



Силабус освітнього компонента Програма навчальної дисципліни



Безпека банківських систем

Шифр та назва спеціальності

F5 – Кібербезпека та захист інформації

Спеціалізація

Освітня програма

Кібербезпека

Рівень освіти

Перший (бакалаврський)

Семестр

6

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Кафедра

Кібербезпеки (328)

Тип дисципліни

Вибіркова

Форма навчання

Денна, заочна

Мова викладання

Українська, англійська

Викладачі, розробники



СВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua

Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.

Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.

[Детальніше про викладача на сайті кафедри](#)



КОРОЛЬ Ольга Григорівна

olha.korol@khpi.edu.ua

Кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 175, з яких 19 навчальних посібників, 74 статті у закордонних виданнях та фахових виданнях України, 18 патентів на корисну модель, 9 у наукометричній базі Scopus, гарант освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Національна безпека держави», «Інформаційна безпека держави», «Комплексний тренінг «Безпека веб-застосунків», у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Безпека банківських систем" є вибірковою навчальною дисципліною. 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.

Мета та цілі дисципліни

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. Формування професійної компетентності майбутніх фахівців з кібербезпеки, достатньої для роботи на посаді адміністратора інформаційної безпеки банку та необхідної для розвитку кар'єри.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК4. Здатність спілкуватися іноземною мовою.

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.

СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.

СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).

СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

PH4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

PH5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

PH7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

PH9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

PH10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

PH11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.

PH12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.

PH13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.

PH14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації;

PH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

PH16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

PH18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

PH19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

PH21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 24 год., лабораторні роботи – 24 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Основи криптографічного захисту, Основи побудови та захисту сучасних операційних систем, Комплексні системи захисту інформації.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проекти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Структура внутрішньої платіжної системи комерційного банку. Послуги та механізми безпеки. Основні складові інформаційної безпеки держави. Нормативні документи. Основні принципи і механізми забезпечення ІБ в ОБС України. Основні функції АБС. Структурна схема СУІБ НСМЕП.	2
Тема 2. Правове забезпечення банківської безпеки. Рекомендації міжнародних стандартів. Постанова НБУ від 28.09.2017 № 95. Групові та часткові показники ІБ. Концепція побудови синергетичної моделі загроз. Стандарт СОУ Н НБУ 65.1 СУІБ 1.0: 2010. Система управління інформаційною безпекою.	2
Тема 3. Доступ до банківської інформації. Основні банківські інформаційні ресурси. Політики довіри. Концепція інфраструктури безпеки. Мета і сервіси інфраструктури безпеки. Механізми автентифікації.	2
Тема 4. Ризики у банківській діяльності. Класифікація кібератак на АБС. Статистика цільових атак 2020-2021. Синергетична модель загроз безпеці БІР. Удосконалена модель зловмисника.	2
Тема 5. Сертифікати відкритих ключів. Система PGP. Основні механізми технології відкритих ключів та PGP в автоматизованих банківських систмах. Протоколи сертифікації.	2
Тема 6. Оцінка ризиків у банківській діяльності. Аудит інформаційної безпеки. Методики оцінки ризиків.	2
Тема 7. Безпека мікропроцесорних карток. Внутрішньо-платіжна система комерційного банку. Стандарти пластикових карток. Механізми забезпечення безпеки валідності. Смарт-карти. Контактні та безконтактні смарт-карти. Операційні системи смарт-карт. 3D Secure.	2
Тема 8. Системи електронного обміну даними. Переваги впровадження СУІБ. Цілі та результат впровадження ISO27001. Опис критичних бізнес-процесів та програмно-технічних комплексів, які забезпечують їх функціонування. Структура мережі банку. Принципи забезпечення безперервності роботи. Методологія оцінювання ризиків. Впровадження та функціонування СУІБ.	2
Тема 9. Технологія захисту міжбанківських платежів. Платіжна система First Virtual: безпека без шифрування. EDI-системи. Система EDIFACT. Безпека EDI-систем. Платіжна система First Virtual: безпека без шифрування.	2
Тема 10. Актуальні проблеми інформаційної та кібербезпеки в банківській сфері. Правове підґрунтя. Використання хмарних технологій. Методи поширення шкідлоносів. Атаки на банкомати. Шкідносні семпли. Андромеда. Крадіжки через ATM Switch.	2
Тема 11. Цифрові валюти. Криптовалюти. Організація транзакції BITCOIN. Поняття про BLOCKCHAIN. Майнінг основні етапи. Моделі та механізми отримання конценцусу. Основи протоколів смарт-	2

контрактів.

Тема 12. Захищені протоколи.

2

Протокол SSL в АБС. Протокол Alert. Протокол SET. Технологія ОАЕР.

Загальна кількість годин

24

Лабораторні заняття

Теми лабораторних занять

Кількість
годин

Вагові
коефіцієнти a

Тема 1. Вивчення системи захисту інформації GnuPG та Kleopatra.

4

0,1

Ознайомлення з принципами асиметричного шифрування та електронного підпису. Практична робота з GnuPG і Kleopatra для генерації ключів, шифрування, дешифрування та перевірки автентичності повідомлень.

Тема 2 Вивчення системи захисту даних VeraCrypt 1.24.

4

0,1

Дослідження методів шифрування дисків та розділів. Створення захищених томів у VeraCrypt, налаштування параметрів безпеки, тестування захищеного доступу до даних.

Тема 3. Вивчення системи захисту даних КриптоБанк 5.0.

4

0,1

Робота з прикладною системою для захисту банківських даних. Ознайомлення з функціями шифрування, контролю доступу та управління ключами у середовищі банківської інформаційної безпеки.

Тема 4. Дослідження захисту інформації у спрощених EDI-системах.

4

0,1

Вивчення протоколів електронного обміну даними. Практичне застосування механізмів автентифікації, цілісності та конфіденційності у спрощених EDI-системах.

Тема 5. Розробка системи “Банкоматик”.

4

0,1

Створення програмної моделі банкомата з базовими механізмами автентифікації користувачів та захисту транзакцій. Аналіз вразливостей і впровадження базових методів захисту.

Тема 6. Вивчення захисту повідомлень в протоколі SET.

4

0,1

Ознайомлення з протоколом Secure Electronic Transaction (SET) для забезпечення безпеки електронних платежів. Виконання практичних завдань із захисту повідомлень, автентифікації та шифрування.

Загальна кількість годин

24

$\sum_{i=1}^n a_i = 0,6$

Контрольні роботи

Теми контрольних робіт

Вагові
коефіцієнти b

Тема 1. Захист внутрішніх платіжних систем та банківських даних.

0,1

Вивчення структури внутрішніх платіжних систем, механізмів автентифікації та сертифікації, оцінки ризиків і стандартів безпеки в автоматизованих банківських системах.

Тема 2. Актуальні кіберзагрози та технології захисту у банківській сфері.

0,1

Аналіз сучасних кіберзагроз для банків: атаки на банкомати, міжбанківські

платежі та електронні системи обміну даними. Розгляд методів запобігання атакам і засобів захисту банківської інфраструктури.

Загалом

$$\sum_{i=1}^m b_i = 0,2$$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення

Кількість годин

Тема 1. Нормативно-правова база інформаційної безпеки у банківській сфері.	8
---	---

Ознайомлення з законами, постановами НБУ та міжнародними стандартами, що регламентують безпеку банківських систем.

Тема 2. Автоматизовані банківські системи (АБС) та їх захист.	8
--	---

Вивчення архітектури АБС, основних загроз та механізмів захисту даних у банківській інфраструктурі.

Тема 3. Міжнародні стандарти інформаційної безпеки в банках.	8
---	---

Розгляд ISO/IEC 27001, PCI DSS та інших стандартів, що застосовуються для захисту банківських даних.

Тема 4. Механізми автентифікації та авторизації в банківських системах.	8
--	---

Аналіз методів підтвердження особи користувачів: паролі, токени, біометрія, багатофакторна автентифікація.

Тема 5. Кіберзагрози для банківської сфери та класифікація кібератак.	8
--	---

Вивчення основних видів атак (фішинг, DDoS, атаки на банкомати) та методів протидії.

Тема 6. Захист платіжних карток та електронних транзакцій.	8
---	---

Розгляд стандартів EMV, 3D Secure, протоколів SET та технологій безпеки смарт-карт.

Тема 7. Системи управління інформаційною безпекою (СУІБ) у банку.	6
--	---

Призначення, структура та функції СУІБ, побудова політик і процедур захисту.

Тема 8. Оцінка та управління ризиками в банківській діяльності.	6
--	---

Методи ідентифікації, аналізу та мінімізації ризиків, пов'язаних із кіберзагрозами.

Тема 9. Захист міжбанківських платежів та EDI-систем.	6
--	---

Особливості безпеки систем SWIFT, EDIFACT, First Virtual, їх уразливості та засоби захисту.

Тема 10. Цифрові валюти та блокчейн у банківській сфері.	6
---	---

Вивчення криптовалют, смарт-контрактів, моделей консенсусу та можливостей інтеграції у банківську систему.

Загальна кількість годин

72

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.



Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 31.12.2023. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 27.10.2022. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
3. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 6 травня 2015 року № 287/2015. Дата оновлення: 16.09.2020. URL: <https://zakon.rada.gov.ua/laws/show/287/2015#Text>
4. Про національну безпеку: Закон України від 21.06.2018 № 2469-VIII. Дата оновлення: 31.03.2023. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
5. Указ Президента України: Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" № 96/2016. Дата оновлення: 28.08.2021. URL: <https://zakon.rada.gov.ua/laws/show/96/2016#Text>
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229. Дата оновлення: 04.05.2008. URL: <https://zakon.rada.gov.ua/laws/show/1229/99#Text>
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: <https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf>
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: <https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf>
9. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22. https://tzi.ua/assets/files/1.1_003_99.pdf
10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806). <https://tzi.com.ua/downloads/2.5-004-99.pdf>
11. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806). <https://tzi.com.ua/downloads/1.1-002-99.pdf>
12. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. <https://tzi.com.ua/downloads/1.1-005-07.pdf>
13. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, наказ ДСТСЗІ СБУ від 04.12.2000 № 53 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806). <https://tzi.com.ua/downloads/1.4-001-2000.pdf>
14. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020. – 678 с. <https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnohii-zakhystu.pdf>
15. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсєєв, О.В. Мілов, С.Е. Остапов, О.В. Северінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.

Додаткова література

16. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL:

<https://www.iso.org/ru/contents/data/standard/08/28/82875.html>

17. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL:

<https://www.iso.org/ru/contents/data/standard/08/05/80585.html>

18. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL:

<https://www.iso.org/ru/contents/data/standard/08/05/80585.html>

19. Кравченко П. Блокчейн і децентралізовані системи. Ч. 1 – Харків: ПРОМАРТ, 2019. – 452 с.

<https://repository.kpi.kharkov.ua/server/api/core/bitstreams/0e26ed5b-990d-4271-85f8-573434a7722f/content>

20. Кравченко П. Блокчейн і децентралізовані системи. Ч. 3 – Харків: ПРОМАРТ, 2020. – 306 с.

21. Євсєєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПТОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсєєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.

<http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf>

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k :

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,4	0,2		0,4

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.

Розрахунок підсумкової оцінки проводиться за формулою:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \dots + K_m \cdot b_m}{\sum_{i=1}^m b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Шкала оцінювання

Поточні оцінки за кожну складову (Π , K , I , ...))

виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.

Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: <http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/>

Погодження

Силабус погоджено

30.08.2025



Завідувач кафедри
Сергій ЄВСЄЄВ

30.08.2025



Гарант ОП
Сергій ЄВСЄЄВ