СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«БЕЗПЕКА БАНКІВСЬКОЇ ДІЯЛЬНОСТІ»

Рівень освіти	перший (бакалаврський)
Спеціальність	071, 072
Тривалість викладання	12 чверть
Заняття:	
лекції:	2 години на тиждень
практичні	2 години на тиждень
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: http://do.nmu.org.ua/course/view.php?id=2661

Кафедра, що викладає Економічного аналізу та фінансів

Викладач:
Крилова Олена Валер'янівна
Доцент, канд. техн. наук.

Персональна сторінка
https://eaf.nmu.org.ua/ua/pro_kaf/title_krylova.php

E-mail:
krylova.o.v@nmu.one

1. Анотація до курсу

Безпека банківської діяльності це вибіркова дисципліна, яка обирається для формування індивідуальної освітньої траєкторії і спеціалізується на коректному розумінні безпеки банківської діяльності, формуванні концепції безпеки діяльності банківської установи, яка включає безпеку банківської установи у фінансовій, інтелектуальній, кадровій, техніко-технологічній, правовій та інформаційній сферах, та особливо фокусується на запроваджені безпекових заходів у відповідь на новітні загрози.

Мета та завдання курсу

Мета дисципліни – формування у майбутніх фахівців умінь та компетенцій щодо використання методів і механізмів оцінки та аналізу стану рівня безпеки банківської діяльності для формування навиків розробки системи заходів - плану безперервності діяльності бізнесу (BCP- business continuity plan).

Завдання курсу:

– Ознайомитись з поняттям, основними категоріями та

концептуальними засадами безпеки банківської діяльності;

– вивчити визначення індикаторів та складових безпеки банківської діяльності;

– ознайомитись з правовими засадами забезпечення безпеки банківської діяльності;

– набути знань щодо управління системою забезпечення безпеки банківської установи;

– скласти уяву про особливості організації інфраструктурних та процедурних безпекових заходів, захисту операційної діяльності та організації ефективної KYC системи;

– ознайомитись зі сутністю поняття комерційної таємниці, банківської таємниці, системою внутрішнього контролю, комплаєнс як вагомими складовими безпеки банківської діяльності;

– спілкуватися професійною мовою з фахових питань та доносити інформацію щодо кращих практик забезпечення безпеки банківської установи до одногрупників, викладача під час спеціальних завдань та контрольних заходів;

– навчитися управлінню власною навчальною діяльністю та часом (тайм-менеджмент), набути рівня автономності, особливо під час самостійного навчання;

– напрацювати спроможність нести відповідальність за рішення (відповіді, стиль виконання завдань, оформлення тощо), прийняті під час виконання навчальних завдань;

– напрацювати звичку формувати власні професійні судження з урахуванням соціальних та етичних аспектів;

– розвивати уміння критичного мислення.

2. Результати навчання

Оцінювати рівень безпеки банківської діяльності, маючи уявлення про індикатори та складові безпеки банківської системи і концепції безпеки банківської установи, види загроз та викликів, визначати особливості організації діяльності спеціальних підрозділів відповідальних за розробку та реалізацію плану безперервності діяльності

Основні результати навчання:

- знати та розуміти механізм та закономірності функціонування банківської системи на рівні національного банку, виконання банківських операцій, надання банківських послуг та реалізації банківських продуктів
- розуміти принципи, методи та інструменти державного та ринкового регулювання діяльності в сфері фінансів, банківської справи та страхування
- знати та вміти застосовувати спеціалізовані інформаційні системи, сучасні фінансові технології та програмні продукти
- вдентифікувати джерела та розуміти методологію визначення і методи отримання економічних даних, збирати та аналізувати необхідну фінансову інформацію, розраховувати показники, що характеризують стан фінансових систем
- Розуміти вимоги до діяльності за спеціальністю, зумовлені необхідністю забезпечення сталого розвитку України, її зміцнення як демократичної, соціальної, правової держави

4. Структура курсу

ЛЕКЦІЇ
1. Поняття, основні категорії та концептуальні засади безпеки банківської діяльності. 1.1 Правові, економічні умови та система захисту банківської діяльності в Україні. 1.2 Принципи побудови та засоби забезпечення системи безпеки банківської діяльності.
2. Індикатори та складові безпеки банківської діяльності. 2.1 Класифікація та характеристика загроз. 2.2 Складові безпеки банківської діяльності
3. Правові засади забезпечення безпеки банківської діяльності 3.1 Нормативно-правові акти, що регулюють відносини із забезпечення безпеки банківської діяльності. 3.2 Поняття і правове регулювання банківської та комерційної таємниці банку. 3.3 Організація роботи з інформацією, що становить банківську та комерційну таємницю, конфіденційну інформацію банку. 3.4 Правові засади організації обробки та обміну сенсетивної інформації з іншими юрисдикціями та при взаємодії банків з представниками органів виконавчої влади, правоохоронних органів і засобів масової інформації. 3.5 Організація навчання персоналу банку із забезпечення безпеки банківської діяльності.
4. Управління системою забезпечення безпеки банківської установи 4.1 Особлива роль функції комплаєнсу при побудові внутрішніх процесів. 4.2 Організація системи внутрішнього контролю, роботи 3х ліній захисту та їх взаємодія. 4.3 Структура, завдання і функції підрозділу безпеки банку. 4.4 Обов'язки персоналу банку із забезпечення його безпеки
5. Організація інфраструктурних та процедурних безпекових заходів 5.1 Організація безпекових заходів. 5.2 Інфраструктурні вимоги та особливості проектування, розташування споруд банків. 5.3 Організація пропускної системи, відомчої охорони. Взаємодія банку з органами державної служби охорони. 5.4 Забезпечення безпеки касових операцій та операцій з готівкою.
6. Порядок доступу до банківської інформації 6.1 Порядок доступу до банківської інформації. 6.2 Організація службового діловодства. 6.3 Нормативна база банку з питань безпеки його діяльності. 6.4 Відповідальність за порушення встановленого режиму роботи банку.
7. Захист операційної діяльності. Організація ефективної KYC системи 7.1 Захист операційної діяльності. Організація ефективної KYC (know your customer) системи. 7.2 Правові засади інформаційно-аналітичної роботи в банках. 7.3 Загальна характеристика інформаційних баз і порядок користування ними. 7.4 Організація роботи з управління інформаційними ризиками.
8. Особливості використання новітніх технологій: хмарні та технології on-premise 8.1 Особливості використання новітніх технологій (хмарні та технології on-premise). 8.2 Інженерно-технологічні засоби захисту банківської безпеки.
9. Розробка плану безперервності діяльності (BCP- business continuity plan) 9.1 Розробка плану безперервності діяльності (BCP- business continuity plan). 9.2 Особливості розробки, впровадження та аудиту BCP для банківських установ. 9.3 Опрацювання стандарту ISO 22301 розробленого для управління безперервністю бізнесу, щоб допомогти організаціям мінімізувати ризик збоїв.

10. Запровадження інституту бездоганної ділової репутації як основи кадрової політики банку
10.1 Організація due diligence відносно працівників банку.
10.2 Запровадження інституту бездоганної ділової репутації.
10.3 Розробка ефективних політик та протоколів, які регламентують взаємодію персоналу та керівництва банку.
10.4 Політика банку щодо взаємодії зі стейкхолдерами.

5. Практичні заняття

1. Поняття, основні категорії та концептуальні засади безпеки банківської діяльності
2. Індикатори та складові безпеки банківської діяльності
3. Правові засади забезпечення безпеки банківської діяльності
4. Управління системою забезпечення безпеки банківської установи
5. Організація інфраструктурних та процедурних безпекових заходів
6. Порядок доступу до банківської інформації
7. Захист операційної діяльності. Організація ефективної KYC системи
8. Особливості використання новітніх технологій: хмарні та технології on-premise
9. Розробка плану безперервності діяльності (BCP- business continuity plan)
10. Запровадження інституту бездоганної ділової репутації як основи кадрової політики банку.

Інформація для здобувачів заочної форми навчання. На сайті НТУ «ДП» розміщено графік навчального процесу. Протягом року передбачено заняття з викладачем відповідно до розкладу: 6 год. лекційних занять, 4 год. практичних занять, решту практичних завдань здобувач опановує самостійно. Здобувачі заочної форми навчання виконують передбачені навчальним планом індивідуальні завдання (контрольні роботи, практичні завдання, презентації, тестові завдання) та подають їх на кафедру на початку сесії, обов'язково до проведення контрольних заходів з дисципліни. Умови завдань розміщено на сторінці курсу на платформі Moodle. Форма контролю – залік.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина	**Разом**
60	40	**100**

Практичні роботи приймаються за тестами по кожній темі практичного заняття.

Теоретична частина оцінюється за результатами здачі контрольної тестової роботи, яка містить 30 запитань, з яких 30 – прості тести (1 правильна відповідь).

6.3. Критерії оцінювання підсумкової роботи

20 тестових завдань місять три завдання з п’ятьма варіантами відповідей, одна правильна відповідь оцінюється у п’ять балів (разом п’ятнадцять), десять завдань з чотирма варіантами відповідей, одна правильна відповідь оцінюється у чотири бали (разом сорок балів), сім тестових завдань з трьома правильними відповідями, одна правильна відповідь оцінюється у один бал (разом сім балів).

Відповіді приймаються у форматі програм Microsoft Office та цифрових копій впродовж часу, відведеного на здачу теоретичної частини. Несвоєчасно вислана відповідь враховується такою, що не здана, якщо здача заліку здійснюється дистанційно. При проведенні заліку в аудиторному форматі, здача заліку проводиться згідно вимогам організації навчального процесу в НТУ «Дніпровська політехніка».

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

8 Рекомендовані джерела інформації

Базові

1. Зубок М.І. Забезпечення економічної безпеки банків: навчальний посібник/ М. І. Зубок. - К.: Університет економіки та права "КРОК", 2018. - 260 с.

2. Шелудько С.А. Міжнародні стандарти банківської справи. Київ: Кондор, 2020. С.260

3. Карась П.М., Приходько Н.В., Пащенко О.В. Банківська система. Херсон: Олді-плюс, 2020. С.292

4. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній. Київ: Сідкон, 2021. С.372

5. Бенько М. Обліково-аналітичне забезпечення економічної безпеки підприємств. Київ: Ліра-К, 2021. С.560

6. Когут Ю. І. Корпоративна безпека.Київ: Дакор, 2021. С.460

7. Когут Ю. І. Кібертероризм: історія, цілі, обєкти. Київ: Сідкон, 2021. С. 304

8. Крилова О.В.Демчук Н.І.,Остапчук Ю.Ю.Сучасний стан і тенденції розвитку споживчого та іпотечного кредитування в Україні « Ефективна економіка.2019. №10. URLhttp;www/ economy nayka.com.ua.

9. Крилова О. В., Орлова М. С., Замковой О. І. Актуальні проблеми фінансової безпеки суб'єктів господарювання в умовах FinTech трансформації фінансового ринку. Економічний вісник Дніпровської політехніки. 2022. №3 (75). С. 87-75.

10. Крилова О. В., Волчанська Л. В. Інформаційне забезпечення операційної діяльності банку та особливості бухгалтерського обліку. Держава, галузі, підприємства, бізнес: реалії і тенденції економічного, інформаційного та

технічного розвитку : монографія / за ред. : Л. М. Савчук., Л. М. Бандоріної . Дніпро : Пороги, 2020. С. 325-338.

11. Крилова О. В., Антипенко Н. В., Владика Ю. П., Волчанська Л. В. Банківська система : навч. посіб. Дніпро : Пороги, 2020. 324с.

12. Кадала В. В., Хайлова Т. В., Гузенко О. П. Банківське право: навчальний посібник / за ред. д-ра юрид. наук, проф. Б. В. Деревянка; МВС України, Донецький юридичний інститут. Львів : «Магнолія 2006», 2020. 172 с.

13. Банки з державною участю в Україні: теорія, методика та практика: монографія / В.В. Огородник; Міністерство освіти і науки України, Державний вищий навчальний заклад «Університет банківської справи». Київ: Університет банківської справи, 2019. 319 с.

14. Економічна безпека держави: навчально-методичний посібник / Живко З.Б., Черевко О.В., Копитко М.І., Зачосова Н.В., Живко М.О., Середа В.В., Занора В.О., Бієвець А.В.; за ред. Живко З.Б. - Черкаси : Видавець Чабаненко Ю.А., 2019. - 240 с.

Додаткові

https://www.iso.org/publication/PUB100442.html	ISO 22301, Security and resilience – Business continuity management systems – Requirements, the International Standard for implementing and maintaining effective business continuity plans, systems and processes.
https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en	ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements
https://www.cisa.gov/financial-services-sector	CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
https://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf	Banking and Finance Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan
https://home.treasury.gov/about/offices/domestic-finance/financial-institutions	G-7 FUNDAMENTAL ELEMENTS OF CYBER EXERCISE PROGRAMMES
https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector	EU Cybersecurity Initiatives in the Finance Sector