НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»
УДК (впишіть правильний УДК!)

«До захисту допущено»
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2023 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Назва дослідження дуже довга, не влізає в один рядочок аж ніяк взагалі ой людоньки що робити»**

Виконав:
студент II курсу, групи ФХ-N3
Іванов Петро Сидорович _____

Керівник:
посада, степінь, звання
Прізвище Ім'я По-батькові _____

Рецензент:
посада, степінь, звання
Прізвище Ім'я По-батькові _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2023

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2023 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Іванов Петро Сидорович

1. Тема роботи: «*Назва дослідження дуже довга, не влізає в один рядочок аж ніяк взагалі ой людоньки що робити*», науковий керівник дисертації: посада, степінь, звання Прізвище Ім'я По-батькові,

затверджені наказом по університету №__ від «__» _____ 2023 р.

2. Термін подання студентом роботи: «__» _____ 2023 р.

3. Об'єкт дослідження: *(впишіть об'єкт дослідження)*

4. Предмет дослідження: *(впишіть предмет дослідження)*

5. Перелік завдань: *(впишіть теми та задачі, які ви розкриваєте у роботі; можна робити це попунктно)*

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: *(якщо у вас є окремий ілюстративний матеріал окрім власне роботи (креслення, макети тощо), зазначайте; інакше вказуйте «Презентація доповіді»)*

7. Орієнтовний перелік публікацій: *(впишіть наявні публікації або «планується доповідь на всеукраїнській конференції»)*

8. Дата видачі завдання: 10 вересня 2022 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2022 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2022 р.	Виконано
3	...	...	Виконано

Студент _____ Петро ІВАНОВ

Керівник _____ Ім'я ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота містить: ??? стор., ??? рисунки, ??? таблиць, ??? джерел.

У рефераті роботи ви повинні коротко (два-три абзаци) викласти, що саме було зроблено у цій роботі. Перші три речення реферату (після статистичних даних) повинні окреслити мету роботи, об'єкт та предмет дослідження. Після цього викладаються основні результати, одержані в ході дослідження.

Наприкінці анотації великими літерами зазначаються ключові слова. Ось так:

КЛЮЧОВІ СЛОВА, СИМЕТРИЧНА КРИПТОГРАФІЯ, ФІЗТЕХ НАЙКРАЩІЙ

ABSTRACT

The English abstract must be the exact translation of the Ukrainian "annotation" (including statistical data and keywords).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ФТІ — Фізико-технічний інститут

$\oplus$ — операція побітового додавання

(Якщо ви не використовуєте перелік умовних позначень, просто приберіть даний розділ.)

(БУДЬ ЛАСКА, ПРОСЛІДКУЙТЕ, ЩОБ НОМЕР СТОРІНКИ СПІВПАДАВ ІЗ СПРАВЖНІМ! Це залежить від того, наскільки великим є ваш зміст. Номер сторінки проставляється у файлі thesis.tex, рядок 35.)

ВСТУП

Актуальність дослідження. Актуальність даного дослідження полягає у тому, що без нього ви не одержите диплом про вищу освіту. Відповідно, ви повинні оформити результати вашого дослідження належним чином.

Вступ є однією із самих формалізованих частин дипломної роботи. На початку ви у двох-трьох абзацах повинні окреслити проблематику та актуальність вашого дослідження, після чого переходити до мети та завдання.

Метою дослідження є певна абстрактна недосяжна річ на кшталт загальнолюдського щастя на горизонті. Для досягнення мети необхідно розв'язати **задачу дослідження**, яка полягає у чомусь суттєво більш конкретному. Для розв'язання задачі необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) (наступний пункт, пов'язаний із теоретичним дослідженням);

3) (і ще один, наприклад, про експериментальну перевірку результатів);

4) (і взагалі, краще із науковим керівником проконсультуйтесь, як ваші завдання правильно писати).

Об'єктом дослідження є якісь процеси або явища загального характеру (наприклад, «інформаційні процеси в системах криптографічного захисту»).

Предметом дослідження є конкретний математичний чи фізичний об'єкт, який розглядається у вашій роботі та який можна трактувати як певну властивість об'єкта дослідження (наприклад, «моделі та методи диференціального криптоаналізу ітеративних симетричних блочних шифрів»).

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: і тут коротенький перелік (наприклад, але не

обмежуючись: методи лінійної та абстрактної алгебри, теорії імовірностей, математичної статистики, комбінаторного аналізу, теорії кодування, теорії складності алгоритмів, методи комп'ютерного та статистичного моделювання)

Наукова новизна отриманих результатів полягає... – тут необхідно перелічити, що саме нового з точки зору науки несе ваша робота. До усіх тверджень, які сюди виносяться, подумки (а іноді й явним чином) потрібно ставити слово «вперше» – і ці твердження повинні залишатись істинними.

Практичне значення результатів полягає... – тут необхідно зазначити практичну користь від результатів вашої роботи. Що саме можна покращити, підвищити (або знизити), зробити гарного (або уникнути поганого) після вашого дослідження.

Апробація результатів та публікації. Наприкінці вступу необхідно зазначити перелік конференцій, семінарів та публікацій, в яких викладено результати вашої роботи. Якщо результати вашої роботи ніде не доповідались, опускайте даний абзац.

1 (НАЗВА ПЕРШОГО РОЗДІЛУ)

На початку кожного розділу рекомендується вставити одне-два-абзац речень, у яких коротенько представили, про що тут взагалі буде мова.

1.1 (Назва першого підрозділу)

Перший розділ повинен бути присвячений огляду попередніх результатів за тематикою вашого дослідження. У даному розділі повинні міститись вс' визначення та описи, необхідні для подальшого викладення матеріалу, та результати ваших попередників.

Зауважимо, що наводити детальні доведення не ваших результатів необхідно наводити лише тоді, коли вони містять якусь вкрай важливу інформацію для саме ваших результатів.

Також зауважимо, що абсолютно на всі не ваші результати повинні стояти належним чином оформлені посилання.

Розмір першого (оглядового) розділу не повинен перевищувати третини вашої дипломної роботи (без урахування додатків).

1.2 (Назва другого підрозділу)

Наведемо основні правила оформлення текстів у системі LaTeX.

Для абзацу робіть пусті рядки у файлі. Курсивний текст робиться командою emph: *ось так*. Жирний текст робиться командою textbf: **ось так**.

«Лапки» робляться двома знаками більше та двома знаками менше. Довге тире у тексті — трьома дефісами, коротке – двома дефісами; у формулах мінуси робляться одним дефісом: $a - b$.

Пишіть звичайний текст звичайним текстом, а формули, позначення

змінних та операцій (усі формули, усі позначення змінних та усі операції) беріть у знаки долара, ось так: $E = mc^2$, $a_1 = a^{(2)} \cdot a_{n,k}$, $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$. Якщо вам не подобається, як LaTeXподав формулу для експоненти (мені, наприклад, не подобається), то можна внести у код формули деякі корективи та написати ось так: $e^x = \sum\limits_{k=0}^{\infty} \frac{x^k}{k!}$.

Для прикладу різні варіації коми у формулах: (a, b) vs. (a,b). Поки пакет icomma працює, різниця видна наочно.

Виключна формула (формула окремим рядком) робиться через подвійні знаки долара або через оточення equation. Зауважте, що при цьому змінюється оформлення формул:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

Формули за помовчанням не підтримують кирилічні літери. Зверніть увагу на порожній рядок перед попереднім реченням у tex-файлі: без нього не буде створено абзац.

Із більш специфічних позначень — ось так, скажімо, можна подати перестановку:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ a & 5 & 9 & 6 & 4 & 8 & 2 & 1 & 7 \end{pmatrix},$$

де $a = 3$. Зауважте, що у попередньому реченні нема порожнього рядочку перед «де» (та, відповідно, абзацу після формули), а кома внесена у виключну формулу, бо інакше вона переїде у наступний рядок тексту.

Декілька формул поспіль треба збирати в єдине ціле оточеннями gather або eqnarray; назви оточень із зірочками вказують LaTeX'у не нумерувати дані формули. Наприклад, ось рекуренти для циклових чисел та чисел Стірлінга I роду:

$$\begin{aligned} c(n+1,k) &= c(n,k-1) + nc(n,k); \\ s(n+1,k) &= s(n,k-1) - ns(n,k). \end{aligned}$$

Зверніть увагу на символ «~» у попередньому абзаці tex-файлу між «І» та «роду»; це нерозривний пробіл, який не дасть рознести пов'язані частини по різних рядках. Тільду треба ставити перед усіма посиланнями (команди ref та cite), перед тире та у місцях, які не можна розривати за правилами граматики.

Для специфічних позначень ви можете задавати власні команди (їх рекомендовано заносити у файл «`02_redefinitions`»). Наприклад, подивіться, як оформлюється теорема Лагранжа-Бюрмана із використанням введених команд `\Coef` та `\compinv`:

Теорема 1.1 (Лагранж, Бюрман)**.** *Для будь-якого ряду* $A \in x\mathcal{R}[[x]]_1$ *та* $k \in \mathbb{N}$ *справедливе співвідношення*

$$n \operatorname{Coef}[x^n] \left(A^{\langle -1\rangle}(x)\right)^k = k \operatorname{Coef}[x^{n-k}] \left(\frac{x}{A(x)}\right)^n .$$

Доведення. Доведення ви подивитесь деінде, а тут подивіться, як воно оформлюється (зокрема, на квадратик наприкінці :)). □

Наслідок 1.1. *Будь-ласка, перевіряйте граматику. Латеховські редактори зазвичай не мають інтегрованих спелчекерів української мови, тому використовуйте сервіси, наведені, наприклад, тут: https://coma.in.ua/30584*

Іноді написаний файл треба компілювати двічі для одержання ефекту (скажімо, для коректної побудови усіх гіперпосилань та побудови змісту). Скажімо, оце посилання на теорему 1.1 (теорему Лагранжа-Бюрмана) з першої компіляції може показати вам знаки питання «??». Однак після повторної компіляції ви одержите те, що потрібно.

Онлайн-сервіси на кшталт Overleaf справляються з такими ситуаціями за одну компіляцію. Однак той же Overleaf має звичку компілювати pdf-файли навіть за наявності помилок у тексті, просто ігноруючи відповідні місця. Якщо ви працюєте у Overleaf, то переконайтесь, що у вас нема червоних помилок після компіляції. На щастя, останні апдейти Overleaf вивалюють червоні помилки прямо вам в

очі, тому їх нескладно помітити.

Якщо вам потрібна якась фіча, запитайте в Сенсея. Майже напевно вона є.

На жаль деякі пакети шаблону викликають незрозумілі конфлікти. Поки що не вдалось інтегрувати у шаблон такі пакети, як color та tikz. Якщо без кольорового забарвлення тексту ще можна пережити, то використовувати діаграми tikz поки що рекомендується за допомогою милиць:

– створюєте окремий допоміжний tex-проект, у якому за допомогою tikz створюєте діаграму;

– компілюєте допоміжний tex-проект;

– вставляєте створену діаграму з pdf-файлу у диплом як зображення.

Ми ж зі свого боку продовжуємо працювати над покращенням даного шаблону.

1.3 (Назва третього підрозділу)

Надамо деякі рекомендації щодо використання даного стильового файлу.

Теорема 1.2. *Використовуйте оточення* theorem *для теорем.*

Доведення. Для доведень використовуйте оточення *proof.* □

Теорема 1.3. *Нумерація відбувається автоматично*

Твердження 1.1. *Використовуйте оточення* claim *для тверджень.*

Лема 1.1. *Використовуйте оточення* lemma *для лем.*

Наслідок 1.2. *Використовуйте оточення* corollary *для наслідків.*

Означення 1.1. Використовуйте оточення *definition* для визначень.

Приклад 1.1. Використовуйте оточення *example* для прикладів, на які є посилання.

Зауваження. Використовуйте оточення *remark* для зауважень. Зверніть увагу, як веде себе команда **emph**

Висновки до розділу 1

Наприкінці кожного розділу ви повинні навести коротенькі підсумки по його результатах. Зокрема, для оглядового розділу в якості висновків необхідно зазначити, які задачі у даній тематиці вже були розв'язані, а саме поставлена вами задача розв'язана не була (або розв'язана погано), тому у наступних розділах ви її й розв'язуєте.

Якщо ваш звіт складається з одного розділу, пропускайте висновок до нього – він повністю включається в загальні висновки до роботи

2 (НАЗВА ДРУГОГО РОЗДІЛУ)

До другого розділу також краще написати малесенький вступ. Зокрема, це збільшує загальний об'єм роботи та покращує її читабельність.

2.1 (Якийсь підрозділ)

У другому розділі необхідно наводити розв'язання поставленої перед вами задачі у теоретичному або аналітичному сенсі (хоча, звісно, все залежить від того, яка саме задача перед вами поставлена).

Для подання матеріалів можна використовувати таблиці (наприклад, Таблицю 2.1). Розмір шрифту у таблиці може бути меншим за 14 pt (наприклад, 12 pt, або навіть 10 pt, якщо так таблиця виглядає зрозуміліше та компактніше).

Таблиця 2.1 – Розрахунок якоїсь фантастичної дичини у декілька кроків

Параметр x_i	Параметр x_j				Перший крок		Другий крок	
	X_1	X_2	X_3	X_4	w_i	$K_{\text{в}i}$	w_i	$K_{\text{в}i}$
X_1	1	1	1.5	1.5	5	0.31	19	0.32
X_2	1	1	1.5	1.5	5	0.31	19	0.32
X_3	0.5	0.5	1	0.5	2.5	0.16	9.25	0.16
X_4	0.5	0.5	1.5	1	3.5	0.22	12.25	0.20
Разом:					16	1	59.5	1

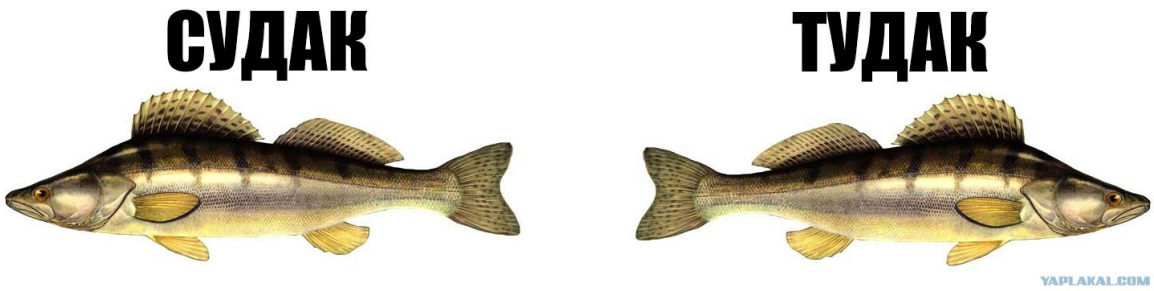
Бажано, щоб кожен пункт завдань, окреслених у вступі, відповідав певному розділу або підрозділу у дипломній роботі.

Теорема 2.1. *Нумерація у наступних розділах також*

проставляється автоматично та коректно.

2.2 (Якийсь наступний підрозділ з дуже-дуже довгою назвою, загальна кількість слів в якій, однак, не повинна перевищувати 12 слів)

Для подання матеріалів також дуже зручними є рисунки (наприклад, рисунки 2.1 або 2.2).



(а) (б)

Рисунок 2.1 – Різні види риб: (а) судак, (б) тудак.

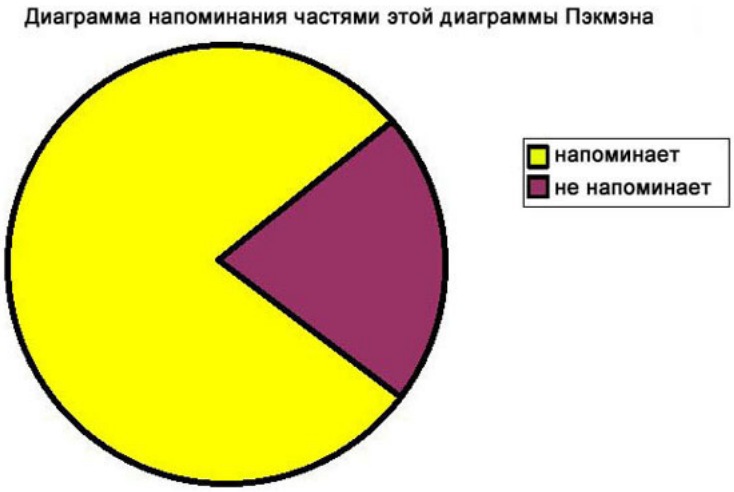


Рисунок 2.2 – Частка кругових діаграм, які схожі на Пекмена

2.3 Оформлення посилань

Посилання до роботи рекомендовано робити за допомогою підсистеми BibTex. Це максимально зручно, повірте мені. Усі притомні світові журнали надають посилання на свої статті у вигляді bib-файлів, з яких просто треба перенести відомості у свій файл. Існують інструменти автоматизованого створення bib-файлів, наприклад, JabRef. Якщо у вас нема автоматизованого механізму, то посилання на джерела у bib-файлах легко створюються вручну. Головне — не забувати чотири простих правила:

1) Імена авторів необхідно подавати у вигляді «Прізвище, Ім'я» та розділяти ключовим словом «and», наприклад:

```
author = "Яковлєв, Сергій Володимирович and Дамблдор,
Альбус Персиваль Вульфрік Брайан"
```

2) Після усіх полів запису необхідно ставити кому, окрім останнього.

3) Джерела у переліку посилань з'являться тільки після того, як ви зробите посилання на нього у тексті, наприклад, див. роботи [1, 2].

Висновки до розділу 2

Наприкінці розділу знову наводяться коротенькі підсумки.

3 (НАЗВА ТРЕТЬОГО РОЗДІЛУ)

3.1 (якийсь підрозділ)

Подивіться, як нераціонально використовується простір, якщо не писати вступи до розділів. :)

Зазвичай третій розділ присвячено опису практичного застосування або експериментальної перевірки аналітичних результатів, одержаних у другому розділі роботи. Втім, це не обов'язкова вимога, і структура основної частини диплому більш суттєво залежить від характеру поставлених завдань. Навіть якщо у вас є певне експериментальне дослідження, але його загальний опис займає дві сторінки, то краще приєднайте його підроздіром у попередній розділ.

При описі експериментальних досліджень необхідно:

– наводити повний опис експериментів, які проводились, параметрів обчислювальних середовищ, засобів програмування тощо;

– наводити повний перелік одержаних результатів у чисельному вигляді для їх можливої перевірки іншими особами;

– представляти одержані результати у вигляді таблиць та графіків, зрозумілих людському оку;

– інтерпретувати одержані результати з точки зору поставленої задачі та загальної проблематики ваших досліджень.

У жодному разі не потрібно вставляти у даний розділ тексти інструментальних програм та засобів (окрім того рідкісного випадку, коли саме тексти програм і є результатом проведення експериментів). За необхідності тексти програм наводяться у додатках.

Висновки до розділу 3

Висновки до останнього розділу є, фактично, підсумковими під усім дослідженням; однак вони повинні стостуватись саме того, що розглядалось у розділі.

ВИСНОВКИ

Загальні висновки до роботи повинні підсумовувати усі ваші досягнення у даному напрямку досліджень.

За кожним пунктом завдань, поставлених у вступі, у висновках повинен міститись звіт про виконання: виконано, не виконано, виконано частково (І чому саме так). Наприклад, якщо першим поставленим завданням у вас іде «огляд літератури за тематикою досліджень», то на початку висновків ви повинні зазначити, що «у ході даної роботи був проведений аналіз опублікованих джерел за тематикою (...), який показав, що (...)». Окрім простої констатації про виконання ви повинні навести, які саме результати ви одержали та проінтерпретувати їх з точки зору поставленої задачі, мети та загальної проблематики.

В ідеалі загальні висновки повинні збиратись з висновків до кожного розділу, але ідеал недосяжний. :) Однак висновки не повинні містити формул, таблиць та рисунків. Дозволяється (та навіть вітається) використовувати числа (на кшталт «розроблена методика дозволяє підвищити ефективність пустопорожньої балаканини на 2.71%»).

Наприкінці висновків необхідно зазначити напрямки подальших досліджень: куди саме, як вам вважається, необхідно прямувати наступним дослідникам у даній тематиці.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Воронцов К. В. *LaTeX 2ε в примерах*. Рос. 2005, с. 59 с. URL: http://www.ccas.ru/voron/download/voron05latex.pdf.

[2] Львовский С. М. *Набор и верстка в системе LaTeX*. Рос. 3-е вид. 2003, с. 448 с. URL: http://www.mccme.ru/free-books/llang/newllang.pdf.

ДОДАТОК А ТЕКСТИ ПРОГРАМ

Тексти інструментальних програм для проведення експериментальних досліджень необхідно виносити у додатки.

А.1 Програма 1

Зауважте, як змінилась нумерація.

Теорема А.1. *Нумерація теорем та іншого також повинна змінитись.*

ДОДАТОК Б ВЕЛИКІ РИСУНКИ ТА ТАБЛИЦІ

Якщо результати вашої роботи описуються величезними рисунками і таблицями (один аркуш та більше) у незліченній кількості, їх також необхідно виносити у додатки.