Міністерство освіти і науки України
Тернопільський національний технічний університет
імені Івана Пулюя

Кафедра кібербезпеки

Методичні вказівки

до виконання курсового проєкту
з дисципліни

Прикладна криптологія

для студентів денної форми навчання
напряму підготовки
125 Кібербезпека

Тернопіль – 2021

Методичні вказівки та основні вимоги до підготовки, оформлення та захисту курсових робіт з дисципліни «Прикладна криптологія» / Укладач: к.т.н., доц. завідувач кафедри кібербезпеки ТНТУ Загородна Наталія Володимирівна – Тернопіль: ТНТУ, 2021. – 28 с.

Укладач: Загородна Наталія Володимирівна
кандидат технічних наук, доцент, зав.каф. кафедри кібербезпеки ТНТУ ім. І. Пулюя

Рецензенти: Литвиненко Я.В. доктор технічних наук, професор
професор кафедри комп'ютерних наук ТНТУ ім. І. Пулюя

Боднарчук І.О. кандидат технічних наук, доцент,
завідувач кафедри комп'ютерних наук ТНТУ ім. І. Пулюя

Затверджено на засіданні кафедри кібербезпеки Тернопільського національного технічного університету ім. І. Пулюя (протокол № 1 від 25 серпня 2021 р.).

Схвалено та рекомендовано до друку Методичною комісією факультету комп'ютерно-інформаційних систем та програмної інженерії Тернопільського національного технічного університету ім. І. Пулюя
(протокол № 1 від 31.08.2021 р.)

ЗМІСТ

ВСТУП

Методичні вказівки висувають загальні вимоги до організації та проведення курсового проєктування, тематики, змісту та обсягу, порядку розробки та захисту курсових робіт (КР) у відповідності до вимог освітніх (кваліфікаційних) характеристик дисципліни "Прикладна криптологія" спеціальності 125 "Кібербезпека" та діючих нормативно-технічних документів ТНТУ ім. І.Пулюя.

Методичні вказівки спрямовані на забезпечення єдиного підходу та єдиних вимог до курсового проєктування (його проведення та оформлення результатів проєктування), уникнення помилок, які найчастіше зустрічаються в курсовому проєктуванні, а також на удосконалення курсового проєктування на основі узагальненого позитивного досвіду.

Методичні вказівки є загальними для всіх студентів, які вивчають дисципліну "Прикладна криптологія" і повинні надати методичну допомогу з питань курсового проєктування як студентам, так і їх керівникам.

Загальні вимоги до курсового проєкту:

- ✓ чіткість побудови;
- ✓ логічна послідовність викладу матеріалу, переконлива аргументація;
- ✓ точність викладу, яка виключає можливість суб’єктивного та
- ✓ неоднозначного тлумачення;
- ✓ конкретність викладу результатів роботи;
- ✓ доведення висновків та обґрунтованість рекомендацій.

1. МЕТА ТА ЗАВДАННЯ КУРСОВОГО ПРОЄКТУ

Важливим етапом в процесі вивчення навчальної дисципліни «Прикладна криптологія» є курсовий проєкт. Курсовий проєкт виступає як одна з найважливіших форм самостійної роботи студентів. В процесі написання курсового проєкту студенти повинні глибше дослідити теоретичні та практичні аспекти реалізації різноманітних крипто-протоколів.

Курсовий проєкт – це вид самостійної навчально-наукової роботи студентів з елементами дослідження, яка має на меті закріплення, поглиблення і узагальнення знань, одержаних за час навчання та їх застосування до комплексного вирішення фахового завдання.

Змістом курсового проєкту з дисципліни «Прикладна криптологія» є програмна реалізація криптопротоколу та тестування його роботи.

Метою написання курсового проєкту можна визначити:

- ✓ поглиблення знань студентів з актуальних проблем криптографічного захисту інформаційно-комунікаційних систем;
- ✓ систематизація здобутих знань з навчальної дисципліни;
- ✓ застосування здобутих знань та вмінь для вирішення практичних завдань;
- ✓ розвиток умінь самостійного критичного опрацювання літературних джерел та міжнародних криптографічних стандартів;
- ✓ формування дослідницьких умінь студентів;
- ✓ стимулювання студентів до самостійного наукового пошуку;
- ✓ розвиток уміння аналізувати сучасний досвід та узагальнювати власні спостереження;
- ✓ формування вміння практичної реалізації результатів дослідження проблеми в самостійно виконаних розробках.

Виконання курсового проєкту з дисципліни «Прикладна криптологія» спрямоване на досягнення наступних цілей:

- ✓ поглиблення та закріплення теоретичних знань, здобутих студентами в процесі лекційних та лабораторних занять;
- ✓ формування вмінь щодо виконання наукових досліджень за своєю спеціальністю;
- ✓ підготовка до подальшої професійної діяльності;
- ✓ підготовка до виконання випускної кваліфікаційної роботи.

Курсовий проєкт є самостійною роботою студента, що виконується на основі вивчення спеціальної літератури з питань досліджуваної теми, законодавчих та нормативних актів, систематизації та обробки статистичних матеріалів, виявлення резервів та ресурсів для криптографічного захисту

інформаційно-комунікаційної системи, підвищення ефективності роботи інформаційної системи, розробки пропозицій, спрямованих на вирішення практичних завдань щодо вдосконалення захищеності.

Терміни виконання курсового проєкту визначаються графіком навчального процесу.

2. ПОСЛІДОВНІСТЬ ВИКОНАННЯ КУРСОВОГО ПРОЄКТУ

Підставою для написання курсового проєкту є завдання (додаток В), яке складається керівником курсового проєкту спільно зі студентом. У завданні зазначається тема курсового проєкту, зміст завдання та терміни виконання.

Курсову роботу з дисципліни «Прикладна криптологія», змістом якої є розробка програмного забезпечення, що реалізує криптографічні протоколи, рекомендується виконувати в такій послідовності:

- ✓ Вибір криптопротоколу та оформлення завдання на курсовий проєкт;
- ✓ Опрацювання літературних джерел щодо засобів криптографічного захисту ІКС;
- ✓ Збір інформації необхідної для програмної реалізації протоколу;
- ✓ Аналіз та опрацювання зібраної інформації;
- ✓ За необхідності додатковий збір інформації, недостатність якої була виявлена в процесі аналізу;
- ✓ Програмна реалізація протоколу;
- ✓ Тестування роботи ПЗ;
- ✓ Порівняльний аналіз отриманих результатів з результатами, отриманими з використанням стандартних бібліотек з криптопримітивами;
- ✓ Оформлення пояснювальної записки згідно вимог;
- ✓ Надання курсового проєкту керівнику для попереднього рецензування;
- ✓ Доопрацювання курсового проєкту за наявності відповідних вимог керівника;
- ✓ Отримання позитивної рецензії керівника;
- ✓ Захист курсового проєкту у вигляді презентації.

Після завершення написання курсового проєкту студент здає її на кафедру в межах терміну зазначеного в завданні. Керівник визначає ступінь готовності роботи та надає рецензію у вигляді рекомендацій для доопрацювання та ступеня готовності роботи. Після доопрацювання у разі необхідності робота допускається до захисту.

Оцінка за курсову роботу складається з двох частих (модульної семестрової та залікової/екзаменаційної оцінки) При визначенні модульної

семестрової (максимум 75 балів) оцінки за курсову роботу враховуються її обсяг і якість, ступінь обґрунтування обраної ідеї захисту, правильність оформлення, оригінальність і самостійність вирішення поставленого завдання. При визначенні залікової/екзаменаційної враховується глибина знань з обраної теми, вміння представляти результати роботи, збирати та аналізувати інформацію, орієнтуватися в нормативних документах, обґрунтовувати і захищати свої пропозиції.

3. ЕТАПИ ПРОВЕДЕННЯ ДОСЛІДЖЕННЯ ТА НАПИСАННЯ КУРСОВОГО ПРОЄКТУ

Процес написання курсового проєкту, змістом якої є встановлення операційної системи, розробка та налаштування політик локальної та мережевої безпеки, доцільно розділити на три етапи:

I. Початковий;
II. Підготовчий;
III. Основний.

I. Початковий етап: вибір криптопротоколу

Це відповідальний етап, адже потрібно визначити проаналізувати криптографічний алгоритм, визначити аналогічні та виконати порівняльний аналіз з ними. На даному етапі розглядаються відомі криптографічні засоби (з посиланням на джерела та наведенням їх технічних характеристик) для розв’язання задачі.

II. Підготовчий етап роботи над курсовою роботою

На підготовчій стадії:

1) збирається та аналізується технічна документація та наукова література про обраний криптопротокол та стандарти, що його описують. Що більше інформації буде зібрано, тим більш обґрунтованими будуть політики безпеки;

2) проводиться вибір середовища розробки з врахуванням наступних аспектів:

a наявності стандартних криптографічних бібліотек;
b особливостей протоколу;
c порівняльного аналізу характеристик рішень та огляду криптографічних засобів, що ці рішення реалізують;

3) визначається головне призначення обраного протоколу та формулюється кінцева мета його використання;

4) формулюються інші обмеження чи особливості використання криптопроколу;

ІІ. Основний етап роботи над курсовою роботою

На основному етапі відбувається написання програмного продукту, тестування його роботи, порівняльний аналіз отриманих результатів з результатами стандартних бібліотек та написання пояснювальної записки. Під час виконання даного етапу необхідно проаналізувати коректність виконання криптографічного протоколу. Цей аналіз, для прикладу, можна робити на основі логічної моделі Берроуза - Абаді - Нідхема (BAN-логіки). За результатами аналізу потрібно зробити висновок про стійкість протоколу та можливість виявлення несанкціонованого втручання.

4. СТРУКТУРА ТА ЗМІСТ КУРСОВОГО ПРОЄКТУ

Курсовий проєкт повинна мати практичний характер та авторський підхід, а не бути переказом загальновідомих положень і висновків. У процесі викладу матеріалу не дозволяється пряме переписування з літературних джерел без посилання на оригінал. **Робота, в якій виявлені елементи плагіату, оцінюється незадовільно і повертається на переробку чи доопрацювання.** При написанні курсового проєкту автор повинен давати посилання на дані, відомості, матеріали отримані з літературних та інших інформаційних джерел.

Структурно курсовий проєкт повинен складатися з таких елементів:

- ✓ Титульна сторінка;
- ✓ Завдання на курсовий проєкт;
- ✓ Зміст;
- ✓ Загальна характеристика криптопротоколу;
- ✓ Аналіз відомих реалізацій протоколу;
- ✓ Аналіз та обґрунтування вибору методів, які будуть використовуватись для досягнення мети проєктування;
- ✓ Аналіз коректності криптографічних протоколів;
- ✓ Розробка алгоритму роботи програмного засобу;
- ✓ Розробка ПЗ;
- ✓ Тестування роботи ПЗ;
- ✓ Висновки;

- ✓ Список використаних джерел;
- ✓ Додатки (за необхідністю).

Загальний обсяг роботи **25-35** сторінок друкованого тексту оформленого згідно вимог.

Порядок розміщення, коротка характеристика та зміст структурних елементів курсового проєкту

1. **Титульна сторінка.** Форма титульної сторінки наведена в додатку Б.
2. **Завдання на курсовий проєкт.** Бланк завдання розміщений у дод. В.
3. **Зміст** повинен містити найменування та нумерацію початкових сторінок усіх розділів та підрозділів. Приклад оформлення змісту курсового проєкту наведений у додатку Г.
4. **Загальна характеристика криптопротоколу** (5-7 стор.).
5. **Аналіз відомих реалізацій протоколу** (3-4 стор.).
6. **Аналіз та обґрунтування вибору методів, які будуть використовуватись для досягнення мети проєктування** (4-6 стор).
7. **Аналіз коректності криптографічних протоколів** (2-3 стор.).
8. **Розробка алгоритму роботи програмного засобу** (3-4 стор.)
9. **Розробка ПЗ** (5-6 стор.)
10. **Тестування роботи розробленого ПЗ** (2-3 ст.)
11. **Висновки** (4-5 стор.). В даному розділі коротко описується підсумок виконаної роботи. Доцільно вказати види інформаційно-комунікаційних систем, на яких впровадження розроблених криптопротоколів підвищить рівень захищеності. Варто окреслити напрями подальших досліджень.
12. **Список використаних джерел.** Відомості про джерела, які включені до списку, необхідно давати згідно з вимогами існуючого державного стандарту. Використані джерела у списку слід розміщувати в алфавітному порядку. Джерела на іноземні мові (латинський алфавіт) розміщуються в кінці списку**.**

Приклад оформлення списку використаних джерел наведено у додатку Д.

13. **Додатки.** До додатків включають допоміжний матеріал, спрямований на посилення повноти сприйняття проведеного дослідження. Матеріал, що надається в додатках, повинен відповідати обраній темі дослідження.

5. ОСНОВНІ ВИМОГИ ДО ОФОРМЛЕННЯ КУРСОВОГО ПРОЄКТУ

Текст роботи

Курсовий проєкт виконується з допомогою текстового редактора Microsoft Word. Мова курсового проєкту − державна, стиль − науковий, чіткий, без орфографічних і синтаксичних помилок, послідовність – логічна. Пряме переписування у роботі матеріалів із літературних джерел є неприпустимим.

Робота має бути надрукована на одному боці сторінок стандартного білого паперу формату А4 (210х297 мм).

Текст друкується шрифтом Times New Roman; розмір шрифту – 14; інтервал – 1,5. Щільність тексту по всій роботі однакова (стандартна).

Текст курсового проєкту необхідно друкувати, залишаючи поля таких розмірів: ліве – 30 мм, праве – 10 мм, верхнє – 20 мм, нижнє – 20 мм. Абзацний відступ 1,25 см. (5 знаків).

Текст основної частини роботи поділяється на розділи і підрозділи згідно з планом, затвердженим науковим керівником та відображається у змісті.

Заголовки структурних частин курсового проєкту «ЗМІСТ», «ВСТУП», «РОЗДІЛ» (разом з номером розділу та конкретною назвою), «ВИСНОВКИ», «СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ», «ДОДАТКИ» друкують жирним шрифтом великими літерами симетрично до тексту. Розміщують по центру сторінки. Заголовки підрозділів друкують маленькими літерами (крім першої великої) з абзацного відступу, вирівнювання по ширині сторінки. Крапку в кінці заголовків не ставлять. Якщо заголовок складається з двох або більше речень, їх розділяють крапкою.

Відстань між заголовком структурної частини курсового проєкту та текстом повинна дорівнювати 2 інтервалам (2 пропущеним рядкам тексту). Між заголовками підрозділів та текстом немає пропусків (текст підрозділу розміщується одразу в наступному рядку). (див. рис. 2)

Кожну структурну частину курсового проєкту треба починати з нової сторінки. Частини розділу (підрозділи) друкують один за одним з відстанню в один інтервал (1 рядок). Не допускається розміщувати найменування підрозділу в нижній частині сторінки, якщо після нього розташовано тільки один рядок тексту, в таких видках його необхідно починати з нової сторінки.

Нумерація

Нумерацію сторінок, розділів, підрозділів, пунктів, підпунктів, малюнків, таблиць, формул подають арабськими цифрами без знака «№».

Першою сторінкою частин курсового проєкту є титульна сторінка, її включають до загальної нумерації сторінок (див. додаток А). На титульній сторінці **номер не ставлять**, на наступних сторінках номер проставляють **у правому нижньому куті сторінки** без крапки в кінці.

Номер розділу ставиться після слів «РОЗДІЛ». Далі після крапки у тому ж рядку йде назва розділу (***Приклад***: **РОЗДІЛ 1. ЗАГАЛЬНА ХАРАКТЕЛИСТИКА ТА ВСТАНОВЛЕННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX TAILS**). Такі структурні елементи курсового проєкту як «ЗМІСТ», «ВСТУП», «ВИСНОВКИ», «СПИСОК ВИКОРИСТНИХ ДЖЕРЕЛ», «ДОДАТКИ» не нумерують як розділи.

Підрозділи нумерують у межах кожного розділу. Номер підрозділу складається з номера розділу і порядкового номера підрозділу, між якими ставлять крапку. В кінці номера підрозділу повинна стояти крапка. (***Приклад:*** **1.3. Текст підрозділу** (третій підрозділ першого розділу)). Потім у тому ж рядку йде заголовок підрозділу.

Ілюстрації та таблиці

Ілюстрації (рисунки) та таблиці необхідно подавати безпосередньо після тексту, де вони згадані вперше, або на наступній сторінці. Ілюстрації і таблиці, які розміщені на окремих сторінках курсового проєкту, включають до загальної нумерації сторінок (бажано їх подавати у вигляді додатків). Таблиці та ілюстрації розміри яких перевищують формат А4, враховують як одну сторінку і розміщують у додатках.

Ілюстрації позначають словом **«Рис.»** і нумерують послідовно в межах розділу, за винятком ілюстрацій, поданих у додатках. Ілюстрації повинні мати назву, яку розміщують після її номера під ілюстрацією (**друкують жирним шрифтом вирівнювання по центру**). Після назви повинно бути посилання на джерело (оформлено згідно правил) звідки запозичена ілюстрація, у випадку коли вона розроблена автором, відповідне зазначається у дужках після назви ілюстрації. (***Приклад:*** **Рис. 2.3. Скріншот налаштування мережевих з'єднань (**третій рисунок другого розділу)).

За необхідності під ілюстрацією розміщують пояснювальні дані. Якщо в курсовому проєкті подано одну ілюстрацію, то її нумерують за загальними правилами.

Схематичний приклад оформлення ілюстрації в курсовій роботі наведено на рис. 2.

Рисунок 2 - Приклад оформлення ілюстрації в курсовому проєкті

Традиційно у курсовій роботі цифровий матеріал оформляється у вигляді таблиці.

Кожна таблиця повинна мати назву, яку розміщують над таблицею та друкують починаючи з великої літери симетрично до тексту жирним шрифтом. Назва повинна бути стисло сформована та відображати зміст таблиці. Після назви таблиці (як її продовження) повинно бути посилання на джерело (оформлено згідно правил) звідки запозичена таблиця, у випадку коли вона розроблена автором, відповідне зазначається у дужках.

Одразу після назви (без пропуску рядка) розміщують таблицю.

Заголовки граф починаються з великих літер, підзаголовки − з малих, якщо складають одне речення із заголовком, і з великих − якщо вони є самостійними. Графу з порядковими номерами рядків до таблиці включати не треба.

Таблицю розміщують після першого згадування про неї в тексті, таким чином, щоб її можна було читати без повороту переплетеного блоку роботи або з поворотом за годинниковою стрілкою. Таблицю, що містить велику кількість рядків, можна переносити на інший аркуш. При перенесенні таблиці на інший аркуш (сторінку) назву розміщують тільки над її першою частиною. У разі перенесення таблиці на іншу сторінку над подальшими частинами пишеться: **«Продовження табл. (вказується номер таблиці)»**.

Таблицю з великою кількістю граф можна ділити на частини і розмішувати одну частину під іншою у межах одної сторінки. Якщо рядки або графи таблиці виходять за формат сторінки, то в першому випадку в кожній частині таблиці повторюють заголовки граф, в другому випадку – заголовки рядків.

Якщо цифрові або інші дані в якому-небудь рядку таблиці не подають, то в ньому ставлять прочерк.

Таблиці нумерують послідовно у межах розділу (за винятком тих, що розміщені в додатках). Перед назвою розміщують напис «Таблиця» **(вирівнювання тексту по правому краю)** із зазначенням її номера, який складається з номера розділу і порядкового номера таблиці, між якими ставиться крапка: наприклад (***Приклад:*** **Таблиця 2.4** (четверта таблиця другого розділу)).

У таблицях слід обов'язково зазначати одиниці виміру. Якщо всі одиниці виміру є однакові для всіх показників таблиці, вони наводяться у заголовку. Одиниці виміру мають наводитися у відповідності до стандартів. Числові величини у таблиці повинні мати однакову кількість десяткових знаків.

Формули та рівняння

Формули в курсовому проєкті слід оформляти в текстовому редакторі формул.

Рівняння і формули треба виділяти з тексту вільними рядками та вирівнювати по центру тексту. Вище і нижче кожної формули потрібно залишати не менше одного вільного рядка (див. рис. 5).

Пояснення значень символів і числових коефіцієнтів треба подавати безпосередньо під формулою в тій послідовності, у якій вони подані у формулі. Значення кожного символу і числового коефіцієнта треба подавати з нового рядка. Перший рядок пояснення починають зі слова «де» без двокрапки.

Якщо рівняння не вміщується в один рядок, його переносять після знака рівності (=) або після знаків плюс (+), мінус (–), множення (х) і ділення (:).

Формули в курсовому проєкті (якщо їх більше одної) нумерують у межах розділу. Номер формули складається з номера розділу і порядкового номера формули в розділі, між якими ставлять крапку. Номери формул пишуть на рівні відповідної формули в круглих дужках (***Приклад*****: (3.1)** (перша формула третього розділу)).

Нумеровані переліки

Перед нумерованим переліком ставлять двокрапку. Для першої деталізації переліку варто використовувати арабські цифри з дужкою. Наприкінці кожної позиції переліку (крім останньої) ставиться крапка з комою, або двокрапка, якщо є подальша деталізація. В курсовому проєкті переліки повинні бути без геометричних прикрас, крім цифр можна використовувати латинські чи кириличні букви, а також знак «тире». Після останнього пункту переліку ставиться крапка. Перелік пишуть малими літерами з абзацного відступу

Примітки

Примітки до тексту і таблиць, у яких вказують довідкові та пояснювальні дані, нумерують послідовно в межах одної сторінки та розміщують в низу сторінки. Якщо приміток на одному аркуші декілька, то після слова «Примітки» ставлять двокрапку та подають нумерований перелік приміток. Якщо є одна примітка, то її не нумерують і після слова «Примітка» ставлять крапку і дальше з великої букви наводять текст примітки.

Посилання

При написанні курсового проєкту необхідно давати посилання на джерела, матеріали або окремі результати інших досліджень, що наводяться в роботі. Наведення частин інших робіт без посилання вважається **плагіатом.**

Посилання на джерело в тексті слід зазначати згідно його порядкового номера у списку використаних джерел. Номер джерела виділяють двома квадратними дужками. (***Приклад:*** **«... у працях [1-7]...», «... у праці [10]...”»)**. Якщо дається конкретний текст, тоді необхідно, крім номера джерела, вказати сторінку, чи сторінки, звідки взято текст, ілюстрацію тощо. (***Приклад:*** **[7, с.134], [13, с. 45-46]**).

У можна посилатися на розділи, підрозділи, ілюстрації, таблиці, формули, рівняння, додатки, самої курсового проєкту вказуючи при цьому їхні номери.

Приклад:

«...у розділі 2...»; «...дивися підрозділ 2.4...»;

«...відповідно до підрозділу 2.3...»;

«...на рис. 1.5...»;

«...у табл. 3.2...»;

«...згідно табл. 3.2...» або «...виходячи із табл. 3.2...», «див. табл. 1.3»;

«...(див. табл. 3.2)...»;

«...за формулою (3.5)...»;

«... у рівняннях (1.9)-(1.12)...»; «...у додатку Б...» або «...(додаток Б).»

На всі таблиці повинні бути посилання в тексті, при цьому слово «таблиця» в тексті пишуть скорочено «табл.».

Список використаних джерел

При написанні курсового проєкту мають бути наведені джерела, звідки запозичений матеріал. Вони вказуються у відповідних посиланнях та в

бібліографічному списку. Список використаних джерел повинен бути наведений після висновку з нової сторінки. Джерела у списку слід розміщувати в алфавітному порядку (спочатку джерела кириличним шрифтом, а потім латиницею).

Оформлений список використаних джерел повинен бути згідно діючих державних стандартів. Приклад оформлення списку використаних джерел подано у додатку Г.

Додатки

Додатки оформлюють як продовження курсового проєкту на наступних його сторінках або у вигляді окремої частини, розміщуючи їх у порядку появи посилань у тексті.

Якщо додатки оформлюють на наступних сторінках курсового проєкту, кожний такий додаток повинен починатися з нової сторінки. Додаток повинен мати заголовок, надрукований угорі малими літерами з першої великої симетрично відносно тексту сторінки. Посередині рядка над заголовком малими літерами з першої великої друкується жирним шрифтом слово «Додаток» і велика літера, що позначає додаток (***Приклад:*** **Додаток А**).

Додатки слід позначати послідовно великими літерами української абетки, за винятком літер Ґ, Є, З, І, Ї, Й, О, Ч, Ь. Один додаток позначається як додаток А.

Якщо недостатньо літер для нумерації додатків, продовжують їх нумерувати подвійними літерами таким чином: АА, АБ, АВ, …, БА, ББ і т. д.

Ілюстрації, таблиці, формули та рівняння слід нумерувати в межах кожного додатка (**Приклад: «Рис. А.3» – третій рисунок додатка А;**
«Таблиця А.2» – друга таблиця додатка А; «Формула (А.1)» – перша формула додатка А). Якщо в додатку одна ілюстрація, одна таблиця, одна формула, одне рівняння, їх нумерують: «Рис. А.1», «Таблиця А.1», «Формула В.1».

Якщо додаток має продовження, то продовження додатка пишуть з абзацного відступу рядка з першої великої літери, вказуючи номер додатка і номер таблиці, рисунка або формули (***Приклад***: **«Продовження табл. А.4»,**
«Продовження додатка Б», «Продовження рис. В.2»).

6. ПОРЯДОК ЗАХИСТУ ТА ОЦІНЮВАННЯ КУРСОВОГО ПРОЄКТУ

Захист курсового проєкту проходить відповідно до графіка, затвердженого кафедрою, в присутності комісії у складі керівника та двох-трьох членів кафедри.

Процедура захисту включає:

- ✓ презентацію ілюстративного матеріалу та доповідь автора;
- ✓ запитання до автора;
- ✓ оголошення відгуку наукового керівника або його виступ;
- ✓ відповіді студента на запитання членів комісії із захисту курсового проєкту та осіб, присутніх на захисті;
- ✓ заключне слово студента;
- ✓ рішення комісії про оцінку роботи.

Під час захисту курсового проєкту студент зобов'язаний дати вичерпні відповіді на всі зауваження у відгуках та рецензіях, а також у виступах на захисті.

За результатами захисту курсового проєкту студент отримує оцінку («відмінно», «добре», «задовільно», «незадовільно»), яку викладач виставляє в екзаменаційну відомість.

Оцінку «відмінно» (А) отримує студент, у якого акуратно і правильно оформлений курсовий проєкт, вона містить практичний результат і глибокий аналіз питань обраної теми, висновки про позитивні моменти і недоліки, пропозиції щодо усунення недоліків.

Оцінку «добре» (В, С) одержує студент за роботу, у якій виконані всі зазначені вимоги, але є деякі недоліки методичного характеру, недостатньо аргументовані висновки й пропозиції. Робота має бути виконана правильно й акуратно.

Оцінку «задовільно» (Д, Е) отримує студент, у якого робота містить недостатньо елементів наукового дослідження, неглибокий аналіз, висновки і пропозиції погано аргументовані, текст оформлений неакуратно.

«Незадовільно» (FX, F) оцінюються курсові проєкти, які за змістом і оформленням не відповідають діючим вимогам.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. Монографія Харків, Видавництво Форт, 2012 р.
2. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
3. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.
4. Брюс Шнайер "Прикладная криптография: протоколы, алгоритмы, исходный код на языке С". : Пер. с англ . - СП б . : ООО" Диалектика", 2017 – 1040 с.
5. Свейгарт Эл. Криптография и взлом шифров на Python. : Пер. с англ . - СП б . : ООО" Диалектика", 2020. - 512 с

Допоміжна

1. Н.Смарт Криптография: Пер с англ. – М.:Техносфера, 2005. –525 с.
2. Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с англ. — М.: Издательский дом "Вильямс", 2005. — 424 с.
3. Антоненко О. Криптографічні методи перетворення інформації: навч. посіб. – Бердянськ: БДПУ, 2015. – 180 с
4. Душкин Р.В. Математика и криптография: тайны шифров и логическое мышление. - – М.: Диалектика-Вильямс, 2017. – 288 с.
5. Альбов А.С. Квантовая криптография [Электронный ресурс]. — СПб.: Страта, 2015 .— 248 с. Режим доступу: https://rucont.ru/efd/638845
6. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. – М.: URSS, 2019. – 376 с
7. Васильева И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата. – М.: Юрайт, 2019. - 349с.

Інформаційні ресурси

1. http://dl.tntu.edu.ua Електронні навчальні курси ТНТУ імені І. Пулюя.
2. Форум фахівців інформаційної безпеки https://xss.is
3. https://en.wikipedia.org/wiki/IPsec
4. https://en.wikipedia.org/wiki/HTTPS
5. www.cryptography.com
6. www.nist.gov
7. www.cryptography.org
8. www.iso.org
9. www.financialcryptography.com

Додаток А

Варіанти завдань на курсовий проєкт

1. Засоби автентифікації користувачів за допомогою алгоритму DES.
2. Засоби автентифікації користувачів за допомогою алгоритму ГОСТ.
3. Засоби автентифікації користувачів за допомогою алгоритму AES.
4. Засоби автентифікації користувачів за допомогою алгоритму Threefish.
5. Засоби автентифікації користувачів за допомогою алгоритму ElGamal.
6. Засоби автентифікації користувачів за допомогою алгоритму SEAL.
7. Засоби автентифікації користувачів за допомогою алгоритму Panama.
8. Засоби автентифікації користувачів за допомогою алгоритму ORIX.
9. Засоби автентифікації користувачів за допомогою алгоритму 3DES.
10. Засоби автентифікації користувачів за допомогою алгоритму SOBER.
11. Засоби автентифікації користувачів за допомогою алгоритму PIKE.
12. Засоби автентифікації користувачів за допомогою алгоритму Widemouthed Frog.
13. Засоби автентифікації користувачів за допомогою алгоритму Blowfish.
14. Засоби автентифікації користувачів за допомогою алгоритму асиметричного шифрування McEliece.
15. Засоби автентифікації користувачів за допомогою алгоритму асиметричного шифрування Pohlig-Hellman.
16. Засоби автентифікації користувачів за допомогою алгоритму Serpent.
17. Засоби автентифікації користувачів за допомогою алгоритму MARS.
18. Засоби автентифікації користувачів за допомогою алгоритму RC6.
19. Засоби для шифрування даних за допомогою алгоритму Seal.
20. Засоби для шифрування даних за допомогою регістрів зсуву з нелінійним зворотнім зв’язком.
21. Засоби для шифрування даних за допомогою алгоритму RC5.
22. Засоби для шифрування даних за допомогою алгоритму AES.
23. Засоби для шифрування даних за допомогою алгоритму ГОСТ.
24. Засоби для шифрування даних за допомогою алгоритму Threefish.
25. Засоби для шифрування даних за допомогою алгоритму RSA.

32

26. Засоби для шифрування даних за допомогою алгоритму ElGamal.
27. Засоби для створення електронного цифрового підпису DSA.
28. Засоби для створення електронного цифрового підпису ECDSA.
29. Засоби для створення електронного цифрового підпису ГОСТ.
30. Засоби для автентифікації даних за допомогою алгоритму SHA-3.
31. Засоби для автентифікації даних за допомогою алгоритму Skein.
32. Засоби для автентифікації даних за допомогою алгоритму BMW.
33. Засоби для автентифікації даних за допомогою алгоритму Blake.
34. Засіб захищеного зберігання паролів.

35. Засоби автентифікації користувачів за протоколом Фейга-Шаміра.
36. Засоби автентифікації користувачів за протоколом Шнорра.
37. Засоби автентифікації користувачів за допомогою ключової хешфункції MD2.
38. Засоби генерування та обміну сеансовими ключами за протоколом Діффі-Хеллмана.
39. Засоби генерування та обміну сеансовими ключами за протоколом ECDH
40. Засоби генерування та обміну сеансовими ключами за протоколом "точка-точка".
41. Засоби генерування та обміну сеансовими ключами за протоколом Shamir.
42. Засоби генерування та обміну сеансовими ключами за протоколом Needham-Schroeder.
43. Засоби генерування та обміну сеансовими ключами за протоколом Otway-Rees.
44. Розробка протоколу спільного підписання контракту у разі наявності арбітра.
45. Розробка протоколу групового підписання документу.
46. Розробка протоколу довіреного підписання документу.
47. Розробка протоколу сліпого підписання документу.
48. Розробка протоколу розподілення знання секрету

ДОДАТОК Б
Приклад оформлення титульної сторінки курсового проєкту

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

кафедра кібербезпеки

КУРСОВИЙ ПРОЄКТ

з навчальної дисципліни «Прикладна криптологія» на тему:
«Протокол розділення секрету»

Студента (ки) _____ курсу, групи _____
спеціальності _____

_____
_____
(прізвище та ініціали)

Керівник: _____

_____
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Оцінка за національною шкалою _____

Кількість балів: _____ Оцінка ECTS _____

Члени комісії: _____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

м. Тернопіль – 2021

ДОДАТОК В Бланк завдання на курсову роботу

https://docs.tntu.edu.ua/base/document?id=369

ДОДАТОК Г

Приклад оформлення списку використаних джерел

Характер	Приклад оформлення
КНИЖКОВІ ВИДАННЯ	
Однотомні видання	
Один автор	1. Дорошенко В. «Просвіта»: її заснування і праця : короткий історичний нарис / В. Дорошенко. — Філадельфія : [б. в.], 1959. — 102 с. 2. Тимошик М. Видавничий бізнес: погляд журналіста, видавця, вченого / М. Тимошик. — К. : Наша культура і наука, 2005. — 328 с. — (Серія "Бібліотека видавця, редактора, автора").
Два автори	1. Адаменко І. І. Фізика рідин та рідинних систем : підручник / І. І. Адаменкою, Л. А. Булавін. — К. : [б. в.], 2006. — 660 с. 2. Аксьонова Л. В. Сучасні тести для дівчат / Л. В. Ак-сьонова, В. Т. Гридіна ; пер. з рос. О. А. Росинська. — Донецьк : БАО, 2004. — 416 с. : іл. — (Книга подарунок).
Три автори	1. Панько Т. І. Українське термінознавство : підруч. для студ. гуманітар. спец. вищ. навч. закл. / Т. І. Панько, І. М. Кочан, Г. П. Мацюк. — Львів : Світ, 1994. — 216 с. 2. Тимошик М. Історія одного журналістського курсу в мемуарах, щоденниках, інтерв'ю, замальовках, записках, есеях, документах, світлинах : [навч. посіб.] / Микола Тимошик, Галина Дацюк, Катерина Таран. — К. : Наша культура і наука, 2008. — 478 с.
Чотири автори	1. Методика нормування ресурсів для виробництва продукції рослинництва / Вітвіцький В. В. [та ін.]. — К. : НДІ "Украгропромпродуктивність", 2006. — 106 с. — (Бібліотека спеціаліста АПК. Економічні нормативи). 2. Механізація переробної галузі агропромислового комплексу : [підруч. для учнів проф.-техн. навч. закл.] / О. В. Гвоздєв, Ф. Ю. Ялпачик, Ю. П. Рогач, М. М. Сердюк. — К. : Вища освіта, 2006. — 478, [1] с. — (ПТО: Професійно-технічна освіта).
П'ять і більше авторів	1. Психология менеджмента / [Власов П. К. и др.] ; под ред. Г. С. Никифорова. — [3-е изд.]. — Х. : Гуманитар. центр, 2007. — 510 с. 2. Формування здорового способу життя молоді : навч.-метод. посіб. для працівників соц. служб для сім'ї, дітей та молоді / Т. В. Бондар [та ін.]. — К. : Укр. ін-т соц. дослідж., 2005. — 115 с. — (Серія "Формування здорового способу життя молоді" : у 14 кн., кн. 13).

Без автора ***Збірники***	1. Історія однієї фотографії: спроба самопрезентації / упорядкув., передм. Г. І. Дацюк. — К. : Спадщина, 2007. — 224 с. : іл. 2. Історія Свято-Михайлівського Золотоверхого монастиря / [авт. тексту В. Клос]. — К. : Грані-Т, 2007. — 119 с. — (Грані світу).
Матеріали конференцій, з'їздів	1. Кібернетика в сучасних економічних процесах : зб. текстів виступів на республік. міжвуз. наук.-практ. конф. / Держкомстат України, Ін-т статистики, обліку та аудиту. — К. : ІСОА, 2002. — 147 с. 2. Проблеми обчислювальної механіки і міцності конструк-цій : зб. наук. праць / наук. ред. В. І. Моссаковський. — Дніпропетровськ : Навч. кн., 1999. — 215 с.
Словники	1. Географія : словник-довідник / [авт.-уклад. Ципін В. Л.]. — Х. : Халімон, 2006. — 175, [1] с. 2. Європейський Союз : словник-довідник / [ред.-упоряд. М. Марченко]. — 2-ге вид., оновл. — К. : К.І.С., 2006. — 138 с.
Атласи	1. Україна : екол.-геогр. атлас : присвяч. всесвіт. дню науки в ім'я миру та розвитку згідно з рішенням 31 сесії ген. конф. ЮНЕСКО / [наук. редкол.: С. С. Куруленко та ін.] ; Рада по вивч. продукт. сил України НАН України [та ін.]. — К. : Варта, 2006. — 217, [1] с.
Каталоги	Пам'ятки історії та мистецтва Львівської області : каталог-довідник / [авт.-упоряд. М. Зобків та ін.]. — Львів : Новий час, 2003. — 160 с.
Законодавчі матеріали	1. Кримінально-процесуальний кодекс України : за станом на 1 груд. 2005 р. / Верховна Рада України. — Офіц. вид. — К. : Парлам. вид-во, 2006. — 207 с. — (Бібліотека офіційних видань). 2. Кодекс законів про працю України з постатейними матеріалами : офіц. текст : за станом на 1 черв. 2006 р. : зб. нормат. актів. — К. : Юрінком Інтер, 2006. — 306 с.
Стандарти	1.Видання. Основні види. Терміни та визначення : ДСТУ 3017–95. — [Чинний від 01-01-96]. — К. : Держстандарт України, 1995. — 47 с. — (Національні стандарти України). Бібліографічний запис. Заголовок. Загальні вимоги та правила складання : ДСТУ ГОСТ 7.80:2007. — [Чинний від 04-01-2008]. — К. : Держспоживстандарт України, 2007. — 47 с. — (Національні стандарти України).
Багатотомні видання	
	Багаторівневий опис
Багатотомний документ	1. Історія української культури : у 2 т. / НАН України. — К. : Наукова думка, 2001.

в цілому	Т. 1 : Українська культура XIII — першої половини XVII століть. — 848 с. : іл. Т. 2 : Українська культура другої половини XVII-XVIII століть. — 1246 с. : іл. ***або*** Історія української культури : у 2 т. / НАН України. — К. : Наукова думка, 2001. — Т. 1 : Українська культура XIII — першої половини XVII століть. — 848 с. : іл. — Т. 2 : Українська культура другої половини XVII-XVIII століть. — 1246 с. : іл. ***Примітка**: Відповідно до пункту 6.1.2. стандарту "Після відомостей першого рівня відомості подальших рівнів записують з нового рядка чи в підбір. При записі з нового рядка наприкінці відомостей кожного рівня ставлять крапку. При записі у підбір перед відомостями другого та наступних рівнів ставлять точку і тире".* **Однорівневий опис** 1. Антологія української юридичної думки : в 10 т. / Інститут держави і права ім. В. М. Корецького НАН України ; заг. ред Ю. С. Шемшученко. — К. : Юридична книга, 2002–2004. — 10 т. ***Примітка**: Відповідно до пункту 6.2.6. стандарту на багатотомний документ може бути складено однорівневий бібліографічний опис із обов'язковим зазначенням кількості томів документа.*
Окремий том багатотомного документа	**Під загальною назвою багатотомного документа** ***Багаторівневий опис*** 1. Антологія української юридичної думки : в 10 т. / Інститут держави і права ім. В. М. Корецького НАН України. — К. : Юридична книга, 2002– . — Т. 1 : Загальна теорія держави і права, філософія та енциклопедія права. —2002. — 568 с. ***Однорівневий опис*** Антологія української юридичної думки. В 10 т. Т. 1. Загальна теорія держави і права, філософія та енцикло-педія права / Інститут держави і права ім. В. М. Ко-рецького НАН України. — К. : Юридична книга, 2002. — 568 с. **Під власною назвою тома** Загальна теорія держави і права, філософія та енцикло-педія права / Інститут держави і права ім. В. М. Коре-цького НАН України. — К. : Юридична книга, 2002. — 568 с. — (Антологія української юридичної думки : в 10 т. / Інститут держави і права ім. В. М. Корецького НАН України ; т. 1). ***Примітка**: Відповідно до пункту 6.2.7. стандарту на окремий том багатотомного документа може бути складений як багаторівневий, так і однорівневий бібліографічний опис під загальною назвою багатотомного документа або під власною назвою тома. **Варіант можна обирати самостійно.***

НЕОПУБЛІКОВАНІ ДОКУМЕНТИ	
Препринти	1. Шиляев Б. А. Расчеты параметров радиационного повреждения материалов нейтронами источника ННЦ ХФТИ/ANL USA с подкритической сборкой, управляемой ускорителем электронов / Шиляев Б. А., Воеводин В. Н. — Х. ННЦ ХФТИ, 2006. — 19 с. — (Препринт / НАН Украины, Нац. науч. центр "Харьк. физ.-техн. ин-т" ; ХФТИ 2006-4). 2. Панасюк М. І. Про точність визначення активності твердих радіоактивних відходів гамма-методами / Панасюк М. І., Скорбун А. Д., Сплошной Б. М. — Чорнобиль : Ін-т пробл. безпеки АЕС НАН України, 2006. — 7, [1] с. — (Препринт / НАН України, Ін-т пробл. безпеки АЕС ; 06-1).
Депоновані наукові праці	1. Социологическое исследование малых групп населения / В. И. Иванов [и др.] ; М-во образования Рос. Федерации, Финансовая академия. – М., 2002. – 110 с. – Деп. в ВИНИТИ 13.06.02, № 145432. 2. Разумовский, В. А. Управление маркетинговыми исследованиями в регионе / В. А. Разумовский, Д. А. Андреев. – М., 2002. – 210 с. – Деп. в ИНИОН Рос. акад. наук 15.02.02, № 139876.
Дисертації	1. Копистинська І. Тенденції сучасного вітчизняного книговидання: організаційний, тематичний та реклам-но-промоційний аспекти (1991–2003 рр.) : дис. ... канд. філол. наук: 10.01.08 / Копистинська Ірина Михайлівна. — К., 2004. — 223 с.
Автореферати дисертацій	1. Новосад І. Я. Технологічне забезпечення виготовлення секцій робочих органів гнучких гвинтових конвеєрів : автореф. дис. … канд. техн. наук : 05.02.08 / Іван Якович Новосад. — Тернопіль, 2007. — 20, [1] с.
Авторські свідоцтва	1. А. с. 1007970 СССР, МКИ[3] В 25 J 15/00. Устройство для захвата неориентированных деталей типа валов / В. С. Ваулин, В. Г. Кемайкин (СССР). – № 3360585/25–08 ; заявл. 23.11.81 ; опубл. 30.03.83, Бюл. № 12.
Патенти	1. Пат. 2187888 Российская Федерация, МПК[7] H 04 B 1/38, H 04 J 13/00. Приемопередающее устройство / Чугаева В.И.; заявитель и патентообладатель Воронеж. науч.-исслед. ин-т связи. – № 2000131736/09 ; заявл. 18.12.00 ; опубл. 20.08.02, Бюл. № 23 (II ч.).
ЧАСТИНА КНИГИ, ПЕРІОДИЧНОГО, ПРОДОВЖУВАНОГО ВИДАННЯ	

Один автор	1. Козіна Ж. Л. Теоретичні основи і результати практичного застосування системного аналізу в наукових дослідженнях в області спортивних ігор // Теорія та методика фізичного виховання. — 2007. — № 6. — С. 15—18, 35—38.
Два автори	2. Гранчак Т. Інформаційно-аналітичні структури бібліотек в умовах демократичних перетворень / Тетяна Гранчак, Валерій Горовий // Бібліотечний вісник. — 2006. — № 6. — С. 14—17.
Чотири і більше авторів	3. Регіональні особливості смертності населення України / Л. А. Чепелевська [та ін.] // Вісник соціальної гігієни та організації охорони здоров'я України. — 2007. — № 1. — С. 25—29.
ЕЛЕКТРОННІ РЕСУРСИ	
Електронний ресурс локального доступа (на компакт-диску CD, DVD)	1. Богомольний Б. Р. Медицина екстремальних ситуацій [Електронний ресурс] : навч. посіб. для студ. мед. вузів III—IV рівнів акредитації / Б. Р. Богомольний, В. В. Кононенко, П. М. Чуєв. — 80 Min / 700 MB. — Одеса : Одес. мед. ун-т, 2003. — (Бібліотека студента-медика) — 1 електрон. опт. диск (CD-ROM). — Систем. вимоги: Pentium ; 32 Mb RAM ; Windows 95, 98, 2000, XP ; MS Word 97-2000.— Назва з контейнера. 2. Розподіл населення найбільш численних національностей за статтю та віком, шлюбним станом, мовними ознаками та рівнем освіти [Електронний ресурс] : за даними Всеукр. перепису населення 2001 р. / Держ. ком. статистики Украї-ни ; ред. О. Г. Осауленко. — К. : CD-вид-во "Інфодиск", 2004. — 1 електрон. опт. диск (CD-ROM) : кольор. ; 12 см. — (Всеукр. перепис населення, 2001). — Систем. вимоги: Pentium-266 ; 32 Mb RAM ; CD-ROM Windows 98/2000/NT/XP. — Назва з титул. екрану.

Електронні ресурси віддаленого доступа	***Опис сайта в цілому*** 1. Национальный информационно-библиотечный центр «ЛИБНЕТ» [Электронный ресурс] / М-во культуры РФ, Рос. гос. б-ка, Рос. нац. б-ка. – М. : Центр «ЛИБНЕТ», 2004. — Режим доступа: http://www.nilc.ru/, для доступа к информ. ресурсам требуется авторизация. — Назва з екрану. ***Опис електронного видання (журналу, книги, розміщених в Інтернет)*** 1. Український пульмонологічний журнал. — 2008. — № 2. — Режим доступу до журн.: http://www.ifp.kiev.ua/doc/journals/upj/08/pdf08-2/72.pdf (16.05.09). — Назва з екрану. 2. ДСТУ ГОСТ 7.1:2006. Бібліографічний запис, бібліографічний опис. Загальні вимоги та правила складання [Електронний ресурс] : метод. рекомендації з впровадження / Міністерство освіти і науки України, Львівський Національний університет імені Івана Франка, Наукова бібліотека ; уклад. Галевич О. К., Штогрин І. М. – Львів, 2008. — 20 с. — Режим доступу до вид.: http://www.franko.lviv.ua/library/doc/metodychka. pdf (16.05.2009). — Назва з екрану.
	Опис частини електронного видання (сторінки, статті із журналу, книги, розміщених в Інтернет) 1. Нові вимоги до оформлення бібліографічного опису літературних джерел [Електронний ресурс] // Український пульмонологічний журнал. — 2008. — № 2. — С. 72. — Режим доступу до журн.: http://www.ifp.kiev.ua/doc/journals/upj/08/pdf08-2/72.pdf (16.05.09). — Назва з екрану. 2. Бібліотека і доступність інформації у сучасному світі: електронні ресурси в науці, культурі та освіті : (підсумки 10-ї Міжнар. конф. „Крим-2003") [Електронний ресурс] / Л. Й. Костенко, А. О. Чекмарьов, А. Г. Бровкін, І. А. Павлуша // Бібліотечний вісник — 2003. — № 4. — С. 43. — Режим доступу до журн.: http:// www.nbuv.gov.ua/articles/2003/03klinko.htm (16.05.09). — Назва з екрану. ***Опис частини сайту (інформації, розміщеної на одній із сторінок сайту)*** 1. Гетте Н. Типология журналов [Электронний ресурс] // Журнальний зал: культура, искусство, литература : [сайт] / Н. Гете, И. Телятникова ; Омский государственный університет. — Режим доступа: http://www.univer.omsk.su/omsk/bibstuds/jourhall/page1.htm (13.05.09). — Загл. с экрана. 2. Справочники по полупроводниковым приборам // [Персональная страница В. Р. Козака] / Ин-т ядер. физики. [Новосибирск, 2004-2008]. – Режим доступа: http://www.inp.nsk.su/~kozak/start.htm (13.03.06). — Загл.

	с экрана. 3. ГОСТ 7.82–2001. Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления [Електронний ресурс] // Нормативная база ГСНТИ : [сайт] / НТЦ «Информрегистр». — М. : ГСНТИ, 1998—. — Режим доступа: http://www.gsntinorms.ru/norms/common/ doc.asp?0& / norms/ stands/7_82.htm (16.05.2009). — Загл. с экрана. — Сайт обновлен 3 декабря 2004 г.

Примітки:

1. Усі умовні розділові знаки, котрі відділяють окремі зони чи елементи у межах зон бібліографічного опису (за винятком граматичної пунктуації у назві видання) відділяються проміжками з двох сторін.
2. Якщо видання має лише одного автора, його прізвище все одно повторюється в області відповідальності після скісної лінії.
3. Дані, котрі взяті не з титульного аркуша книжкового видання, беруться у квадратні дужки. Так, у квадратних дужках потрібно писати відомості про упорядників, авторів, вид видання, котрі наведені на звороті титульного аркуша. У квадратні дужки береться також вся інформація, котра взята не безпосередньо з видання, а встановлена самостійно на основі аналізу видання.
4. Усі частини бібліографічного опису, крім перших слів нових зон бібліографічного опису та власних назв, пишуться з малої літери. Таким чином, додаткові відомості про назву (підручник, посібник тощо), інформація про відповідальність (автор-упорядник, редактор) потрібно писати з малої літери.