Силабус освітнього компонента

Атестація (Єдиний державний кваліфікаційний іспит (ЄДКІ))

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип освітнього компонента
Обов'язкова, Спеціальна (фахова) підготовка

Семестр
8

Мова викладання
Українська

Розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів
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 освітнього компонента

Метою проведення атестації є: поглиблення й закріплення компетентностей та результатів навчання, що були засвоєні здобувачем під час навчання за відповідною освітньо-професійною програмою; оцінювання рівня сформованості компетентностей випускників, передбачених відповідним рівнем національної рамки кваліфікацій і освітньо-професійною програмою підготовки фахівців до вимог Стандарту вищої освіти.

Формат освітнього компонента

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

Компетентності

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
КЗ 6. 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.
КЗ 7. 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.
КЗ 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь яких інших проявів недоброчесності.
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Результати навчання

РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їх ефективність;
РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
РН 12 – розробляти моделі загроз та порушника;
РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;
РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
РН 36 – виявляти небезпечні сигнали технічних засобів;
РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
РН 50 – забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз;
РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Обсяг освітнього компонента

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

Передумови для освітнього компонента (пререквізити)

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

Вимоги до освітнього компонента та його особливості

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 та навчальні матеріали

Основні документи та положення:

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. Євсєєв 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 доброчесності

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися, 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

Завідувач кафедри
28.08.2024 Сергій ЄВСЕЄВ

Гарант ОП
28.08.2024 Сергій ЄВСЕЄВ