



Силабус освітнього компонента Програма навчальної дисципліни



Атестація (Публічний захист кваліфікаційної роботи)

Шифр та назва спеціальності

КЗ – Національна безпека (за окремими
сферами забезпечення і видами діяльності)

Спеціалізація

Освітня програма

Національна безпека у сфері кіберзахисту

Рівень освіти

Перший (бакалаврський)

Семестр

8

Інститут

ННІ комп'ютерних наук та інформаційних
технологій

Кафедра

Кібербезпеки (328)

Тип дисципліни

Обов'язкова

Форма навчання

Денна

Мова викладання

Українська

Викладачі, розробники



ЄВСЕЄВ 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. Провідний лектор з дисциплін: Математичні основи криптології, Комп'ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

[Детальніше про викладача на сайті кафедри](#)



ТКАЧОВ Андрій Михайлович

andrii.tkachov@khpi.edu.ua

Кандидат технічних наук, старший науковий співробітник кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: більше 60 публікацій, 25 статей у закордонних виданнях та фахових виданнях України, 6 патентів на корисну модель, гарант освітньо-професійної програми "Національна безпека у сфері кіберзахисту" першого (бакалаврського) рівня вищої освіти.

[Детальніше про викладача на сайті кафедри](#)



КОРОЛЬОВ Роман Володимирович

korolevrv01@ukr.net

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

Кількість наукових публікацій: понад 40, з яких 1 навчальний посібник, 23 статті у закордонних виданнях та фахових виданнях України, 10 патентів на корисну модель. Провідний лектор з дисциплін: «Фізичні основи технічних засобів розвідки», «Основи стеганографічного захисту інформації», «Корпоративні мережі та системи доступу», «Безпека та аудит бездротових та рухомих мереж». Гарант освітньо-професійної програми «Управління інформаційною безпекою» першого (бакалаврського) рівня вищої освіти.

[Детальніше про викладача на сайті кафедри](#)



МІЛЕВСЬКИЙ Станіслав Валерійович

stanislav.milevskyi@khpi.edu.ua

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

Автор понад 100 наукових та навчально-методичних праць. Гарант освітньо-наукової програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Основи машинного навчання для кібербезпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій», «Математичні моделі управління ІТ-проєктами» у студентів бакалавріата та магістратури, «Моделювання механізмів кібербезпеки», «Математичні методи, моделі та інформаційні технології у наукових дослідженнях» у аспірантів.

[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

Атестація є заключним етапом підготовки здобувачів відповідного рівня вищої освіти за освітньо-професійною програмою "Національна безпека у сфері кіберзахисту" спеціальності "Національна безпека (за окремими сферами забезпечення і видами діяльності)". Атестація проводиться у формі публічного захисту кваліфікаційної роботи та завершується отриманням документу встановленого зразка про присудження ступеня бакалавра із присвоєнням кваліфікації: бакалавр з національної безпеки у сфері кіберзахисту.

Кваліфікаційна робота має передбачати розв'язання складної задачі кіберзахисту у сфері національної безпеки, виявляти та протидіяти загрозам національній безпеці України (за окремими сферами забезпечення і видами діяльності).

Мета та цілі дисципліни

Метою проведення атестації є:

- поглиблення, закріплення та перевірка компетентностей та результатів навчання, що були засвоєні здобувачем під час навчання за освітньо-професійною програмою «Національна безпека у сфері кіберзахисту» першого (бакалаврського) рівня вищої освіти;
- оцінювання рівня сформованості компетентностей випускників, передбачених відповідним рівнем національної рамки кваліфікацій і освітньо-професійною програмою «Національна безпека у сфері кіберзахисту» першого (бакалаврського) рівня вищої освіти до вимог Стандарту вищої освіти.

Формат занять

Самостійна робота, консультації, індивідуальне завдання – дипломний проєкт/робота.

Підсумковий контроль: атестація у формі публічного захисту на відкритому засіданні екзаменаційної комісії.

Компетентності

ІК. Здатність здійснювати управлінську діяльність при вирішенні складних спеціалізованих завдань у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній), у тому числі в умовах кризових ситуацій, що передбачає застосування теорій та наукових методів відповідної галузі і характеризується комплексністю та невизначеністю умов.

ЗК1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК5. Здатність спілкуватися іноземною мовою.

ЗК6. Здатність до адаптації та дії в новій ситуації.

ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ЗК9. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.

ФК–1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

ФК–2. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).

СК3. Здатність використовувати знання щодо ролі, місця та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконанні обов'язків з питань забезпечення національної безпеки.

СК4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки.

СК5. Здатність використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки.

СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань національної безпеки, взаємодіяти з іноземними партнерами.

СК7. Здатність визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.

СК8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

СК9. Здатність використовувати знання щодо безпекової складової зовнішньої політики України та інших держав.

СК10. Здатність засвоювати основні теоретичні поняття та набуття практичних навичок дослідження, підготовки документів та їх використання в управлінській діяльності.

СК11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.

СК12. Здатність виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності.

СК13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку.

СК14. Здатність здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки, готувати пропозиції щодо підвищення її ефективності.

Результати навчання

РН1. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

РН2. Вміти використовувати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

РН4. Вільно спілкуватися державною мовою.

РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.

РН6. Вміти адаптовуватись до нових викликів та дій у певних ситуаціях.

РН7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.

РН8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

- РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
- РН10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
- РН11. Вміти пояснювати роль, місце та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконання обов'язків з питань забезпечення національної безпеки.
- РН12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.
- РН13. Вміти використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки.
- РН14. Вміти читати й розуміти фахову іншомовну літературу, використовуючи її у соціальній і професійній сферах, а також демонструвати культуру мислення та виявляти навички щодо організації культурного діалогу з іноземними партнерами на рівні, необхідному для професійної діяльності.
- РН15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.
- РН16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.
- РН17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.
- РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
- РН19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.
- РН20. Вміти виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності.
- РН21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку, здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки та готувати пропозиції щодо підвищення її ефективності.

Обсяг дисципліни

Загальний обсяг – 90 год. (3 кредити ECTS): самостійна робота – 90 год.

Передумови вивчення дисципліни (пререквізити)

Для успішної атестації необхідним є набуття компетентностей і програмних результатів зі всіх попередніх освітніх компонентів освітньо-професійної програми та успішного проходження практичної підготовки.

Вимоги до освітнього компонента та його особливості

Процес навчання по даному освітньому компоненту передбачає самостійну роботу та проведення консультацій.

При самостійній роботі студент повинен розглянути теми рекомендованих кафедрою розділів кваліфікаційної роботи з використанням основної літератури, що зазначена в силабусі, а також додаткової літератури, рекомендованої керівником кваліфікаційної роботи, повторити матеріал попередніх курсів, який використовується при виконанні кваліфікаційної роботи, підготувати пояснювальну записку. Текст пояснювальної записки перевіряється на плагіат та на відповідність діючим нормам та стандартам. На кваліфікаційну роботу надається рецензія від призначеного

кафедрою рецензента. Кваліфікаційна робота оприлюднюється в електронному репозитарії бібліотеки НТУ "ХПІ".

Програма освітнього компонента

Атестація – це встановлення відповідності засвоєних здобувачами окремого рівня освіти та обсягу знань, умінь, навичок, компетентностей вимогам стандартів вищої освіти.

Перелік напрямів роботи:

Тематика 1. Теорія та практика національної безпеки (за окремими сферами забезпечення і видами діяльності).

Тематика 2. Об'єкти критичної інфраструктури.

Тематика 3. Інформаційно-комунікаційні системи та мережі.

Тематика 4. Технології забезпечення кіберзахисту.

Тематика 5. Процеси управління інформаційною та/або кібербезпекою об'єктів критичної інфраструктури.

Тематика 6. Захист державних інформаційних ресурсів та урядових комунікацій.

Тематика 7. Протидія інформаційним операціям та гібридним загрозам.

Тематика 8. Забезпечення безпеки в умовах надзвичайних ситуацій та воєнних дій.

Тематика 9. Правове забезпечення кібербезпеки та національної безпеки.

Тематика 10. Системи аналізу ризиків та моделювання загроз національній безпеці.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Про вищу освіту: Закон України (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004). URL: <https://zakon.rada.gov.ua/laws/show/1556-18#Text>
2. Про освіту: Закон України (Відомості Верховної Ради (ВВР), 2017, № 38-39, ст.380). URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text>
3. СТЗВО – ХПІ – 2.01-2021 ССОНП. Дипломні проекти та дипломні роботи. Загальні вимоги до виконання (зі змінами) URL: <https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2022/12/STZVO-HPI-2.01-2021-SSONP.-Diplomni-proekti-ta-diplomni-roboti.-Zagalni-vimogi-do-vikonannya-zi-zminami.pdf>
4. СТЗВО-ХПІ-3.01-2021 ССОНП. Текстові документи у сфері навчального процесу. Загальні вимоги до виконання (зі змінами) URL: <https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2022/12/STZVO-HPI-3.01-2021-SSONP.-Tekstovi-dokumenti-u-sferi-navchalnogo-protsesu.-Zagalni-vimogi-do-vikonannya-zi-zminami.pdf>
5. СТБУЗ 1.01-2000 ССОНП. Організація навчального процесу. Основні положення. URL: <https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2019/10/STVUZ-1.01-2000-SSONP.-Organizatsiya-navchalnogo-protsesu.-Osnovni-polozhennya.pdf>
6. Положення про організацію освітнього процесу в Національному технічному університеті "Харківський політехнічний інститут" (третя редакція) (протокол Вченої ради №6 від 05.07.2024) URL: https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2024/09/Polozhennya_pro_organizatsiyu_osvitnogo_2024_final_ppravka_3.pdf
7. Положення про систему запобігання та виявлення академічного плагіату у випускних кваліфікаційних роботах здобувачів вищої освіти Національного технічного університету «Харківський політехнічний інститут». URL: <http://library.kpi.kharkov.ua/files/documents/polozhennya-proekt-plagiat.pdf>
8. Положення про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів URL: <https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2024/09/Polozhennya-pro-kryteriyi-otsinyuvannya-znan-ta-vmin-i-pro-rejtyng-zdobuvachiv.pdf>
9. Порядок організації поточного, семестрового контролю та атестації здобувачів освіти із застосуванням дистанційних технологій навчання в Національному технічному університеті «Харківський політехнічний інститут» (Затверджено Наказ №119 ОД від 07.04.2022р.) URL:

<https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2022/04/Poryadok-organizatsiyi-potochnogo-semestrovogo-kontrolyu-ta-atestatsiyi-zdobuvachiv-osviti-iz-zastosuvannyam-distantsiynih-tehnologij-navchannya-v-NTU-HPI-1.pdf>

Додаткова література

10. Євсєєв С.П. Кібербезпека: сучасні технології захисту. / Євсєєв С.П., Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678. – Режим доступу: <http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tehnologii-zakhystu.pdf>.
11. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
<http://kist.ntu.edu.ua/textPhD/tzi.pdf>.
12. Bonaventure O. Computer Networking: Principls, Protocols and Practice. - Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. - 272 p.
<https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf>.
13. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсєєв, О.В. Мілов, С.Е. Остапов, О.В. Сєверінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
https://acrobat.adobe.com/id/urn%3Aaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover
14. Безпека інформаційно-комунікаційних систем. К. : Видавнича група BVH, 2009. – 608 с.
https://is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf
15. Богуш В. М., Юдін О. К. Інформаційна безпека держави. - К.: "МК-Прес", 2005. - 432с.
16. Термінологічний довідник з питань технічної захисту інформації / Коженевський С.Р., Кузнєцов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. - К.: ДУІКТ, 2007. - 365 с.
17. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. - Львів: Видавництво Львівської політехніки, 2019. - 580 с. - ISBN 978-966-941-339-0.
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf
18. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 Управління інформаційною безпекою, 125 Кібербезпека / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК "Орхідея", 2018. - 166 с. URL:
<https://ir.stu.cn.ua/bitstream/handle/123456789/19246/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%80%D0%B6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y>
19. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL:
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>
20. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. URL:
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>
21. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. URL: <https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>
22. 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>
23. 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>
24. 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>
25. 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>



26. 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>
27. 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>
28. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: <https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf>
29. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: <https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf>
30. 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). URL: <https://tzi.com.ua/downloads/1.4-001-2000.pdf>
31. 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). URL: <https://tzi.com.ua/downloads/2.5-004-99.pdf>
32. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 15.10.2008 № 172). URL: <https://tzi.com.ua/downloads/2.5-005%20-99.pdf>
33. НД ТЗІ 3.6-003-16 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
34. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі (наказ Адміністрації від 28.10.2023 № 924). URL: <https://www.cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-vnesennya-zmin-do-normativnogo-dokumenta-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi-3-7-003-2005-vid-28-zhovtnya-2023-roku-924>
35. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю. URL: https://zakononline.com.ua/documents/show/83554_83554
36. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e. <https://www.coursehero.com/file/55121963/handbook-all-engpdf/>
37. 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>
38. 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>
39. 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>.

Система оцінювання

Критерії оцінювання успішності здобувача та розподіл балів

Випускна кваліфікаційна робота здобувача захищається (приймається) на відкритому засіданні екзаменаційної комісії. На закритому

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C

Атестація (Публічний захист кваліфікаційної роботи)



Національний технічний університет
«Харківський політехнічний інститут»

засіданні екзаменаційна комісія приймає рішення щодо оцінки захисту на основі таких критеріїв:

1. Оцінка пояснювальної записки - 60%
2. Захист (зміст доповіді, якість ілюстративного матеріалу, відповіді на запитання) – 30%
3. Відгук керівника, висновок рецензента – 10%.

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 ЄВСЕЄВ

30.08.2025

Гарант ОП
Андрій ТКАЧОВ