**Силабус освітнього компонента**
Програма навчальної дисципліни

# Атестація (єдиний державний кваліфікаційний іспит (ЄДКІ))

**Шифр та назва спеціальності**
F5 – Кібербезпека та захист інформації

**Інститут**
ННІ комп`ютерних наук та інформаційних технологій

**Спеціалізація**

**Кафедра**
Кібербезпеки (328)

**Освітня програма**
Кібербезпека

**Тип дисципліни**
Обов'язкова

**Рівень освіти**
Перший (бакалаврський)

**Форма навчання**
Денна, заочна

**Семестр**
8

**Мова викладання**
Українська

## Викладачі, розробники

**ЄВСЄЄВ 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 статтей 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

**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

**ПОГАСІЙ Сергій Сергійович**

Serhii.Pohasii@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Гарант освітньо-наувої програми «Кібербезпека» третього (доктор філософії) рівня вищої освіти, провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для 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. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених Стандартом вищої освіти та освітньо-професійною програмою зі спеціальності "Кібербезпека та захист інформації".

## 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 «Кібербезпека» першого (бакалаврського) рівня вищої освіти;
- оцінювання рівня сформованості компетентностей випускників, передбачених відповідним рівнем національної рамки кваліфікацій і освітньо-професійною програмою «Кібербезпека» першого (бакалаврського) рівня вищої освіти до вимог Стандарту вищої освіти.

## Формат занять

Самостійна робота, консультації.
Підсумковий контроль: атестація у формі єдиного державного кваліфікаційного іспиту.

## Компетентності

ІК. Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК4. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
ЗК8. 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.
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 технологій, сучасні методи і моделей 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).
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
СК9. Здатність застосовувати методи та засоби технічного 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.
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
РН4. 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.
РН5. 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.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. 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.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. 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.
РН14. 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;
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
РН21. 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 – 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

Єдиний державний кваліфікаційний іспит (ЄДКІ) містить завдання зі стислим зрозумілим описом, що охоплюють сфери законодавчої та нормативно-правової бази забезпечення інформаційної і/або кібербезпеки, управління інформаційною та/або кібербезпекою, криптографічного та технічного захисту інформації, безпеки інформаційно-комунікаційних систем, комплексних систем захисту інформації.
ЄДКІ проводять за такими принципами: академічна доброчесність; об'єктивність; прозорість і публічність; нетерпимість до корупційних та пов'язаних з корупцією діянь; інтеграція у міжнародний освітній та науковий простір; єдність методики оцінювання результатів.

## Програма освітнього компонента

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

Єдиний державний кваліфікаційний іспит проводять у формі зовнішнього незалежного оцінювання відповідно до програми ЄДКІ, використовуючи різні види завдань.
Завдання кваліфікаційного іспиту розробляють відповідно до програми ЄДКІ.
Програма ЄДКІ складається з розділів щодо законодавчої та нормативно-правової бази, державних та міжнародних вимог, практик і стандартів в галузі інформаційної та/або кібербезпеки; інформаційних технологій в інформаційній та/або кібербезпеці; безпеки інформаційно-комунікаційних систем; комплексних систем захисту інформації; управління інформаційною та/або кібербезпекою; криптографічного захисту інформації; технічного захисту інформації.

## 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. Стандарт вищої освіти за спеціальністю 125 Кібербезпека та захист інформації для першого (бакалаврського) рівня вищої освіти від 04 жовтня 2018 року № 1074, з урахуванням змін у Стандарті вищої освіти зі спеціальності 125 Кібербезпека та захист інформації (наказ Міністерства освіти і науки України від 13.01.2022 р. №26) URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-

osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf
4. Програма єдиного державного кваліфікаційного іспиту зі спеціальності 125 Кібербезпека на першому (бакалаврському) рівні вищої освіти (наказ Міністерства освіти і науки України від 04.11.2022 р. № 980) URL: https://kb.khmnu.edu.ua/wp-content/uploads/sites/6/63861d8f5ff01844854871.pdf
5. Постанова Про атестацію здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту. URL: https://zakon.rada.gov.ua/laws/show/497-2021-%D0%BF#Text
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_pravka_3.pdf

## Додаткова література

1. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв 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-tekhnolohii-zakhystu.pdf.
2. 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.
3. 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.
4. Євсеєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.
https://acrobat.adobe.com/id/urn%3Aaaid%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
5. Безпека інформаційно-коммунікаційних систем. К. : Видавнича група BHV, 2009. – 608 с.
https://is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf
6. Богуш В. М., Юдін О. К. Інформаційна безпека держави. - К.: "МК-Прес", 2005. - 432с.
7. 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.
8. Бобало Ю.Я., Горбатій 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
9. 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
10. 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
11. 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
12. 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

13. 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
14. 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
15. 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
16. 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
17. 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
18. 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
19. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
20. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
21. 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
22. 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
23. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної 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
24. НД ТЗІ 3.6-003-16 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
25. 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
26. 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
27. 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/
28. 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
29. 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
30. 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

Критерії оцінювання результатів кваліфікаційного іспиту за спеціальністю "Кібербезпека та захист інформації", затверджуються відповідальними державними органами (МОН, Адміністрація Держспецзв'язку, Міноборони).
Виконання всіх екзаменаційних завдань з єдиного державного кваліфікаційного іспиту є обов'язковим. Підсумкова оцінка комплексного іспиту визначається як середня з позитивних оцінок за кожен вид екзаменаційних завдань.

### Шкала оцінювання

| 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**<br>Сергій ЄВСЕЄВ |
| | 30.08.2025 | | **Гарант ОП**<br>Сергій ЄВСЕЄВ |