2										2
	Тема 7	7 тиждень	2		3								5
	Тема 8	8 тиждень	2								5		7
Змістовий модуль 2.	**Тема 9**	9 тиждень	2		3								5
	Тема 9	10 тиждень	2										2
	Тема 10	11 тиждень	2										2
	Тема 11	12 тиждень	2		3								5
	Тема 11	13 тиждень	2										2
	Тема 12	14 тиждень	2										2
	Тема 13	15 тиждень	2		3								5
	Тема 14 **Тема 15**	16 тиждень	2								5		7
	Екзамен												40
Усього			32		18						10		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		

4. Рекомендована література

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994);
2. Закон України “Про захист персональних даних” (2010)
3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)
4. Закон України “Про національну безпеку (2018)
5. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229;
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.
11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
14. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в

автоматизованій системі.

Додаткова

21. ISO/IEC 27001. "Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью.

22. ISO/IEC 27002. "Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью."

23. ISO/IEC 27005. "Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности

Інформаційні ресурси в Інтернеті

24. http://bezopasnost.biz

25. http://dstszi.gov.ua

26. www.itsec.ru Інтернет-журнал «Інформаційна безпека».

27. www.inside-zi.ru Інформаційно-методичний журнал «Захист інформації.