Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий
Фізико-технічний інститут
Кафедра математичних
методів захисту інформації

ПЕРЕДДИПЛОМНА ПРАКТИКА
ПО-9
Робоча програма навчальної дисципліни (Силабус)

Реквізити освітньої компоненти

Рівень вищої освіти	*перший (бакалаврський)*
Галузь знань	*11 Математика та статистика*
Спеціальність	*113 «Прикладна математика»*
Освітня програма	*Математичні методи криптографічного захисту інформації*
Статус дисципліни	*Нормативна*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*4- курс, 8 семестр*
Обсяг дисципліни	*180 годин / 6 кредитів ECTS*
Семестровий контроль/ контрольні заходи	*Переддипломна практика,* *Залік*
Розклад занять	http://rozklad.kpi.ua
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*к.ф-м.н., доцент Ніщенко Ірина Іванівна* *nishchenkoii-ipt@lll.kpi.ua*
Розміщення курсу	https://ecampus.kpi.ua/login

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивченя та результати навчання

Програму освітньої компоненти «Переддипломна практика» складено відповідно до освітньо-професійної програми «Математичні методи криптографічного захисту інформації» підготовки здобувачів вищої освіти за спеціальністю 113 “Прикладна математика” та відповідно до «Положення про проведення практики студентів вищих навчальних закладів України» від 8 квітня 1993р. № 93, «Методичних рекомендацій по складанню програм практики студентів вищих навчальних закладів України» від 14.02.1996р. № 31-5197 та навчальних планів для напряму підготовки 113 «Прикладна математика» .

Переддипломна практика студентів 4 курсу є невід'ємною частиною освітньо-професійної програми підготовки фахівців, основним завданням якої є формування і розвиток професійних знань в галузі прикладної математики, закріплення отриманих теоретичних знань і опанування практичними навичками і досвідом для виявлення наукової проблеми, пошуку та обґрунтування шляхів її вирішення.

Згідно з кваліфікаційною характеристикою бакалавра за спеціальністю «Прикладна математика» студенти отримують знання з математики, інформатики, інформаційних технологій та таких професійно орієнтованих дисциплін як математичне моделювання та системний аналіз, теорія складності та скінченні автомати, математичні методи захисту інформації тощо. Спеціалісти з даної спеціальності отримують уміння і навички, які дозволяють створювати нові математичні методи і технології комп'ютерної обробки інформації, дають змогу використовувати сучасні інформаційно-комунікаційні технології в діяльності, пов'язаній з захистом інформаційних ресурсів, проєктуванні, реалізації, впровадженні та експлуатації автоматизованих систем.

Мета переддипломної практики. Преддипломна практика студентів є невід´ємною складовою частиною процесу підготовки спеціалістів. ЇЇ основною метою та завданнями є :

1. Опанування студентами сучасними методами, навичками, вміннями та способами організації праці, пов'язаними з майбутньою професійною діяльністю.
2. Використання студентами одержаних знань, професійних навичок та вмінь для прийняття самостійних рішень під час роботи.
3. Виховання в студентах потреби систематично поповнювати свої знання і застосовувати їх в практичній діяльності.
4. Набуття студентами навичок роботи зі спеціальною літературою, патентними матеріалами, оформлення документації з програмного забезпечення.
5. Отримання студентами вміння підготувати наукову статтю, доповідь, реферат за матеріалами самостійних досліджень.
6. Проводення студентами науково-дослідних, проєктних та супроводжувальних робіт з:

- проєктування баз та банків даних для інформаційних систем;
- розробки систем моделей і методів аналізу і оптимізації інформаційних систем;
- розробки нових інформаційних технологій та автоматизованих інформаційних систем в наукових установах та підприємствах різних форм власності;
- розробки систем підтримки прийняття рішень в інформаційних та інших комп´ютерних системах;
- розробки, налагодження експертних систем і супроводження програмних продуктів для автоматизованих інформаційних систем.

Здобувач вищої освіти повинен вміти:

- на основі набутих теоретичних і практичних знань вирішити конкретну наукову проблему; розробити комплексні підходи до її вивчення;
- провести експериментальні дослідження, обробити результати і довести їх придатність;
- узагальнювати і систематизувати отримані результати.

Предметом переддипломної практики є набуття навичок самостійної дослідницької роботи, розширення наукового світогляду бакалаврів, складання плану розв'язування поставленої задачі, визначення структури та логіки майбутньої бакалаврської роботи.

У процесі проходження переддипломної практики у відповідності до освітньо-наукової програми «Математичні методи криптографічного захисту інформації» підготовки бакалавра зі спеціальності 113 "Прикладна математика" студент має оволодіти такими *загальними компетентностями*:

- ЗК 2 Здатність застосовувати знання у практичних ситуаціях.
- ЗК 3 Здатність генерувати нові ідеї
- ЗК 5 Здатність проведення досліджень на відповідному рівні.
- ЗК 7 Здатність до пошуку, обробки та аналізу інформації з різних джерел

-ЗК 8 Знання та розуміння предметної області та розуміння професійної діяльності

ЗК 9 Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

ЗК 10 Навички у використанні інформаційних і комунікаційних технологій

ЗК 13 Навички міжособистісної взаємодії.

- ЗК 11 Здатність працювати в міжнародному контексті

- ЗК 12 Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків.

цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Щодо опанування *спеціальних (професійних, фахових) компетентностей***,** а саме:

ФК 1 Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем.

- ФК 2. Здатність виконувати завдання, сформульовані у математичній формі.

- ФК 3. Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень.

ФК 4 Здатність розробляти алгоритми та структури даних, програмні засоби та програмну документацію

ФК 5 Здатність проектувати бази даних, інформаційні системи та ресурси.

ФК6 Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, з використанням стандартних офісних додатків.

ФК7 Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення

ФК8 Здатність використовувати сучасні технології програмування та тестування програмного забезпечення.

- ФК 9. ЗдЗдатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, з використанням стандартних офісних додатків.Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, з використанням стандартних офісних додатків.атність до проведення математичного і комп'ютерного моделювання, аналізу та обробки даних, обчислювального експерименту, розв'язання формалізованих задач за допомогою спеціалізованих програмних засобів.

- ФК 10. Здатність створення документів встановленої звітності, використання нормативноправових документів.

- ФК 12. Здатність до пошуку, систематичного вивчення та аналізу науково-технічної інформації, вітчизняного й закордонного досвіду, пов'язаного із застосуванням математичних методів для дослідження різноманітних процесів, явищ та систем.

- ФК 13. Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних.

- ФК 15. Здатність брати участь у складанні наукових звітів із виконаних науково-дослідних робіт та у впровадженні результатів проведених досліджень і розробок.

ФК18 Навички розв'язування специфічних математичних та комп'ютерних задач, які виникають при розробці, реалізації та аналізі криптографічних систем.

Завданням дисципліни «Переддипломна практика» є досягнення *програмних результатів навчання*, набуття знань та умінь, що безпосередньо стосуються науково-дослідної діяльності, а саме:

РН 1 Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці.

-РН 3 Формалізувати задачі, сформульовані мовою певної предметної галузі; формулювати їх математичну постановку та обирати раціональний метод вирішення; розв'язувати отримані задачі аналітичними та чисельними методами, оцінювати точність та достовірність отриманих результатів.

РН 4 Виконувати математичний опис, аналіз та синтез дискретних об'єктів та систем, використовуючи поняття й методи дискретної математики та теорії алгоритмів.

РН5 Уміти розробляти та використовувати на практиці алгоритми, пов'язані з апроксимацією функціональних залежностей, чисельним диференціюванням та інтегруванням, розв'язанням систем алгебраїчних, диференціальних та інтегральних рівнянь, розв'язанням крайових задач, пошуком оптимальних рішень

РН7 Вміти проводити практичні дослідження та знаходити розв'язок некоректних задач.

РН 8 Поєднувати методи математичного та комп'ютерного моделювання з неформальними процедурами експертного аналізу для пошуку оптимальних рішень.

РН 9 Будувати ефективні щодо точності обчислень, стійкості, швидкодії та витрат системних ресурсів алгоритми для чисельного дослідження математичних моделей та розв'язання практичних задач.

РН 10 Володіти методиками вибору раціональних методів та алгоритмів розв'язання математичних задач оптимізації, дослідження операцій, оптимального керування і прийняття рішень, аналізу даних.

РН 11 Вміти застосовувати сучасні технології програмування та розробки програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів.

РН 12 Розв'язувати окремі інженерні задачі та/або задачі, що виникають принаймні в одній предметній галузі: в соціології, економіці, екології та медицині.

РН 13 Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп'ютерної математики. Р

Н 14 Виявляти здатність до самонавчання та продовження професійного розвитку.

РН 15 Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.

РН 16 Демонструвати навички взаємодії з іншими людьми, уміння працювати в команді.

РН 17 Уміти здійснювати збір, опрацювання, аналіз, систематизацію науково-технічної інформації, уникаючи при цьому академічної недоброчесності.

РН 18 Ефективно спілкуватися з питань інформації, ідей, проблем та рішень зі спеціалістами та суспільством загалом.

РН 19 Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні проблеми.

РН 20 Демонструвати навички професійного спілкування, включаючи усну та письмову комунікацію українською мовою та принаймні однією з офіційних мов ЄС.

РН 21 Вміти формулювати та розв'язувати алгебраїчні та комбінаторні задачі, будувати та реалізовувати комбінаторні алгоритми та алгоритми прикладної алгебри, аналізувати теоретичну та практичну складність таких алгоритмів

РН 22 Володіти основними принципами та методами побудови симетричних та асиметричних криптографічних систем у різних моделях обчислення, а також методами їх аналізу

РН 23 Використовувати у професійній діяльності криптографічні примітиви та

протоколи.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Практичні та дослідницькі навички та теоретико-методологічні знання, отримані під час освоєння навчальної дисципліни «Переддипломна практика», можна використовувати в подальшому для здійснення науково-дослідної діяльності.

Необхідними навичками для освоєння навчальної дисципліни «Переддипломна практика» є знання дисциплін загальної та професійної підготовки: “Теорія керування ”, “Аналіз даних”, “Числові моделі та алгоритми”, “Теорія інформації та кодування”, “Асиметричні криптографічні системи та протоколи”, “Іноземна мова”.

3. Зміст навчальної дисципліни

На навчальну дисципліну «Переддипломна практика» відводиться 180 годин / 6 кредитів ECTS, семестрова атестація – залік.

За результатами проходження переддипломної практики здобувач вищої освіти повинен вміти написати невелику наукову доповідь на тему, пов´язану з індивідуальним завданням. У вступній частині потрібно зробити огляд спеціальної наукової літератури та патентних матеріалів у заданому напрямку. У дослідній частині роботи необхідно показати вміння теоретично обгрунтувати вирішення проблеми. Після цього – привести алгоритми і методи розв´язання поставленої задачі, а також програмну реалізацію.

Як правило, орієнтація студентів та залучення до науково-технічної і науково-дослідницької роботи, ознайомлення з тематикою робіт кафедри здійснюється не пізніше третього курсу.

Практично робота над дипломною роботою починається в період переддипломної практики. До початку переддипломної практики кафедра проводить збори студентів, котрі направляються на переддипломну практику. На ці збори запрошуються керівники дипломного проєктування студентів та консультанти з інших кафедр. В період переддипломної практики студенти повинні вивчати питання, безпосередньо пов'язані з темами їхніх дипломних робіт. Перелік цих питань студенти отримують від своїх керівників дипломного проєктування та консультантів з відповідних розділів.

При проведені практики необхідно ознайомити студентів з:

- правилами техніки безпеки, протипожежної безпеки та виробничої санітарії на підприємствах;
- організаційними структурами підприємств;
- основними заходами з захисту комерційної таємниці та забезпечення надійності персоналу.

Організація та проведення практики регламентовані наступними документами:

- наказ по університету про направлення на практику і призначення керівників;
- робоча програма (силабус) практики;
- щоденники, робочі програми та індивідуальні завдання для проходження практики;
- журнал відвідування практики;
- графіки відвідування керівниками практики занять з метою здійснення контролю;
- звіти про виконання програми практики;
- екзаменаційні відомості щодо заліку з практики.

Відповідальність за організацію, проведення і контроль практик покладається на завідувача відповідної кафедри. Для керівництва практикою завідувачем кафедри призначаються керівники практики від університету (кафедри).

Обов´язки керівника практики від кафедри:

1. Ознайомитися з програмою та навчально-методичною документацією з проведення практики.

2. Ознайомитися зі змістом та особливостями укладеного з підприємством Договору про практику.
3. Провести організаційні збори з групою студентів:
   - проінформувати про термін проведення практики;
   - ознайомити з програмою практики;
   - ознайомити з вимогами до ведення щоденників практики;
   - ознайомити з вимогами до складання звіту про практику;
   - видати студентам щоденники і дати рекомендації щодо їхнього ведення;
   - видати кожному студентові індивідуальне завдання з практики.
4. Ознайомити керівника від підприємства з програмою практики, узгодити з ним індивідуальні завдання.
5. Систематично контролювати виконання графіку практики та консультувати студентів з питань виконання програми практики.
6. Систематично проводити контроль за веденням щоденників та сладанням студентами звіту.
7. Систематично інформувати кафедру про процес проходження практики.
8. На заключному етапі проведення практики:
   - перевірити та підписати щоденники і звіти;
   - провести заліки з практики.

Переддипломна практика розпочинається з проведення настановчої конференції, в якій беруть участь здобувачі, керівник практики від випускової кафедри.

Після закінчення практики доповісти на засіданні кафедри і засіданні Вченої ради факультету/інституту про проведену практику.

Згідно ст.51, ст.50 Кодексу законів про працю Україн (із змінами та доповненнями) тривалість робочого часу студентів під час проходження практики складає 24 години (віком від 15 до 16 років на тиждень), 36 годин на тиждень (віком від 16 до 18 років). Від 18 років і старше - не більше 40 годин на тиждень. При зарахуванні студентів на штатні посади на час проходження практики на них розповсюджуеться законодавство про працю та правила внутрішнього трудового розпорядку підприємства. На студентів не зарахованих на штатні посади також розповсюджуються правила внутрішнього трудового розпорядку підприємства.

Під час проходження практики студент зобов´язаний:

До початку практики отримати консультації керівника практики від кафедри щодо оформлення всіх необхідних документів.

1. Своєчасно прибути на місце проходження практики.
2. У повному обсязі виконувати завдання, передбачені програмою практики, індивідуальні завдання та вказівки керівника.
3. Дотримуватися правил охорони праці та техніки безпеки.
4. Нести відповідальність за виконану роботу.
5. Своєчасно скласти залік з практики.

Місце проходження практики бакалаврів визначається наказом Міністерства освіти України від 08.04.1993р. № 93, в якому, зокрема встановлено, що практика студентів вищих навчальних закладів проводиться на базах практики, які мають відповідати вимогам практики.

Галузеві міністерства і відомства, що мають в своєму підпорядкуванні вищі навчальні заклади, за погодженням з Міністерством освіти України можуть закріплювати за ними підприємства терміном до 5 років.

При наявності в вищих навчальних закладах державних, регіональних замовлень на підготовку спеціалістів перелік баз практики надають цим закладам органи, які формували замовлення на спеціалістів. При підготовці спеціалістів вищими навчальними закладами за цільовими договорами з підприємствами, організаціями, установами бази практик передбачаються в цих договорах.

У зв´язку з науковими напрямками фізико-технічного інституту, рекомендовано такі бази практики:

1 Інститут космічних досліджень НАНУ-НКАУ

2 Інститут математики НАНУ

3 Міжнародний науково-навчальний центр інформаційних технологій та систем НАНУ та Міносвіти та науки України

4 Інститут прикладного системного аналізу НАНУ

5 Корпорація Інком

6 Ю.ТОВ «Самсунг Електронікс»

7 Институт кибернетики имени В. М. Глушкова НАН Украины

8 ТОВ «АВТОР»

9 ТОВ «Глобал Лоджик Україна»

10 ТОВ «Науково-виробничий центр «Безпека інформаційних технологій і систем»»

11 ТОВ «ДИНА»

4. Навчальні матеріали та ресурси

Базова література:

1. Положення про організацію освітнього процесу в КПІ ім. Ігоря Сікорського. – 2020. [Електронний ресурс] – Режим доступу: http://osvita.kpi.ua/node/39

2. Методичні рекомендації з питань організації практики студентів та складання робочих програм практики Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» [Текст] / Уклад.: Н. М. Лапенко, І.Л. Співак, І.В. Федоренко, О.М. Шаповалова; за заг. ред. П.М. Яблонського. – К.: КПІ ім. Ігоря Сікорського, 2018. – 29 с.

3. Головенкін В.П. Інженерна педагогіка (електронне видання): Підручник. – К.: НТУУ «КПІ ім.. Сікорського», 2017. [Електронний ресурс]. – Режим доступу: http://www.kpi.ua/.

4. Головенкін В.П. Педагогіка вищої школи (Андрагогіка): Підручник. – К.: НТУУ «КПІ», 2009. – 406 с.

Додаткова література:

1. Закон України про вищу освіту. Закон від 01.07.2014 № 1556-VII [Електронний ресурс]. – Доступний http://zakon1.rada.gov.ua/laws/show/1556-18
2. Роз'яснення МОН щодо деяких питань практичної реалізації положень нового Закону України «Про вищу освіту» : [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/publish/article7art_icN247526620.
3. Положення про навчання студентів та аспірантів, стажування наукових і науково педагогічних працівників у провідних вищих навчальних закладах та наукових установах за кордоном, затверджене Постановою Кабінету Міністрів України від 13 квітня 2011 року № 411 – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/411-2011- %D0%BF.
4. Національна доктрина розвитку освіти України у XXI столітті // Освіта України, 2001, № 29.
5. Положення про проведення практики студентів вищих навчальних закладів України: Наказ Міністерства освіти України від 8 квітня 1993 р. № 93.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

В рамках дисципліни заплановано наступні види навчальних занять:

- самостійна робота над індивідуальним завданням.

Структура компонентів дисципліни взаємоузгоджена, матеріал вивчається в логічній послідовності. Теми та порядок освоєння дисципліни «Переддипломна практика» наведено нижче.

№ п/п	Найменування теми	Всього годин
1	**Тема 1. Організація процесу переддипломної практики**	
1.1	1.1 Настановча конференція	2
1.2	1.2 Інформування здобувачів вищої освіти про мету, завдання і зміст переддипломної практики, місце її проходження	2
1.3	1.3 Ознайомлення здобувачів вищої освіти з порядком проходження переддипломної практики	2
1.4.	1.4 Інструкції щодо виконання робочої програми практики, порядку оформлення всіх необхідних документів, щоденнику практики.	4
1.5.	Інструктажі з питань охорони праці та техніки безпеки	3
2	**Тема 2.** Практична та емпірично-пошукова діяльність	
2.1	2.1 Пошук та вирішення конкретної наукової проблеми; розробка комплексних підходів до її вивчення, обговорення з науковим керівником (керівником практики в організації)	80
2.2	2.2 Проведення експериментальних досліджень, обробка результатів і доведення їх правомірності	55
2.3	2.3 Узагальнення і систематизація отриманих результатів	10
3	**Тема 3. Результати переддипломної практики**	
3.1	Підсумкова конференція	6
3.2	Підготовка звіту за результатами проходження практики	8
3.3	Залікове заняття. Захист звіту за результатами проходження практики	8
	Всього годин	**180**

Приклади індивідуальних завдань складено таким чином, щоб студент міг проявити самостійність в розв'язанні виробничих, наукових та організаційних завдань.

1. Оцінки стійкості сімейства блокових шифрів TEA відносно атаки зсуву
2. Розв’язок алгебраїчних рівнянь малих степенів над скінченними полями
3. Моделювання та аналіз систем криптографічного захисту інформації
4. Розробка та дослідження статистики помилок каскадного кодексу на базі кодів РС та БЧХ
5. Аналіз перемішуючих властивостей групових операцій, заданих на одному носієві

6. Дослідження властивостей лямбда-параметру, що характеризує стійкість криптографічних перетворень до лінійного криптоаналізу

7. Вразливості реалізацій ГПВЧ в мовах програмування

8. Методи аутентифікації для спеціалізованих інформаційно-телекомунікаційних систем

9. Експерементальні дослідження алгоритмів стиснення бітових послідовностей

10. Порівняльний аналіз статистичних властивостей стиснутих та псевдовипадкових послідовностей

11. Аналіз стійкості систем розподілу секрету із використанням формальних методів аналізу протоколів

12. Реалізація та застосування методики оцінки якості генераторів випадкових та псевдовипадкових послідовностей

13. Дослідження криптографічних властивостей експоненціальних перетворень над полями характеристики 2

14. Дослідження незбалансованих фейстелевських схем блокових шифраторів.

15. Аналіз статистичних властивостей учасника конкурсу e – Stream алгоритму Creupt MT3 Stream Cipher.

16. Розробка та застосування алгоритму кубічної атаки до типових схем побудови потокових шифрів дослідження швидкої атаки.

17. Аналіз стійкості сучасних блокових шифрів до лінійно – різницевого криптоаналізу.

18. Дослідження стійкості алгоритмів гамування до методу ймовірного слова.

19. Аналіз методів факторизації багатослівних чисел та розробка бібліотеки програм факторизації для розподільних обчислювальних систем.

20. Аналіз методів дискретного логорифмування та розробка бібліотеки програм обчислення дискретного логарифмування для розподільних обчислювальних систем.

21. Дослідження стійкості асиметричних криптосистем, заснованих на факторизації для різних моделей обчислень.

22. Розробка механізмів шифрування та геджування для оперативних систем мобільних теміналів на прикладі ОС Windous Mobile та Simbian.

23. Блокові шифратори. Принципи побудови, криптоананалізу.

24. Застосування кубічних атак до блочних, поточних шифрів та до хеш – функцій.

25. Дослідження стійкості 1024-бітного RSA та 160-бітної криптографії на елептичних кривих.

26. Реалізація механізмів автентифікації та цифрового підпису для мобільних терміналів на прикладі ОС Simbian.

27. Розробка механізмів шифрування та геджування для оперативних систем мобільних теміналів на прикладі ОС Windous Mobile та Simbian.

28. Дослідження стійкості асиметричних криптосистем, заснованих на обчисленні дискретного логарифму для різних моделей обчислень.

29. Дослідження методів оптимізації реалізації основних симетричних алгоритмів для різної архітектури обчислювальної техніки.

30. Дослідження інфраструктури відкритих ключів та використання відміток часу.

31. Протоколи SSL і TLS та їх вразливості.

22. Протокол Kerberos та його реалізація.

23. Дослідження доказової стійкості деяких узагальнень схеми Фейстеля до диференціального аналізу

24.Аналіз існуючих протоколів квантових грошей.

25.Криптоаналіз однієї модифікації протоколу Диффі – Хелмана вироблення спільного ключа.

26. Дослідження схеми блочного шифрування у моделі псевдо випадковості.

27. Аналіз методу вбудовування публічних параметрів для протидії атакам збоїв

28. Дослідження залежності оцінок стійкості сучасних потокових шифрів від вибору особливих точок атак компромісу.

29. Дослідження впливу лінійного замішування на диференціальні характеристики незбалансованих схем Фейстеля.

30. Побудова атак збоїв на сімейство шифрів «Калина».

31. Реалізація та дослідження атаки за побічним каналом на алгоритм шифрування IDEA.

6. Самостійна робота здобувача вищої освіти (СР)

З метою успішного здійснення самостійної роботи здобувача вищої освіти необхідно керуватися узагальненим календарним планом переддипломної практики за нижче наведеними формами – щоденника практики та індивідуального плану проходження практики.

Щоденник практики

№ п/п	Назва робіт	Тижні проходження практики					Примітки про виконання
		1	2	3	4	5	
1.	Проходження інструктажу з ТБ	+					
2.	Остаточне узгодження індивідуального завдання практики з науковим керівником		+				
3.	Проведення експериментальних досліджень			+			
4.	Узагальнення і систематизація отриманих результатів				+		
5.	Оформлення щоденника практики, робочої програми та звіту					+	

Самостійна робота здобувача вищої освіти передбачає складання й захист звіту про проходження переддипломної практики. Даний звіт повинен мати відомості про виконання всіх розділів програми практики у відповідності до індивідуального плану здобувача вищої освіти. Звіт повинен бути підписаний і оцінений керівником практики. У звіті необхідно подати кількісний та якісний аналіз проведеної роботи. Звіт повинен складатись зі вступу,

основної частини, висновків, списку використаних джерел та додатків.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Поточний та підсумковий контроль за виконанням здобувачами вищої освіти програми практики здійснює керівник практики від кафедри.

Щоденник практики є основним документом здобувача вищої освіти під час проходження практики. Під час практики здобувач вищої освіти щодня коротко чорнилом повинен записувати в щоденник усе, що він зробив за день для виконання календарного графіку проходження практики.

Докладні записи ведуться в робочих зошитах, які є продовженням щоденника. Не рідше, як раз на тиждень, здобувач вищої освіти зобов'язаний подавати щоденник на перегляд керівнику практики, який надає письмові зауваження, додаткові завдання й підписує записи, що їх зробив здобувач вищої освіти. Після закінчення практики щоденник разом із звітом має бути переглянутий керівником практики, який складає відгук й підписує його. Оформлений щоденник разом із звітом здобувач вищої освіти повинен здати на кафедру. Без заповненого щоденника практика не зараховується. Переддипломна практика завершується підсумковою конференцією.

Виведення оцінки за практику для кожного бакалавра-практиканта відбувається на заліковому занятті після виконання ним усіх завдань відповідно до плану переддипломної практики.

На залікове заняття кожен здобувач вищої освіти повинен подати пакет звітної документації, який включає:

1. Загальний звіт про проходження практики.
2. Відгук керівника практики від кафедри.
3. Щоденник практики, оформлені належним чином.

Завідувачем кафедри призначається комісія з прийому звітів з практики. До складу комісії входять керівник практики від кафедри та науковий керівник здобувача вищої освіти. Оцінка з практики вноситься в залікову відомість. Звіт з практики зберігається на кафедрі три роки.

Звіт з практики є основним документом, який пред´являється при здачі заліку. Обсяг звіту становить 10-15 сторінок машинописного тексту. Звіт оформляється відповідно до стандартів щодо науково-технічного звіту (ДСТУ – 3008-95).

Звіт включає наступні розділи:

1. Індивідуальне завдання.
2. Огляд літературних джерел за заданою тематикою.
3. Теоретичні відомості про метод розв´язання, його обгрунтування.
4. Програмна реалізація розроблених алгоритмів (виноситься в Додаток).
5. Аналіз результатів, висновки.
6. Список використаної літератури.

До звіту додаються щоденник з підписами і печаткою, що передбачені, та відгук керівника від підприємства. Звіт має бути зшитим.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: індивідуальна практична робота.

Семестровий контроль: залік.

Умови допуску до семестрового контролю:

Обов'язкові:

- Виконані індивідуальний план проходження практики
- Оформлений звітний пакет документів

Необов'язкові:

- Позитивний результат першої атестації та другої атестації.

Критерії оцінювання

Для оцінювання успішності здобувачів вищої освіти застосовується рейтингова система (РСО), яка враховує:

• виконання індивідуального завдання практики;

• підготовку та захист звітної документації.

Система рейтингових (вагових) балів:

№ з/п	Контрольний захід	%	Ваговий бал	Кіл-ть	Всього
1.	Виконання індивідуального завдання	60	60	1	60
2.	Захист звіту з практики	40	40	1	40
	Всього				100

При складанні звіту необхідно викладати матеріал у стислій формі. Завдання, процеси і структуру керування викладати у формі схем, таблиць і графіків із застосуванням коротких текстових пояснень. Збір матеріалу для звіту повинен проводитися послідовно і систематично в ході проходження практики у відповідних структурних підрозділах підприємства. Остаточне оформлення звіту і складання висновків проводиться у відведений для цього час. До звіту додається щоденник практики.

За результатами проходження переддипломної практики здобувач вищої освіти отримує відповідні оцінки (ECTS та традиційних).

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Оцінка за практику вноситься в заліково-екзаменаційну відомість і в залікову книжку здобувача вищої освіти та враховується під час визначення стипендії разом з оцінками за результатами підсумкового семестрового контролю.

Підсумки переддипломної практики обговорюються на засіданнях кафедр, а загальні підсумки практики підводяться на засіданнях Вченої ради інституту щорічно.

Робочу програму навчальної дисципліни (силабус):

Склав: доц. каф. ММЗІ Ніщенко Ірина Іванівна.

Ухвалено кафедрою математичних методів захисту інформації (протокол № 6 від 22.06.2022)

Погоджено Методичною комісією НН ФТІ (протокол № 6 від 30.06.2022)