Силабус курсу
ПЕРЕДДИПЛОМНА ПРАКТИКА

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність - F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Рік навчання: 2
Семестр: 3
Кількість кредитів: 5
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

Переддипломна практика (далі практика) є невід'ємною складовою частиною процесу підготовки здобувачів другого (магістерського) рівня вищої освіти у вищих навчальних закладах і проводиться на оснащених відповідним чином базах навчальних закладів, сучасних IT компаніях, підприємствах, я також у організаціях різних галузей господарства, освіти, охорони здоров'я, культури, торгівлі і державного управління.

Практика проводиться у третьому семестрі впродовж десяти тижнів (450 годин / 15 кредитів). Вона є завершальним етапом в циклі підготовки здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти, що покликаний сприяти забезпеченню якісної теоретичної підготовки, формуванню в них професійних практичних знань, умінь та навичок, необхідних для подальшої діяльності та передує виконанню здобувачами вищої освіти кваліфікаційної роботи.

Мета практики

Метою практики є закріплення здобутих теоретичних знань щодо забезпечення безпеки інформаційної діяльності, методів захисту в кіберпросторі, управління мережевою безпекою, комплексу заходів виявлення і дослідження шкідливого програмного забезпечення; навиків в постановці і проведенні дослідницьких робіт та практичне використання знань в галузі інформаційних технологій для ефективного розв’язування складних спеціалізованих завдань та практичних проблем під час професійної діяльності, зокрема у сфері кібербезпеки.

Цілі практики є:

- поглиблення навичок самостійної роботи;
- розширення наукового світогляду здобувачів ОП;
- дослідження проблем практики та вміння пов’язувати їх з обраним теоретичним напрямком дослідження;
- вміння визначати структуру та логіку майбутньої роботи як висококваліфікованого фахівця.

Завдання практики

Завданням практики є формування в умовах виробництва професійних здібностей здобувача ОП на підставі використання його теоретичних знань в різних ситуаціях, які притаманні майбутній професійній діяльності спеціаліста.

Результати практики

Проходження практики в умовах конкретного підприємства забезпечує досягнення окремих результатів навчання, визначених освітньою програмою, 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.

Програма практики

Під час проходження практики здобувачі ОП повинні виконати наступний комплекс робіт:

- дослідити об'єкт практики:
- здійснити збір матеріалів для кваліфікаційної роботи та виконання індивідуальних завдань, що узгоджені з керівником практики.
- виконати індивідуальне завдання.
- оформити звіт про проходження практики та захистити його в університеті.

Рекомендовані джерела інформації

1. Яцків В.В., Терещенко О.С. Розвідка кіберзагроз з використанням мови опису правил YARA. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2022), Тернопіль, 2022. – С. 40-42.
2. Цаволик Т., Яцків В., Яцків Н., Івасьєв С. Виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах на основі MITRE ATT&CK. Вимірювальна та обчислювальна техніка в технологічних процесах. Технічні науки. – 2023. – С.16 – 22. https://doi.org/10.31891/2219-9365-2023-74-7
3. Терещенко О.С., Яцків В.В. Сучасні платформи розвідки кіберзагроз з відкритим кодом. Матеріали проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. – С. 100-103.
4. Yatskiv V., Tsavolyk T., Yatskiv N., Koval V., Ivasiev S. Algorithm and data encoding/decoding devices based on two-dimensional modular correction codes. Proceedings of the 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2023), Khmelnytskyi, Ukraine, March 22–24, 2023, Vol-3373, 2023, ISSN 1613-0073. – P. 388-400. https://ceur-ws.org/Vol-3373/paper25.pdf
5. Yatskiv V., Nyemkova E., Kulyna S., Kulyna H., Ivasiev S. Data Encryption Method Based on the Redundant Residue Number System. Proceedings of the 5th International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS,

Khmelnytskyi, Ukraine, March 28, 2024, Vol-3675, 2024. – P. 223-235. URL: https://ceur-ws.org/Vol-3675/paper16.pdf
6. Yakymenko I., Martyniuk O., Martyniuk S., Yakymenko Y., Kasianchuk M. Hierarchical Encryption in a Residual Number System. Proceedings. *International Conference on Advanced Computer Information Technologies, ACIT,* 2024. P. 496–499. https://ieeexplore.ieee.org/document/10712567
7. Yakymenko I., Karpinski M., Shevchuk R., Kasianchuk M. Symmetric Encryption Algorithms in a Polynomial Residue Number System. *Journal of Applied Mathematics*. Hindawi. vol. 2024. P. 1-12. https://onlinelibrary.wiley.com/doi/10.1155/2024/4894415
8. Tymoshchuk, D., Yatskiv, V., Tymoshchuk, V., & Yatskiv, N. (2024). Interactive Cybersecurity Training System Based on Simulation Environments. *Measuring And Computing Devices in Technological Processes*, (4), 215–220. https://doi.org/10.31891/2219-9365-2024-80-26
9. Tymoshchuk D., Yatskiv V. Using Hypervisors To Create A Cyber Polygon. Measuring And Computing Devices In Technological Processes, №3, 2024. – С.52-56. https://doi.org/10.31891/2219-9365-2024-79-7
10. Tymoshchuk D., Yatskiv V. Slowloris DDOS Detection and Prevention in Real-Time. August 16, 2024; Oxford, UK: VII International Scientific and Practical Conference «Theoretical and Empirical Scientific Research: Concept and Trends», 2024, 171-176. https://doi.org/10.36074/logos-16.08.2024.036
11. Shevchuk R., Yakymenko I., Kasianchuk M. Encryption Using Residue Number System: Research Trends and Future. Proceedings. *International Conference on Advanced Computer Information Technologies, ACIT,* 2024. P. 552–559. https://ieeexplore.ieee.org/document/10712566
12. Sachenko, V. Yatskiv, J. Sieck, Jun Su. Image Transmission in WMSN Based on Residue Number System. International Journal of Computing, Volume 23(1) 2024. – Pp. 126-133. https://doi.org/10.47839/ijc.23.1.3444
13. Nykolaychuk Ya.M., Yakymenko I.Z., Vozna N.Ya., and Kasianchuk M.M. Residue Number System Asymmetric Cryptoalgorithms. *Cybernetics and Systems Analysis*. 2022. Vol. 58, No. 4, P. 611-618. https://link.springer.com/article/10.1007/s10559-022-00494-7
14. Kovalchuk O., Karpinski M., Banakh S., Kasianchuk M., Shevchuk R., Zagorodna N. Prediction Machine Learning Models on Propensity Convicts to Criminal Recidivism. *Information.* 2023. № 14. P. 161. https://www.mdpi.com/2078-2489/14/3/161
15. Kovalchuk O., Karpinski M., Babala L., Kasianchuk M., and Shevchuk R. The Canonical Discriminant Model of the Environmental Security Threats. *Complexity.* 2023. Vol. 2023, Article ID 5584750. 15 pages. https://onlinelibrary.wiley.com/doi/10.1155/2023/5584750
16. Kovalchuk O., Karpinski M., Babala L., Kasianchuk M., and Shevchuk R. Decision-Making Supporting Models Concerning the Internal Security of the State. *Intl Journal of Electronics and Telecommunications*. 2023. Vol. 69, N. 2. P. 301-307.
17. Kasianchuk M., Yakymenko I., Yatskiv V., Karpinski M., Yatskiv S. Method of Multi-Bit Numbers Multiplication in Residue Number System for Asymmetric Cryptosystems. *CEUR Workshop Proceedings*. 2022. Vol. 3156. P. 365–377. https://ceur-ws.org/Vol-3156/paper27.pdf
18. Davletova, A., Yatskiv, V., Ivasiev, S., & Karpinskyi, M. Encryption Method Based on Codes. ACPS. 2024; Volume 9, Number 1: pp. 24 – 31 https://doi.org/10.23939/acps2024.01.024
19. Davletova, A., Yatskiv V., Ivasiev S., Kulyna S., Tsavolyk, T., & Drapak, V. Enhancing Cryptographic System Security Based on Finite Fields: proceedings of 14th International Conference on Advanced Computer Information Technologies (ACIT'2024) (19-21 September, Ceske Budejovice). CZECH REPUBLIC, 2024. P. 476-480.

Політика оцінювання

Підсумковий бал (за 100-бальною шкалою) з практики визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Заліковий модуль 1 (оформлення звіту) – 50%

Заліковий модуль 2 (захист звіту) - 50%

Неподання звіту є підставою для повторного проходження практики, а у випадку зневажливого ставлення до практики і порушення дисципліни - для відрахування з вузу.

Виконання та оформлення звіту:

90–100 балів (Відмінно) – завдання практики виконано у повному обсязі, звіт подано своєчасно, оформлено згідно з усіма вимогами, без зауважень щодо змісту та структури.

75–89 балів (Добре) – завдання виконано у повному обсязі, звіт подано своєчасно, проте є незначні недоліки в оформленні чи деталізації матеріалу.

60–74 бали (Задовільно) – завдання виконано частково, звіт містить суттєві недоліки оформлення чи змістового наповнення, або поданий із запізненням.

1–59 балів (Незадовільно) – завдання практики не виконано, звіт відсутній чи не відповідає вимогам.

Захист звіту:

90–100 балів (Відмінно) – презентація проведена чітко й логічно, висвітлено всі питання, наочні матеріали якісні та доречні, відповіді на додаткові запитання повні й аргументовані.

75–89 балів (Добре) – презентація проведена, але є окремі недоліки у викладі матеріалу, структурі або відповідях на питання.

60–74 бали (Задовільно) – презентація проведена формально, наочні матеріали слабкі чи відсутні, відповіді неповні або нечіткі.

1–59 балів (Незадовільно) – здобувач не з’явився на захист або не продемонстрував знань із програми практики.

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)