Силабус освітнього компонента

Атестація (Публічний захист кваліфікаційної роботи)

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Освітньо-професійна програма "Кібербезпека"

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

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

Семестр
3

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 "Кібербезпека" спеціальності "Кібербезпека та захист інформації".
Атестація проводиться у формі публічного захисту кваліфікаційної роботи та завершується отриманням документу встановленого зразка про присудження ступеня магістра із присвоєнням кваліфікації: магістр з кібербезпеки та захисту інформації .
Захист кваліфікаційної роботи спрямований на перевірку рівня професійної підготовки студентів та їхньої здатності вирішувати актуальні завдання в галузі інформаційної безпеки.

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, індивідуальне завдання – дипломний проєкт/робота. Підсумковий контроль: атестація у формі публічного захисту на відкритому засіданні екзаменаційної комісії.

Компетентності

ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-2. Здатність проводити дослідження на відповідному рівні.
КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг освітнього компонента

Загальний обсяг – 300 год. (10 кредитів ECTS): самостійна робота – 300 год.

Передумови для освітнього компонента (пререквізити)

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

Вимоги до освітнього компонента та його особливості

Процес навчання по даному освітньому компоненту передбачає самостійну роботу та проведення консультацій.
Атестація включає кілька основних компонентів:
1. Захист кваліфікаційної магістерської роботи - магістранти презентують свої наукові дослідження, проведені в рамках магістерської роботи. Кваліфікаційна робота повинна демонструвати здатність студента здійснювати науково-дослідницьку діяльність, аналізувати сучасні кіберзагрози та пропонувати ефективні рішення для їхньої нейтралізації. Тематика роботи має відповідати актуальним викликам у сфері кібербезпеки, включаючи захист інформаційних систем, аналіз загроз, розробку криптографічних рішень, політики безпеки тощо.
2. Оцінка знань у галузі кібербезпеки - студенти повинні продемонструвати володіння теоретичними знаннями з основ кібербезпеки, сучасних технологій захисту інформації, мережевої безпеки, криптографії та правових аспектів кіберзахисту. Оцінка відбувається у формі письмового іспиту або співбесіди з комісією.
3. Практична демонстрація навичок - у деяких випадках атестація може включати практичні завдання, пов'язані з розробкою рішень для захисту інформаційних систем, проведенням аналізу вразливостей, налаштуванням систем моніторингу та реагування на інциденти. Це дозволяє оцінити здатність студентів застосовувати свої знання на практиці.
Атестаційна комісія оцінює:
Рівень теоретичних знань у сфері кібербезпеки.
Якість проведеного наукового дослідження та його відповідність сучасним викликам.
Здатність студентів вирішувати реальні завдання у сфері захисту інформаційних систем.
Оригінальність та новизну запропонованих рішень.
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. Сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур, сфери інформаційної безпеки та/або кібербезпеки.
Тематика 2. Інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології.
Тематика 3. Інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур.
Тематика 4. Системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків).
Тематика 5. Інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси).
Тематика 6. Програмне та програмно-апаратне забезпечення (засоби) кіберзахисту.
Тематика 7. Системи управління інформаційною безпекою та/або кібербезпекою.
Тематика 8. Технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки

Успішне проходження атестації є підтвердженням високої кваліфікації випускників, що дозволяє їм претендувати на посади в галузі кібербезпеки в різних організаціях, компаніях чи державних структурах.

Література та навчальні матеріали

Основні документи та положення:

1. Методичні вказівки до виконання магістерських робіт для студентів спеціальності 125 "Кібербезпека та захист інформації" / уклад. О. В. Мілов, О. Г. Король, Н. І. Воропай. – Харків: НТУ "ХПІ". – 51 с. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/e02b0d47-b1f7-4417-8f45-2fb38e98ad7c/content
2. 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
3. Про освіту: Закон України (Відомості Верховної Ради (ВВР), 2017, № 38-39, ст.380). URL: https://zakon.rada.gov.ua/laws /show/2145-19#Text
4. 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
5. 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
6. СТВУЗ 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
7. 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
8. 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-plagyat.pdf

9. 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
10. 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-distantsijnih-tehnologij-navchannya-v-NTU-HPI-1.pdf
11. Стандарт вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти (наказ Міністерства освіти і науки України від 18.03.2021 р. №332) URL: https://mon.gov.ua/npa/pro-zatverdzhennya-standartu-vishoyi-osviti-za-specialnistyu-125-kiberbezpeka-dlya-drugogo-magisterskogo-rivnya-vishoyi-osviti
12. 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:

13. 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.
14. 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.
15. 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.
16. 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
17. Безпека інформаційно-коммунікаційних систем. К. : Видавнича група BHV, 2009. – 608 с. https://is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf
18. 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.
19. 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
20. 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
21. 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
22. 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

23. 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
24. 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
25. 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
26. 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
27. 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
28. 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
29. 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
30. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
31. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
32. 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
33. 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
34. 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
35. НД ТЗІ 3.6-003-16 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
36. 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
37. 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
38. 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/
39. 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
40. 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

41. 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 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%.

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	28.08.2024		Завідувач кафедри Сергій ЄВСЕЄВ
	28.08.2024		Гарант ОП Ольга КОРОЛЬ