Силабус курсу

ПІДГОТОВКА ТА ЗАХИСТ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Ступінь вищої освіти – магістр
Галузь знань – 12 Інформаційні технології
Спеціальність - 125 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Рік навчання: 1, 2
Семестр: 1-3
Кількість кредитів: 15
Мова викладання: українська

Відповідальний підрозділ:
кафедра кібербезпеки

Контактна інформація

E-mail: kb@wunu.edu.ua
Адреса: вул. О. Теліги, 8, корп. 6, к. 6501, Тернопіль, 46003

Опис дисципліни

Кваліфікаційна робота є обов'язковим компонентом освітнього процесу за другим (магістерським) рівнем вищої освіти, формою підсумкової атестації та підставою для присвоєння кваліфікації «магістр» відповідно до освітньо-професійної програми «Кібербезпека». Вона виконується на основі теоретичних знань і практичних навичок, здобутих здобувачем ОП протягом усього періоду навчання, а також результатів самостійної науково-дослідної діяльності, пов'язаної з розробкою конкретних теоретичних і науково-виробничих задач прикладного характеру, що визначаються стандартом спеціальності «Кібербезпека та захист інформації».

Мета освітньої компоненти

Метою кваліфікаційної роботи є самостійне розв'язання складної наукової чи прикладної задачі у сфері інформаційної безпеки та/або кібербезпеки шляхом проведення наукового дослідження або виконання інноваційного проєкту, що ґрунтується на здобутих теоретичних знаннях, практичних навичках і методології наукової діяльності.

Завдання освітньої компоненти:

Поглибити й систематизувати знання з теорії та практики інформаційної безпеки й кібербезпеки.

Визначити та сформулювати наукову проблему, об'єкт, предмет і завдання дослідження.

Провести критичний аналіз наукових джерел, сучасних технологій, стандартів і практик у сфері кіберзахисту.

Обґрунтувати методи, моделі, засоби та інструменти, придатні для вирішення поставленої задачі.

Виконати теоретичні та/або експериментальні дослідження, здійснити аналіз і інтерпретацію результатів.

Сформулювати науково обґрунтовані висновки та практичні рекомендації для підвищення рівня захисту інформаційних систем і процесів.

Продемонструвати здатність до самостійної науково-дослідної діяльності, дотримання академічної доброчесності та етики наукової роботи.

Результати виконання освітньої компоненти

Кваліфікаційна робота спрямована на перевірку та підтвердження здатності здобувача реалізовувати результати навчання, зокрема:

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.

Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

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.

Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

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.

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.

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.

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.

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.

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.

Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

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.

Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

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.

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.

Впроваджувати повний цикл аналізу артефактів; проводити відновлення видалених / пошкоджених файлів та інших даних з цифрових носіїв та / або систем.

Тематика кваліфікаційних робіт

Тематика кваліфікаційної роботи може бути запропонована здобувачем вищої освіти та погоджена з науковим керівником. Обрана тема повинна бути актуальною, відповідати сучасному рівню розвитку науки і техніки, а також потребам практики у сфері інформаційної безпеки та/або кібербезпеки.

Здобувачі також мають можливість обрати тему з переліку, запропонованого кафедрою, який формується з урахуванням наукових напрямів її діяльності, а також тематики організацій та установ, де проходить виробнича чи переддипломна практика (стажування).

При визначенні тематики кваліфікаційних робіт необхідно враховувати реальні науково-практичні задачі, вирішення яких сприятиме підвищенню рівня захищеності інформаційних систем і процесів.

Рекомендовані джерела інформації

1. Закон "Про вищу освіту" [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18
2. Загальні методичні рекомендації з підготовки, оформлення, захисту та оцінювання кваліфікаційних робіт здобувачів вищої освіти першого (бакалаврського) і другого (магістерського) рівнів. Тернопіль: ЗУНУ, 2024. 83 с.
3. ДСТУ 3008:2015 Національний стандарт України. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Введ. 01.07.2017 - К.: ДП "УкрНДНЦ, 2016. – 25 с.
4. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання : Національний стандарт України : [Чинний від 2016–07–01]. Київ : ДП «УкрНДНЦ», 2016. 17 с.
5. Методологічне та інструментальне забезпечення наукових досліджень: навчальний посібник/В. Г. Бодров. Ірпінь: Університет ДФС України, 2020. 323 с.
6. Самсонов В., Сільвестров А., Тачиніна О. Методологія наукових досліджень та приклади її використання: навчальний посібник. К.: НУХТ, 2022. 385 с.

Політика оцінювання

Кваліфікаційна робота подається здобувачем у встановлені строки та повинна відповідати методичним вимогам до структури й оформлення.

Попередньо робота проходить нормоконтроль і перевірку на академічну доброчесність, зокрема з використанням програмного забезпечення для виявлення плагіату; унікальність тексту має бути не нижче встановленого порогу. Робота, що містить ознаки академічного плагіату, фабрикації чи фальсифікації, до захисту не допускається.

Попередній захист кваліфікаційної роботи здійснюється на кафедрі, де комісія оцінює якість виконання завдання, науковий рівень дослідження та готовність роботи до основного

захисту. За результатами попереднього захисту робота може бути допущена до основного захисту, направлена на доопрацювання або відсторонена від подальшого розгляду.

До основного захисту кваліфікаційна робота допускається за наявності позитивного відгуку наукового керівника та рецензії, а також погодження завідувача кафедри.

Захист передбачає презентацію результатів дослідження, відповіді на запитання членів екзаменаційної комісії та обговорення. Рішення про оцінку захисту та присвоєння кваліфікації приймається екзаменаційною комісією на закритому засіданні й оголошується одразу після нього.

Оцінювання кваліфікаційної роботи здійснюється за основними критеріями, кожен із яких оцінюється за 100-бальною шкалою.

Результуюча оцінка визначається як середнє арифметичне всіх критеріїв. Оцінювання здійснюється за критеріями:

- актуальність теми;
- рівень теоретичної та практичної підготовки;
- обґрунтованість висновків і рекомендацій;
- вміння аргументовано представляти результати.

Актуальність теми: оцінюється наукова та практична значущість теми, її відповідність сучасним проблемам у сфері кібербезпеки.

90–100 балів (Відмінно) – тема повністю актуальна, відповідає сучасним науковим і практичним вимогам.

75–89 балів (Добре) - тема актуальна, але частково охоплює сучасні проблеми.

60–74 балів (Задовільно) - тема частково актуальна, має обмежене значення для практики.

1-59 балів (Незадовільно) - тема неактуальна або не відповідає сучасним вимогам.

Рівень теоретичної та практичної підготовки: оцінюється глибина теоретичних знань та здатність застосовувати їх на практиці, використання сучасних методів і технологій.

90–100 балів (Відмінно) – демонструються глибокі теоретичні знання та високий практичний рівень.

75–89 балів (Добре) - знання достатні для виконання завдань, практичні навички частково розвинуті.

60–74 балів (Задовільно) - базові знання та обмежені практичні навички.

1-59 балів (Незадовільно) - знання і навички недостатні для виконання завдань.

Обґрунтованість висновків і рекомендацій: оцінюється логічність і достовірність висновків, практична цінність рекомендацій.

90–100 балів (Відмінно) – висновки повністю обґрунтовані, рекомендації практично значущі.

75–89 балів (Добре) - висновки логічні, частково обґрунтовані, рекомендації частково практичні.

60–74 балів (Задовільно) - висновки частково обґрунтовані, рекомендації обмежено придатні.

1-59 балів (Незадовільно) - висновки необґрунтовані, рекомендації непридатні.

Вміння аргументовано представляти результати: оцінюється логічність і чіткість презентації, здатність аргументовано відповідати на запитання комісії.

90–100 балів (Відмінно) – презентація зрозуміла, відповіді на всі запитання повністю аргументовані.

75–89 балів (Добре) - презентація зрозуміла, більшість запитань аргументовані.

60–74 балів (Задовільно) - презентація частково логічна, відповіді на запитання частково правильні.

1-59 балів (Незадовільно) - презентація нечітка, відповіді на запитання неадекватні.

Шкала оцінювання

За шкалою університету	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75–84		C (добре)
65–74	задовільно	D (задовільно)
60–64		E (достатньо)
35–59	незадовільно	FX (незадовільно з можливістю повторного складання)
1–34		F (незадовільно з обов’язковим повторним курсом)