МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«___» _____ 2025 р.

ПРОГРАМА ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ

Ступінь вищої освіти – **магістр**
Галузь знань – **12 Інформаційні технології**
Спеціальність – **125 Кібербезпека та захист інформації**
Освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Тернопіль – 2025 р.

Програма переддипломної практики для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології

Укладач: д.т.н., професор, професор кафедри кібербезпеки Касянчук Михайло Миколайович

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 12 від 24.06.2025 р.

Завідувач кафедри кібербезпеки Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності «Кібербезпека та захист інформації», протокол № 5 від 24.06 2025 р.

Голова ГЗС, гарант ОПП Василь ЯЦКІВ

1. Загальні положення

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 ІТ 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 за спеціальністю F5 Кібербезпека та захист інформації галузі знань F Інформаційні технології, 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.

Програма містить вказівки з організації проведення практики, вивчення всебічної діяльності об’єкта – бази практики, роботи над індивідуальними завданнями, збору матеріалів для виконання кваліфікаційної роботи.

2. Мета та завдання практики

2.1 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.

2.2 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 фахівця.

2.3. Перелік компетентностей, формування котрих забезпечує вивчення дисципліни:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КЗ5. 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.

КФ11. Здатність використовувати програмно-апаратні засоби та інструменти аналізу артефактів, відновлення даних, а також шифрування та захищеного зберігання інформації в інформаційних системах та мережах.

2.4. Результати практики

Проходження практики в умовах конкретного підприємства повинне забезпечити наступні 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.

РН24. Впроваджувати повний цикл аналізу артефактів; проводити відновлення видалених / пошкоджених файлів та інших даних з цифрових носіїв та / або систем.

3. 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.

Для успішного проходження практики необхідно дотримуватися рекомендованого календарного графіку проходження практики (додаток 1).

4. Бази практики

Базами практики здобувачів ОП можуть бути сучасні підприємства малого і середнього бізнесу, організації, інформаційні відділи банків, науково-дослідницькі інститути, підрозділи комп'ютеризації різних державних структур та адміністрацій, ІТ-компанії та інші установи, що займаються проектуванням, впровадженням та експлуатацією інформаційних систем.

Перелік баз практики щорічно коригується кафедрою на основі аналізу підсумків проведення практики в попередньому році з метою забезпечення підвищення якості та ефективності практичної підготовки здобувачів ОП. При наявності державних, регіональних

замовлень на підготовку фахівців перелік баз практики надають кафедрі органи, які формували замовлення на фахівців. При підготовці фахівців за цільовими договорами з підприємствами, організаціями, установами бази практики передбачаються у цих договорах. З базами практики (підприємствами, організаціями, установами будь-яких форм власності) завчасно укладаються договори на її проведення.

Відбору баз практик передує робота кафедри щодо вивчення виробничих можливостей підприємств з точки зору придатності їх для проведення практики здобувачів за спеціальністю. При цьому враховуються перспективи сучасних напрямів розвитку ІТ-галузі.

Кафедра заздалегідь визначає бази практики і розподіляє по них здобувачів ОП, повідомляючи їх про це до початку практики. Вибір баз практики здійснюється кафедрою кіберблезпеки із врахуванням завдань практики та можливістю їх реалізації. Наказом ректора університету здійснюється скерування здобувачів ОП на відповідні бази практики, визначається керівник практики від кафедри для кожного зі здобувачів.

На початку практики кожному здобувачу ОП видається щоденник практики. У щоденнику проставляються відмітки бази практики про те, що здобувач ОП прибув / вибув на базу практики. Календарний план проходження практики заповнюється та затверджується керівниками від університиету та бази практики.

5. Керівництво практикою

Навчально-методичне керівництво практикою і контроль за роботою здобувачів ОП здійснюється керівником практики від кафедри і від бази практики.

Керівник практики від кафедри:

- перед початком практики контролює підготовку бази практики;
- забезпечує проведення всіх організаційних заходів перед направленням здобувачів ОП на практику;
- проводить інструктаж про порядок проходження практики та з техніки безпеки, перевіряє надання здобувачам ОП необхідних документів (скерування, програми, щоденника, індивідуального завдання тощо);
- спільно з керівником практики від бази практики складає календарний графік проходження практики;
- повідомляє здобувачів ОП про систему звітності з практики, яка затверджена кафедрою, а саме подання письмового звіту та вимог до його оформлення;
- у тісному контакті з керівником від бази практики забезпечує високу якість її проходження згідно з програмою;
- у складі комісії приймає звіт з практики;
- консультує здобувачів ОП з питань, пов'язаних з виконанням індивідуальних завдань з практики.

Керівник практики від бази практики зобов'язаний:

- скласти календарний графік проходження практики спільно з керівником практики від університету;
- забезпечити якісне проведення інструктажу з правил техніки безпеки на місці проходження практики;
- забезпечити умови виконання здобувачами ОП програми практики та індивідуальних завдань;
- забезпечити дотримання здобувачами ОП правил внутрішнього розпорядку;
- контролювати хід виконання календарного графіку практики та підготовку звітів про практики.

6. Обов'язки здобувача ОП під час проходження практики

На початку практики здобувачі ОП проходять інструктаж по охороні праці та техніці безпеки згідно з порядком, встановленим на даному підприємстві. При проходженні практики здобувач ОП повинен:

- вивчити і строго дотримуватись правил техніки безпеки при роботі з комп'ютерними системами та мережами на базі практики;
- повністю виконати завдання, передбачені програмою практики;
- підготувати звіт про практику та захистити його у визначений термін.

Під час практики здобувач ОП повинен щодня коротко записувати в щоденник усе, що зробив за день для виконання календарного графіка проходження практики.

Здобувачі ОП несуть особисту відповідальність за неявку на базу практики. Під час перебування на базі практики здобувачі ОП повинні виконувати покладені на них обов'язки і правила внутрішнього розпорядку.

7. Форми та методи контролю

Для здійснення поточного та підсумкового контролю виконання окремих розділів і всієї програми практики здобувач повинен вести щоденник практики. Всі основні етапи практики фіксуються у щоденнику.

7.1 Індивідуальне завдання

Перед початком проходження практики здобувачі ОП одержують від викладачів кафедри індивідуальні завдання, які вони повинні виконати в період проходження практики.

Індивідуальне завдання видаються з урахуванням тематики кваліфікаційних робіт з метою допомоги у підборі необхідного матеріалу та формування навичок самостійної роботи, уміння використовувати теоретичні знання в конкретних видах діяльності, аналізувати і оцінювати рівень інформаційної безпеки на основі теоретичних знань, які вони одержали в навчальному закладі, надбання здобувачами ОП під час практики умінь та навичок самостійного розв'язання завдань, пов’язаних з використанням комп’ютерної техніки в своїй роботі, активізації діяльності здобувачів ОП, розширення їх світогляду.

7.2 Вимоги до звіту

Проходження практики завершується написанням кожним здобувачем ОП індивідуального звіту про виконану роботу.

Звіт рецензується і підписується керівником практики від підприємства і здається на кафедру до захисту. Керівник практики від підприємства підписує також щоденник і пише відгук про проходження практики.

Рекомендується наступна структура звіту про проходження практики:

- титульний аркуш (додаток 2);
- зміст, який містить назви всіх розділів і підрозділів;
- вступ;
- основна частин, що містить виконання індивідуального завдання;
- висновки;
- перелік використаних джерел;
- додатки (за необхідності).

7.3 Захист звіту

У ході практики здобувач ОП повинен скласти письмовий звіт, підписати його у керівника від бази практики. Разом із оформленим відповідним чином щоденником практики

здати звіт керівнику практики від університету на протязі першого тижня, наступного після практики семестру. Захист звіту відбувається в терміни, встановлені кафедрою.

Захист звіту про практики відбувається перед комісією, до якої входять керівники практики від кафедри і інші викладачі. В деяких випадках пов'язаних з специфікою бази практики, захист звітів може проводитись на місці проходження практики. Тоді до складу комісії залучаються представники бази практики.

За результатами захисту звіту здобувачеві ОП виставляється відмітка про залік.

8. 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)

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.

Додаток 1

Календарний план проходження практики

№ п\п	Завдання практики	Тривалість виконання (дні)
1	В результаті проведення обстеження об'єкта дослідження, здобувач ОП повинен ознайомитися з технологіями проектування, організації та тестування системи захисту інформації.	5
2	Аналіз актуальних питань та заходів забезпечення інформаційної безпеки для різних сфер діяльності.	10
3	Дослідження (в залежності від індивідуального завдання) методів оцінки загроз для інформаційної безпеки; методів та засобів управління інформаційною безпекою в інформаційно - телекомунікаційних (автоматизованих) системах; методів проведення зворотної розробки програмного забезпечення та апаратних пристроїв; переваг та нових можливостей застосування технології блокчейн; проведення тестування комп'ютерних систем на проникнення; методів реверс інжинірингу для їх використання в сучасних умовах; принципів побудови сучасного програмного забезпечення; концепцій та підходів до розробки та впровадження надійних, безпечних систем IoT; методів та засобів криптографічного захисту інформації в умовах широкого використання сучасних інформаційних технологій; методів захисту інформації в комп'ютерних системах та мережах і з особливостями їх апаратної та програмної реалізацій; основних методів, моделей та алгоритмів захисту інформації.	20
4	Вироблення пропозиції та рекомендації щодо забезпечення кібернетичної безпеки, визначення методів та засобів реалізації захисту інформації.	5
5	Виконання індивідуального завдання практики. Формування програми та проведення досліджень. Викладення загальної методики та основних методів досліджень; розробка експериментальної частини й покрокової методики досліджень; проведення теоретичних та (або) експериментальних досліджень; участь (по можливості) у лабораторних випробуваннях; аналіз і узагальнення одержаних результатів.	5
6	Оформити звіт	5
	Всього:	50

Додаток 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

Звіт

про проходження переддипломної практики
здобувача ІІ курсу денної форми навчання

"_КБм-21___" _____
група прізвище, ім'я та по-батькові

_____
/база практики/

Період з "_____" до "_____"

Керівник практики:
від підприємства

_____ _____ _____
/посада/ /підпис/ /П.І.П./

від кафедри

_____ _____ _____
/посада/ /підпис/ /П.І.П./

Тернопіль 20___ р.