Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

А. М. Гребенюк, Е. В. Рижков,
Ю. П. Синиціна, С. О. Прокопов

ІНФОРМАЦІЙНІ ТА КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

Навчальний посібник

Дніпро
2023

УДК 004
І-74

Рекомендовано до друку
Навчально-методичною радою
Дніпропетровського державного
університету внутрішніх справ
(протокол № 10 від 20 червня 2023 р.)

РЕЦЕНЗЕНТИ:

Володимир СЕНИК – завідувач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент;

Юрій ГРИЦЮК – професор кафедри програмного забезпечення Національного університету «Львівська політехніка», доктор технічних наук, професор.

І-74 Інформаційні та комунікаційні технології : навч. посіб. / А. М. Гребенюк, Е. В. Рижков Ю. П. Синиціна, С. О. Прокопов. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2023. 337 с.

ISBN 978-617-560-017-7

Навчальний посібник призначено для вивчення дисциплін «Інформаційні та комунікаційні технології». Зміст навчального посібника розроблено у відповідності до вимог Типових освітніх програм за відповідними спеціальностями та робочих навчальних програм вивчення дисципліни. Передбачається отримання здобувачами сукупності теоретичних і практичних знань, навичок і вмінь щодо використання інформаційних та комунікаційних технологій у професійній діяльності. Розраховано на здобувачів першого (бакалаврського рівня) за спеціальностями 081 «Право» і 262 «Правоохоронна діяльність». Даний посібник може бути використаний під час підготовки практичних працівників Національної поліції.

ISBN 978-617-627-148-2

ЗМІСТ

ВСТУП

Інформаційні та комунікаційні технології у сучасному суспільстві є звичними але визначальними за багатьма напрямками діяльності людства.

Не є виключенням і їх значення у діяльності представників правоохоронних органів, в тому числі Національної поліції.

Починаючи від організації і здійснення діловодства, реєстрації протиправних діянь, використання спеціалізованих поштових сервісі, складання звітів із використанням інструментів демонстраційного характеру, використання хмарного середовища, а також безліч інших можливостей у сфері правоохоронної діяльності – все це повсякденні приклади реалізації сучасних можливостей інформаційних та комунікаційних технологій. Деякі з них є універсальними для всіх користувачів комп'ютерної техніки та інших технічних гаджетів. Але є і специфічні, притаманні переважно або виключно суб'єктам правоохоронної діяльності.

Вивчення навчального курсу призначено розширити горизонт уяви здобувачів про функціональні можливості стандартного програмного забезпечення сучасної інформаційної техніки та сформувати у них навички його використання для потреб служб та підрозділів Національної поліції, а також скласти уяву та надати первинний досвід про комунікаційні потреби, можливості та буденні приклади діяльності суб'єктів МВС України.

Взагалі, представлений матеріал навчального посібника здатен сформувати у здобувачів корисні навички використання сучасних інформаційних та комунікаційних технологій, які у свою чергу значно підвищать ефективність їх подальшої діяльності як суб'єктів реалізації правоохоронної функції.

Посібник може бути в нагоді науковим, науково-педагогічним працівникам, здобувачам вищої освіти закладів зі специфічними умовами навчання, практичним працівникам Національної поліції та всім, хто цікавиться питаннями сучасних можливостей інформаційних та комунікаційних технологій.

Розділ 1
СУЧАСНИЙ СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОГО ТА КОМУНІКАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

1.1. Технічне та програмне забезпечення комп'ютерних систем

Розвиток комп'ютерної техніки відбувається стрімко, у геометричній прогресії. Насамперед вона призначена для реалізації обробки та зберігання інформації і є базою для об'єднання усіх сучасних технічних засобів управління інформаційними ресурсами.

Згідно з енциклопедичним словником, технічне забезпечення (апаратне забезпечення, англ. hardware) – сукупність електричних, електронних та механічних компонентів комп'ютера.

Розглянемо, яким чином побудований комп'ютер. Більшість сучасних комп'ютерів побудовані за принципів, що описаний Джорджем фон Нейманом ще в 1945 році. Його основні складові – процесор, запам'ятовуючі пристрої та пристрій вводу-виводу.

На основній (системній або материнській) платі комп'ютера розташовані блоки, що здійснюють обробку інформації та роз'єми для додаткових блоків, що відповідають за інші пристрої комп'ютера. До всіх елементів підводиться електроживлення з блоку живлення.

Головним елементом комп'ютера є процесор. Основною його характеристикою є тактова частота, що відповідає кількості елементарних операція, що виконуються за секунду часу. Процесор включає в себе блок керування та арифметико-логічні пристрій (АЛП). Основна задача АЛП – виконувати всілякі логічні та арифметичні дії для обробки інформації, що зберігається в ПК; керуючий пристрій – забезпечує керування та контроль всіх складових комп'ютера.

Запам'ятовуючі пристрої забезпечує зберігання вихідної та проміжної інформації в двійковій формі (тобто у вигляді нулів та одиниць). Вони мають оперативні (ОЗУ), постійні (ПЗУ) та зовнішні (ЗЗУ) запам'ятовуючі пристрої. Оперативні запам'ятовуючі пристрої зберігаються інформацію, що безпосередньо використовує комп'ютер. Тільки ця інформації оперативно доступна процесору.

Зовнішні запам'ятовуючі пристрої (наприклад жорсткий диск чи

вінчестер), має значно більшу ємність, але повільніший доступ. Наразівін використовується для зберігання інформації великих розмірів.

Постійні запам'ятовуючі пристрої використовуються для зберігання інформації, яка записується при виготовленні пристрою («прошивка»).

У якості пристроїв вводу частіше за все використовують мишу та клавіатуру, а пристроїв виводу – монітор, принтер тощо.

Робота комп'ютера передбачає поєднання апаратного та програмного забезпечення. Програмне забезпечення (програмні засоби, англ. software) – це комплект комп'ютерних програм і файлів з даними, безяких комп'ютер не зможе функціонувати.

Усе програмне забезпечення умовно можна поділити на системне, спеціальне та прикладне.

1. Системне програмне забезпечення – це сукупність програм які забезпечують керування компонентами комп'ютерної системи, таким як процесор, оперативна пам'ять, пристрій вводу-виводу та ін., тим самим виступаючи посередником між апаратурою та користувачем. Воно не виконує конкретних практичних задач, а забезпечує роботу інших програм.

Системне програмне забезпечення поділяється на:

– базове (операційні системи, оболонки та мережева операційна система);

– сервісне (утиліти та антивірусні програми).

Зазначимо, що утиліти – це програми, що служать для обслуговування комп'ютера та виконують допоміжні операції обробки даних, прикладом чого можуть бути діагностика апаратних і програмних засобів, оптимізації дискового простору, що використовується та ін..

2. Спеціальне програмне забезпечення – сукупність програм для обробки, налагодження та впровадження нових програмних продуктів (транслятори, середа розробки програм, редактори зв'язку та ін.)

3. Прикладне програмне забезпечення – сукупність програм для забезпечення автоматизації розробки та експлуатації функціональних задач користувача та інформаційних систем в цілому. До цього класу програмного забезпечення відносять: текстові та графічні редактори, електроні таблиці, системи управління базами даних та ін.

1.2. Основні принципи створення інформаційних об'єктів у середовищі операційної системи MS Windows і програмного комплексу MS Office

Створення електронних документів програмно-технічними засобами забезпечує автентичність, достовірність, цілісність та придатність до використання.

Переважно електронне документування здійснюється на базі операційної системи MS Windows і програмного комплексу MS Office, що включає в себе:

– редактор текстів – Microsoft Word;
– електронну таблицю – Microsoft Excel;
– програму для створення слайдів і мультимедіа-презентацій – Microsoft PowerPoint;
– систему управління базами даних – Microsoft Access;
– інформаційну систему для роботи з електронною поштою – Microsoft Outlook;
– інші продукти і можливості (OneNote, Publisher, Lync, Project, Visio, InfoPath.

У додатках Office містяться стандартні команди, основні операції для спільної роботи, шаблони документів, які можна використовувати при створенні юридичних документів, службових записок, листів, факсів, звітів, довідників, бюлетенів, розкладів, порядків денних і т.п. Окрім шаблонів під час створення нових документів в Office передбачено можливість використання так званого майстра – спеціального автоматизованого документу.

Серед безлічі програм для редагування тексту документів, що використовуються в організаціях, найпопулярнішим є текстовий редактор Microsoft Word. Він дозволяє:

– виводити текст редагованого документа на екран;
– вносити до нього зміни, доповнення, виправлення;
– переставляти місцями фрагменти тексту;
– автоматично перевіряти орфографію;
– використовувати різні шрифти;
– збагачувати текст таблицями, малюнками, діаграмами та ін .;
– працювати одночасно з декількома документами;
– переносити фрагменти одного документа в інший.

Незважаючи на всі переваги Microsoft Office у наш час усе більша кількість людей використовує замість нього сервіс Google Docs , мова про який піде далі.

1.3. Методи роботи в онлайн сервісі Google Docs, комп'ютерних мережах локального та глобального типу

Google Docs – це текстовий редактор, що дозволяє створювати та форматувати документи, а також працювати над ними сумісно з іншими користувачами.

Зовнішньо Google Docs дуже схожий на MS Office Word, але й має ряд відміностей. Так, перевагами Google Docs порівняно з MS Office є такі:

– безкоштовно;

– хмарне зберігання навіть якщо персональний комп'ютер зламається, буде можливість працювати з документами;

– зручній обмін файлами – немає необхідності заливати весь файл,достатньо просто відправити посилання;

– колективна праця над одним і тим самим документом одночасно може працювати декілька чоловік;

– голосове ведення;

– кросплатформеність можливість роботи в будь-якійопераційній системі.

Недоліки:

– повільна робота – особливо з великими документами та при повільному Інтернеті;

– залежність від аканту – усі документи прив'язання до вашогогугл-акаунту, загубили доступ до аканту – загубили документи;

– залежить від Інтернету – за/за умови відсутності доступу ви не зможетенічого відкрити.

Отже, відмінності між Google Docs і MS Office Wordполягає у тому, що перші пристосовані для роботи в Інтернеті, а другі більше пристосовані для роботи в корпоративних мережах. Розглянемо ці явища докладніше.

Комп'ютерна мережа – це система зв'язку комп'ютерів чи комп'ютерного обладнання.

Усі комп'ютерні мережі мають одне єдине призначення – забезпечення спільного доступу до загальних ресурсів. Зазвичай виділяють три можливих види ресурсів: апаратні, програмні та інформаційні. Наприклад, принтер – це апаратний ресурс. Коли всі учасники невеличкої групи (наприклад, співробітники офісу), використовують загальний принтер, це значить, що вони використовують єдиний загальний ресурс.

Окрім апаратних ресурсів, можливо використовувати програмні. Зокрема, для розв'язування складної математичної задачі можна підключитися до більш потужного ПК і відправити розрахунки до нього.

Дані, що зберігаються на віддаленому комп'ютері, створюють інформаційний ресурс. Найбільш яскравий приклад – Інтернет, який в першу чергу представляє собою інформаційно-довідкову систему.

Комп'ютерні мережі дозволяють об'єднувати інформацію незалежно від відстані між комп'ютерами. Отже, залежно від фізичного розташування комп'ютерні мережі поділяються на: локальні, корпоративні та глобальні.

1. Локальні комп'ютерні мережі об'єднають комп'ютери, що знаходяться поблизу один від одного. Такі мережі дозволяють:
   – сумісно використовувати апаратні ресурси;
   – сумісно використовувати програмні ресурси;
   – створювати та сумісно використовувати інформаційні ресурси;
   – централізувати заходи по інформаційній безпеці.
2. Корпоративна мережа – це об'єднання комп'ютерів у межах однієї організації.
3. Глобальна мережа – це об'єднання комп'ютерів, що розташовані на великій відстані для загального використання світових інформаційних ресурсів. Найбільш відомою глобальною мережею є Інтернет. Однією з причин створення технології Інтернет була необхідність в мережі, що буде стійкою до часткових пошкоджень. Це можливо було зробити за рахунок децентралізації обробки інформації. Тобто, основу глобальних мереж складають потужні вузли зв'язку – хост- комп'ютери, що поєднані між собою. За несправності одного з вузлів інформація посилається через інший вузол, таким чином забезпечуючи роботу усієї системи.

1.4. Безпека та захист в інформаційних системах

Проблема інформаційної безпеки виникла в результаті зростання ролі інформації в сучасному суспільству.

Інформаційна безпека – це міра захисту інформації та інфраструктури, що її підтримує від випадкових чи навмисних впливів, що можуть спричинити збиток власникам чи користувачам інформацією.

Під захистом інформації мається на увазі комплекс мір, що

спрямований на забезпечення інформаційної безпеки. Для цього зазвичай розв’язують три задачі:

– забезпечення доступності інформації;
– забезпечення цілісності інформації;
– забезпечення конфіденційності інформації.

Доступність інформації – це гарантія отримання інформації, що потребується, чи інформаційної послуги користувачем за визначений час.

Цілісність інформації – це гарантія того, що інформація існує в її початковому вигляді, тобто під час її збереження чи передачі не було несанкціонованих змін.

Конфіденційність інформації – це гарантія доступності конкретної інформації лише тим людям, для яких вона призначена.

Режим інформаційної безпеки включає три рівні:

– законодавчо-правовий,
– адміністративний,
– програмно-технічний.

Законодавчо-правовий рівень включає комплекс законодавчих та інших правових актів, що встановлюють статус суб’єктів інформаційних відносин, суб’єктів та об’єктів захисту, методи, форми та способи захисту, їх правовий статус.

Адміністративний рівень включає комплекс заходів та технічних мір, що реалізують практичні механізми захисту в процесі створення та експлуатації систем захисту інформації.

Програмно-технічний рівень включає три підрівня: фізичний, технічний (апаратний) та програмний.

Фізичний підрівень вирішує завдання з обмеженням фізичного доступу до інформації та інформаційних систем, відповідно до нього ставляться технічні засоби, що реалізуються у вигляді автономних пристроїв і систем, наприклад, системи охоронної сигналізації, системи спостереження та ін.

До апаратних засобів відносяться схеми контролю інформації по парності, схеми доступу по ключу і т.д. До програмних засобів захисту, що створює програмний підрівень, належать наразі спеціальне програмне забезпечення, що використовується для захисту інформації, наприклад, антивірусний пакет.

Загроза інформаційної безпеки – це потенційна можливість порушення режиму інформаційної безпеки. Навмисна реалізація загрози називається атакою на інформаційну систему, а особа, яка реалізувала таку загрозу – зловмисником.

Несанкціонований доступ є основним із найбільш розповсюджений способів впливу на інформаційну систему, що дозволяє нанести шкоду будь-якій із складових інформаційної безпеки.

Комп'ютерні віруси – це одна з основних загроз інформаційної безпеки. Сучасний комп'ютерний вірус – це практично непомітний для звичайного користувача ворог, що завжди удосконалюється, знаходячи все нові і більш витончені способи проникнення на комп'ютери користувачів. Необхідність боротьби з комп'ютерними вірусами обумовлена можливістю порушення ними всіх складових інформаційної безпеки. І, на жаль, антивірусні програми та апаратні засоби, не дають повної гарантії захисту відвірусів.

За деструктивними можливостями віруси поділяються на:

– нешкідливі, тобто такі, що жодним чином не впливають на роботу комп'ютера (крім зменшення вільної пам'яті на диску в результаті свого поширення);

– безпечні, вплив яких обмежується зменшенням вільної пам'яті на диску;

– небезпечні віруси, що можуть привести до серйозних збоїв у роботі комп'ютера;

– дуже небезпечні, в алгоритм роботи яких свідомо закладені процедури, які можуть привести до втрати програм, знищити дані, стерти необхідну для роботи комп'ютера інформацію, записану в системних областях пам'яті, і навіть пошкодити апаратні засоби комп'ютера.

Надійний захист від вірусів може бути забезпечений комплексним застосуванням апаратних і програмних засобів і, що важливо, дотриманням елементарної «комп'ютерної гігієни».

Профілактика комп'ютерних вірусів починається з виявлення шляхів проникнення вірусу в комп'ютер і комп'ютерні мережі. Основними шляхами проникнення вірусів до комп'ютерів користувачів є: глобальні та локальні мережі, піратське програмне забезпечення, персональні комп'ютери «загального користування», сервісні служби. Основне джерело вірусів на сьогоднішній день – глобальна мережа Інтернет. Найбільше число заражень вірусом відбувається при обміні електронними листами через поштові сервери E-mail. Для виключення зараження вірусами необхідно уважно ставитеся до програм і документів, що надходять із глобальних мереж. Перш ніж запустити файл на виконання або відкрити документ, обов'язково потрібно/слід його перевірити на наявність вірусів. Маємо використовувати спеціалізовані антивіруси для перевірки «нальоту» всіх файлів, що

надходять електронною поштою (і з Інтернету в цілому) та постійно оновлювати антивірусні програми (Додаток А).

1.5. Правила захисту від комп'ютерних вірусів

1. Уважно ставтеся до програм і документів, що отримуєте з глобальних мереж.
2. Перед тим, як запустити файл на виконання або відкрити документ, обов'язково перевірте його на наявність вірусів.
3. Використовуйте спеціалізовані антивіруси – для перевірки «на льоту» (наприклад, SpIDer Guard з пакета Dr. Web і ін.) всіх файлів, що приходять по електронній пошті (і з Інтернету в цілому).
4. Регулярно перевіряйте комп'ютер звичайними антивірусними програмами, для зручності і системності використовуйте планувальник завдань.
5. Використовуйте ліцензійне програмне забезпечення, придбане вофіційних продавців.
6. Дистрибутиви копій програмного забезпечення (зокрема, копій операційної системи) слід зберігати на захищених від записування дисках.
7. Користуйтеся лише джерелами програм та інших файлів, що добре себе зарекомендували.
8. Постійно оновлюйте вірусні бази використовуваного антивірусу.
9. Намагайтеся не запускається неперевірені файли, зокрема, отримані з комп'ютерної мережі. Перед запуском нових програм обов'язково перевірте їх одним або декількома антивірусами.
10. Обмежте (по можливості) коло осіб, допущених до роботи на конкретному комп'ютері.
11. Користуйтеся утилітою перевірки цілісності інформації. Такі утиліти зберігають у спеціальних базах даних інформацію про системні області дисків (або цілком системні області) та інформацію про файли (контрольні суми, розміри, атрибути, дати останньої модифікації файлів і т.д.). Періодично зберігайте на зовнішньому носії файли, з яким ведеться робота.

12.15. Під час роботи з Word / Excel умикайте захист від макросів, що доповідає про присутність макросу в документі, який відкривається, і надає можливість заборонити цей макрос.

Джерела до розділу 1

1. Закон України «Про Національну поліцію» (ВВР), 2015, № 40-41, Ст. 379.
2. Закон України «Про інформацію» від 02.10.1992 за № 2657-XII.
3. Закон України «Про доступ до публічної інформації» від 13.01.2011 за № 2939-VI.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 за № 2594-IV.
5. Закон України «Про захист персональних даних» від 01.06.2010 за № 2297-VI.
6. Закон України «Про засади запобігання і протидії корупції» від 07.04.2011 за № 3206-VI.
7. Закон України «Про захист інформації в автоматизованих системах» від 05.07.1994 за № 80/94-ВР.
8. Постанова Кабінету Міністрів України «Про затвердження Положення про єдину інформаційну систему МВС та переліку її пріоритетних інформаційних ресурсів» від 14.11.2018 за № 1024.
9. Наказ МВС України «Про затвердження положення про ІТС Інформаційний портал Національної поліції України» від 03.08.2017 за № 595.
10. Наказ МВС від 14.06.2019 № 508 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».
11. Наказ НПУ від 12.02.19 №141 « Про організацію використання систем відеоспостереження органами (підрозділами) поліції» є Доручення НПУ від 29.07.2017 № 7407/07/20-2017 «Про затвердження Методичних рекомендацій щодо порядку формування інформаційної підсистеми «Масові заходи» ІПНП України».
12. Наказ НПУ від 28.12.2018 № 1227 «Про деякі питання щодо введення окремих обліків в ІТС »Інформаційний портал НПУ».
13. Наказ НПУ від 22.05.2018 № 509 «Про організацію інформаційного обліку комп'ютерної техніки та комп'ютерних програм, що використовуються в органах та підрозділах поліції».
14. СТ НПУ від 28.12.2019 № 15392/20/27-2019 «Про надання доступу до інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції» .
15. Інформаційні системи та технології : підруч. / В. Б. Вишня, Є. В. Рижков, В. О. Мирошниченко, Ю. П. Синиціна, О. Д. Станіна. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 280 с.
16. Інформаційне забезпечення юридичної діяльності: підруч. /кол. авт.;

за заг. ред. д.т.н., проф. В. Б. Вишні. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 228 с.

17. Вишня В. Б. Основи інформаційної безпеки : навч. посіб. / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : ДДУВС, 2020. 128 с.

18. Спеціальна техніка в правоохоронній діяльності : навч. посібник / Ю. П. Синиціна, С. О. Прокопов, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 244 с.; іл.

19. Косиченко О. О. Правові інформаційні ресурси Інтернет: довідник. Дніпро: ДДУВС, 2017. 64 с., іл.

20. Косиченко О. О., Махницький О. В. Інформаційне забезпечення юридичної діяльності: навчальний посібник. Дніпро: Дніпропетровський державний внутрішніх справ, 2018. 245 с.

21. Впровадження сучасних систем цифрового радіозв'язку у підрозділах Національної поліції : наук.-практ. рекоменд. / В. О. Мирошниченко, С. О. Прокопов, Е. В. Рижков, Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 29 с.

22. Захист інформаційних ресурсів підрозділів Національної поліції місцевого рівня: методичні рекомендації / О. С. Гавриш, О. В. Махницький, С. О. Прокопов, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2018. 34 с.

23. Синиціна Ю. П., Станіна О. Д. Обґрунтування актуальності цифрової комунікація закладів вищої освіти (Rationale for the relevance of digital communication in higher education institutions) Міжн. колект.моногр. / Selected aspects of digital society development «Digital Economyand Digital Society» III Міжнародна конференція (28-29 травня 2021 р.) – Katowice, University of Technology, Poland, 2021.mon # 45 – 148- 156 с ISBN 978 – 83 – 960717 – 1 – 2.

24. Синиціна Ю. П., Рижков Е. В., Станіна О. Д. Штучний інтелект: що змінилося за 50 років. Theoretical foundations of engineering. Tasks and problems: collective monograph / Boiko T., Boiko P., – etc. – International Science Group. – Boston : Primedia eLaunch, 2021. 485 p. Available at : DOI-10.46299/ISG.2021.MONO.44TECH.III URL : https://isg-konf.com/ru/theoretical-foundations-of-engineering-tasks-and-problems-ru/.

Розділ 2
РОБОТА ЗІ СЛУЖБОВИМИ ДОКУМЕНТАМИ ЗА ДОПОМОГОЮ ТЕКСТОВОГО ПРОЦЕСОРА MS WORD

2.1. Вивчення методів створення шаблонів типових документів WORD з використанням полів форм

Робота з текстом Параметри сторінки визначають розміри полів, орієнтацію сторінки та інше. Значення деяких параметрів сторінки можна налаштувати командами розділу Параметри сторінки (рис. 2.1) на вкладці Макет (Разметка страницы), але найбільш повно налаштування цих параметрів здійснюється в діалоговому вікні (рис. 2.2), що викликається подвійним клацанням по затемненій частині лінійки в режимі розмітки документа (рис. 2.1).

Зміни параметрів відразу відображаються на зразку сторінки документа, який відображається в нижній частині діалогу (рис. 2.1). Щоб знову встановлені значення параметрів використовувалися за замовчуванням для всіх нових документів, необхідно натиснути кнопку «За замовчуванням»(рис. 2.1) і в діалозі підтвердити внесення змін до шаблону NORMAL.

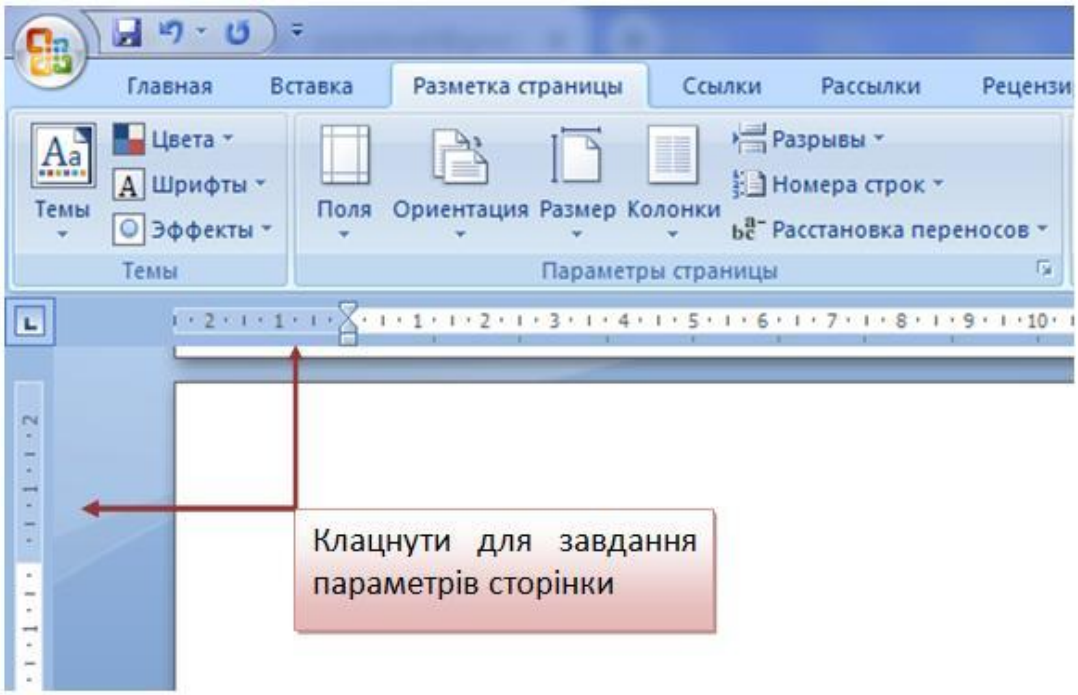


Рис. 2.1. Параметри сторінки на вкладці

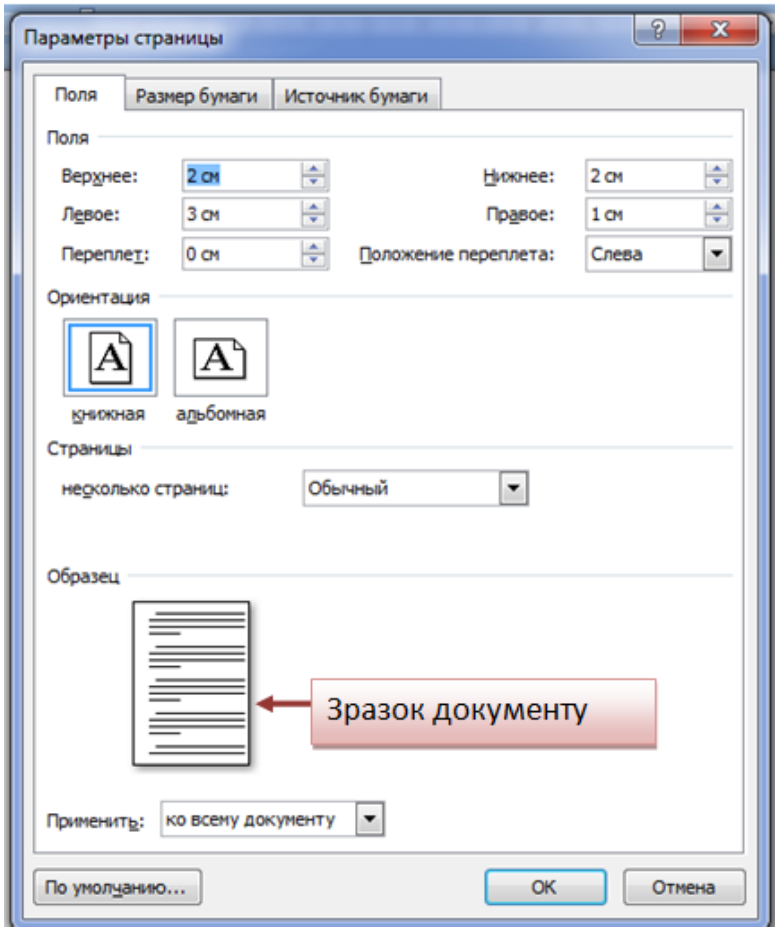


Рис. 2.2. Загальний вигляд діалогового вікна
для налаштування параметрів сторінки

Параметри абзацу (відступи). Параметри абзацу встановлюються в діалозі (рис. 2.3), що відкривається після клацання по стрілці в нижньому правому кутірозділу Абзац вкладки Основна (Главная) (рис. 2.4).

Підчасналаштуванняпараметрів абзацуможна встановити такі значення:

– величину відступу зліва (від лівого поля);
– величину відступу праворуч (від правого поля);
– величину відступу першого рядкаабзацу;
– величину інтервалу між абзацами;
– величину інтервалу між рядками.

Для друкованих документів величину відступу для основного тексту зазвичай не ставлять (необхідне положення тексту визначається шириною полів), але його ставлять для допоміжних матеріалів і назв, якщо вони не вирівнюються по центру. Роль інтервалів полягає в тому,

щоб візуально виділити абзаци. Для документів простої структури використовують відступ першого рядка. Це особливо важливо для текстів і для документів складної структури (науково-технічних). Також використовують відступи між абзацами.

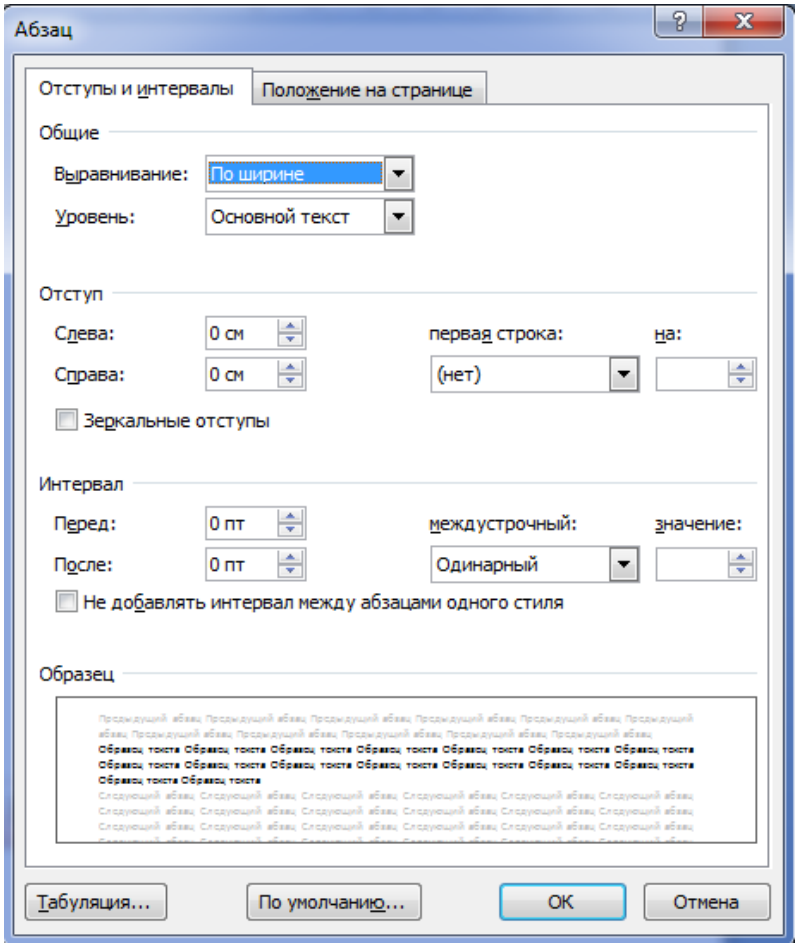


Рис. 2.3. Параметри абзацу

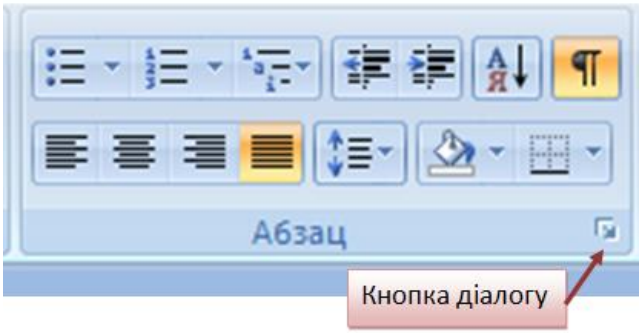


Рис. 2.4. Загальний вигляд кнопки діалогу

Міжрядковий інтервал можна задати кратним розміру рядка (одинарний, полуторний або подвійний), або можна вказати точне значення інтервалу. Важливим є вирівнювання тексту по ширині сторінки. Керування вирівнюванням тексту здійснюється кнопками (рис. 2.4, 2.5), що розташовані в групі Абзац на вкладці Основне (Главная). Усі знов встановлені параметри автоматично відображаються на зразку в нижній частині діалогу.

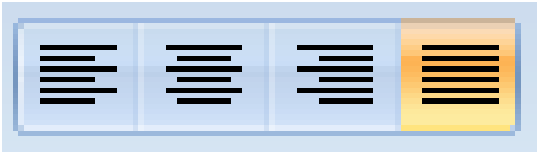


Рис. 2.5. Керування вирівнюваннямтексту

Створення електронних форм службових документів

У сучасному діловодстві спостерігається тенденція до стандартизації документів. Велику частину документообігу складають *форми*, тобто типові документи, у яких змінюються тільки окремі поля, а основна частина залишається незмінною. Текстовий редактор MS Word підтримує роботу з трьома видами форм:

– *друковані форми,* що заповнюються і використовуються за допомогою текстового процесора і в остаточному підсумку мають на увазі створення твердої копії форми, тобто її друк;

– *форми Web*, тобто інтерактивні форми, що заповнюються і використовуються за допомогою технологій Інтернет;

– *поштові форми,* що заповнюються й використовуються за допомогою електронної пошти.

Ми обмежимося найбільш традиційним першим типом. Як приклад візьмемо типовий договір. Узагалі, для підготовки за допомогою комп’ютера друкованих форм використовуються три основних способи:

– можна використовувати звичайний документ, що є вже заповненою формою, як зразок для нової форми. Відповідні частини зразка заміняються новою інформацією, в результаті чого виходить новий екземпляр, який і друкується;

– можна заздалегідь віддрукувати типографським способом бланки форми, а потім заповнювати їх «від руки» чи вводити інформацію в заготовлені порожніполя бланка;

– можна підготувати особливий документ, що дозволяє тільки вводитиінформацію і є захищеним від інших змін.

Перший спосіб не вимагає ніяких спеціальних засобів, але

незручний і загрожує помилками. Другий спосіб був (і, на жаль, ще є) характерним для ручного діловодства. Нині друковані бланки стрімко зникають з побуту сучасного офісу, за винятком тих випадків, коли порожній бланк сам по собі є документом суворої звітності. Утім, засоби Word дозволяють трактувати другий випадок як окремий випадок третього. Третій спосіб, заснований на використанні документів особливого типу, і буде предметом розгляду в цьому параграфі.

Створення електронної форми договору. Відкрийте новий порожній документ і наберіть текст, наприклад договору. Відкрийте вкладку *Файл*. Відкрийте вкладку *Параметри* та розділ *Настройка ленты*. Виберіть *Основні (Главная)* вкладки. Встановіть флажок *Разработчик* і натисніть кнопку *Ок* (рис. 2.6).

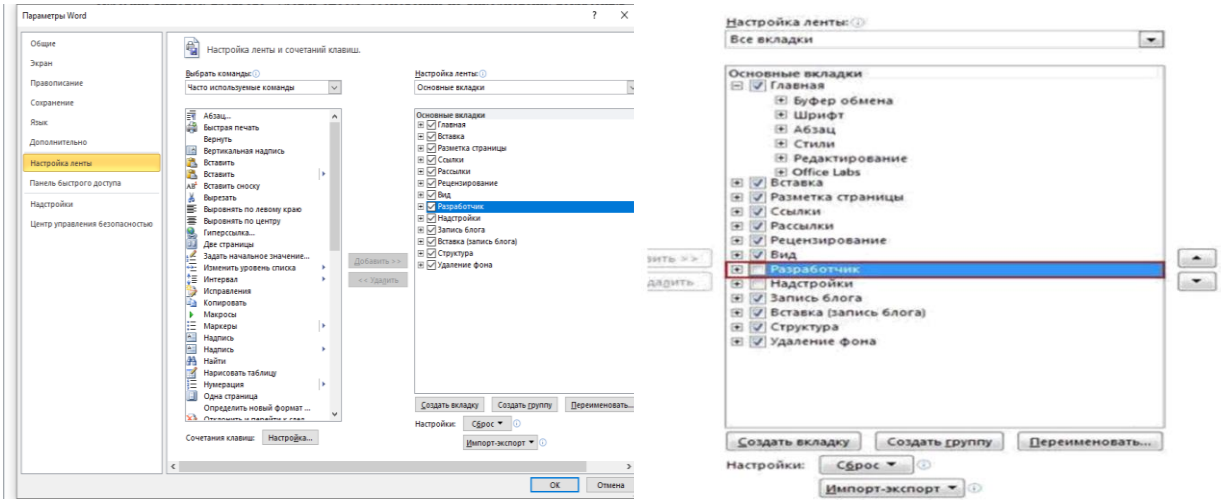


Рис. 2.6. Налаштування вкладки *Разработчик*

За допомогою панелі інструментів *Форми* підготуємо поля форм. Для цього на вкладці *Разработчик* у групі *Элементы управления* натисніть кнопку *Режим конструктора* і виберіть необхідну форму (рис. 2.7).

Якщо нам потрібно підготувати поле для вводу тексту, слід клацнути по тому місцю документа, де буде розміщуватися текстове поле, і визвати команду *Элемент управления содержимым форматированный текст* (1) або *Элемент управления содержимым обычный текст* (2), рис.2.8.

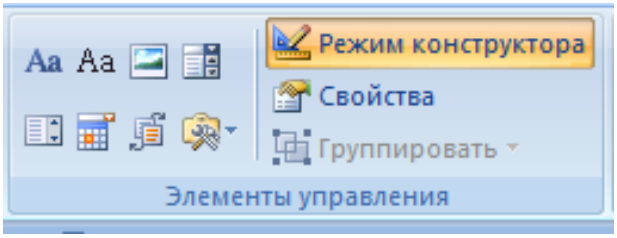


Рис. 2.7. Загальний вигляд вкладки *Разработчик*

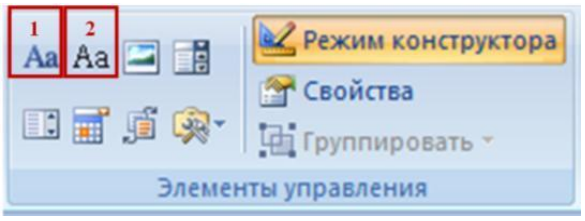


Рис. 2.8. Загальний вигляд команд *Элемент управления содержимым форматированный текст* (1), *Элемент управления содержимым обычный текст* (2)

В елементі управління *Форматированный текст* користувачі можуть виділяти текст напівжирним шрифтом або курсивом, а також вводити кілька абзаців тексту. Щоб обмежити можливості користувачів, додайте елемент управління *Обычный текст* (рис. 2.9, а). Для підготовки поля форми «рисунок» на вкладниці Разработчик в групі Элементы управления виберіть команду Элемент управления содержимым *рисунок* (рис. 2.9, б).

Стандартні блоки використовуються, коли необхідно надати користувачам можливість вибрати конкретний блок тексту. Наприклад, ці елементи управління корисні при створені шаблону договору, в якому залежно від конкретних вимог повинні бути добавлені різні варіанти стандартного тексту. Можна створити для кожного варіанту елементу управління змістом *форматированный текст*і помістити їх всі в елемент управління *стандартный блок*, використовуючи його як контейнер, рис. 2.10.

У Полі зі списком, що розкривається користувачі можуть вибрати один із наданих пунктів або ввести особистий варіант, тільки один із доступних пунктів.

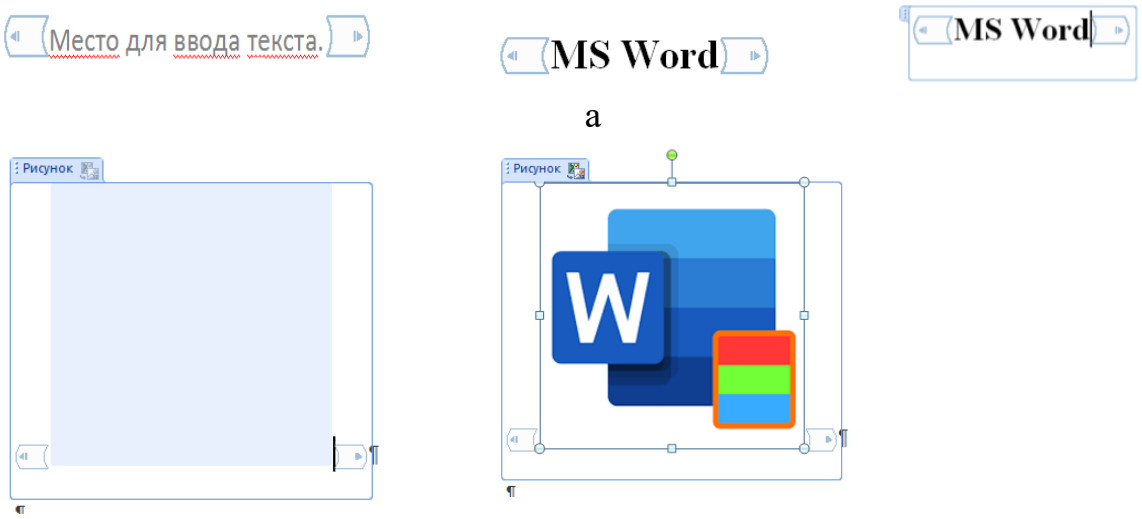


Рис. 2.9. Створення та загальний вигляд вкладок «*Обычный текст*» та «*Рисунок*»

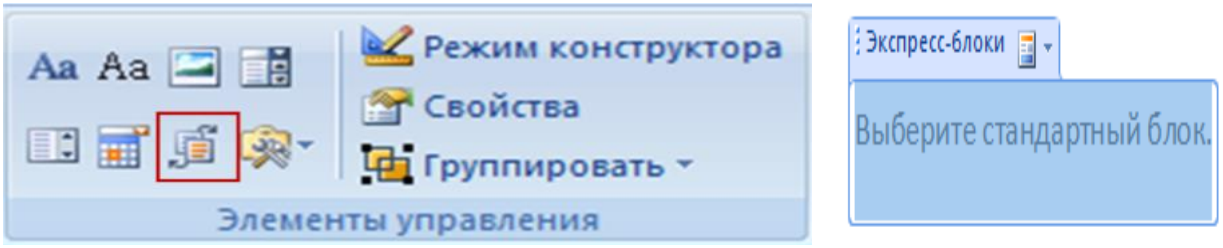


Рис. 2.10. Загальний вигляд команди *Стандартні блоки*

Для цього на вкладці Разработчик у групі Элементы *управления* виберіть команду *Элемент управления содержимым поле со списком* (1) або *Элемент управления содержимым раскрывающийся список* (2), а потім на вкладниці Разработчик у групі Элементы управления натисніть кнопку *Свойства* (рис. 2.11).

Щоб створити список пунктів, у діалоговому вікні *Свойства* елементу управління *поле со списком* або *Свойства – раскрывающегося списка* натисніть кнопку *Добавить*.

Введіть необхідні значення у вікні і повторюйте цей шаг до тих пір, поки всі значення не окажуться у списку, що розкривається. Якщо встановити прапорець *Содержимое нельзя редактировать*, користувачі не зможуть міняти вибрані пункти (рис. 2.11).

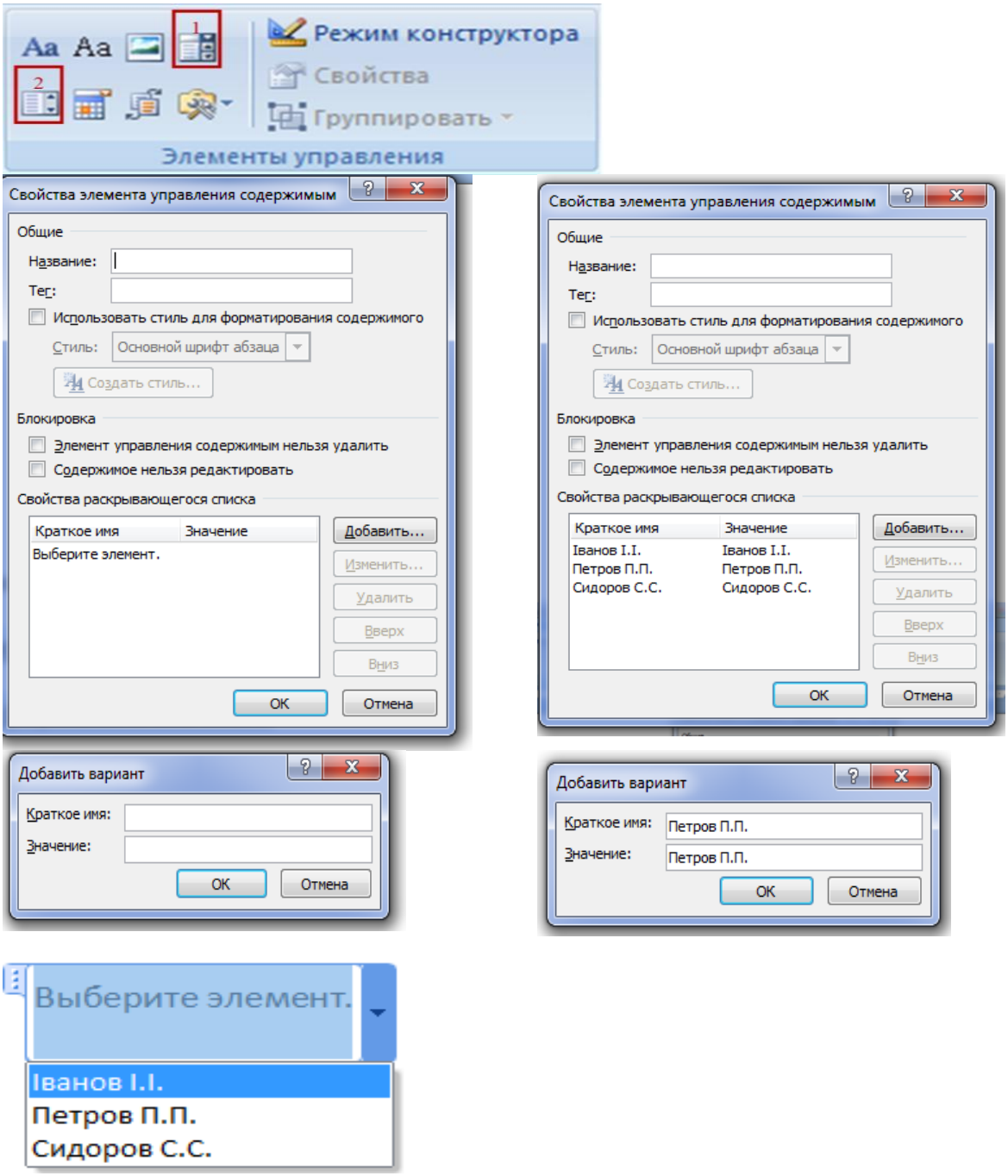


Рис. 2.11. Процес створення списку, що випадає

Вставка елементу управління *Выбор даты*. Клацніть «мишею» у тому місці, де потрібно вставити дату. На вкладниці Разработчик у групі Элементы управления виберіть команду *Элемент управления содержимым Выбор даты* (рис. 2.12). Захист форми встановлює такий режим захисту, за якого можливе тільки введення значень у поля

форми, але неможливе редагування основного тексту і налаштування параметрів полів форми.

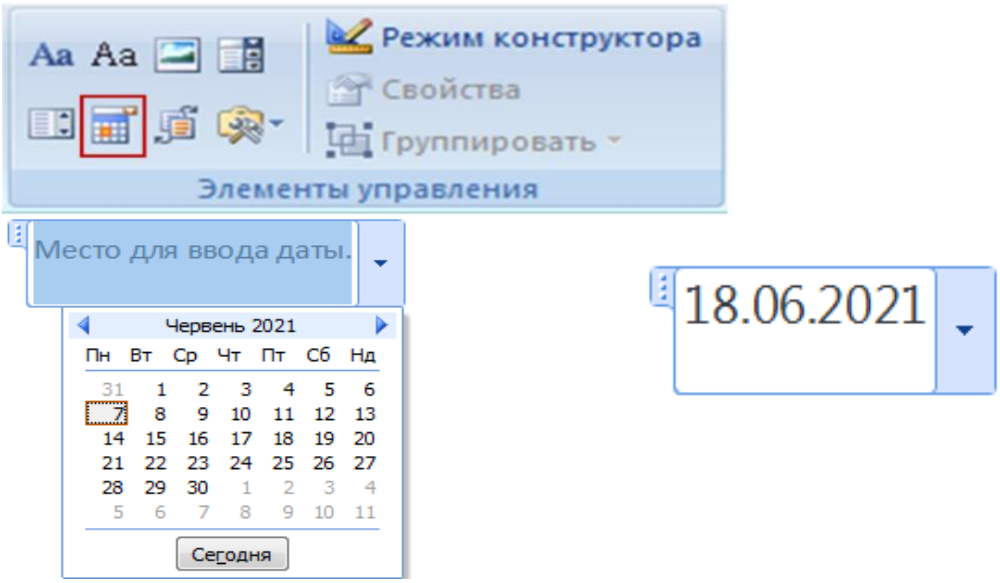


Рис. 2.12. Загальний вигляд команди *Выбор даты*

Відкрийте форму, якій необхідний захист. На вкладниці *Основна (Главная)* у групі *Редактирование* послідовно виберіть команди *Выделить*, а потім *Выделить все* або нажміть комбінацію клавіш *CTRL+A*. На вкладниці Разработчик у групі Элементы *управления* натисніть кнопку *Группировать* і виберіть команду *Группировать* (рис. 2.13).

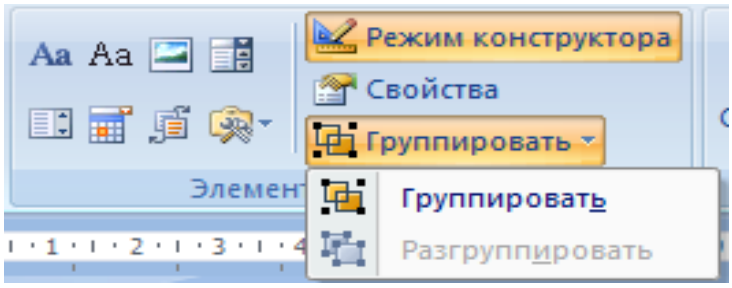


Рис. 2.13. Загальний вигляд команди *Группировать*

2.2. Побудова таблиці з використанням стандартних функцій в MS WORD

Обчислення в таблицях MS Word. Зазвичай таблиці, створені в MS Word, використовуються для компактної демонстрації даних. Для обчислень будь-якої складності з табличними даними використовуються електронні таблиці MS Excel. Якщо необхідно в документі MS Word створити таблицю зі складними обчисленнями, то така таблиця спочатку створюється в Excel, а потім переноситься (копіюється) в документ MS Word. Однак часто трапляються випадки, коли в таблиці необхідно виконати невелику кількість простих розрахунків. Наприклад, підрахувати суму чисел або кількість даних в рядку або стовпці. Такі обчислення простіше проводити безпосередньо в таблиці MS Word.

Розглянемо виконання розрахунків в таблиці MS Word на прикладі. Перш за все необхідно створити таблицю і заповнити її даними. У таблиці на рис. 2.14 для полегшення розуміння адреси умовно показані в синіх прямокутниках в лівих верхніх кутах клітинок. У реальних таблицях MS Word адреси клітинок не показуються, але вони саме такі.

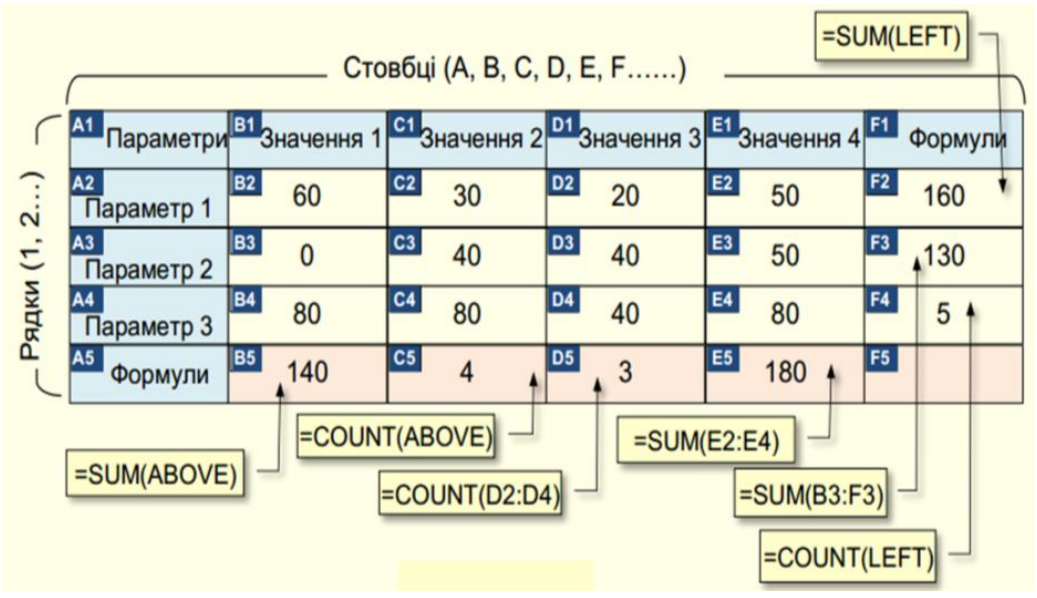


Рис. 2.14. Створення таблиці для проведення розрахунків

Порожні клітинки таблиці слід заповнити нулями, оскільки у процесі використання формул діапазон клітинок, що беруть участь в обчисленнях, визначається автоматично.

Наприклад, у процесі обчислення суми вибираються всі клітинки з числами, що йдуть підряд зліва від формули. Якщо в цій послідовності буде порожня клітинка, або клітинка з текстом, то діапазон обчислень буде обмежений саме цією клітинкою. Курсор необхідно встановити у клітинку, до якої передбачається вставити формулу. Зазвичай це клітинка знизу чи ліворуч від діапазону з даними, але можуть бути й інші варіанти.

Далі на вкладці *Робота з таблицями, Макет* в групі *Дані* натиснути кнопку *Формула* (рис. 2.15).

Відкриється діалог *Формула* (рис. 2.15). В поле *Формула* за замовчанням зазначено функцію = SUM (ABOVE), якщо для формули обрана клітинка знизу від діапазону (наприклад, клітинка B5, рис. 2.14), або = SUM (LEFT), якщо для формули обрана клітинка ліворуч від діапазону (наприклад, клітинка F2 рис. 2.14).

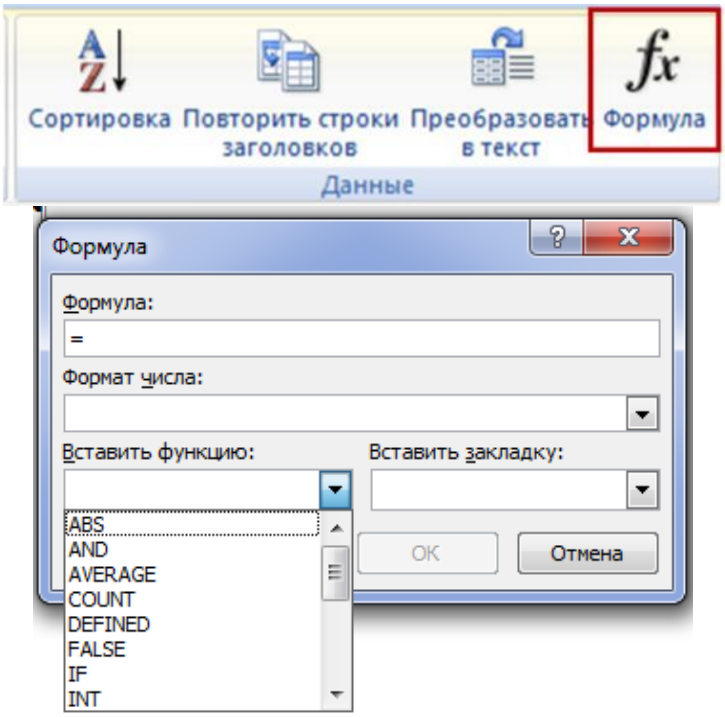


Рис. 2.15. Загальний вигляд діалогу *Формула*

За цими формулами буде обчислена сума значень у діапазоні клітинок у діапазоні над або ліворуч від формули.

Праворуч від назви функції в дужках за допомогою позиційних аргументів вказується діапазон клітинок, із вмістом яких будуть

виконані обчислення. Зазвичай значення позиційного аргументу вказується автоматично залежно від положення клітинки з формулою відносно діапазону клітинок із даними: дані над або під формулою, дані ліворуч або праворуч від формули тощо. Але іноді позиційний аргумент потрібно ввести самостійно.

Значення позиційних аргументів на прикладі функції SUM наведено в таблиці 2.1.

У деяких випадках використання позиційних аргументів не дозволяє отримати шуканий результат. Наприклад, потрібно визначити кількість клітинок із числами. Якщо використовувати формули з позиційними аргументами = COUNT (ABOVE) (клітинка C5 рис. 2.14), або = COUNT (LEFT) (клітинка F4 рис. 2.14), то будуть отримані неправильні результати, так як в діапазон клітинок будуть включені всі клітинки з будь-якими даними, в тому числі і з текстом.

У цьому випадку для отримання правильного результату необхідно точно вказати посилання на конкретні клітинки для формули. Формат посилань на конкретні клітинки наведено в таблиці на табл. 2.2

Таблиця 2.1

Значення позиційних аргументів для формули SUM

№	Положення діапазону клітинок з числами	Значення позиційного аргументу для формули SUM
1	Над клітинкою	=SUM(ABOVE)
2	Під клітинкою	=SUM(BELOW)
3	Над клітинкою і під нею	=SUM(ABOVE,BELOW)
4	Ліворуч від клітинки	=SUM(LEFT)
5	Праворуч від клітинки	=SUM(RIGHT)
6	Ліворуч і праворуч від клітинки	=SUM(LEFT,RIGHT)
7	Ліворуч від клітинки і над нею	=SUM(LEFT,ABOVE)
8	Праворуч від клітинки і над нею	=SUM(RIGHT,ABOVE)
9	Ліворуч від клітинки і під нею	=SUM(LEFT,BELOW)
10	Праворуч від клітинки і під нею	=SUM(RIGHT,BELOW)

Таблиця 2.2

Формат посилань на конкретні клітинки

Клітинка або діапазон	Формат запису посилання
Клітинка в першому стовпці та другому рядку	A2
Перші дві клітинки в першому рядку	A1, B1
Діапазон клітинок від клітинки в першому стовпці першого рядка до клітинки в третьому стовпці другого рядка	A1:C1

Формат числа, у якому надається результат обчислень за формулою обирається із списку в полі Формат номерів рис. 2.16.

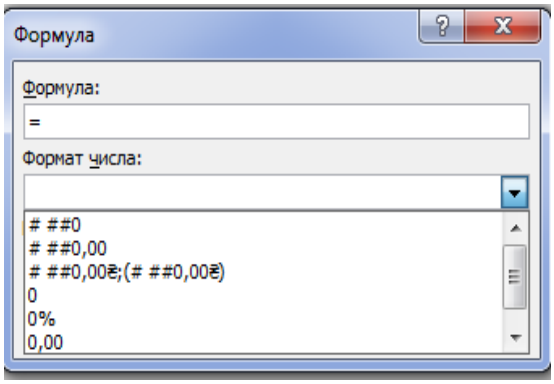


Рис. 2.16 Загальний вигляд *Формату числа*

У таблицях Word можна робити обчислення за багатьма формулами. Усі доступні формули можна отримати із списку поля *Вставити функцію* (рис. 2.17).

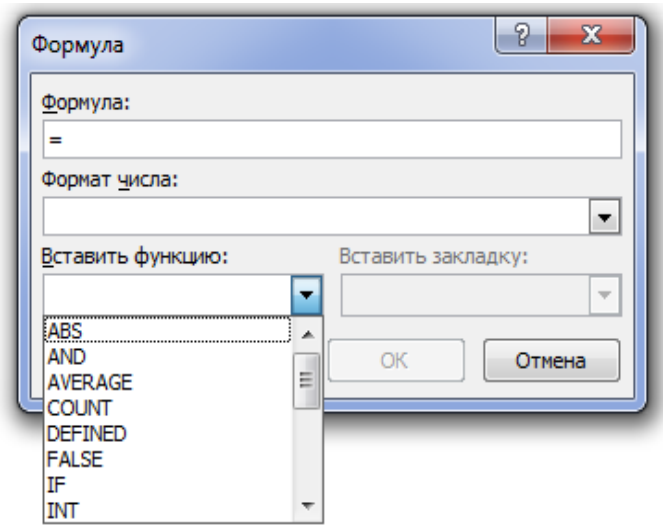


Рис. 2.17. Загальний вигляд списку поля *Вставити функцію*

Опис деяких функцій з цього списку наведено в таблиці. 2.3.

Таблиця 2.3

Опис функцій

Функція	**Призначення**	**Приклад**	**Значення, яке повертається**
SUM()	Знаходить суму елементів, вказаних в дужках.	=SUM(RIGHT)	Сума значень, розташованих у клітинках праворуч
COUNT()	Підраховує кількість елементів, вказаних в дужках.	=COUNT(LEFT)	Кількість значень, розташованих зліва від клітинки з формулою
AVERAGE()	Знаходить середнє (арифметичне) елементів, вказаних в дужках.	=AVERAGE(RIGHT)	Середнє арифметичне всіх значень, розташованих праворуч від клітинки з формулою в тому ж рядку.
INT()	Округлює значення в дужках до найближчого цілого числа в менший бік.	=INT(5,67)	5
MAX()	Повертає найбільше значення серед елементів, вказаних в дужках.	=MAX(ABOVE)	Найбільше значення серед тих, що розташовані в клітинках над формулою (виключаючи заголовки).
MIN()	Найбільше значення серед тих, які знаходяться в клітинці над формулою (виключаючи заголовки).	=MIN(ABOVE)	Найменше значення серед тих, що розташовані в клітинках над формулою (виключаючи рядки заголовків).
PRODUCT()	Знаходить добуток елементів, вказаних в дужках.	=PRODUCT(LEFT)	Добуток всіх значень, розташованих у клітинках зліва від формули.

У процесі роботи з таблицями Word дані в них можуть змінюватися, проте результати обчислень за формулами при цьому автоматично не змінюються. Щоб оновити результати формул необхідно виконати наступні дії:

Для оновлення результатів окремих формул:

1. Виділітьформули,які необхідно оновити. Щоб виділити кілька формул, утримуйте CTRL.
2. Виконайте одну з таких дій:

– Клацніть формулу правою кнопкою миші і виберіть команду Оновити поле.

– Натисніть клавішу F9.

– Для оновлення результатів всіх формул в таблиці:

– Виділіть таблицю, що містить результати формул, які необхідно оновити, і натисніть клавішу F9.

2.3. Редактор формул в текстовому процесорі Microsoft WORD

Введення формул звичайне для документів науково-технічного характеру. Для цього використовується редактор формул, що дозволяє створювати і редагувати формульні об’єкти безпосередньо в документі. Запуск редактора формул – вкладка Вставка → Символи→Формула. Відразу відкривається вікно з колекцією вбудованих формул (рис. 2.17), в яку входять раніше створені формули. Колекцію формул можна розширяти, додаючи до неї нові формули. Для цього спочатку необхідно створити нову формулу, виділити її цілком або будь-яку її частину і натиснути кнопку Зберегти виділений фрагмент в колекції формул.

Для створення формули необхідно натиснути кнопку Вставити нову формулу, відкриється контекстна вкладка *Робота з формулами* з *Конструктором* формул і віконцем для безпосереднього введення формули (рис. 2.18).

Панель інструментів конструктора формул складається з кнопок, що являють собою набори шаблонів, які містять поля для введення символів.

Приклади наборів шаблонів для кнопок *Дріб, Індекс, Радикали, Інтервали, Дужки і Функції* наведені на рис. 2.19.

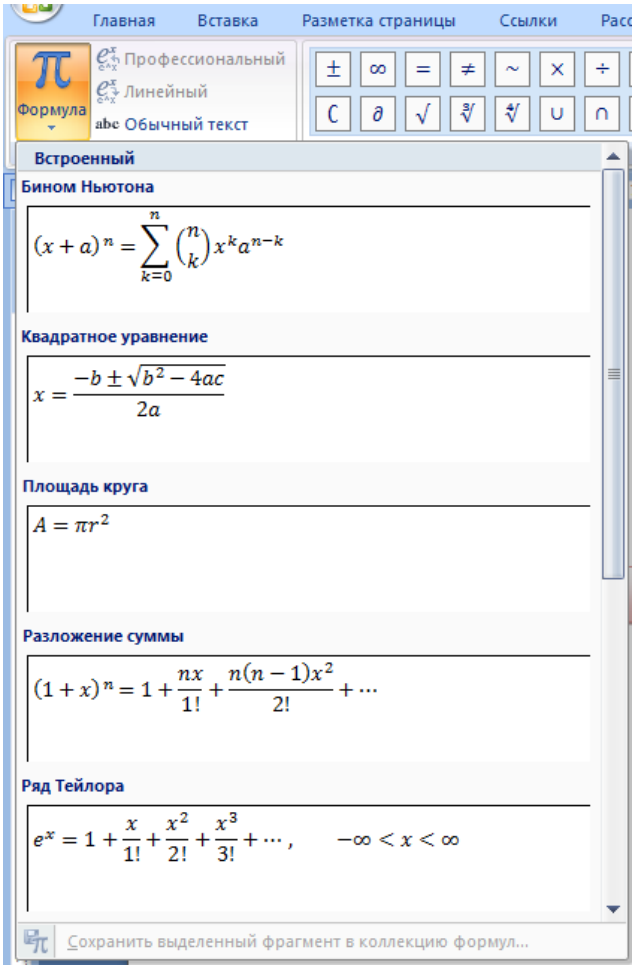


Рис. 2.17. Загальний вигляд вікна з колекцією вбудованих формул

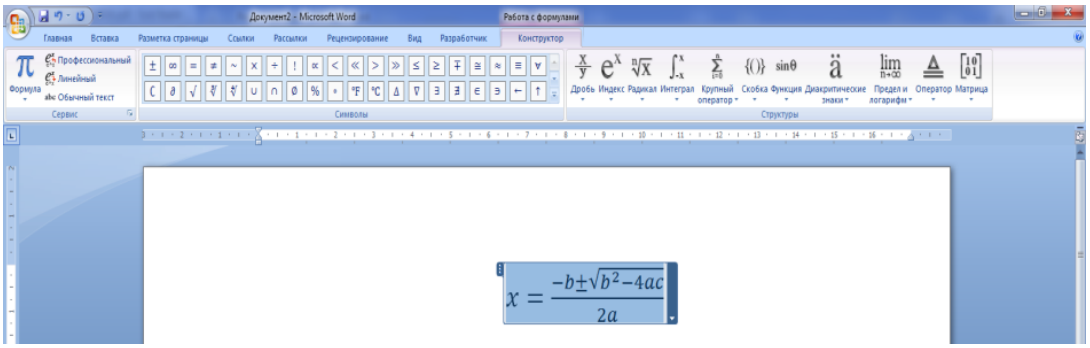


Рис. 2.18. Загальний вигляд віконця для безпосереднього введення формули

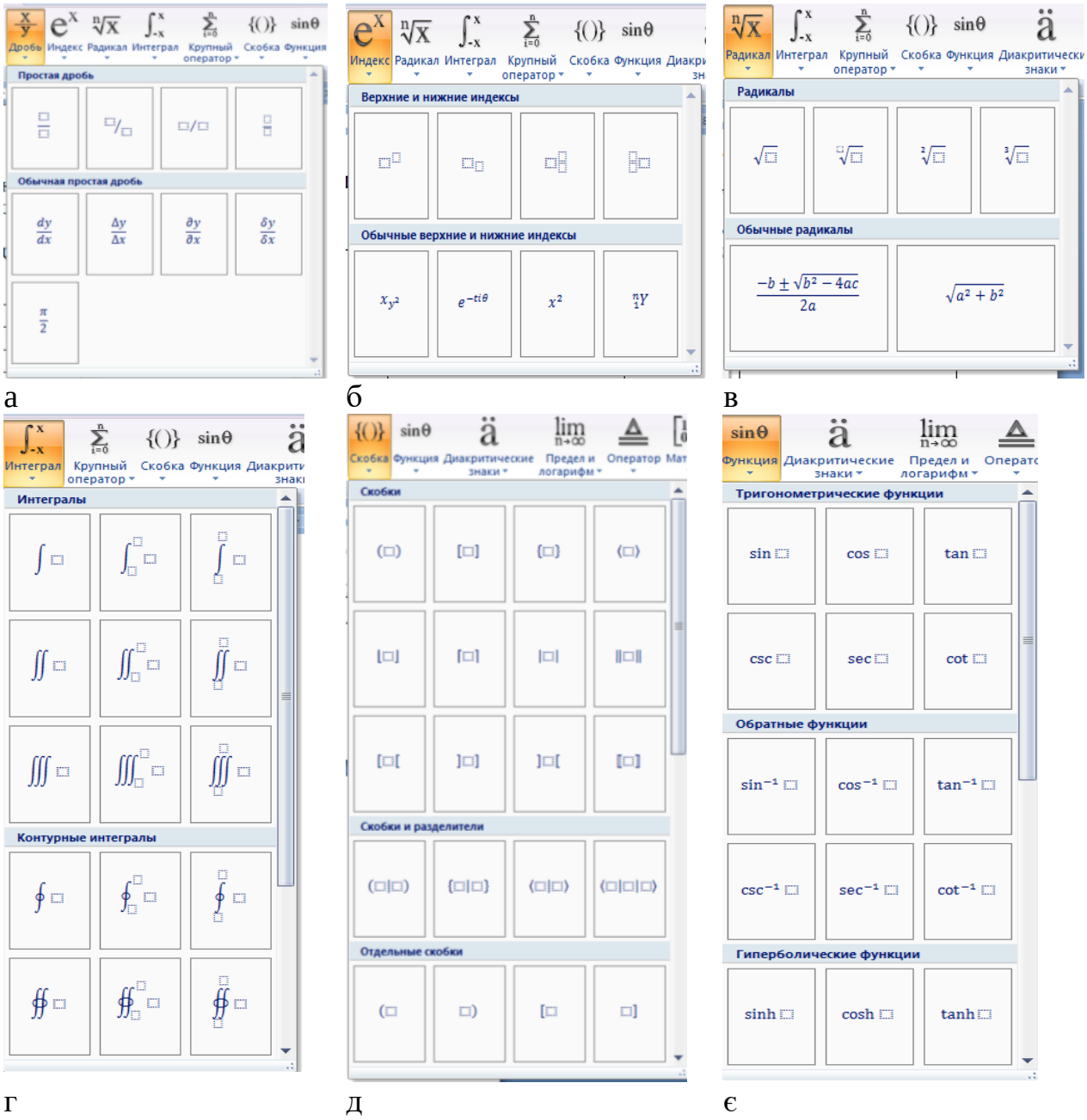


Рис. 2.19. Приклади наборів шаблонів для формул

Створення формули зводиться до вибору потрібного шаблону та заповнення його полів певними символами, що можна набирати з клавіатури або вибирати в розділі «символи».

Введення і редагування формул завершується натисканням клавіші *Enter* або клацанням по полю документа поза віконцем формули.

Введена формула автоматично вставляється в документ. Далі

формулу можна форматувати з використанням інструментів вкладки *Основне (Главная)*, наприклад, змінювати тип, розмір, колір й інші параметри шрифту. Для цього формула виділяється клацанням і потім до неї застосовується певний інструмент форматування.

Для редагування формули досить зробити на ній подвійне клацання миші. Прицьому автоматично відкривається вікно редактора формул.

Створення колонок. Виберіть текст, що ви хочете зробити колонками. Виберіть вкладку *Макет (Разметка страницы)*і натисніть команду *Колонки* (рис. 2.20).

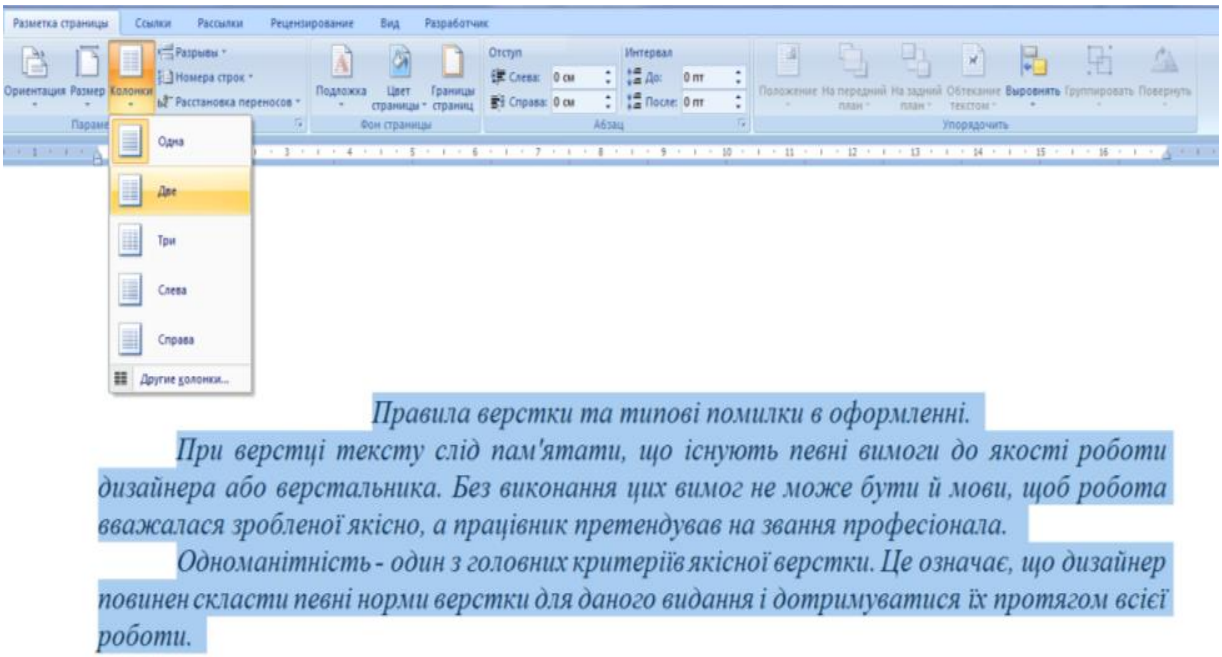
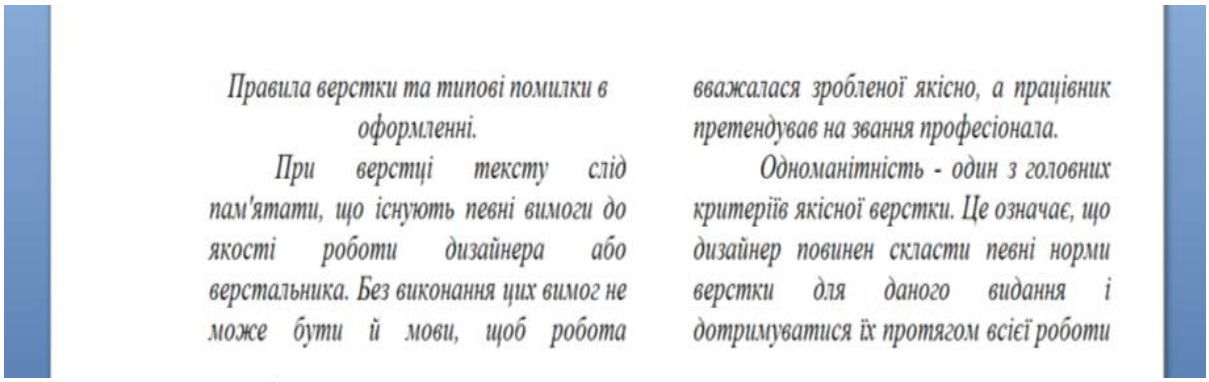


Рис. 2.20. Створення колонок

У спадному меню виберіть кількість колонок, що слід створити. У нашому прикладі, ми хочемо зробити дві колонки у ворді. Текст буде перетворений на дві колонки (рис. 2.21).



Правила верстки та типові помилки в оформленні.

При верстці тексту слід пам'ятати, що існують певні вимоги до якості роботи дизайнера або верстальника. Без виконання цих вимог не може бути й мови, щоб робота вважалася зробленої якісно, а працівник претендував на звання професіонала.

Одноманітність - один з головних критеріїв якісної верстки. Це означає, що дизайнер повинен скласти певні норми верстки для даного видання і дотримуватися їх протягом всієї роботи

Рис. 2.21. Загальний вигляд тексту на дві колонки

Вибір кількості колонок у ворді не обмежується створенням 2 або 3 колонок у спадному меню. Виберіть «Інші стовпці» у нижній частині меню, щоб відкрити діалогове вікно «Колони». Вкажіть необхідну кількість колонок у поле «Кількість стовпців», рис. 2.22.

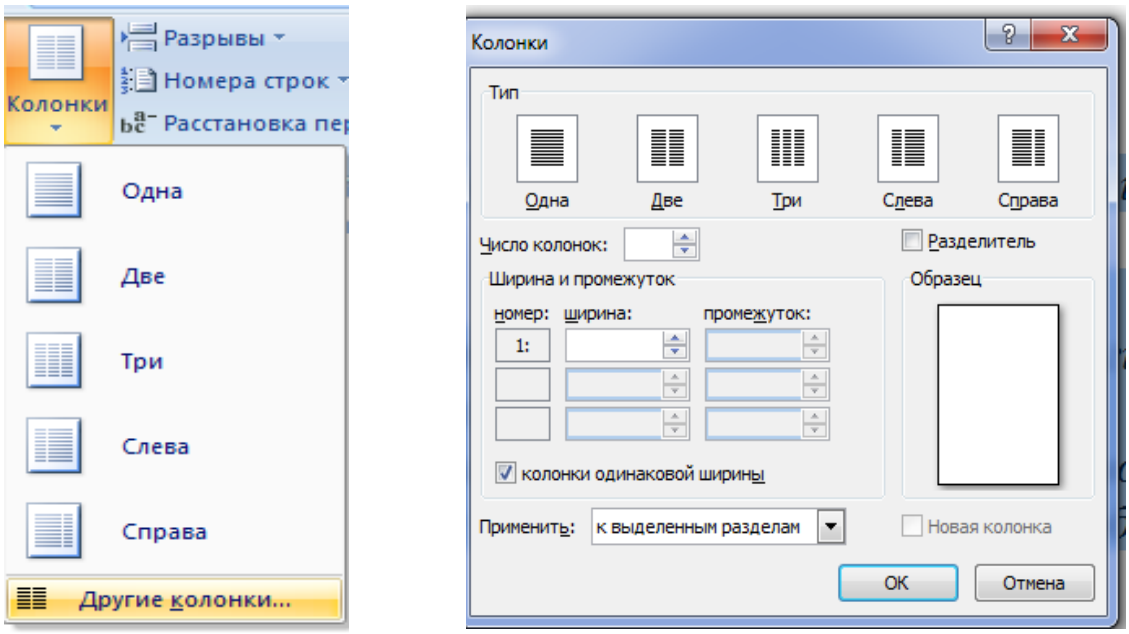


Рис. 2.22. Вибір кількості стовпців

Для того, щоб прибрати колонки у ворді: встановіть курсор у будь-якому місці де текст представлений у вигляді колонок, натисніть команду *Колонки* на вкладці*Макет (Разметка страницы)*;в спадному меню виберіть *Одна*.

Колонтитул – це графічна або текстова інформація, що знаходиться зверху або знизу сторінки над або під основним текстом

(рис. 2.23). Найчастіше в колонтитулах вказується назва глави, номер розділу, автор книги й елемент графічного оформлення, наприклад, логотип. Використання колонтитулів дозволяє не лише поліпшити зовнішній вигляд документа, але і швидко зорієнтуватися в документі. Правильно складений і візуально естетичний колонтитул – це візитівка документа.

Колонтитул можливо розробити для кожного розділудокумента, також різняться колонтитули парних і непарних сторінок. Переважно/зазвичай, у документах використовують лише верхній або тільки нижній колонтитул. Робота з колонтитулами доступна тількив режимі розмітки сторінки.

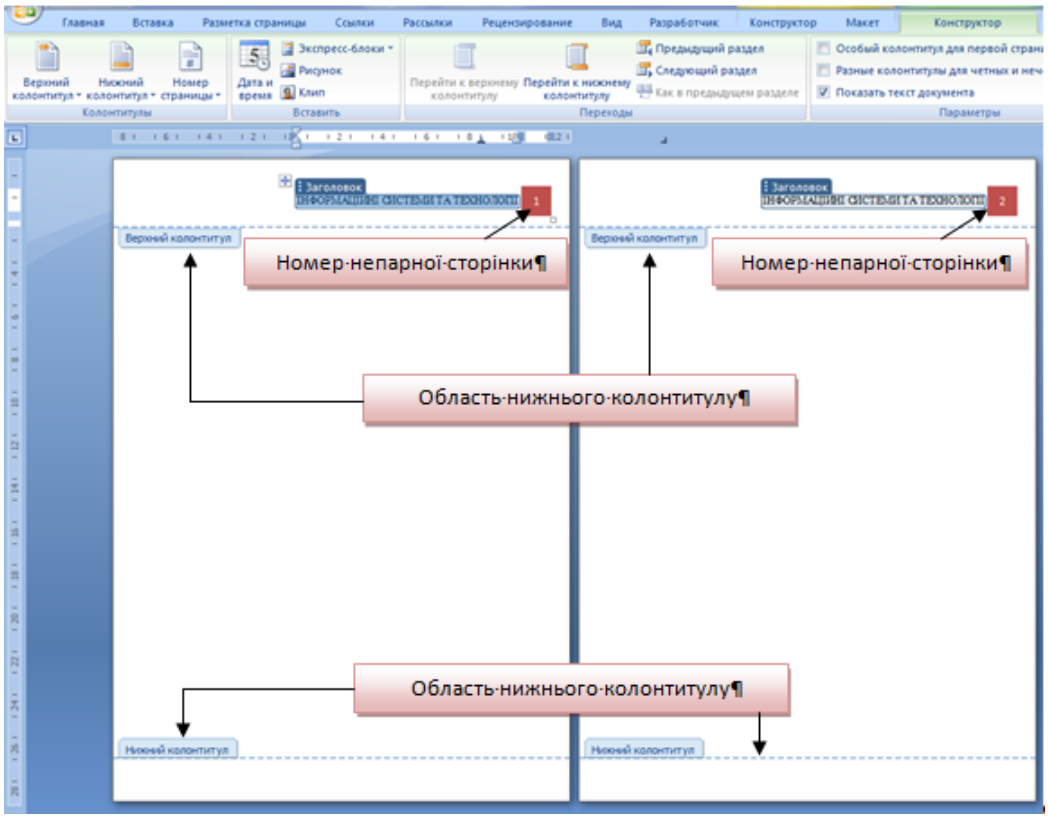


Рис. 2.23. Загальний вигляд верхнього та нижнього колонтитулу

Техніка створення верхнього та нижнього колонтитулів ідентична.

Додавання верхнього колонтитула можливе кількома способами.

Перший спосіб. На вкладці Вставка в групі Колонтитули клацнути кнопку Верхній колонтитул (рис. 2.24) і в списку, що розкрився зі зразків колонтитулів клацанням обрати потрібний.

Відбудеться перехід до області створення колонтитула (автоматично відкриється вкладка *Конструктор* → *Робота з*

колонтитулами (рис. 2.25), а на стрічці відобразяться спеціальні групи і кнопки для роботи з колонтитулами), при цьому основний текст забарвиться в сірий колірі буде недоступним для редагування.

До області в квадратних дужках вводиться необхідний текст. Для колонтитула парної сторінки це зазвичай номер глави або розділу, а для колонтитула непарної сторінки – назва глави або розділу.

Для завершення роботи з колонтитулами необхідно клацнути кнопку Закрити колонтитули в групі Закрити або двічі клацнути в будь-якому місці сторінки поза колонтитулом.

Другий спосіб. Клацнути правою кнопкою миші уверхній частині сторінки в області заголовка й обрати команду Змінити верхній колонтитул.

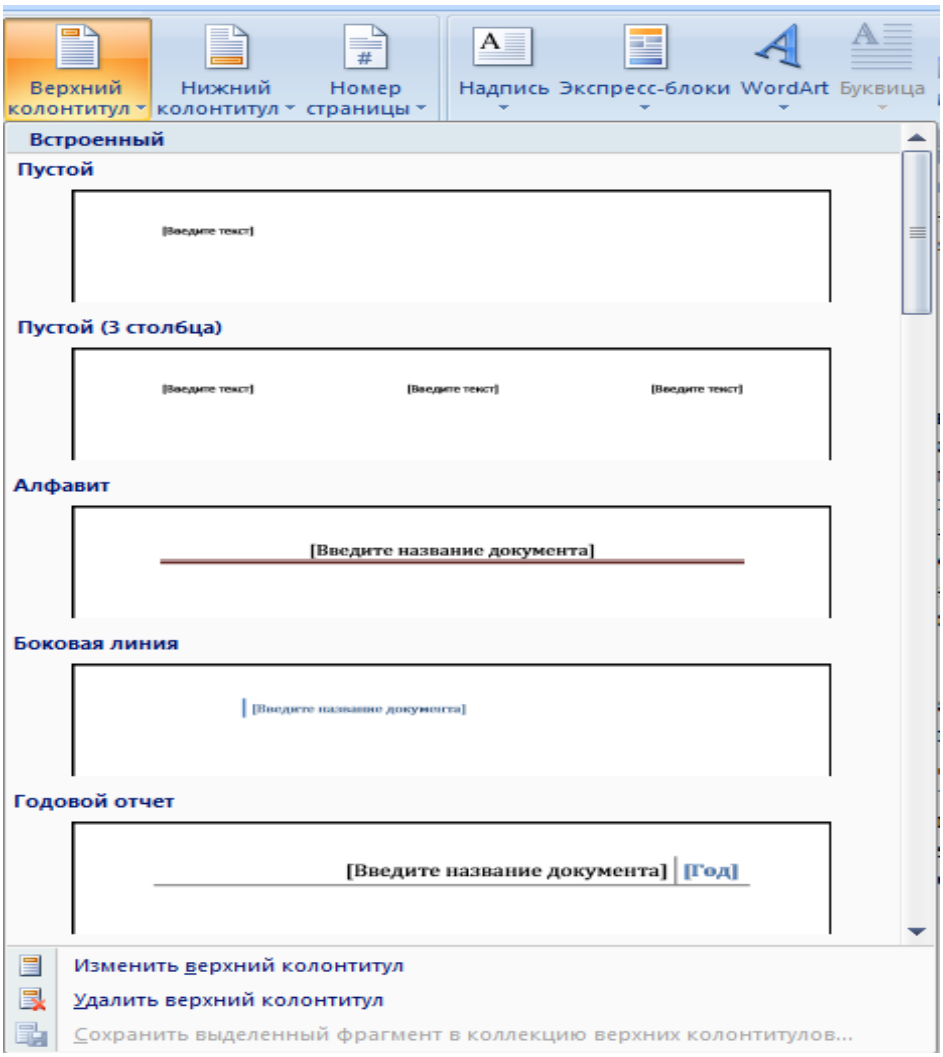


Рис. 2.24. Загальний вигляд вікна «Верхній колонтитул»

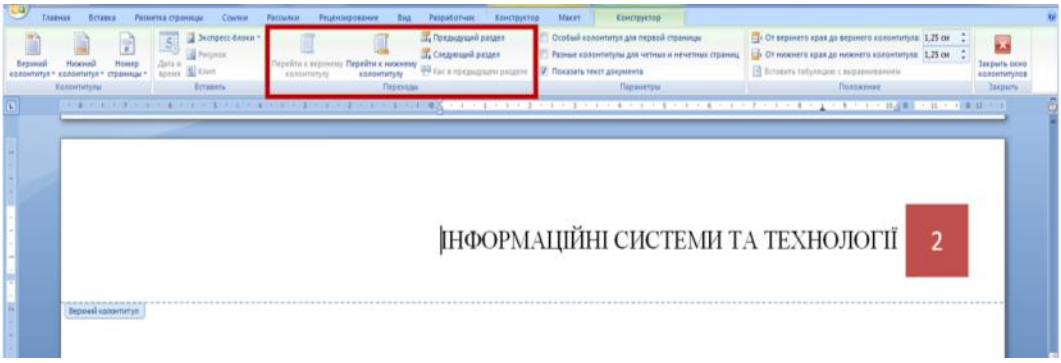


Рис. 2.25. Створення колонтитулу

Розглянуті методи застосовуються як для створення, так і для редагування колонтитулів. Перехід між колонтитулами. Під час редагування колонтитулів може знадобитися перехід від верхнього до нижнього колонтитула (або навпаки). Для цього на вкладці *Конструктор* → *Робота з колонтитулами* в групі *Навігація (Переходы)* (рис. 2.25) клацайте по кнопках Перейти до верхнього колонтитулаабо Перейти до нижнього колонтитула. Якщо документ розбитий на кілька розділів, то для кожного з них можна створити незалежні один від одного колонтитули, перехід між якими здійснюється кнопками Попередній і Наступний.

2.4. Автоматизація підготовки ділових документів (створення макросів)

Макрос – це набір певних дій, команд або інструкцій, що згруповані в одну цілісну команду, яка забезпечує автоматичне виконання того чи іншого завдання.

Області застосування макросів:

1. Прискорення часто виконуваних операцій. У числі таких – форматування іредагування.

2. Об’єднання декількох команд в цілісну дію «від і до». Наприклад, за допомогою макросу можна вставити таблицю заданого розміру з необхідною кількістю рядків і стовпців.

3.Спрощення доступу до деяких параметрів таінструментів, розташованих у різних діалогових вікнах програми.

4. Автоматизація складних послідовностей дій. Послідовність макросів може бути записана чи створена з нуля шляхом введення коду до редактору Visual Basic на однойменному мовою програмування.

Включення макросів. За замовчуванням макроси доступні не у всіх версіях MS Word, точніше, вони просто не включені. Щоб активувати їх необхідно включити Інструментарій розробника програмного забезпечення. Після цього на панелі управління програми з'явиться вкладка *Розробник*. У версіях програми, в яких макроси доступні спочатку (наприклад, MS Word 2016), засоби для роботи з ними знаходяться у вкладці *Вид*в групі *Макрос*.

1. Відкрийте меню *Файл* (кнопка *Microsoft Office* раніше).
2. Виберіть пункт *Параметри* (раніше *Параметри Word*).
3. Відкрийте у вікні *Параметри* категорію *Основні* і перейдіть в групі *Основні параметри роботи*.
4. Встановіть галочку напроти пункту *Показувати вкладку* Розробник *на стрічці*.
5. На панелі керування з'явиться вкладка *Розробник*, в якій і буде перебувати пункт *Макрос* (рис. 2.26*)*.

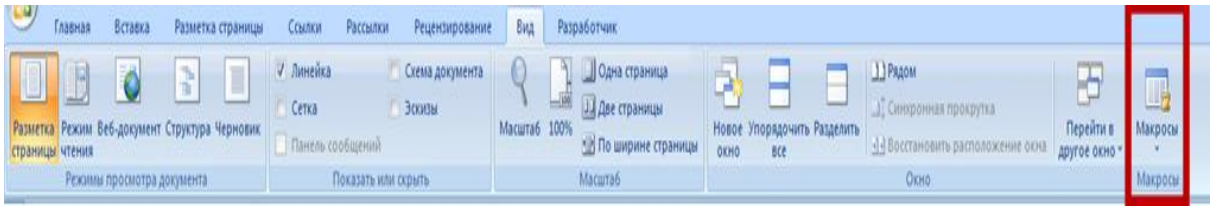


Рис. 2.26. Загальний вигляд вікна Макрос

Запис макросів

1. У вкладці *Розробник* або, залежно від використовуваної версії MS Word, у вкладці *Вид*, натисніть кнопку *Макрос* і виберіть пункт *Запис макросу* (рис. 2.27).

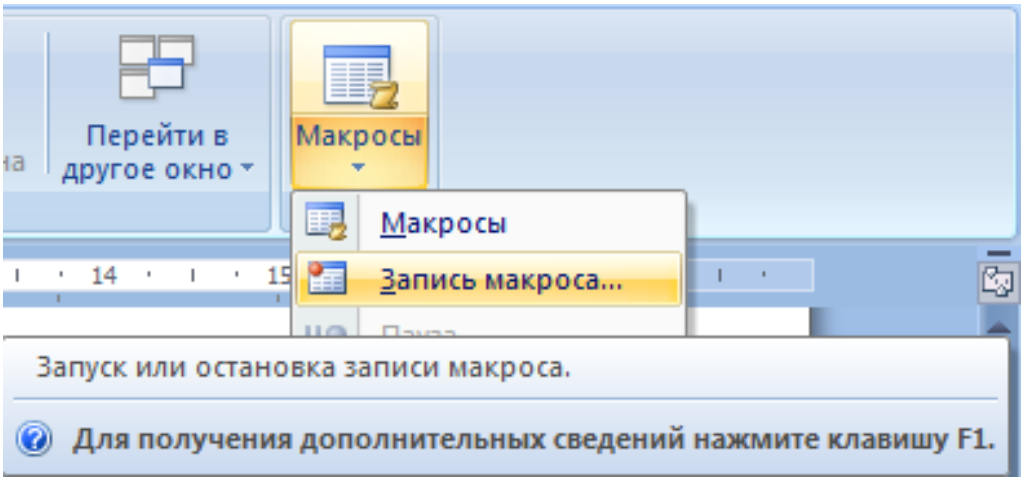


Рис.2.27. Запуск та зупинка запису *Макросу*

2. Задайте ім’я для створюваного макросу. *Ім’я макросу* не має містити пробілів, ком, двокрапок і т.п. Припустимі символи кирилиці, латиниці, цифри й нижнє підкреслення. Ім’я макросу завжди має починатися з букви й не повинне збігатися із вбудованим іменем MS Word або MS Excel або іменем іншого об’єкта в книзі (наприклад, не повинне мати ім’я Workbook, Cells або Эта Книга). Краще давати макросу відразу зрозуміле ім’я, що відображає зразкову суть того, що він робить (рис. 2.28).

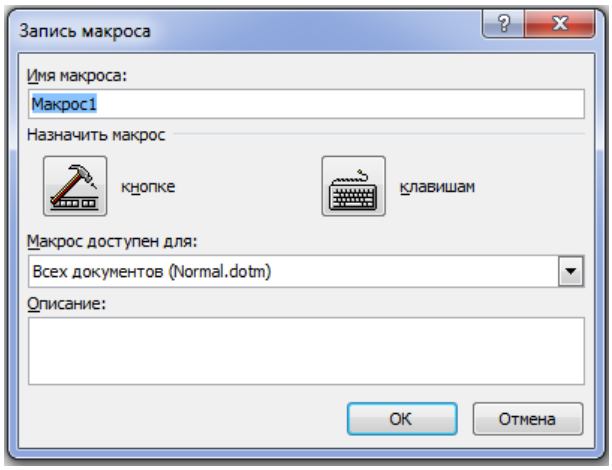
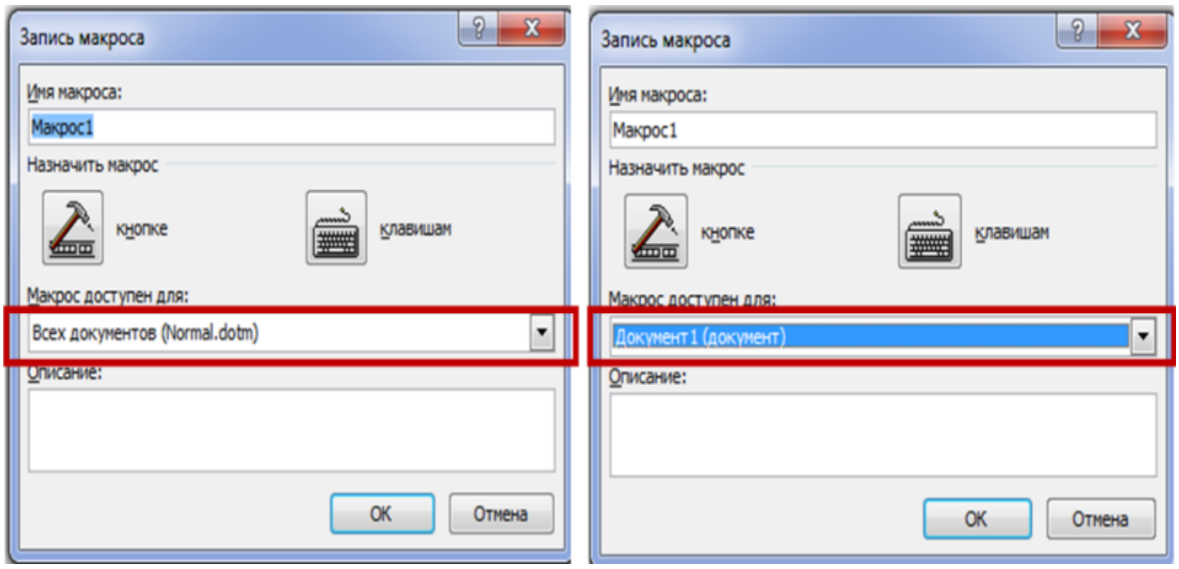


Рис. 2.28. Присвоїти ім’я для створюваного макросу

Якщо ви, створюючи новий макрос, даєте йому точно таке ж ім’я, як у вбудованого до програми, дії, записані вами до нового макросу, будуть виконуватися замість стандартних. Для перегляду макросів, доступних в MS Word за замовчуванням, в меню кнопки *Макрос* виберіть *Команди Word*.

3. У пункті *Макрос доступний для* виберіть те, для чого він буде доступний: шаблон (рис. 2.29, а) або документ (рис. 2.29, б), у якому його слід зберегти. Якщо ви хочете, щоб створений макрос був доступний у всіх документах, із якими ви працюватимете в подальшому, виберіть параметр *Normal.dotm*.



а б

Рис. 2.29. Запис макросу шаблоні (а) та у та у конкретному документі (б)

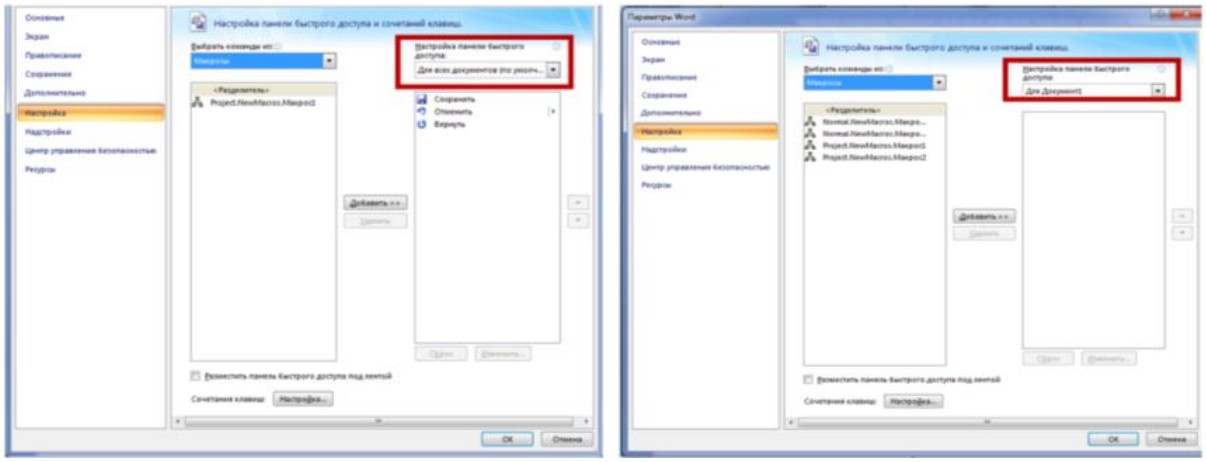
4. У полі *Опис* введіть опис для створюваного макросу.
5. Виконайте дії, зазначені нижче:

– почніть запис – щоб приступити до початку запису макросу, не зв'язуючи його при цьому з кнопкою на панелі управління або комбінацією клавіш, натисніть *ОК*;

– створіть кнопку – щоб зв'язати створюваний макрос з кнопкою, розташованої на панелі керування, виконайте наступне:

– натисніть *кнопці*;

– виберіть документ або документи, в яких потрібно додати створюваний макрос на панель швидкого доступу (розділ *Налаштування панелі швидкого доступу*) (рис. 2.30);



а б

Рис. 2.30. Налаштування швидкого доступу макросу для всіх документів (а) або для окремого (б)

У вікні *Макрос* (раніше *Вибрати команди з*) виберіть макрос, що слід записати, натисніть *Додати* (рис. 2.31).

Якщо ви хочете налаштувати цю кнопку, натисніть *Змінити*. Виберіть відповідний символ для створюваної кнопки в полі *Символ* (рис. 2.32).

Введіть ім’я макросу, що буде відображатися у подальшому в полі *Ім’я, що відображається*. Для початку запису макросу двічі натисніть кнопку *ОК*. Символ, який ви вибрали, буде відображатися на панелі швидкого доступу.

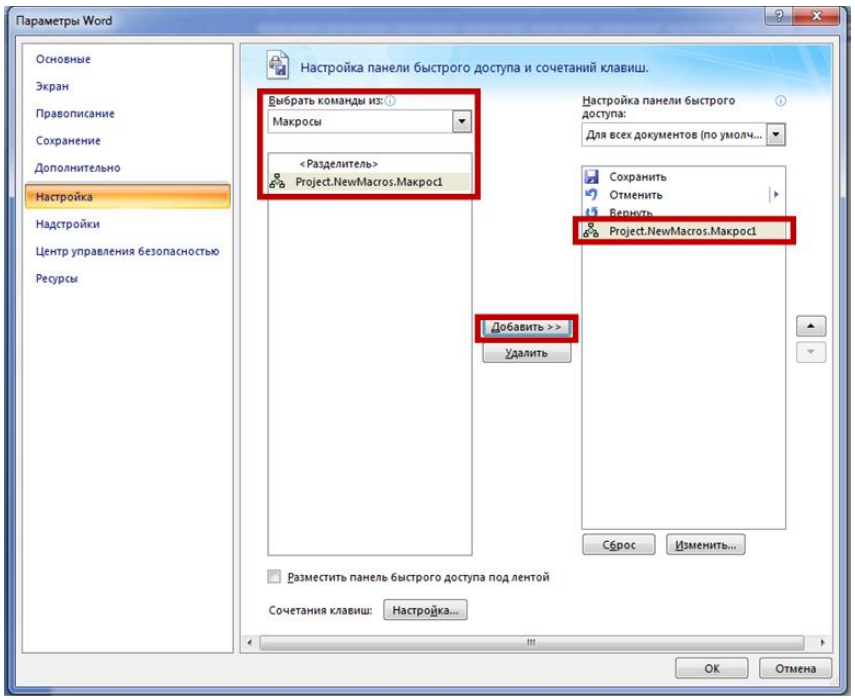


Рис. 2.31. Додавання макросу до панелі швидкого доступу

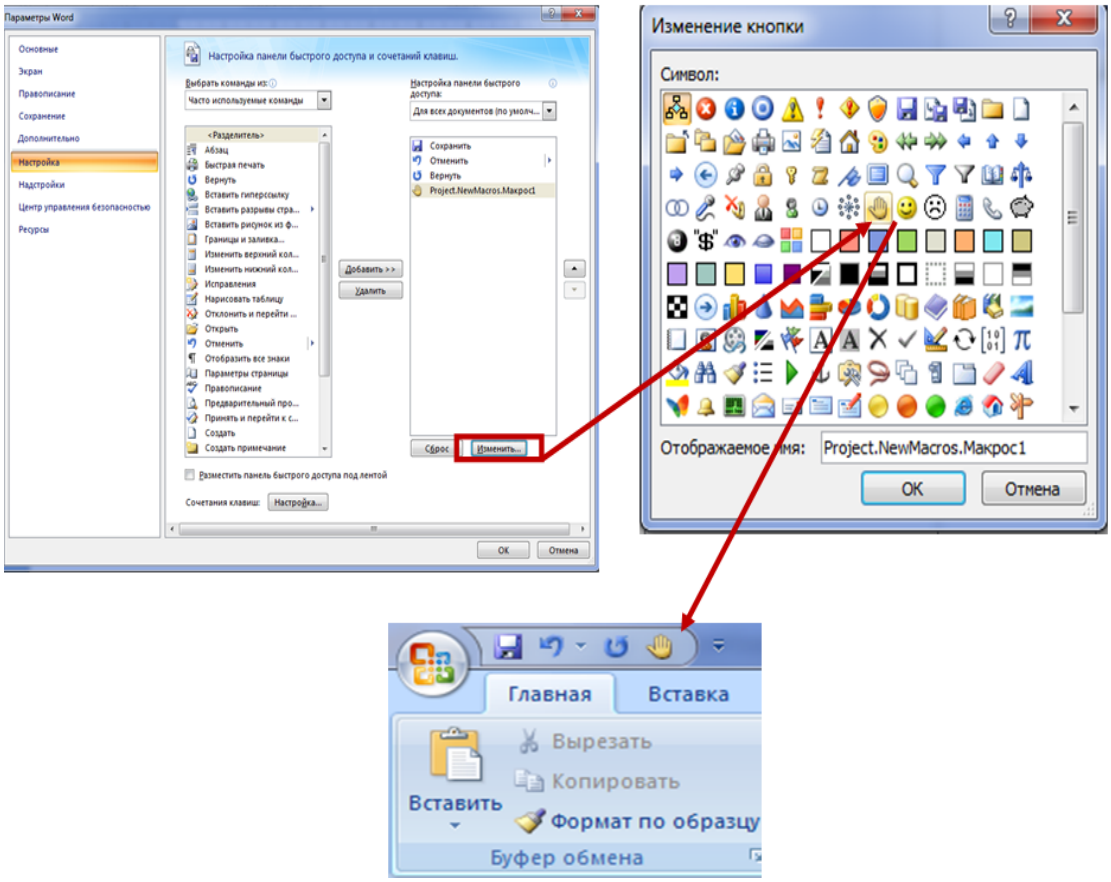


Рис. 2.32. Вибір символу швидкого доступу для макросу

Під час наведення покажчика курсору на цей символ, буде відображатися його ім’я.

6. Призначте поєднання клавіш. Для того, щоб призначити комбінацію клавіш для створюваного макросу, виконайте такі дії:

– натисніть кнопку (раніше *Клавіатура*);

– у розділі *Команди* виберіть макрос, що необхідно записати;

– у розділі *Нове поєднання клавіш* введіть будь-яку зручну для вас комбінацію, після чого натисніть кнопку *Призначити*;

– для початку запису макросу натисніть *Закрити*.

7. Виконайте по черзі всі ті дії, що необхідно включити в макрос. Під час запису макросу можна використовувати мишу для виділення тексту, а ось для вибору команд і параметрів потрібно використовувати саме її. При необхідності, виділити текст можна за допомогою клавіатури.

Швидкий доступ в MS Word. Для зупинки запису макросу натисніть *Зупинити запис*. Ця команда розташована в меню кнопки

Макрос на панелі управління.

Зміна комбінацій клавіш для макросу (рис. 2.33).

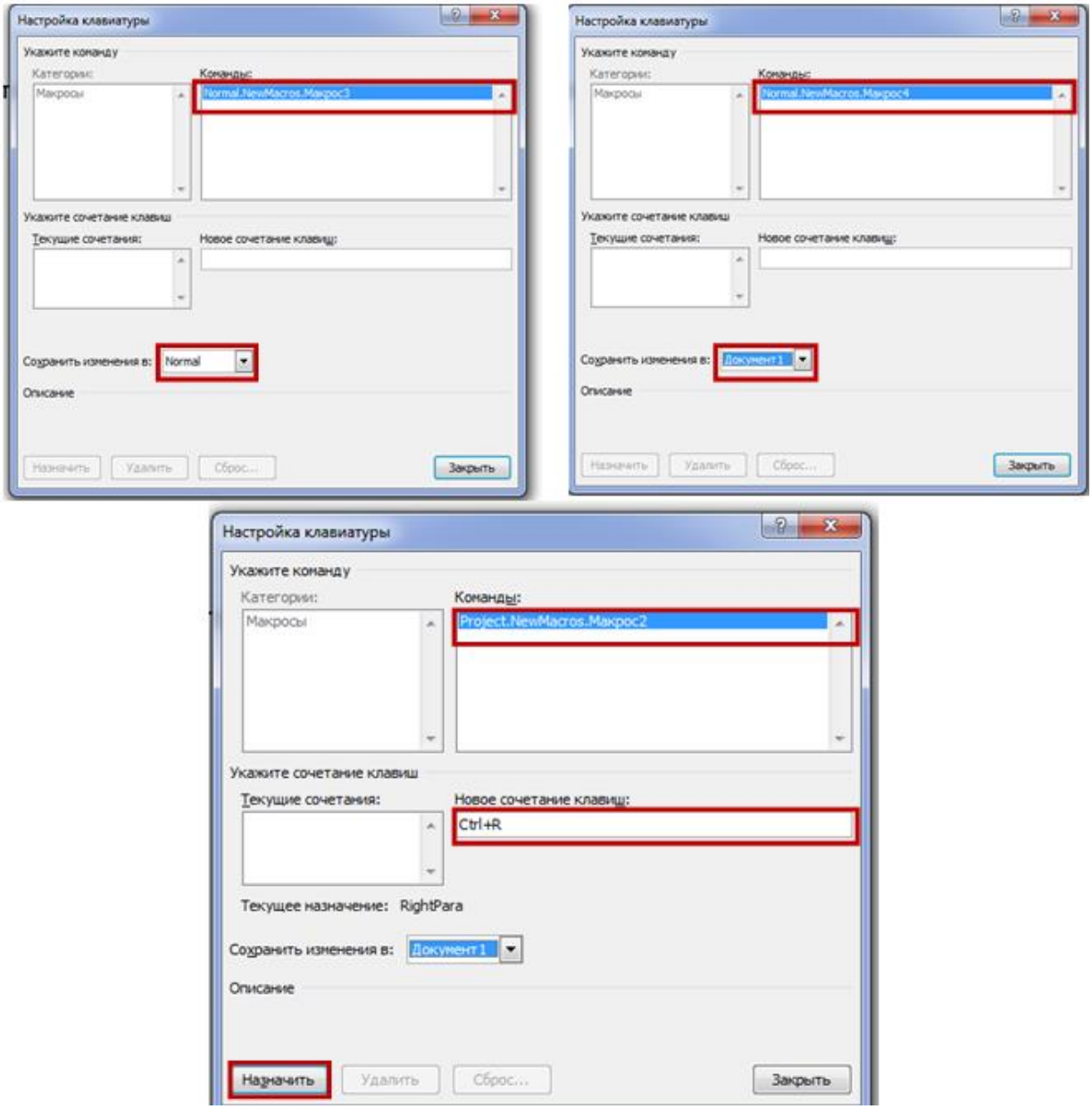


Рис. 2.33. Налаштування комбінації клавіш для макросу

Алгоритм

1. Відкрийте вікно *Параметри* (меню *Файла* бо кнопка *MS Office).*
2. Виберіть пункт *Налаштування*.
3. Натисніть на кнопку *Налаштування*, розташовану поруч із полем *Поєднання клавіши*.
4. У розділі *Категорії* виберіть *Макрос*.

5. У списку, виберіть макрос, що слід змінити.

6. Клацніть по полю *Нове поєднання клавіш*і натисніть клавіші або комбінації клавіш, які ви хочете призначити для конкретного макросу.

7. Переконайтеся, що призначене вами поєднання клавішне використовується для виконання іншої задачі (поле *Поточне поєднання*).

8. 8.У розділі *Зберегти зміни* виберіть відповідний варіант (місце) для збереження місця, де макрос буде запускатися.

9. Натисніть Закрити.

Запуск макросу.

1. Натиснітьна кнопку *Макрос* (вкладка *Вид* або *Розробник*, залежно від використовуваної версії програми).

2. Виберіть макрос, що будете запускати (список *Ім'я макросу*).

3. Натисніть *Виконати*.

Практичні завдання

Завдання № 1. Створення електронної форми договору.

1. Створити новий текстовий документ, що є зразком Протоколу огляду (дуже спрощеного). Наберіть текст Протоколу огляду, наведений нижче. У цьому Протоколі огляду поля для заповнення у зразку Протоколу огляду ці місця відзначені спеціально виділені за допомогою заливання: У вашому прикладі таких точок буде 21. Ваше завдання полягає в тому, щоб вставити замість них спеціальні об'єкти, що звуться **полями форм**. За допомогою викладених вище зведень, здійсніть настроювання форм запропонованого Протоколу огляду. Тобто, помістіть в документ Протокол огляду поля форми у тому ж порядку, у якому заповнюватиметься форма Протоколу огляду (зверху вниз).

Вимоги до форматування: Times New Roman 14, міжрядковий інтервал 1,0, поля верхнє, нижнє, праве – 1,0 ліве – 2,5, абзац 1,27.

Загальний вигляд Протоколу огляду наведено у файлі з назвою «UA version of protocol» Додаток.

Зразок

Зразок

П Р О Т О К О Л

Огляду № Место для ввода текста.

Место для ввода текста. **Место для ввода даты.**

Огляд розпочато о Место для ввода текста.
Огляд закінчено о Место для ввода текста.

Старший слідчий І відділу Департаменту спеціальних розслідування військових злочинів Державного Бюро Розслідувань Выберите элемент. (П.І.Б. слідчого), здійснюючи досудове розслідування кримінального провадження, зареєстрованого у ЄРДР за номером Место для ввода текста. від Место для ввода даты. за ч. 2ст. 437, ч. 2 ст. 437, 440 КК України, в службовому кабінеті № Место для ввода текста. приміщення Державного Бюро Розслідувань (01032, 15 Симона Петлюри, буд. 15), при змішаному освітленні, дотримуючись вимог ст.ст. 104-106, 237 КПК України, провів огляд віртуального простору без спеціальних умов (наприклад, без необхідності надавати дані доступу до закритого облікового запису) використовуючи операційні можливості додатку «Телеграм», а саме спеціального відкритого публічного профайлу, зареєстрованого за користувачем: **"KREML.NOVOSTI", ID: t.me/news_kremlin, located URL: https://www. t.me/news_kremlin**

Огляд проведено на персональному службовому комп'ютері:

Device name: DESKTOP-7ABMTT1, Processor: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz, Installed RAM: 16.0 GB (15.9 GB usable), Device ID: 5D646F90-EF6C-4345-83D5-1394429B74C7, Product ID: 00329-10330-00000-AA552, System type: 64-bit operating system, x64-based processor Windows specifications: Edition: Windows 10 Enterprise, Version: 20H2, OS build: 19042.2130

За результатами огляду встановлено:

Після того як ми відкриваємо посилання за адресою URL: https://www.t.me/news_kremlin, ви маєте можливість отримати інформацію про телеграм-канал. Посередині екрана ви знайдете біле поле з назвою каналу KREML.NOVOSTI і відображення голограми синього кольору за якою можна встановити верифікувати телеграм канал. На цьому ж каналі також можна подивитися кількість підписників [Место для ввода текста.] на дату проведення огляду. В подальшому натискаємо на ідентифікатор синьої кнопки на позначку – «Переглянути у Телеграм». Натискаємо на ліку кнопку мишкою що надасть можливість переглянути повну інформацію за профілем

«Телеграм Робочий додаток».

Знімок № 1 – Опис сторінки Головного каналу користувача за профілем "Kreml. Novosti"

Шляхом натискання лівою кнопкою на «Перегля Телеграму» маємо повну інформацію що дозволить ідентифікувати канал. На наступному зображенні ми можемо переглянути відомості каналу «Телеграм» розділені на три секції. В лівій секції Ви маєте можливість отримати інформацію про поточні оперативні контакти цього профіля, в середньому – це стіна зі всіма повідомленнями абонента (заяви, відео, фото). Відкриваючи канал в додатку надасть Вам

можливість переглянути інформацію щодо останніх повідомлень абонента. В правій частині екрану – Ви можете ознайомитись з відомостями щодо каналу, а саме: Фото профілю, URL адреси, кількість фото, відео матеріалів, поширень). В ході проведення огляду останнє повідомлення, відображено на каналі – Зустріч Президента РФ з Президентом Республіки Азербайджан від Место для ввода даты., час Место для ввода текста..

Знімок № 2 – Опис сторінки Головного каналу користувача за профілем"Kreml. Novosti"

Перемотуючи стіну каналу ми можемо знайти відомості щодо попередніх даних, відображених на даному каналі. Для, прикладу ми знайшли повідомлення про живу трансляцію промови путіна щодо оголошення масових атака України як поста за атаку на Кримський міст.

Знімок № 3 – Опис сторінки Головного каналу користувача за профілем"Kreml. Novosti" від Место для ввода даты.

Натискаючи правою кнопкою мишки на відео ми маємо можливість загрузити відео.

Знімок № 4. – Демонструє можливості завантаження змісту Телеграм каналу "Kreml. Novosti" відМесто для ввода даты., **час** Место для ввода текста.

Шляхом натискання лівої кнопки мишки ми здійснюємо збереження файлу за назвою:

«Совещание_с_постоянными_членами_Совета_Безопасности.mp4».

Розміри відео Место для ввода текста.Kb – Деталі наведенні в подальшому:

Довжина відео Место для ввода текста. хвилини. Виходячи з даних вказаних вище створено Место для ввода даты.о час Место для ввода текста..

Загружено відео так само як і знімки екранів ідентифікується за адресою:

Совещание_с_постоянными_членами_Совета_Безоп асности.md5 file with theresult "cfe62187d3f333a85afd6329d4bd7d19

*Совещание_с_постоянными_членами_Совета_Безопасности.mp4", the Telegram screenshots.md5 file with the result"4584c4cab8a7c96a9ebb21c2f4a67513 *Telegram screenshots.docx" and video properties.md5 file with the result "acfa27a5290a2f3f47cfd1eb4bc0ef5b *video properties.docx"

Для перевірки автентичності використано можливості Total Commander x64 10.51.

Будь-які зміни, внесені до змісту цих файлів будуть змінювати типовий ідентифікаційний номер первинного, вказаного вище файлу.

Зібрані відеоматеріали від копійовано на носії інформації, опечатано та приєднано до матеріалів кримінального провадження.

Старшний слідчий І відділу
Департаменту спеціальних
розслідуваннявійськовних злочиннів
Державного Бюро Розслідувань **Выберите элемент.**
І. Прізвище

Алгоритм виконання:

Перше поле – це номер договору.

Виконайте наступні дії:

1. Клацніть «мишею» праворуч від символу № у першому рядку договору.

2. На вкладниці *Разработчик* в групі ***Элементы управления*** **нажміть кнопку** ***Режим конструктора,*** **а потім** ***Элемент управления содержимым «обычный текст».*** Уведіть будь-яку цифру номера договору замість тексту *Местодля ввода текста* і нажміть *ОК.*

3. Наступна перемінна частина договору – це дата договору. Дата теж вставляється як поле, але це буде не поле форми, а поле дати, що буде заповнено автоматично поточною датою із системної дати комп'ютера (що має бути встановлена правильно!) завжди в день складання договору.

4. Для цього на вкладниці *Вставка* в групі *Текст* виберіть команду ***Дата и время*** і в діалоговому вікні ***Дата и время,*** що відкриється, вибрати ***Формат*** **дати нажати** ***ОК.*** Установіть прапорець ***Обновлять автоматически.***

5. Наступне поле – прізвище виконавця (ім'я замовника, тобто видавництво, вважається фіксованим). Це поле можна оформити як текстове у разі, якщо є тільки один можливий виконавець – автор, але ми допустимо, що видавництво працює з деякою кількістю постійних авторів, і оформимо це поле як список авторів, з яких потрібно вибрати тільки одного. Для його настроювання виконуємо ***Разработчик> Элементыуправления> Режим конструктора> Поле со списком >Свойства***. У діалоговому **вікні** ***Свойства элемента управления*** *содержимым* нажміть кнопку ***Добавить***. В діалоговому вікні *Добавить вариант* ввести ПІБ першого автора і нажати *ОК.* Таким чином введіть ПІБ інших авторів. Довідку по цьому полю введемо таку: *Виберіть зі списку потрібного виконавця.* Для цього у діалоговому вікні ***Свойства элемента управления содержимым*** введіть цей текст в пункті ***Общие>Название***.

6. Таким же чином заповніть поле назви творів (поле зі списком), суми винагороди (текстове поле).

7. Поле терміну виконання роботи оформіть у вигляді поля форми дати. Для цього при включеному ***Режимі конструктора*** виберіть ***Элемент управления содержания «выбор даты»*** і нажміть кнопку ***Свойства***. У вікні, що відкриється, виберіть ***Формат отображения данных і дату***, а потім клавішу ***ОК***.

8. Далі за аналогією оформіть поля: ***Прізвище, ім'я, по батькові***

Виконавця, Паспортні дані і Прізвище, ініціали як прості текстові поля.

9.Поки що наш документ – це звичайний текстовий документ із полями форми. Уся відмінність полягає в тому, що введені поля форми підсвічені сірим й у них не попадає курсор введення.

Главная>Редактирование>Выделить>Выделитьвсе, Разработчик> Элементы управления> Группировать> Группировать інаш документ перетвориться в інтерактивну форму, яку можна заповнити, зберегти на диску й надрукувати. Типовий договір можна оформити на комп'ютері за 5 хвилин і без помилок редагування!

10. Ми створили електронну форму для заповнення типового договору. Можна натиснути на кнопку Сохранить стандартної панелі інструментів.

Одержимо просто документ з полями. Можна звичайно робити так: відкривати вже заповнену форму договору, заповнювати її й зберігати під новим ім'ям. Але набагато доцільніше скористатися механізмом шаблонів.

11. Для того, щоб створити шаблон на основі нашої форми, потрібно взяти незаповнену форму і зберегти її як шаблон: **Файл >Сохранить как> Шаблон** документа>Вибрати дисковод і, якщо необхідно, створити папку > Відкрити створену папку > Задати ім'я файлу (тобто шаблона) > Сохранить.

12. Тепер можна скільки завгодно створювати договори за створеним шаблоном. Для цього потрібно відкрити необхідний шаблон через меню **Файл > Создать**, з'явиться новий документ із текстом договору, а курсор буде знаходиться у полі номеру договору, де за замовчуванням введена цифра 1. Введіть новий номер, натисніть на Tab. Курсор після цього перейде до нового поля введення, введіть знову інформацію і так далі. Після введення останнього поля збережіть новий договір як звичайний файл Word з відповідним ім'ям (Якщо після введення значення останнього поля натиснути на Tab, курсор знову попадає на перше поле, тобто можна відразу ж переходити до підготовки нового варіанта договору). Отриманий документ можна також надрукувати в потрібній кількості екземплярів.

Висновки. Ми створили нескладну шаблон-форму. У юридичній та службові практиці вміння використовувати шаблони-форми має дуже велике значення, тому що при цьому завжди гарантується незмінність основної частини документа і заощаджується час на його підготовку. У нашій роботі не вичерпані всі можливості використання полів форм, наприклад можна в одні поля вводити числові значення, при цьому інші

поля можуть містити формули, що використовують введені значення. Ця робота є лише введенням у створення шаблонів документів із використанням полів форм.

Завдання № 2

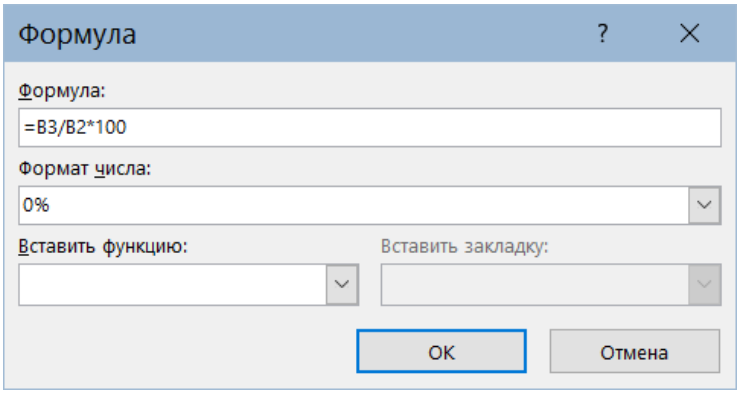
1. Створити таблицю- ЗВІТ за зразком:

	січень	**лютий**	**березень**	**квітень**	**травень**	**червень**	**Сума запершепівріччя**
План розкриття злочинів	45	46	36	58	48	67	?
Факт	56	47	38	48	49	76	?
% виконання плану	?	?	?	?	?	?	

2. Виконати форматування таблиці за зразком.

3. Для розрахунку *% виконання плану* в таблиці необхідно курсор розташувати комірку B5, потім активізувати вкладку *Макет→Данные→Формула*, ввести формулу (рис. 1), встановити процентний формат числа та натиснути кнопку *ОК*.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	
1		**січень**	**лютий**	**березень**	**квітень**	**травень**	**червень**	**Сума за перше півріччя**
2	**План розкриття злочинів**	45	46	36	58	48	67	?
3	**Факт розкриття злочинів**	56	47	38	48	49	76	?
4	**% виконання плану**	=(B3/B2)*100						



5. Виконати розрахунок показників розкриття злочинів за1 півріччя.

6. Виконати розрахунок загального *% виконання плану* за 1 півріччя за планом та за фактом. Для цього ввести до комірки H3 формулу =СУММ(B3:G3).

7. Відпрацювати команди редагування та форматування вкладки *Главная*:

– випробувати різні види та розміри шрифтів. Для швидкого форматування таблиці обрати пункти вкладки *Главная* групи *Стили* та спробувати декілька стилів;

– зробити ширше колонку H. Змінити форму зображення чисел у цієї колонці, -- обираючи *Макет→Данные→Формула* формат *Денежный*.

– вставити новий стовпчик перед 1-им та ввести автоматичну нумерацію стовпчиків, використовуючи команду Главная→*Нумерация.*

Завдання № 3

1. Шість дільничних розкрили відповідну кількість злочинів, загальним обсягом 153 злочини за рік. Розрахувати внесок кожного дільничного до загального фактичного розкриття злочинів на дільниці у відсотках (%) і визначити розподіл загального виконання плану за кожним дільничним.

Розподіл розкриття злочинів на дільниці H.				
№	***ПІБ***	***Кількість розкритих злочинів (факт), шт***	***%***	***Кількість розкритих злочинів (план), шт***
1	Свиридов А. П.	19	?	?
2	Коваль І. Н.	18	?	?
3	Береза А. А.	32	?	?
4	Бабич Н. К.	17	?	?
5	Андрєєв С. С.	53	?	?
6	Короб В. Д.	14	?	?
Разом		?		180

Завдання № 4

1. Вставте такі колонтитули:

верхній колонтитул – ПІБ; верхній колонтитул – №_групи; нижній колонтитул – дата; нижній колонтитул – № стор.

Завдання № 5

1. Створіть таблицю для роботи з формулами

Тип конструкції	Приклад
Дробу	$10\frac{9}{11}$
Оператори	$\int_1^3 x^3 + 5x \quad \sum_{n=1}^{10} x^2 + 2x$
Корінь	$\sqrt{\frac{3RT}{mN_A}} \quad \sqrt[3]{2345}$
Визначники й матриці	$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 6 & 0 \\ 5 & 5 & 3 \end{vmatrix} \quad \begin{pmatrix} 5 & 4 & 2 \\ 3 & 3 & 4 \\ 1 & 2 & 1 \end{pmatrix}$
Векторний запис виразів	$\vec{E} = \frac{\vec{F}}{q}$
Рівняння	$A = \frac{RT_1}{\gamma - 1}\frac{m}{\mu}\left[1 - \left(\frac{V_1}{V_2}\right)^{\gamma-1}\right]$
$r_e = \frac{\sum_{i=1}^{n-1} x_i x_{i+1} - \frac{1}{n-1}\sum_{i=1}^{n-1} x_i \sum_{i=1+1}^{n} x_i}{\sqrt{\left[\sum_{i=1}^{n-1} x_i^2 - \frac{1}{n-1}\left(\sum_{i=1}^{n-1} x_i\right)^2\right]\left[\sum_{i=1+1}^{n} x_i^2 - \frac{1}{n-1}\left(\sum_{i=1+1}^{n} x_i\right)^2\right]}}$	
$\alpha(pH) = \int_{-\infty}^{\infty} \alpha(pH, pK)\rho(pK)dpK = \int_{-\infty}^{\infty} \rho(pK)\frac{c(pK)}{1 + \exp[2.303(pK - pH)]}dpK$	

Завдання № 6

1. Наведений нижче текст необхідно розмістити в дві колонки.

Закон України «Про інформацію» № 2657-XII від 02.10.1992 редакція від 27.07.2023. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text.

Стаття 1. *Визначення термінів*

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

- *документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;*
- *захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;*
- *інформація – будь-які відомості та/або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;*
- *суб'єкт владних повноважень – орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.*

Стаття 2. *Основні принципи інформаційних відносин*

1. Основними принципами інформаційних відносин є:

- *гарантованість права на інформацію;*
- *відкритість, доступність інформації, свобода обміну інформацією;*
- *достовірність і повнота інформації;*
- *свобода вираження поглядів і переконань;*
- *правомірність одержання, використання, поширення, зберігання та захисту інформації;*
- *захищеність особи від втручання в її особисте та сімейне життя.*

Стаття 3. *Державна інформаційна політика.*

1. Основними напрямами державної інформаційної політики є:

- *забезпечення доступу кожного до інформації;*
- *забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;*

– створення умов для формування в Україні інформаційного суспільства;

– забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

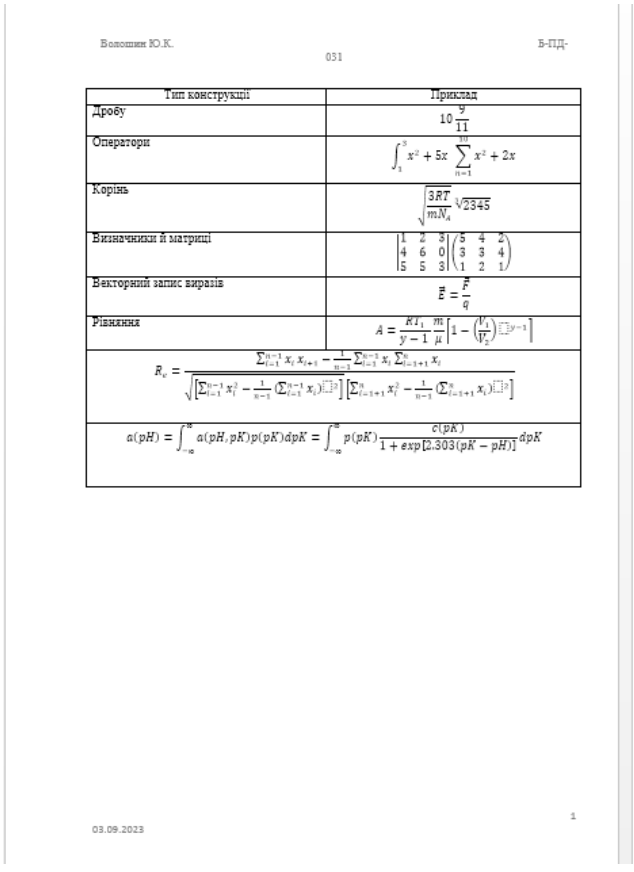
– створення інформаційних систем і мереж інформації, розвиток електронного урядування;

– постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

– забезпечення інформаційної безпеки України;

– сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

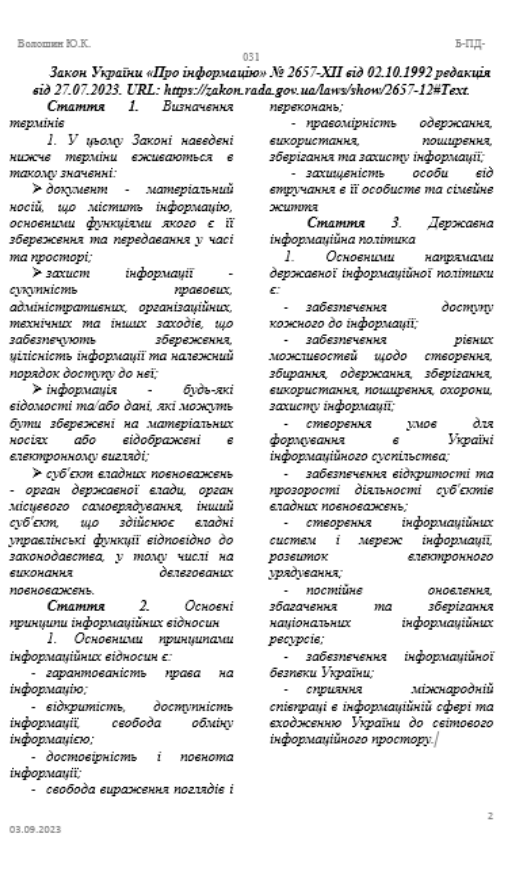
Зразок виконання



Болошин Ю.К. 051 Б-ПД-

Тип конструкції	Приклад
Дробу	$10\frac{9}{11}$
Оператори	$\int_1^3 x^2+5x \sum_{n=1}^{10} x^2+2x$
Корінь	$\sqrt{\frac{3RT}{mN_A}}\sqrt{2345}$
Визначники й матриці	$\begin{vmatrix}1&2&3\\4&6&0\\5&5&3\end{vmatrix}\begin{pmatrix}5&4&2\\3&3&4\\1&2&1\end{pmatrix}$
Векторний запис виразів	$\vec{E}=\frac{\vec{F}}{q}$
Рівняння	$A=\frac{RT_1}{y-1}\frac{m}{\mu}\left[1-\left(\frac{V_1}{V_2}\right)^{y-1}\right]$
$R_{x_i}=\frac{\sum_{i=1}^{n-1}x_i x_{i+1}-\frac{1}{n-1}\sum_{i=1}^{n-1}x_i\sum_{i=1}^{n}x_i}{\sqrt{\left[\sum_{i=1}^{n-1}x_i^2-\frac{1}{n-1}(\sum_{i=1}^{n-1}x_i)^2\right]\left[\sum_{i=1+1}^{n}x_i^2-\frac{1}{n-1}(\sum_{i=1+1}^{n}x_i)^2\right]}}$	
$a(pH)=\int_{-\infty}^{\infty}a(pH,pK)p(pK)dpK=\int_{-\infty}^{\infty}p(pK)\frac{c(pK)}{1+exp[2.303(pK-pH)]}dpK$	

03.09.2023 1



Болошин Ю.К. 051 Б-ПД-

Закон України «Про інформацію» № 2657-XII від 02.10.1992 редакція від 27.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

Стаття 1. *Визначення термінів*

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

➢ документ - матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

➢ захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

➢ інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

➢ суб'єкт владних повноважень - орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Стаття 2. *Основні принципи інформаційних відносин*

1. Основними принципами інформаційних відносин є:

- гарантованість права на інформацію;

- відкритість, доступність інформації, свобода обміну інформацією;

- достовірність і повнота інформації;

- свобода вираження поглядів і переконань;

- правомірність одержання, використання, поширення, зберігання та захисту інформації;

- захищеність особи від втручання в її особисте та сімейне життя

Стаття 3. *Державна інформаційна політика*

1. Основними напрямами державної інформаційної політики є:

- забезпечення доступу кожного до інформації;

- забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

- створення умов для формування в Україні інформаційного суспільства;

- забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

- створення інформаційних систем і мереж інформації, розвиток електронного урядування;

- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

- забезпечення інформаційної безпеки України;

- сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

03.09.2023 2

Збережіть документ із ПІБ, група ПР 2.3 і надішліть на перевірку викладачу.

Завдання № 7

1. Створити макрос, що буде призначений для виконання форматування тексту у наступному вигляді: виділений текст курсивом та у лапках – *«ПІБ»*
2. Прив'язати макрос до кнопки, яку треба створити на панелі задач.
3. Зберегти макрос. Та перевірити його виконання.

Завдання № 8

1. Створити макрос, що буде робити вставку таблиці за зразком.
2. Прив'язати макрос до кнопки, що треба створити на панелі задач.
3. Зберегти макрос. Та перевірити його виконання.

Зразок:

Збережіть документ з ПІБ, група та номер ПЗ і надішліть на перевірку викладачу.

Важливо: *Правильно виконана робота перевірка файл має розширення *docm і має вигляд, як файл зі знаком оклику (рис. 2.34).*

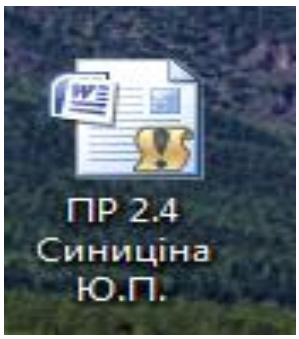


Рис. 2.34. Загальний вигляд файлу з макросом

Завдання № 9.

1. Створити макрос, що буде призначений для виконання форматування тексту у наступному вигляді титульної сторінки. Зразок наведено нижче.
2. Прив'язати макрос до кнопки, що треба створити на панелі задач.
3. Зберегти макрос та перевірити його виконання.

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІЙ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ПРАКТИЧНА РОБОТА 2.4

З ДИСЦИПЛІНИ «ІНФОРМАЦІЙНІ ТА КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ»

Курсанта гр. КП-135
Синиціної Ю.П.

Дніпро, рік

Контрольні питання

1. Охарактеризуйте поняття «форми» у Word
2. У якій вкладці знаходяться елементи керування «формою»?
3. Що таке шаблон типового документа в Microsoft Word?
4. Які можливості надають поля форм у шаблонах типових документів?
5. Які типи полів форм доступні в Microsoft Word і для чого вони використовуються?

6. Як налаштувати поле форми в шаблоні типового документа?
7. Як забезпечити захист полів форми в шаблоні типового документа від змін?
8. Як створити таблицю у Microsoft Word, здійснити переміщення у таблиці, вставити рядок наприкінці таблиці?
9. Як увести формулу до комірки таблиці?
6. Які є способи створення таблиць?
10. Як об'єднати клітинки в одну?
11. Як змінити орієнтацію тексту?
12. Як поміняти розмір шрифту в клітинці?
13. Яким чином можна змінити висоту та ширину комірок?
14. Яким чином проводити розрахунки в таблиці документу Microsoft Word?
15. Охарактеризуйте поняття «*Колонтитул*» у Word
16. Опишіть методи, що застосовуються для створення та для редагування колонтитулів.
17. Можливо розширити Колекцію формул? Яким чином?
18. Яким чином можливо розмістити текст у колонки? Опишіть механізм.
19. Яким чином можливо проводиться налаштування вкладки «Розробник? Опишіть механізм.
20. У якій вкладці або вкладках знаходиться редактор «Макроси»?
21. Опишіть механізм формування кнопки макросу на панелі швидкого доступу та формування «горячих клавіш» макросу на клавіатурі?
22. Яке розширення має файл зі збереженим макросом у документі?
23. Чи можливе створення шаблону документу з макросом?

Джерела до розділу 1

1. Інформаційні системи та технології: підручник / кол. авт.; ред. В. Б. Вишня. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2021. 296 с.
2. Нелюбов В. О., Куруца О. С. Основи інформатики. Microsoft Word 2016: електронний навчальний посібник. Ужгород : ДВНЗ УжНУ, 2018. 96 с.
3. Microsoft Office 2016 / Office365. Керівництво. URL : https://www.microsoft.com/uk-ua/microsoft-365/previous-versions/microsoft-office-2016.
4. Технічна підтримка ресурсів корпорації Google. URL : https://support.google.com/docs/topic/ 9054603?hl=ru&ref_topic=1382883.

Розділ 3
ВИКОРИСТАННЯ ТАБЛИЧНОГО ПРОЦЕСОРА MS EXCEL ДЛЯ АНАЛІТ ИЧНОЇ ДІЯЛЬНОСТІ

3.1. Табличні процесори. Графічне подання даних. Застосування логістичних функцій

Електронна таблиця (ЕТ) – це програма, що моделює на екрані двовимірну таблицю, яка складається з рядків і стовпчиків. Особливістю ЕТ є те, що в них структурування інформації починається безпосередньо на етапі введення даних: із самого початку свого існування в машинній формі вони прив'язуються до структурних підрозділів таблиць – *комірок*.

Основне призначення процесорів електронних таблиць – обробка інформації, що організована в таблиці, проведення розрахунків на її основі і забезпечення візуального представлення збережених даних і результатів їх обробки (у виді графіків, діаграм і т.п.).

Microsoft Excel – табличний процесор, програма для створення й обробки електронних таблиць.

Робочою книгою називають *файл* Microsoft Excel. *Робоча книга* складається з ***листів***, імена яких (Лист1, Лист2, …) виведені на ярликах у нижній частині вікна. Під час натискання на ярлики, можна переходити від листка до листка. Для прокручування ярликів використовують кнопки ліворуч від горизонтальної координатної лінійки (рис. 3.1):

перехід до ярлика першого листка;
перехід до ярлика попереднього листа;
перехід до ярлика наступного листа;
перехід до ярлика останнього листа.

Рис. 3.1. Загальний вигляд ярлика

Робочий лист є таблицею, що складається з 16384 стовпчиків і 1048576 рядків. Стовпчики іменуються латинськими буквами від A до XFD, а рядка – цифрами. Кожна комірка таблиці має адресу, що

складається з імені рядка й імені стовпчика. Наприклад, якщо комірка знаходиться в стовпчику F і рядку 7, то вона має адресу F7.

Виділення декількох суміжних комірок: встановити покажчик миші у комірку, натиснути ЛК миші і, не відпускаючи її, розтягти виділення на всю область.

Виділення декількох несуміжних груп комірок: виділити одну групу комірок, натиснути клавішу *Ctrl* і, не відпускаючи її, виділити інші комірки.

Виділення стовпця чи рядка таблиці: натиснути мишею на його імені. Для виділення декількох стовпців чи рядків необхідно натиснути на імені першого стовпчика чи рядка і розтягти виділення на всю область.

Виділення декількох листів: натиснути клавішу *Ctrl* і, не відпускаючи її, клацати на ярликах листів.

Обчислення в таблицях виконуються за допомогою *формул.* Формула може складатися з математичних операторів, значень, посилань на комірку в імен функцій. Результатом виконання формули є деяке нове значення, що міститься в комірці, де знаходиться формула. Після натискання клавіші Enter у комірці з'явиться результат обчислення. При виділенні комірки, що містить формулу, ця формула з'являється в рядку редагування.

Функціями в Microsoft Excel називають об'єднання декількох обчислювальних операцій для розв'язання визначеної задачі. Функції в Microsoft Excel являють собою формули, що мають один або кілька аргументів. Як аргументи вказуються числові значення або адреси комірок.

Для введення функції в комірку необхідно:

– виділити комірку для формули;

– викликати *Майстер функцій* за допомогою команди *Вставить функцію* вкладки *Формулы* групи інструментів *Библиотека функцій* або кнопки f_x;

– у діалоговому вікні *Мастер функций*, вибрати тип функції в полі *Категория,* потім функцію в списку *Функция* та натиснути кнопку ОК.

Формати чисел. Кожне число в таблиці можна представити в різних форматах (з різною кількістю десяткових позицій, незначущих нулів та ін.). Для зміни формату вмісту комірки необхідно:

– виділити комірку;

– јбрати групи інструментів *Число* вкладки *Главная*;

– у діалоговому вікні *Формат ячеек* вибрати вкладиш *Число*;

– у списку *Числовые форматы* вибрати тип формату вмісту

комірки, а в полях праворуч – параметри формату;

– у полі *Образец* буде відображений приклад вмісту комірки в обраному форматі;

– щоб увести новий формат, необхідно вибрати пункт *Все форматы*, а потім у поле *Тип* увести новий формат та натиснути ОК.

Побудова гістограми виконаємо із застосуванням пункту меню *Вставка, Діаграми* (рис. 3.2, 3.3).

Задайте усі атрибути діаграми (назву, підпис даних, легенда) (рис. 3.4). Розмістіть гістограму на цьому робочому листі.

Щоб розмістити гістограму на окремому робочому листі, необхідно активізувати її, натиснути контекстне меню правої кнопки миші:

Формула починається зі знаку «=«. Для вставки у формулу вбудованих функцій треба натиснути кнопку на кнопку (вставка функції) у полі зліва від рядка формул і обрати у вікні Мастер функцій відповідну функцію.

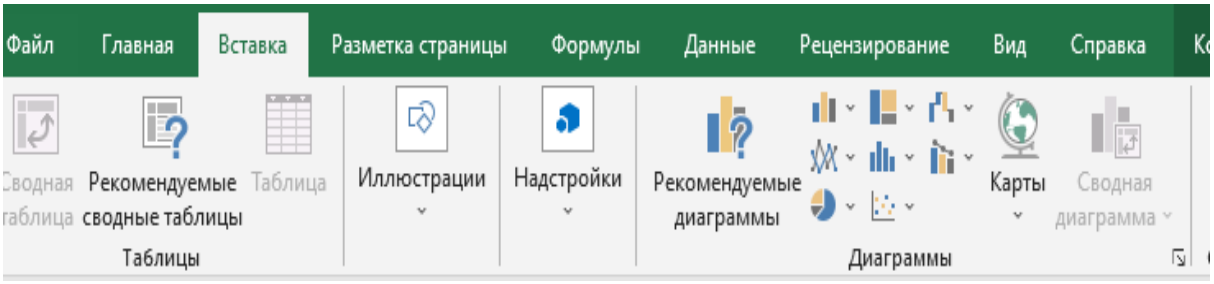


Рис. 3.2. Пункт меню *Вставка, Діаграми*

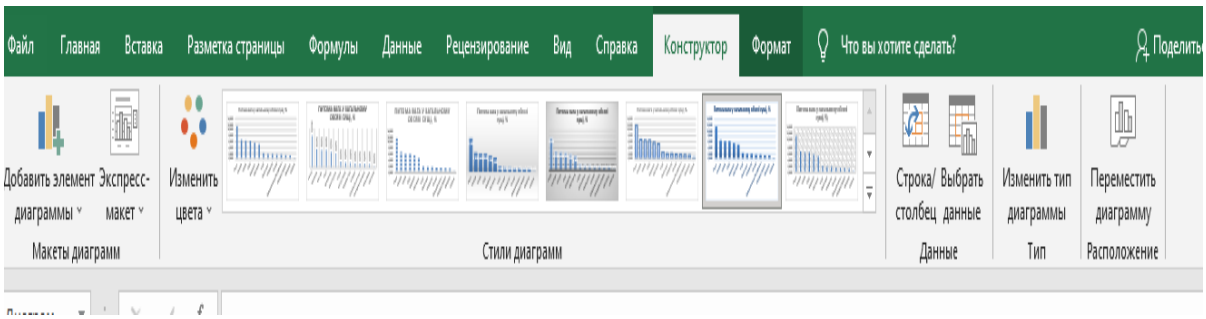


Рис. 3.3. Пункт меню *Конструктор* роботи з діаграмами

У тому ж вікні надається синтаксис функції та можливість викликати команду Справка по функции

Функція СРЗНАЧ, МИН, МАКС знаходять у вкладці Формула – Дригие функції – Статистические. (рис. 3.5).

СРЗНАЧ – функція, що визначає середнє значення.

МИН – функція, що визначає мінімальне значення.

МАКС– функція, що визначає максимальне значення.

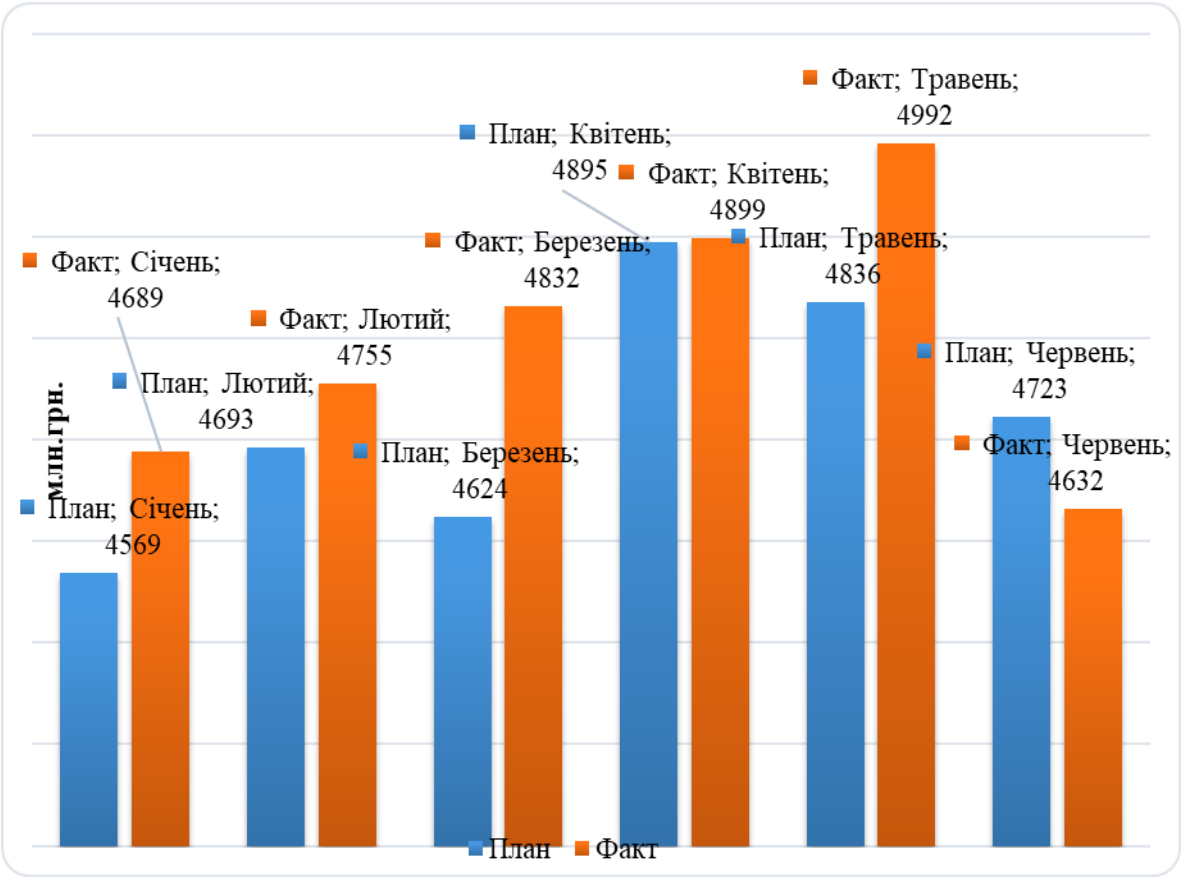


Рис. 3.4. Гістограма плану та факту показників виробництва

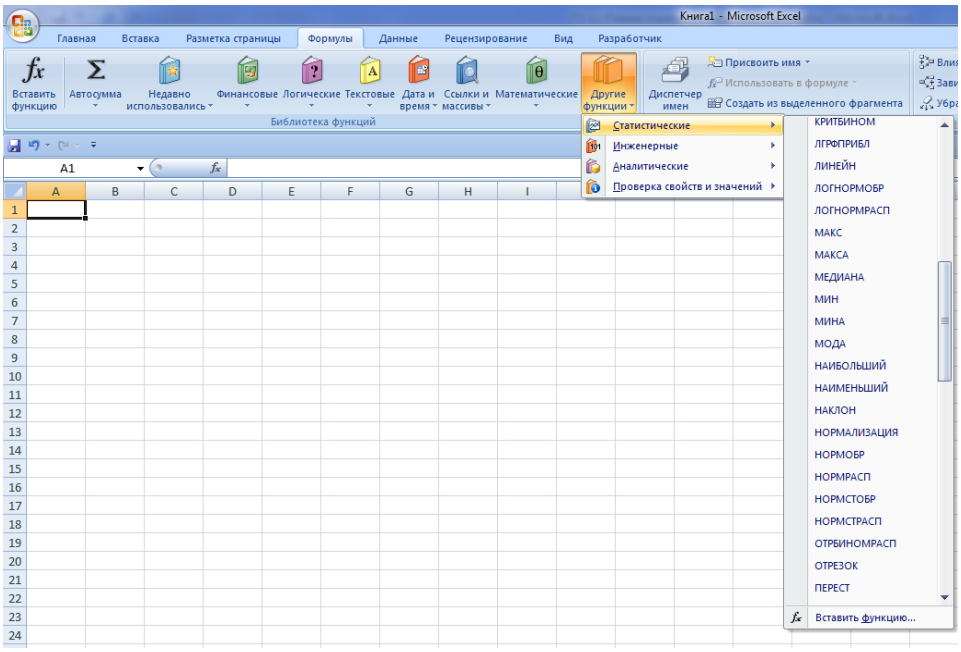


Рис. 3.5. Розташування статистичних функцій СРЗНАЧ, МИН, МАКС

Функція ЕСЛИ широко використовується в Excel для розв'язку багатьох задач. Вона перевіряє, чи виконується умова та повертає одне значення, якщо воно виконується та інше значення, якщо ні. Функція ЕСЛИ розташовується у вкладці *Формула – Логистические* рис. 3.6.

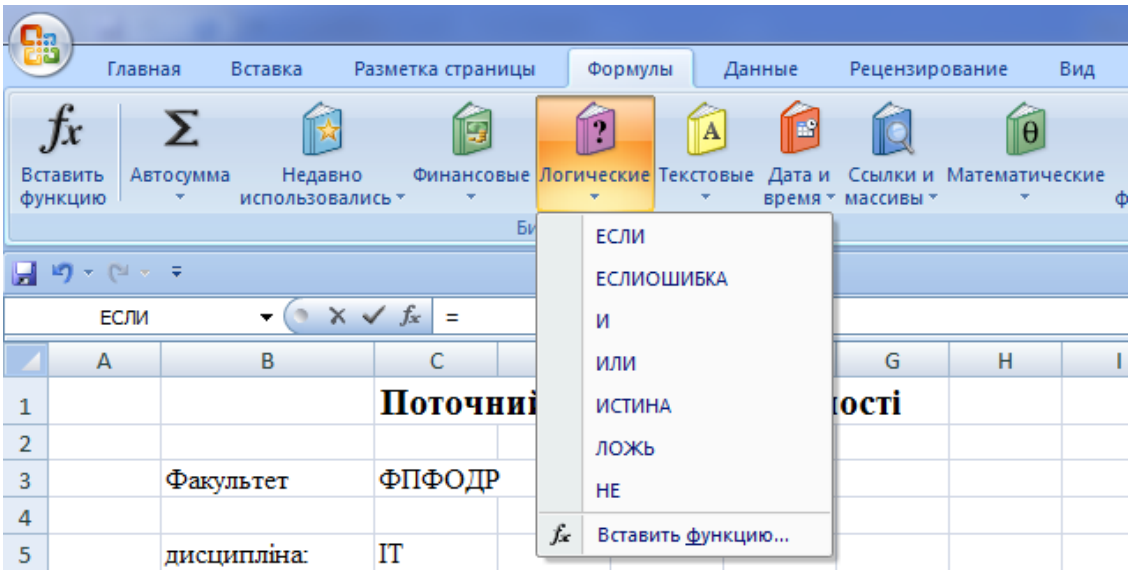


Рис. 3.6. Розміщення вкладки Логістичні функції

Синтаксис функції ЕСЛИ:

=*ЕСЛИ*
([лог_выражение;значение_если_истина];[значение_если_ложь])

лог_выражение – це значення або вираз, що під час обчислення дає значення *ИСТИНА* або *ЛОЖЬ*. Тобто, якщо вираз під час обчислення дає значення *ИСТИНА*, то вираз вірний (рис. 3.7).

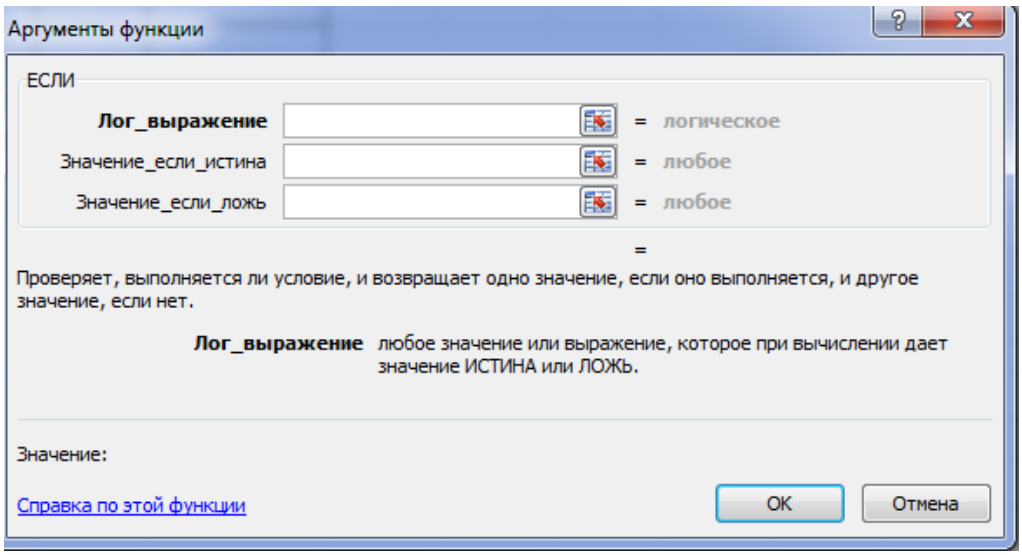


Рис. 3.7. Загальний вигляд вікна Аргументи функції ЕСЛИ

3.2. Вивчення основних понять, створення простої таблиці та організація звичайних обчислень в MS EXCEL

Редактор таблиць Microsoft Excel має дуже широкий набір можливостей для вирішення завдань самої різної складності в різних сферах діяльності. Саме завдяки цьому Ексель став таким популярним серед користувачів по всьому світу. Одним із базових навичок роботи з програмою є проведення найпростіших обчислень і математичних операцій.

Усі розрахунки в Ексель засновані на побудові простих формул, за допомогою яких програма і буде робити обчислення. Для початку слід створити таблицю зі значеннями. Зверніть увагу на те, що кожна клітинка таблиці має свою адресу, який визначається буквою і цифрою. Кожна буква відповідає стовпцю, а кожна цифра під час обчислення рядку.

Формула – це вираз, що задає операції над даними в клітинках електронної таблиці та порядок їх виконання.

Формула може містити:

- числа;
- тексти;
- посилання на клітинки чи діапазони клітинок;
- знаки математичних дій (оператори);
- дужки та імена функцій.

Формула завжди починається зі знаку =

Множення та ділення в Excel дуже прості, але потрібно створити просту формулу. Просто пам’ятайте, що всі формули в програмі Excel починаються зі знака рівності (=), і для їх створення можна використовувати рядок формул.

Для виконання цього завдання використовується арифметичний оператор * (зірочка).

Щоб виконати це завдання, скористайтеся арифметичним оператором / (скісна риска).

Наприклад, якщо ввести = 10/5 у клітинках, у ній відображається 2.

Арифметичні оператори:

Додавання (a+b)	+
Віднімання (a-b)	-
Множення (a*b)	*
Ділення (a/b)	/
Зведення в ступінь (a^b)	^
Витяг коріня (√(b&a))	^(1/X)

Володіючи навичками простих арифметичних обчислень в програмі Microsoft Excel, ви вже зможете спростити собі процес вирішення деяких завдань і заощадити час. Ексель дозволяє вирішувати складні рівняння, виконувати інженерний і статистичний аналіз.

3.3. Вивчення особливостей формування мікрографіків та використання опції «Примітки» у MS EXCEL

Побудова мікрографіків у клітинках у MS Excel.

Міні-діаграми (спарклайни) – це мікрографіки, що містяться в одну клітинку аркуша. Використовуються для наочного відображення зміни даних.

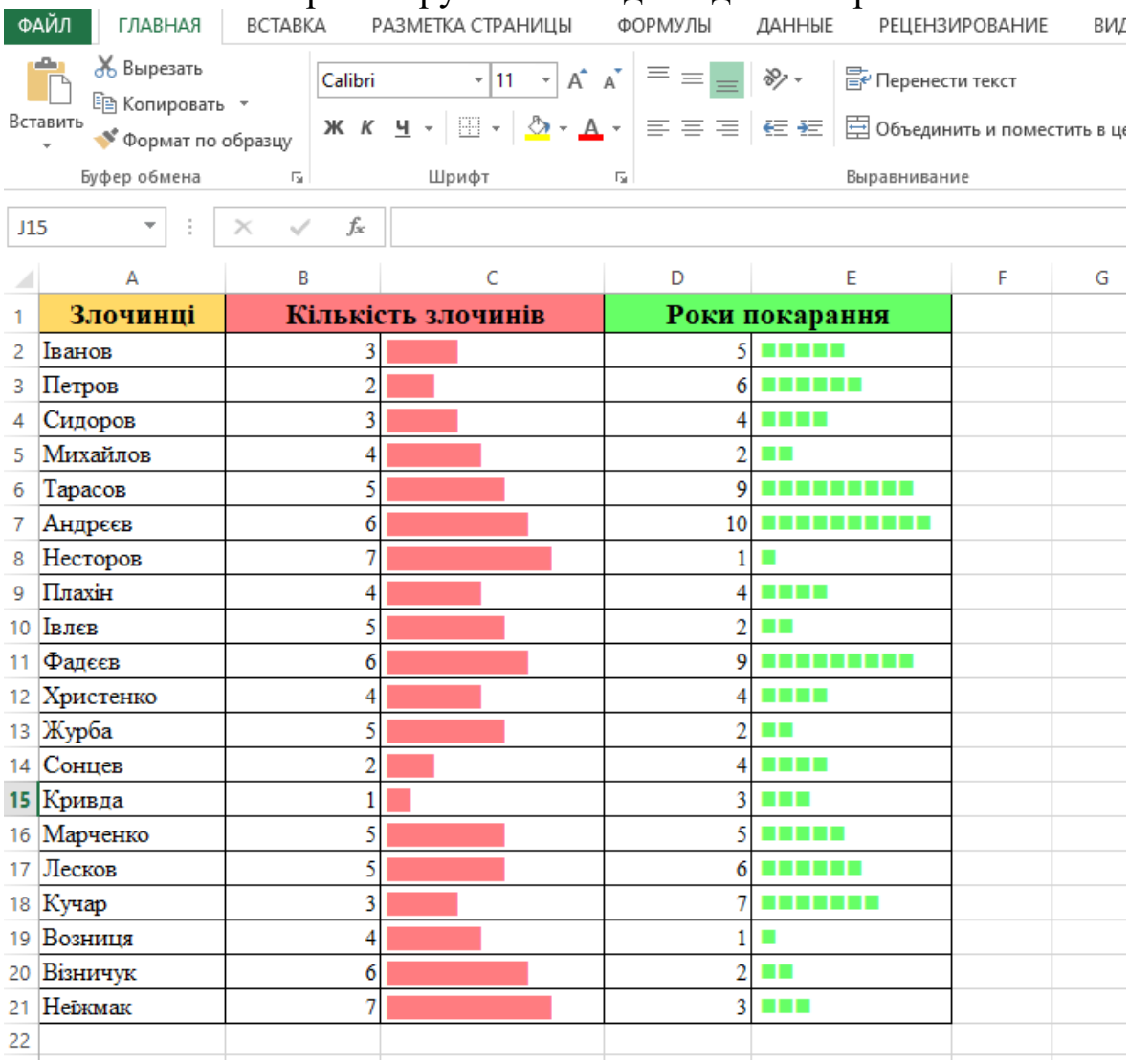
Для створення мікрографіка необхідно перейдіть на вкладку Вставити → область мікрографік (рис. 3.8). MS Excel пропонує три типи мікрографіка: графік, гістограму і діаграму виграш / програш. Остання показує стовпчиками однакової висоти значення + і -.

Рис. 3.8. Меню мікрографіка

Розглянемо побудову мікрографіка на прикладі рейтингу країн із найрозвиненішою економікою в світі за даними 2020 року (табл. 3.1).

Таблиця 3.1

Облік правопорушень та відповідне покарання



	A	B	C	D	E	F	G
1	**Злочинці**	**Кількість злочинів**		**Роки покарання**			
2	Іванов	3		5	■■■■■		
3	Петров	2		6	■■■■■■		
4	Сидоров	3		4	■■■■		
5	Михайлов	4		2	■■		
6	Тарасов	5		9	■■■■■■■■■		
7	Андрєєв	6		10	■■■■■■■■■■		
8	Несторов	7		1	■		
9	Плахін	4		4	■■■■		
10	Івлєв	5		2	■■		
11	Фадєєв	6		9	■■■■■■■■■		
12	Христенко	4		4	■■■■		
13	Журба	5		2	■■		
14	Сонцев	2		4	■■■■		
15	Кривда	1		3	■■■		
16	Марченко	5		5	■■■■■		
17	Лесков	5		6	■■■■■■		
18	Кучар	3		7	■■■■■■■		
19	Возниця	4		1	■		
20	Візничук	6		2	■■		
21	Неїжмак	7		3	■■■		
22							

У таблиці 3.1 наведено побудову мікрографіків з використанням функцій ПОВТОР (REPT) та СИМВОЛ (CHAR) у клітинці D2, де введено наступну функцію:

=ПОВТОР(СИМВОЛ(103);C2),

де 103 – код чорного прямокутника.

Після введення цієї функції для діапазону комірок D2:D11 слід задати шрифт Webdings.

Для побудови іншого типу мікрографіка в комірках E2:E11 введіть наступну функцію:

=ПОВТОР(СИМВОЛ(118);C2),

де 118 – код символу, що відображено у комірках E2:E11.

Після введення даної функції для діапазону комірок E2:E11

необхідно задати шрифт Wingdings.

Створення інших видів символів та їх кольору виконується через зміну коду та типу шрифта.

Створення примітки для комірки

У MS Excel є корисна опція, що дає можливість користувачу задавати для комірок коментарі. Коментарі можуть бути представлено у вигляді тексту чи фото. Така опція є такою, що часто застосовується та функціональною.

Використовуючи Інтернет, можливо створити каталог із товарів (побутової техніки, книг та інш.), як наведено в таблиці 3.2.

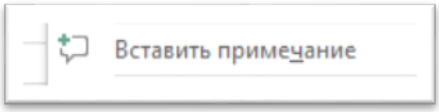
Таблиця 3.2

Товари

№ з/п	Товар	Ціна
1	Телевізор Samsung UE50TU7100	15000
2	Пилосос Samsung	7320
3	Чайник	1528
4	Холодильник Samsung	17500
5	Телефон	12450

Для формування каталогу потрібно додати до окремої папки фото усіх товарів, що наведено в таблиці 3.2.

Для створення примітки в комірці С2 натисніть правою кнопкою миші і з’явиться меню Додати примітку:



У вікні, що з’явилося, введіть назву товару, у нашому випадку: Телевізор. Щоб примітка не приховувалося під час редагування, клацніть по комірці правою кнопкою ще раз і виберіть *Змінити примітку*.

Клацніть правою кнопкою миші на примітці і виберіть пункт формат примітки. У вікні формат примітки активізуйте вкладку *Колір та лінії, Заливка, Колір, Способи заливки, Рисунок* та додайте фото телевізора (рис. 3.9).

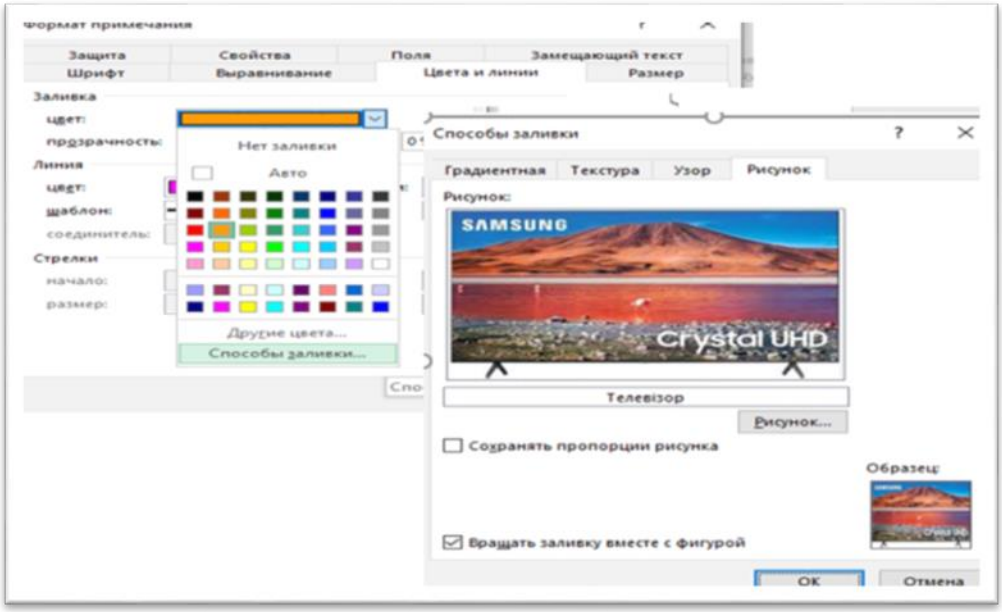


Рис. 3.9. Додавання фото товару до примітки

3.4. Табличний процесор Microsoft Excel: електронні бази даних, математичні функції, форм даних, типи діаграм та фільтрація

Для розв’язання задач в MS Excel необхідно подати електронну таблицю у вигляді списку.

Список – це один із засобів організації даних на робочому листі.

Дані, організовані в список, у термінології MS Excel називаються *базою даних* (БД). Зокрема, рядки таблиці – це *записи бази даних,* а стовпчики – *поля БД.*

Щоб перетворити таблицю MS Excel у список, слід надати стовпчикам імена, які будуть використовуватися як імена полів бази даних.

Створюючи список на робочому листі MS Excel необхідно дотримуватись певних правил:

– на одному робочому листі не варто поміщати більш одного списку, оскільки деякі операції, наприклад, фільтрація, не працюють водночас з кількома списками;

– варто відокремлювати список від інших даних робочого листа хоча б одним незаповненим стовпчиком або одним незаповненим рядком. Це допоможе MS Excel автоматично виділити список під час виконання фільтрації або в процесі сортування даних;

– список може займати весь робочий лист: 16384 рядки і 256 стовпчиків;

– імена стовпчиків мають бути розташовані в першому рядку

списку. MS Excel використовує ці імена під час створення звітів, для пошуку і сортування даних;

– для імен стовпчиків варто використовувати шрифт, тип даних, вирівнювання, формат, рамку чи стиль букв, відмінні від тих, що використовувалися для даних списку;

– щоб відокремити імена стовпчиків від даних, варто розмістити рамку по нижньому краю клітин рядка з іменами стовпчиків. Не рекомендується використовувати порожні рядки або пунктирні лінії;

– дані в кожному стовпчику мусять бути однотипними.

Функції дозволяють виконувати як прості, так і складні обчислення. Функції в Excel використовуються для виконання стандартних обчислень. Значення, що використовуються для обчислення функцій, називають аргументами. Значення, що повертаються функціями як відповідь, називають результатом. Окрім вбудованих функцій, можна використовувати в обчисленнях функції користувачів, що створюються за допомогою засобів Excel.

Синтаксис функцій. Щоб використати функцію, потрібно ввести її як частину формули в комірку робочого аркуша. Послідовність, у якій мають розміщуватися використовувані у формулі символи, називають синтаксисом функції. Усі функції використовують однакові основні правила синтаксису. Якщо порушити правила синтаксису, то Excel покаже повідомлення про помилку у формулі.

Для спрощення роботи з функціями більшість із них було названо від скорочення російськомовних значень цих функцій:

Наприклад:

СУММ – функція, що здійснює додавання елементів;

СРЗНАЧ – функція, що визначає середнє значення.

Формула починається зі знаку «=», за яким вводиться ім’я функції, відкрита дужка, список аргументів, розділених крапкою з комою «;», далі закрита дужка.

Наприклад: =СУММ(B2;C2).

У Microsoft Excel вбудовано такі категорії функцій, як:

– математичні;
– фінансові;
– дата і час;
– грошові;
– статистичні;
– текстові;
– логічні;

– робота з базами даних та інші.

Майстер функцій f_x має такі категорії (рис. 3.10).

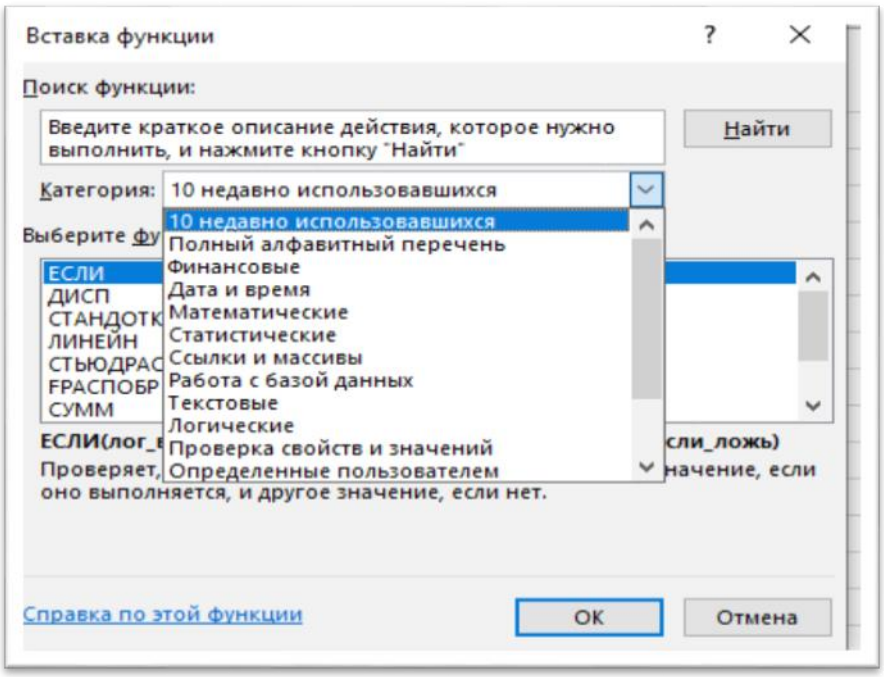


Рис. 3.10. Майстер функцій

Математичні функції виконують різноманітні математичні дії. Вони спрощують різного роду математичні обчислення, наприклад арифметичні та тригонометричні, а також використовуються в наукових і інженерних розрахунках (рис. 3.11).

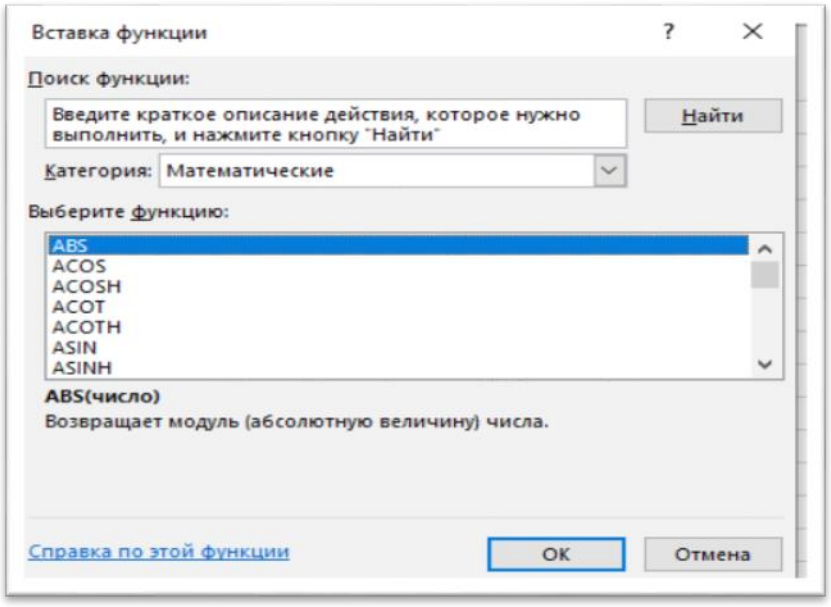


Рис. 3.11. Математичні функції

Microsoft Excel дозволяє підбивати як загальні, так і проміжні підсумки. Під час кожної зміни вихідних даних підсумкові значення обновлюються автоматично. Підсумкові значення зазвичай розташовуються праворуч від детальних даних або під ними.

Фільтрація у списку. За допомогою фільтрів можна виводити та переглядати тільки ті дані, що задовольняють визначеним умовам. MS Excel дозволяє швидко і зручно переглядати необхідні дані зі списку за допомогою простого засобу – *Автофильтр*. Складніші запити до бази даних можна реалізувати за допомогою команди *Расширенный фильтр*.

Щоб використовувати автофільтр, треба спочатку виділити для пошуку область списку із заголовками полів. Потім виконати команду *Автофильтр* в меню *Данные*. Після вибору пункту *Автофильтр* MS Excel розташовує списки, що розкриваються, безпосередньо до відповідних імен стовпчиків списку. Клацнувши по стрілці, можна вивести на екран список усіх унікальних елементів відповідного стовпчика. Якщо виділити деякий елемент стовпчика, то будуть сховані всі рядки, крім тих, що містять виділене значення.

В табл. 3.1 наведено застосування *Автофільтру* до таблиці, в якій відображено відповідні значки.

Елемент стовпчика, який виділений у списку, що розкривається, називається *критерієм фільтра.* Можна продовжити фільтрацію списку за допомогою критерію з іншого стовпчика.

До стовпчиків із текстовим форматом даних таблиці, можна застосувати такі авто фільтри (рис. 3.3).

Таблиця 3.1

Застосування автофільтру до таблиці

	A	B	C	D	E	F
1	№ з/	ПІБ	Марка авто	Колір авт	Швидкість, км/год	Штраф, грн
2	1	Абакумов Станіслав Леонідов	CITROEN C4	СИНІЙ	150	680
3	2	Ангеловський Федір Степанов	ЗАЗ LANOS	БІЛИЙ	96	225
4	3	Бабаєва Олена Володимирівн	ND ROVER RANGE ROVER SPO	ЧОРНИЙ	180	680
5	4	Бойко Леонід Олегович	VOLKSWAGEN CADDY	ЧЕРВОНИЙ	80	225
6	5	Бондарцова Вікторія Костянт	NISSAN PRIMERA	СІРИЙ	174	680
7	6	Вавиленко Сергій Сергійович	HONDA ACCORD	ЗЕЛЕНИЙ	160	510
8	7	Гриценко Степан Іванович	MERCEDES-BENZ S 420	ЧОРНИЙ	126	225
9	8	Гуц Олег Миколайович	RENAULT LOGAN	ЧОРНИЙ	165	510
10	9	Златєва Валерія Федорівна	CHERY AMULET	БЕЖЕВИЙ	149	510
11	10	Кабанова Світлана Василівна	LEXUS IS 250	ЧЕРВОНИЙ	80	225
12	11	Мошенський Кирило Вікторо	MITSUBISHI OUTLANDER	СИНІЙ	115	225
13	12	Обоянец Євген Геннадійович	RENAULT MEGANE SCENIC	БІЛИЙ	180	680
14	13	Порхоменко Віталій Олексан	VOLKSWAGEN PASSAT	СІРИЙ	158	510
15	14	Тренкиншу Іван Олексійович	ЗАЗ 11021	БІЛИЙ	100	225
16	15	Щербина Дмитро Костянтино	HYUNDAI ELANTRA	БІЛИЙ	200	680

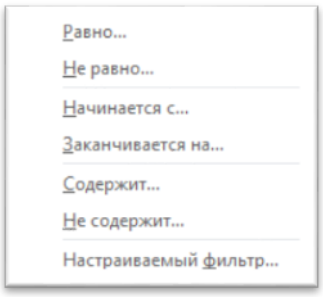


Рис. 3.3. Текстові авто фільтри

Простим критерієм застосування автофільтру є *Пользовательский* автофільтр з однією умовою чи кількома. Для стовпчика ПІБ, який має текстовий формат даних, застосуємо умову, в якій буде відображено усі ПІБ, які починаються із літери Г*, наприклад.

Для таблиці, в якій є числові поля, можна застосовувати такі числові фільтри (рис. 3.4).

Для стовпчика *Швидкість* задамо автофільтр із складною умовою, де буде відфільтровано швидкість більше або дорівнює 150 та менше або дорівнює 180 (рис. 3.5).

До цього авто фільтру застосовано логічний оператор *И,* що вказує на те, що ці умови зв’язані даним оператором. Результат виконання умови авто фільтру наведені (рис. 3.6)

За допомогою автофільтру можна для кожного стовпчика задати потрібні критерії відбору записів, наприклад, вивести на екран тільки ті записи, значення полів яких знаходяться в межах заданого інтервалу.

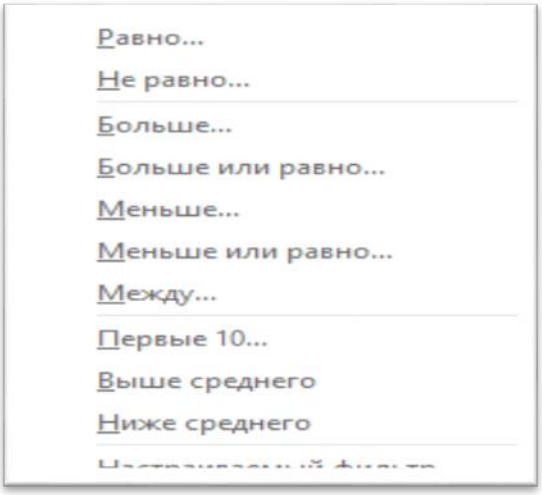


Рис. 3.4. Числові фільтри

Щоб задати необхідний критерій, треба в списку, що розкривається, вибрати пункт *(Условие...),* а потім у діалоговому вікні *Пользовательский автофильтр* ввести потрібні критерії.

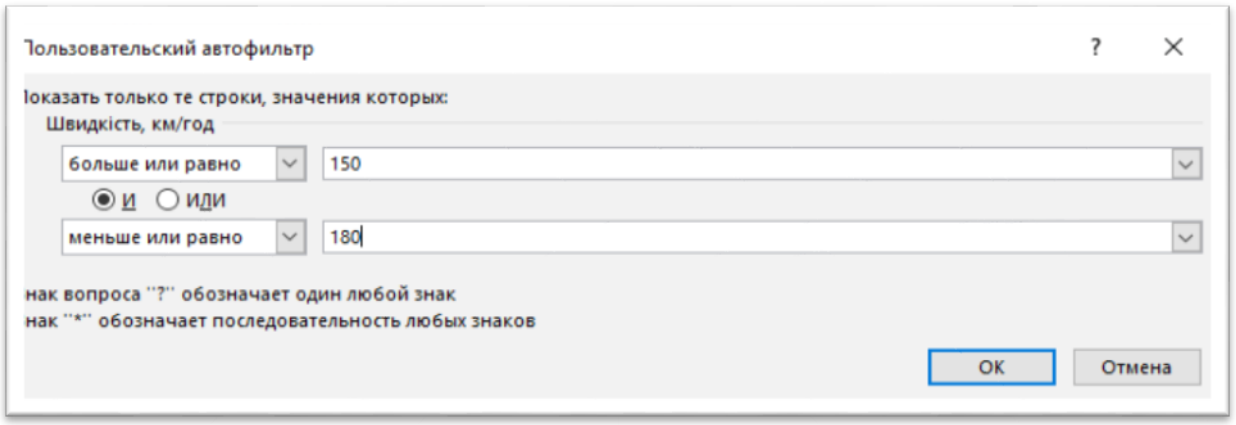


Рис. 3.5. Складна умова авто фільтру

№ з/	ПІБ	Марка авто	Колір авт	Швидкість, км/год	Штраф, грн
12	Обоянец Євген Геннадійович	RENAULT MEGANE SCENIC	БІЛИЙ	180	680
6	Вавиленко Сергій Сергійович	HONDA ACCORD	ЗЕЛЕНИЙ	160	510
1	Абакумов Станіслав Леонідов	CITROEN C4	СИНІЙ	150	680
5	Бондарцова Вікторія Костянт	NISSAN PRIMERA	СІРИЙ	174	680
13	Порхоменко Віталій Олексан	VOLKSWAGEN PASSAT	СІРИЙ	158	510
3	Бабаєва Олена Володимирівн	ND ROVER RANGE ROVER SPO	ЧОРНИЙ	180	680
8	Гуц Олег Миколайович	RENAULT LOGAN	ЧОРНИЙ	165	510

Рис. 3.6. Результат виконання умови автофільтру

Для фільтрації списку або бази даних за складним критерієм, що буде визначений нижче, а також для одержання частини наданого списку з декількома потрібними стовпцями, в MS Excel використовується команда *Расширенный фильтр* меню *Данные*. Відмінність цієї команди від команди *Автофильтр* полягає в тому, що, крім перелічених вище можливостей, відфільтровані записи можна винести в інше місце робочого листа Excel, не зіпсувавши наданий список.

Щоб використовувати команду *Расширенный фільтр*, треба спочатку створити таблицю критеріїв, яку варто розмістити на тому ж робочому листі, що й первісний список, але так, щоб не приховувати

лист під час фільтрації. Для формування таблиці критеріїв необхідно скопіювати імена полів списку в ту частину робочого листа, де буде розташовуватися таблиця критеріїв. При цьому кількість рядків цієї таблиці визначається тільки кількістю критеріїв пошуку. Завдання критеріїв пошуку у виді констант потребує точної копії імен тих стовпчиків списку, що задають умови фільтрації.

Крім таблиці критеріїв, для команди *Расширенный фильтр* треба визначити, як повинен виглядати результат. Це означає, що слід скопіювати у вільне місце робочого листа імена тільки тих полів списку, які визначають вигляд вихідного документу.

Кількість рядків у вихідному документі MS Excel визначить самостійно. Таким чином, для виконання команди *Расширенный фильтр* треба виконати три дії:

– сформувати у вільному місці робочого листа таблицю критеріїв;

– сформувати шапку вихідного документу;

– виділити область пошуку в первісному списку.

Тепер можна запускати команду Расширенный фильтр, яка виведе на екран діалогове вікно.

Практичні завдання

Завдання № 1. Створення електронної електронної бази даних.

1. Створіть новий файл в Microsoft Excel.
2. На аркуші побудуйте таблицю «*Поточний контроль успішності»*
3. Розрахувати середній, максимальний та мінімальний бали за допомогою математичних функцій МИН, МАКС, СРЗНАЧ, використовуючи *Майстер функцій.*
4. Побудуйте гістограму «Рівень успішності», за групою курсантом з вісями ПІБ-Рівень. Вкажіть всі атрибути діаграми: назву, підписи осей.
5. Побудуйте гістограму оцінок, одержаних курсантом за цикл лекцій з вісями ПІБ курсанта-Л1..Л5. Вкажіть всі атрибути діаграми: назву, підписи осей.
6. Побудуйте кругову діаграму для кількості оцінок, одержаних за лекціями. Вкажіть всі атрибути діаграми: назву, підписи осей.

Поточний контроль успішності

Факультет ФПФПКП група № КП-135

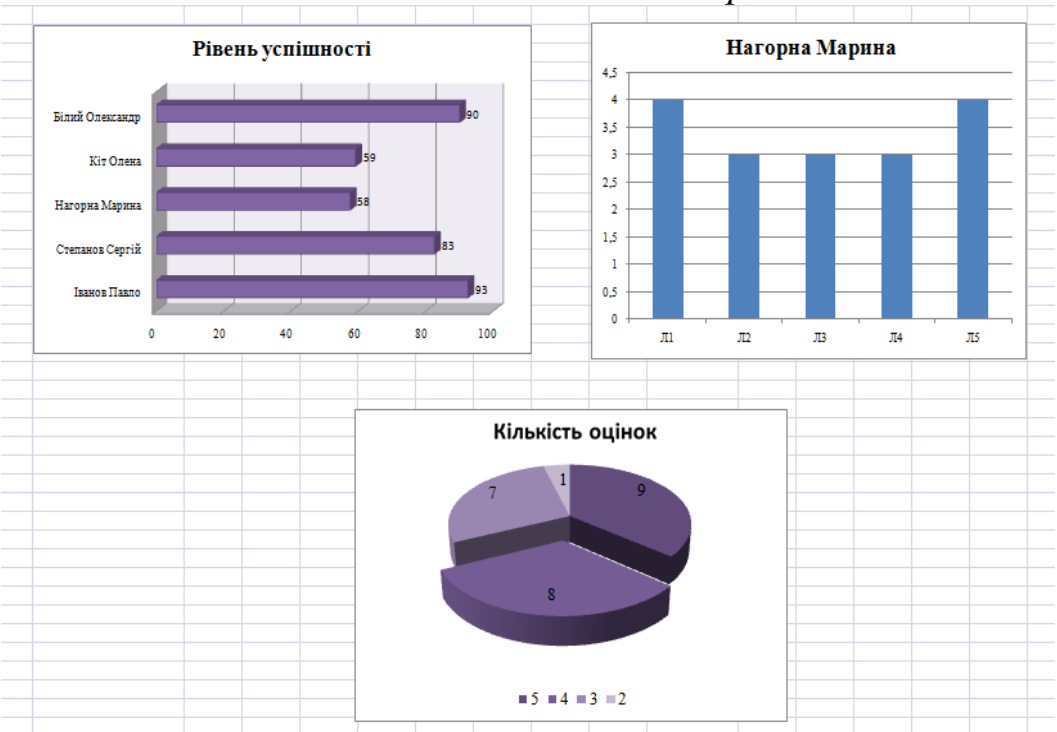
дисципліна: ІТ Модуль 1

№	ПІП	Л1	Л2	Л3	Л4	Л5	МКР-1	Мод.1	Рівень	Залік
1	Іванов Павло	4	4	5	4	5	15	37	93	зараховано
2	Степанов Сергій	5	2	3	5	5	13	33	83	зараховано
3	Нагорна Марина	4	3	3	3	4	6	23	58	незараховано
4	Кіт Олена	3	4	5	3	5	14	34	59	незараховано
5	Білий Олександр	5	3	4	4	5	15	36	90	зараховано
	Максимальний бал	5	5	5	5	5	15	40	100	
	Мінімум							23	58	
	Середній бал	4,2	3,2	4	3,8	4,8	12,6	33	76	
	Максимум							37	93	

Кількість						Всього
5	2	0	2	1	4	9
4	2	2	1	2	1	8
3	1	2	2	2	0	7
2	0	1	0	0	0	1

Пояснення скорочень у таблиці:
Л1 – лекція 1…..Л5 – лекція 5 максимальні бал 5
МКР міжсесійний контроль максимальний бал 15
Мод 1 – модуль 1 – максимальний бал 40

Зразок виконання п.4, 5, 6



Завдання № 2. Створення електронної електронної бази даних.

1. Створіть новий файл в Microsoft Excel.

2. На аркуші побудуйте таблицю. Необхідно створити просту електронну таблицю, в якій виконуються певні дії над числами a та b. Значення a та b в таблиці повинні бути ВЛАСНИМИ.

	A	B	C	D	E	F	G
1							
2							
3	**Вхідні числа**						
4	Число А	53					
5	Число В	4					
6							
7							
8	**ДІЇ**	**Число А**	**Число В**	**Результат**			
9							
10	Складання	53	4	57			
11	Різниця	53	4	49			
12	Множення	53	4	212			
13	Ділення	53	4	13,25			
14	Зведення в ступінь	53	4	7890481			
15	Корінь квадратний	53	4	7,2801099			
16	Визначення більшого значення з дво[	53	4	53			
17	Визначення меншого значення з двох	53	4	4			
18							
19							
20							

Алгоритм виконання

Для створення ЕТ виконайте наступні дії:

1. Заповніть клітинки в рядках 3-5. Використовуйте ті ж адреси клітинок, які використовуються на малюнку. Значення a та b повинні бути власними.

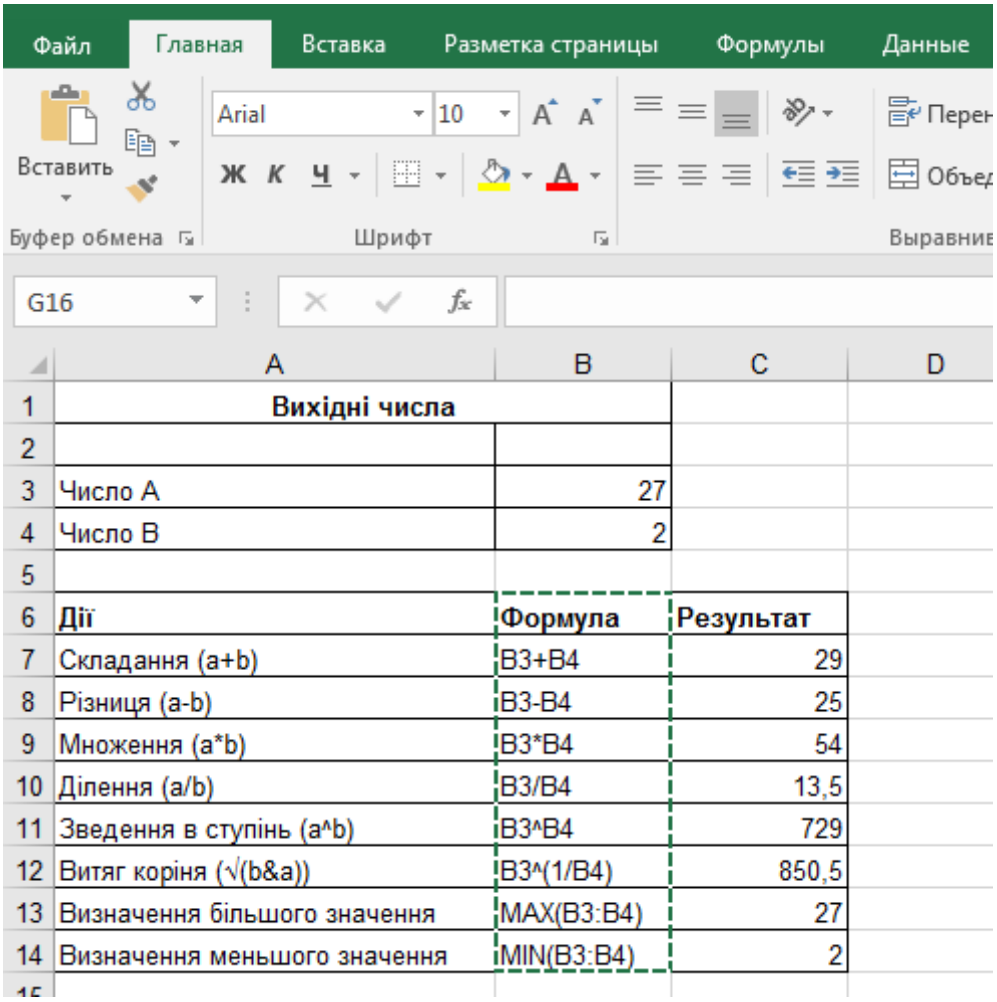
2. Текст Число a та Число b з клітинок A4 і A5 скопіюйте в клітинки B8 і C8.

3. Заповніть всі клітинки стовпчика A.

4. У рядку формул запишіть математичні дії з використанням потрібних клавіш на клавіатурі.

5. Так як в формулах в клітинках D13:D14 використовуються функції МАКС (вибирає максимальне число з безлічі чисел, що знаходяться в зазначеному діапазоні) і МІН (вибирає мінімальне число), для введення формул в клітинках D13:D14 використовуйте Майстер функцій (Статистичні).

У вікні діалогу «Мастер функций» слід вказати діапазон клітинок, з якихвибирається максимальне число.



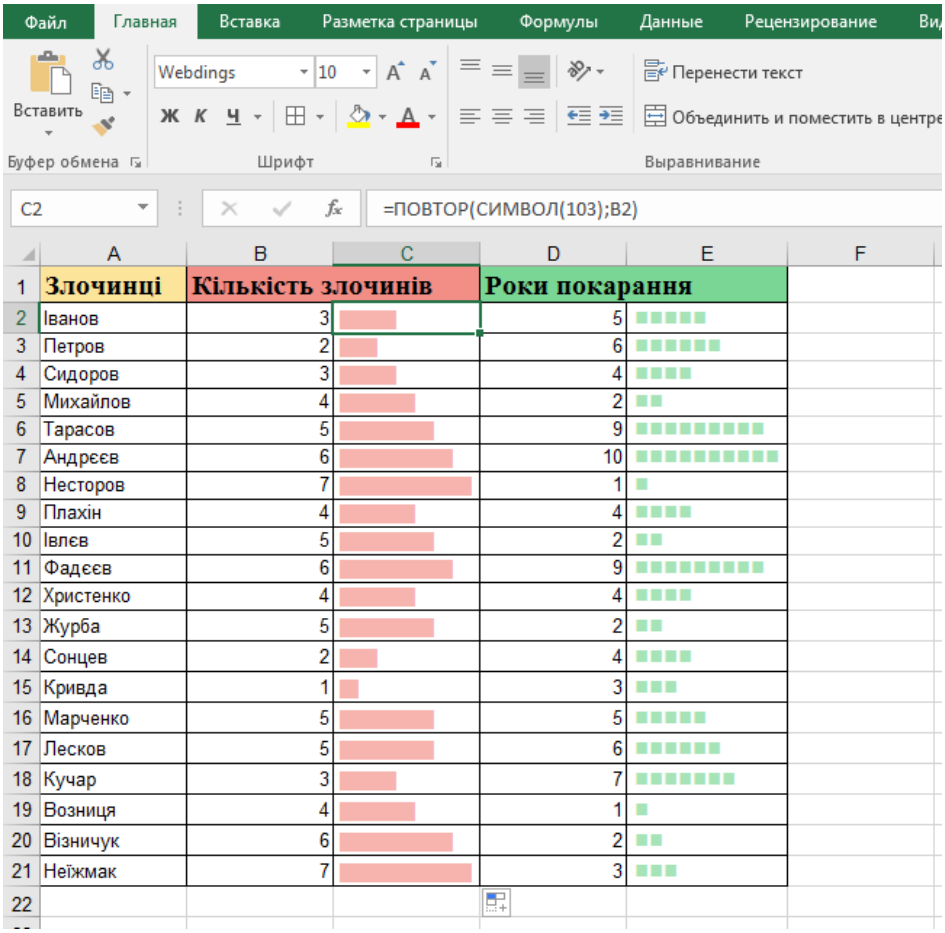
	A	B	C	D
1	**Вихідні числа**			
2				
3	Число A	27		
4	Число B	2		
5				
6	**Дії**	**Формула**	**Результат**	
7	Складання (a+b)	B3+B4	29	
8	Різниця (a-b)	B3-B4	25	
9	Множення (a*b)	B3*B4	54	
10	Ділення (a/b)	B3/B4	13,5	
11	Зведення в ступінь (a^b)	B3^B4	729	
12	Витяг коріня (√(b&a))	B3^(1/B4)	850,5	
13	Визначення більшого значення	MAX(B3:B4)	27	
14	Визначення меньшого значення	MIN(B3:B4)	2	

Завдання № 3

1. Побудувати таблицю за прикладом. У 1-му стовпчику записами ПІБ 20-злочинців, у 2-му-відповідну кількість скоєних злочинів, у 4-му-кількість років відбування покарання.

2. Далі необхідно в 3-му та 5-му стовпчиках побудувати лінійчаті діаграми («лежачі стовпці»).

Стовпець із числами необхідно візуально наочно відобразити у вигляді лінійчатої діаграми («лежачі стовпці»), але при цьому не вдаватися до побудови класичної діаграми через Майстер діаграм (рис. 3.3).



	A	B	C	D	E	F
1	**Злочинці**	**Кількість злочинів**		**Роки покарання**		
2	Іванов	3		5	■■■■■	
3	Петров	2		6	■■■■■■	
4	Сидоров	3		4	■■■■	
5	Михайлов	4		2	■■	
6	Тарасов	5		9	■■■■■■■■■	
7	Андрєєв	6		10	■■■■■■■■■■	
8	Несторов	7		1	■	
9	Плахін	4		4	■■■■	
10	Івлєв	5		2	■■	
11	Фадєєв	6		9	■■■■■■■■■	
12	Христенко	4		4	■■■■	
13	Журба	5		2	■■	
14	Сонцев	2		4	■■■■	
15	Кривда	1		3	■■■	
16	Марченко	5		5	■■■■■	
17	Лесков	5		6	■■■■■■	
18	Кучар	3		7	■■■■■■■	
19	Возниця	4		1	■	
20	Візничук	6		2	■■	
21	Неїжмак	7		3	■■■	
22						

Рис. 3.3. Загальний вигляд мікрографіків

Вказівки щодо виконання.

Для вирішення завдання можна скористатися текстовою функцією ПОВТОР (REPT), яка виводить в осередок будь-який заданий символ потрібну кількість разів. Для виведення нестандартних символів (знаючи їх код) можна використовувати функцію СИМВОЛ (CHAR). У загальному і цілому це виглядаєтак:

Символ з кодом 103 – чорний прямокутник шрифту Webdings, тому не забудьте встановити цей шрифт для осередків C2: C12. Також можна ознайомитися з символами інших шрифтів, наприклад у стовпці E використанийсимвол з кодом 110 з шрифту Wingdings.

Завдання № 3.

Необхідно створити каталог викраденого майна з магазину побутової техніки, де:

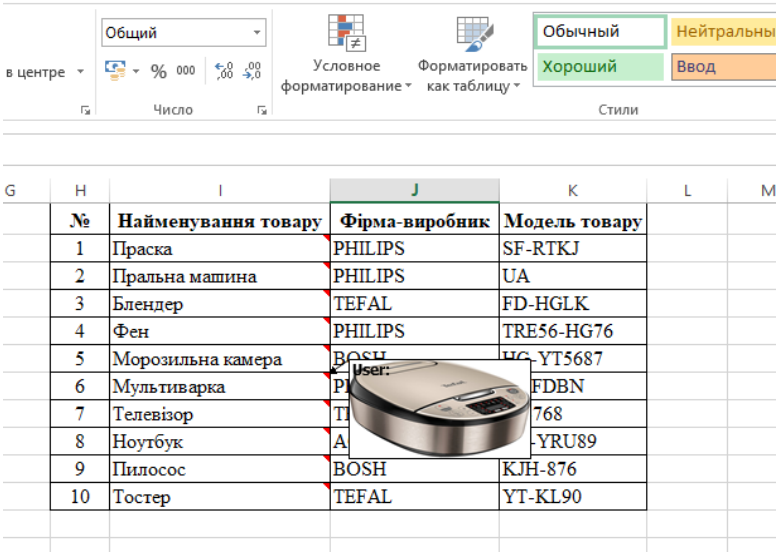
– у першому стовпці буде знаходитися номер товару за списком;
– у другому стовпці буде знаходитися найменування товару;
– у третьому стовпці буде знаходитися фірма - виробник;

– у четвертому стовпці буде знаходитися модель товару.

Всього десять найменувань товару.

Необхідно зробити пошук зображення даного товару у пошуковій системіта додати це зображення як коментар у останню клітинку.

Необхідно використовувати фотографію або малюнок в якості примітки до товару.



№	Найменування товару	Фірма-виробник	Модель товару
1	Праска	PHILIPS	SF-RTKJ
2	Пральна машина	PHILIPS	UA
3	Блендер	TEFAL	FD-HGLK
4	Фен	PHILIPS	TRE56-HG76
5	Морозильна камера	BOSH	HG-YT5687
6	Мультиварка	PH	FDBN
7	Телевізор	TH	768
8	Ноутбук	AS	YRU89
9	Пилосос	BOSH	KJH-876
10	Тостер	TEFAL	YT-KL90

Рис. 3.3. Додавання фото товару до примітки

Алгоритм виконання

1. Клацніть по комірці, в яку будемо вставляти примітку, правою кнопкою миші і виберіть в контекстному меню *Додати примітку (Add comment).*

2. Щоб примітка не приховувалося під час редагування, клацніть по комірці правою кнопкою ще раз і виберіть *Змінити примітку (Edit comment).*

3. Клацанням правої кнопки миші виділіть рамку навколо примітки івиберіть пункт *Формат примітки (рис. 3.3).*

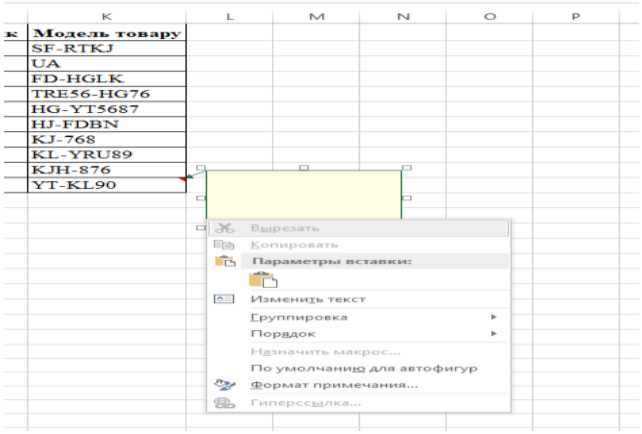


Рис. 3.3. Загальне меню до примітки

4. На панелі інструментів *Формат примітки*, виберіть закладку *Кольори і лінії.* Розгорніть палітру *Колір заливки* і виберіть – *Способи заливки*, далі вкладка *Малюнок*. Натиснувши на кнопці *Малюнок*, виберіть файл із зображенням і встановіть прапорець *Зберігати пропорції малюнка*.

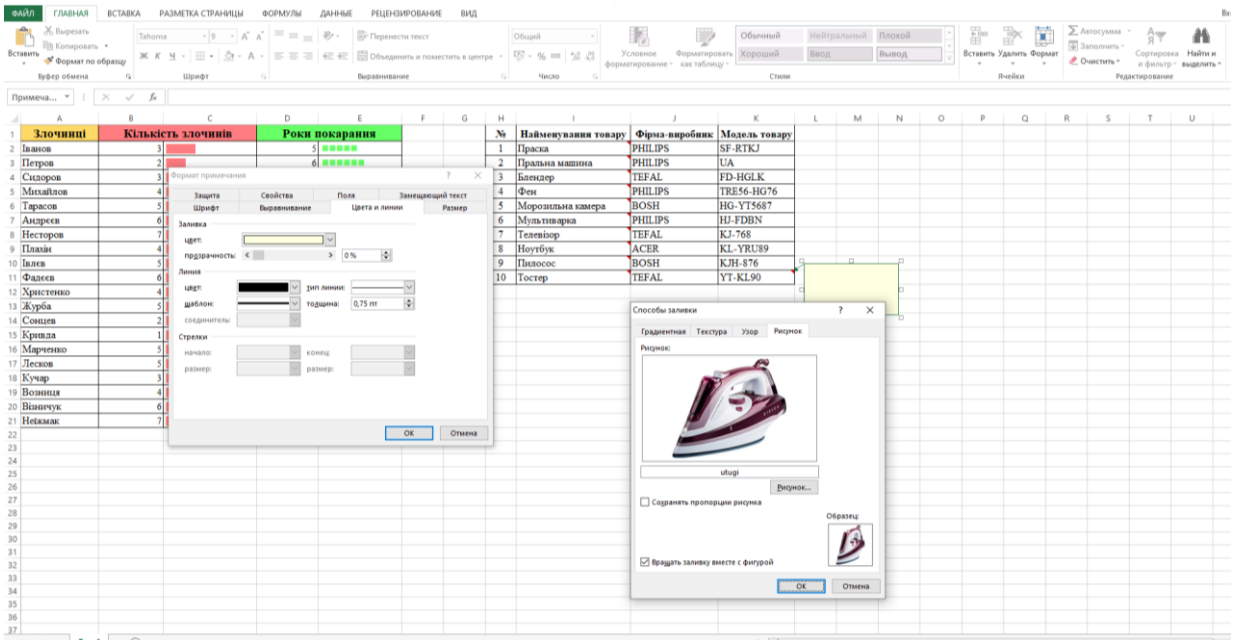


Рис. 3.4. Вставка зображення до примітки

Завдання № 5. Створення електронної електронної бази даних.

1. Створіть новий файл в Microsoft Excel.
2. На аркуші «*Успішність групи*» побудуйте таблицю обчислення середнього, максимального та мінімального балу студентів вашої групи за І семестр 20__-20__ н.р.

Успішність групи

№	ПІБ	Дисципліна1	Дисципліна2	…	Дисципліна7	Середній бал
1	2	3	4		9	10
1						СРЗНАЧ (..)
2						
…						
15						
Середній бал в групі:		СРЗНАЧ (..)	СРЗНАЧ (..)		СРЗНАЧ (..)	
Мінімальний бал в групі:		МИН(..)	МИН(..)		МИН(..)	
Максимальний бал в групі:		МАКС(..)	МАКС(..)		МАКС(..)	

3. Потрібно створити стовпчик 2 – ПІБ студентів (15 осіб).

4. В стовпчики 3-9 внесіть одержані ними бали від 0 до 100 з семи дисциплін.

5. Далі розрахуйте середній, максимальний та мінімальний бали за допомогою математичних функцій МИН, МАКС, СРЗНАЧ, використовуючи *Майстер функцій.*

6. Побудуйте 4 різні типи діаграм на різних аркушах за стовпцями *ПІБ* та *Середній бал*. Вкажіть всі атрибути діаграми: назву, підписи осей.

7. Виконайте копіювання таблиці на інший аркуш «Фільтр».

8. Застосуйте фільтр для таблиці, в якому необхідно відобразити лише тихстудентів, середній бал яких дорівнює 75.

9. Скопіюйте отримані дані за цією умовою та розмістіть їх після таблиці.Скасуйте даний фільтр.

10. Створіть іншу умову фільтру, яка допомагає відобразити тих студентів,середній бал навчання яких становить: $82{,}0 < СБ > 90{,}0$.

Скопіюйте отримані дані за цією умовою та розмістить їх після таблиці.

Контрольні питання

1. Надайте визначення **ЕТ, *робоча книга, робочий лист, функції*?**
2. Яким чином поділяються функції Microsoft Excel?
3. Яким чином проводиться у Microsoft Excel: ***Виділення декількох суміжних комірок, Виділення декількох несуміжних груп комірок, Виділення стовпця або рядка таблиці, Виділення декількох листів*?**
4. Яким чином проводиться у Microsoft Excel: *Обчислення* в таблицях ***Формати чисел*?**
5. Яким чином здійснюється створення, оформлення та редагування діаграм у Microsoft Excel:. ?
6. Що таке атрибути діаграми?
7. Функція СРЗНАЧ, МИН, МАКС: до якої категорії функцій відноситься? Які дії виконуються?
8. Функція ЕСЛИ: до якої категорії функцій відноситься? Які дії виконуються?
9. Яким чином проводиться у Microsoft Excel: *Обчислення. **(математичні дії).***
10. Яким чином здійснюється створення, оформлення та редагування математичних формул (дій) у Microsoft Excel:.
11. Функція МИН, МАКС: до якої категорії функцій відноситься? Які дії виконуються?
12. Надайте пропозиції щодо оптимізації математичних дій.
13. Дайте визначення – «спарклайн».
14. Як виглядає алгоритм дій зі створення мікрографіків?
15. Назвіть особливості використання функцій функцію «ПОВТОР» та «СИМВОЛ».
16. Якому типу шрифтів відповідає – Символ з кодом 103 – чорний прямокутник?
17. Який символ відповідає кодом 110 з шрифту Wingdings?
18. Для чого використовується опція «Примітки»?
19. Чи можуть Примітки дути текстом? Фото? Обґрунтуйте відповідь
20. Що таке робочий лист і робоча книга?
21. Організація обчислень засобами електронних таблиць. Використання вбудованих функцій.
22. Поняття про бази даних (*список*) у середовищі MS Excel,

обмеження та особливості створення і використання.

23. Поняття про принципи роботи з функціями і формулами.
24. Створення та оформлення діаграм.
25. Табличні обчислення, функції
26. Чим відрізняється використання звичайного *Автофильтра* від користувальницького *Автофильтра*?
27. Як відфільтрувати дані за певною умовою?
28. Як використовується майстер функцій?
29. Форматування даних електронної таблиці.
30. Чи є необхідність вводити ідентичні формули в кожній комірці ЕТ?

Джерела до розділу 2

1. Інформаційні системи та технології: підручник / кол. авт.; ред. В. Б. Вишня. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2021. 296 с.
2. Вишня В. Б., Рибальченко Л. В., Косиченко О. О., Махницький О. В., Прокопов С. О., Тютченко С. М. Інформаційне забезпечення юридичної діяльності: Підручник. Дніпро, ДДУВС, 2018. 241 с.
3. Технічна підтримка ресурсів корпорації Google. Електронний ресурс: https://www.microsoft.com/uk-ua/microsoft-365/excel
4. Функції Excel (за алфавітом) URL: https://support.microsoft.com/uk-ua/office/%D1%84%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%97-excel-%D0%B7%D0%B0-%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D1%96%D1%82%D0%BE%D0%BC-b3944572-255d-4efb-bb96-c6d90033e188.
5. Alexander M., Kusleika R., Walkenbach J. Excel 2019 Bible, ISBN 9781119514787, October 2018 Електронний ресурс: https://www.wiley.com/en-ie/Excel+2019+Bible-p-9781119514763#O-Book.

Розділ 4
АВТОМАТИЗАЦІЯ ПІДГОТОВКИ СЛУЖБОВИХ ДОКУМЕНТІВ ЗА ДОПОМОГОЮ ОНЛАЙН СЕРВІСУ GOOGLE DOCS

4.1. Ознайомлення з хмарними сервісами Google

За визначенням Національного Інституту Стандартів і Технології США (NIST) *хмарні обчислення* – це модель забезпечення зручного доступу за потребою будь-де і будь-коли до спільних обчислювальних ресурсів (мереж, серверів, систем зберігання, застосунків і послуг), які можуть бути надані швидко і з мінімальними зусиллями управління та взаємодії з постачальником послуг.

Концепція хмарних обчислень з'явилася ще в 1960 році, коли американський учений, фахівець з теорії ЕОМ Джон Маккарті висловив припущення, що коли-небудь комп'ютерні обчислення стануть надаватися подібно комунальним послугам (public utility). Розповсюдження мереж з високою потужністю, низька вартість комп'ютерів і пристроїв зберігання даних, а також широке впровадження віртуалізації, сервіс-орієнтованої архітектури привели до величезного зростання хмарних обчислень. Кінцеві користувачі можуть не перейматися роботою обладнання технологічної інфраструктури «в хмарі», яка їх підтримує. Аналогією обчислювальних «хмар» зі звичного життя можуть служити електростанції. Хоча домовласник може купити електрогенератор і піклуватися про його справність самостійно, більшість людей воліє отримувати енергію від централізованих постачальників.

Використовуючи хмарні технології можна організувати роботу шляхом впровадження моделі, відомої як послуга *SaaS (Software as a service).* Згідно цієї концепції постачальник надає користувачам хмари програмне забезпечення як послугу. Всі дані зберігаються у хмарі, і для доступу до них користувачеві потрібно тільки наявність веб-браузера. Послуги цього типу на сьогоднішній день надають такі відомі ІТ-компанії як Google, Microsoft та інші.

Найпопулярніше програмне забезпечення, що надається у «хмарі», наступне: електронна бібліотека; сховища даних (Dropbox, SkyDrive,

GoogleDrive); відеоконференції; електронна пошта; офісні сервіси; системи дистанційного навчання.

Розглянемо основні сервіси Google, які набули практичного застосування.

Поштовий сервіс Gmail – безкоштовна електронна пошта з великим обсягом місця для зберігання повідомлень (понад 10,1 Гб), з доступом по POP3 і зручним веб-інтерфейсом. Також є OpenID-провайдером для всіх служб Google (рис.4.1).

Диск Google (англ. *Google Drive*) – сховище даних, що дозволяє користувачам зберігати свої дані на серверах у хмарі і ділитися ними з іншими користувачами в Мережі Інтернет (рис. 4.2).

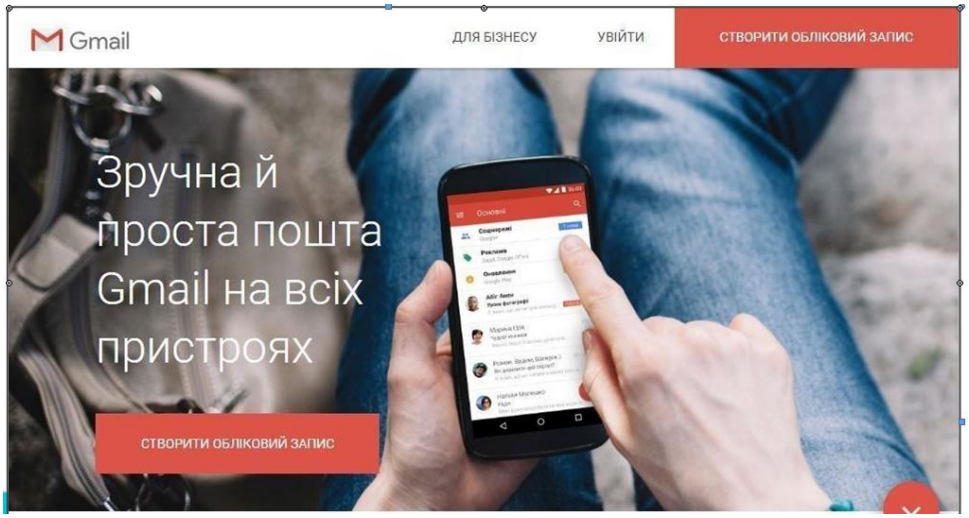


Рис. 4.1. Головна сторінка https://www.google.com/intl/uk/gmail/about

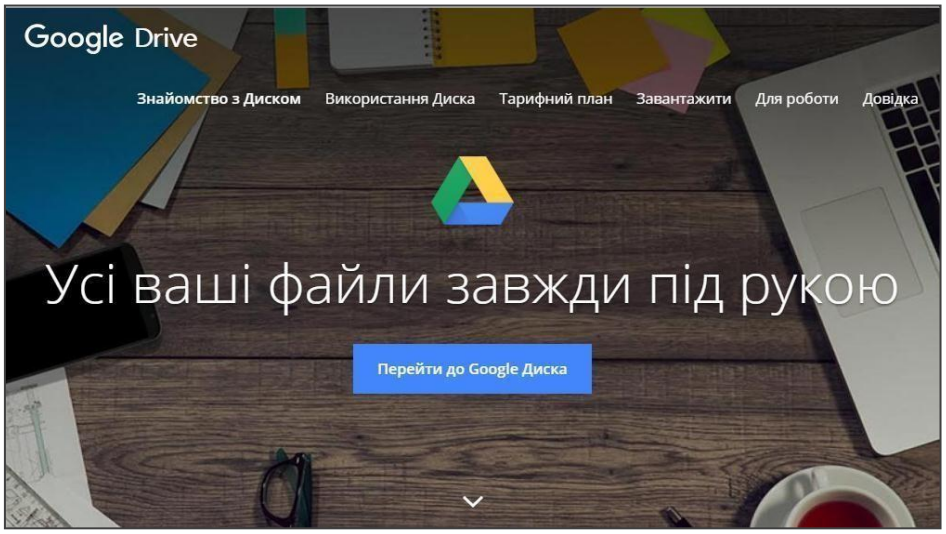


Рис. 4.2. Головна сторінка сервісу *Google Drive* https://www.google.com/intl/uk_ALL/drive/

Функціональні можливості Google Drive:

1. Можливість збереження файлів будь-якого типу.
2. Користувач безкоштовно отримує 15 Гб вільного місця на Google Диску, щоб зберігати фотографії, текстові документи, проекти, малюнки, аудіозаписи, відео тощо.
3. Постійний доступ до файлів користувача.
4. Файли на Диску можна відкрити зі смартфона, планшета або комп'ютера. Тому де б ви не були, ваші файли завжди будуть під рукою.
5. Можливість надання спільного доступу до файлів і папок.
6. Ви легко можете запросити інших переглядати й завантажувати вибрані вами файли та спільно працювати над ними. Більше непотрібно вкладати файли в електронні листи.

На сьогоднішній день існує велика кількість подібних сервісів, які відрізняються один від одного в основному безкоштовним об'ємом дискового простору, що надається у користування. Але на практиці добре зарекомендував себе саме сервіс Google Drive. Особливістю його роботи є те, що він доступний на вже наявномуу користувача аккаунті Gmail. Відмінною рисою даного сервісу є тісна інтеграція з додатком Google Docs. Унаслідок високоївартості професійних програм у мережі Інтернет широко поширене незаконне, піратське використання неліцензійних копій. Використання хмарних сервісів дозволяє не тільки не порушувати авторське право, а й стає найефективнішим способом боротьби з незаконним використанням програмного забезпечення.

Google Docs (укр. Документи Ґуґл) – розроблений Google безкоштовний мережевий офісний пакет, що включає текстовий, табличний редактор і службу для створення презентацій.

Сервіси GoogleDocs дозволяють створювати спільні папки для обміну даними з колегами та студентами, організовувати спільну роботу над документами, створювати форми, анкети, тести. Схожі сервіси також має компанія Microsoft. Проте на практиці хмарні додатки від Google отримали більше розповсюдження.

Google Документи включають цілий набір зручних інструментів для редагування й оформлення документів. Можна використовувати різні шрифти, додавати посилання, зображення, малюнки й таблиці. Також підтримується сумісність із MS Word.

Текстовий редактор Google Документи (Google Docs).

Google Документи (рис. 4.3) включають цілий набір зручних інструментів для редагування й оформлення документів.

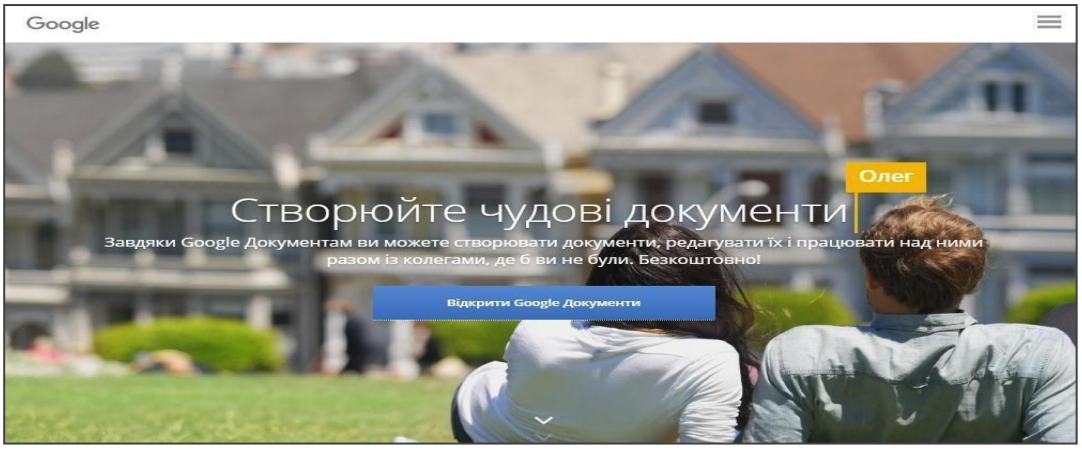


Рис. 4.3 – Головна сторінка сервісу Google Docs
https://www.google.com/intl/uk/docs/about

Можна використовувати різні шрифти, додавати посилання, зображення, малюнки й таблиці. Також підтримується сумісність із MS Word.

Табличний редактор Google Таблиці (Google Sheets)

Сервіс Google Sheets надає можливість представляти дані в Google Таблицях у вигляді кольорових діаграм і графіків (рис. 4.4). Також має вбудовані формули, зведені таблиці й умовнеформатування. Окрім того, Google Таблиці повністю сумісні з MS Excel.

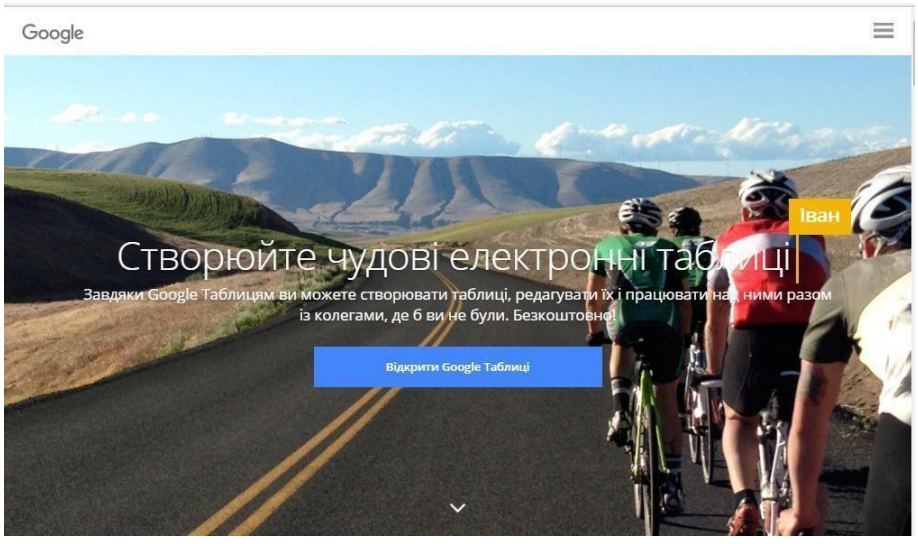


Рис. 4.4 – Головна сторінка сервісу Google Sheets
https://www.google.com/intl/uk/sheets/about

Служба для створення презентацій Google Презентації (Google Slides).

Google Презентації – чудовий спосіб представити нові ідеї. Можна використовувати різні теми, шрифти, додавати відео, анімацію тощо (рис. 4.5). Підтримується зворотня сумісність із MS PowerPoint. Проводити демонстрацію готової презентації можна набудь-якому пристрої.

Окрім переліченого вище функціоналу сервіси Google Docs, Google Sheets і Google Slides мають наступні можливості:

1. Можливість створювати, редагувати та переглядати документи, таблиці та презентації на будь-якому пристрої – телефоні, планшеті або комп'ютері – і навіть без з'єднання з Інтернетом.
2. Ефективна спільна робота. Кілька користувачів можуть одночасно працювати над одним документом.
3. Спільний доступ до документів. Можна відкрити доступ до файлів студентам і колегам. Вони зможуть переглядати документ, редагувати його або залишати коментарі.
4. Редагування документу в реальному часі. Коли користувач редагує ваш документ, ви можете бачити курсор у місці, де вносяться зміни або виділяється текст.

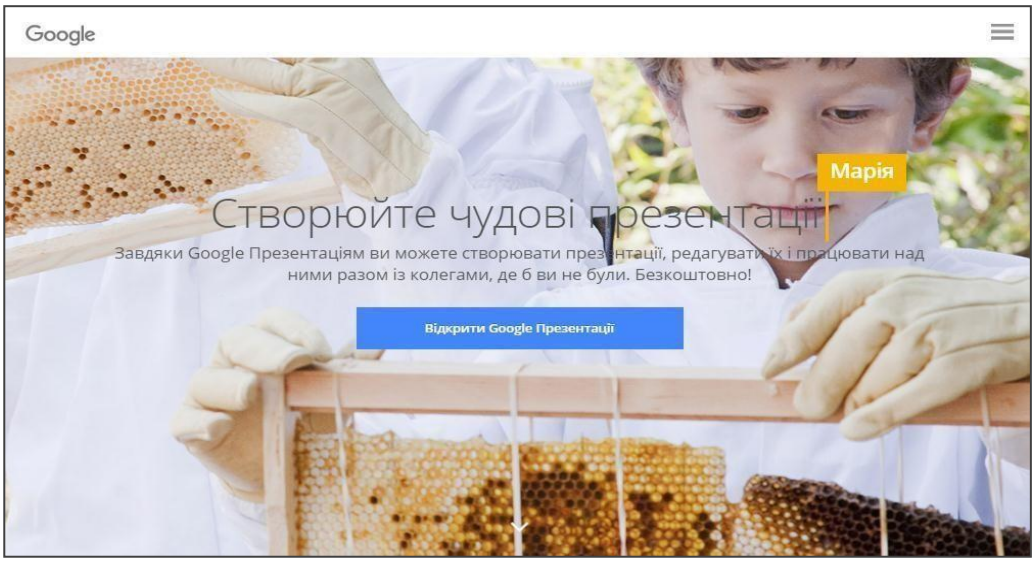


Рис. 4.5 – Головна сторінка сервісу Google Slides
https://www.google.com/intl/uk/slides/about

5. Чат і коментарі. Можна спілкуватись з іншими редакторами в чаті просто у вікні документа або за допомогою коментарів.
6. Автоматичне зберігання. Усі зміни відразу зберігаються автоматично. В історії змін можна завжди переглянути попередні версії документа, відсортовані за датою й автором.
7. Можливість розширення функціоналу шляхом використання спеціальних доповнень.

Компанія Google пропонує й інші хмарні сервіси для роботи. З ними можна ознайомитись за посиланням:

https://www.google.com.ua/intl/ru/about/products/.

Слід відмітити, що використання хмарних технологій такожмає свої недоліки. Основним ризиком вважається безпека даних. Користувачу послуги часто здається, що його дані знаходяться у небезпеці, зберігаючись у віддаленому дата-центрі, ніж у деякому локальному середовищі. Для того, щоб знизити наслідки ризику втрати інформації необхідно обов'язково робити резервні копії своїх даних на локальних носіях. Також постачальники хмарних послуг не можуть гарантувати стовідсоткову доступність своїх сервісів у будь- який час. Небезпечним є також користування послугами лише одного постачальника хмарних сервісів. Тому при використанні хмарних сервісів, як і будь-якої технології, повинний бути виважений підхід.

Робота з поштовим сервісом google

Переходимо на сайт *www.gmail.com* (рис. 4.6).

На даній сторінці обираємо «Створити обліковий запис»

Заповнюємо всі поля форми для реєстрації. Натискаємо кнопку «Далі» та потрапляємо на наступну сторінку Відмовляємося від заповнення профілю – натискаємо кнопку «Ні». Пізніше за бажанням Ви можете додати фотодля вашого профілю.

В результаті отримуємо підтвердження реєстрації. Переходимо на сторінку сервісу Google. (рис. 4.7).

На вашій власній сторінці (рис. 4.8) можна переглянути вхідну кореспонденцію та написати лист. Ви можете перейти до завантаження на диск власнихдокументів та папок.

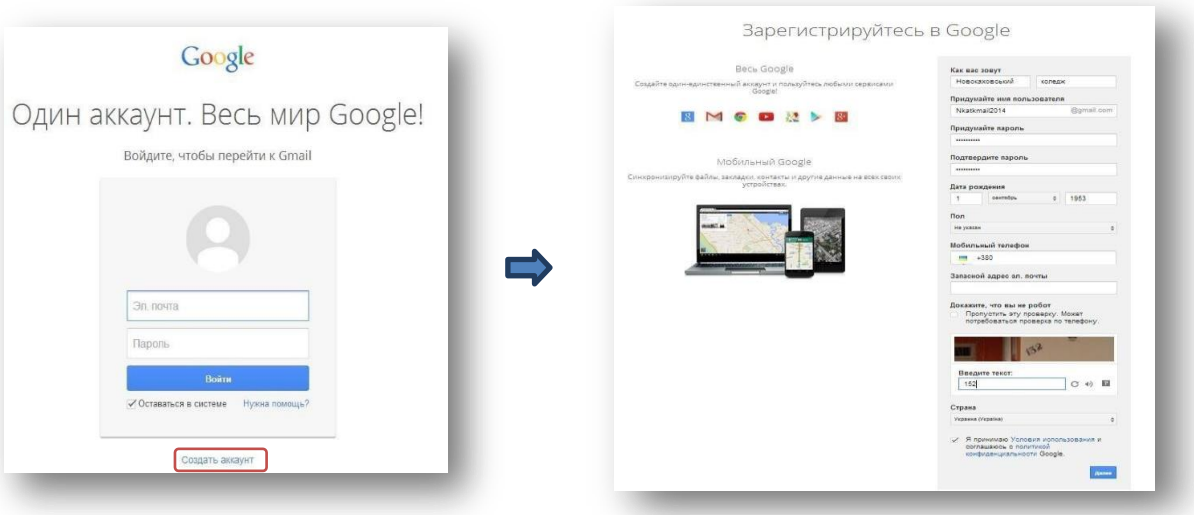


Рис. 4.6. Реєстрація в Google

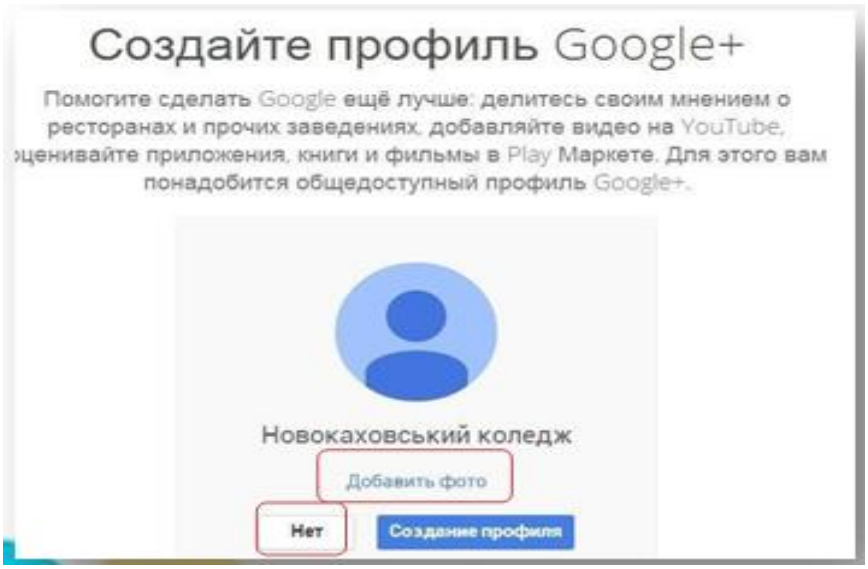


Рис. 4.7. Створення профілю в Google

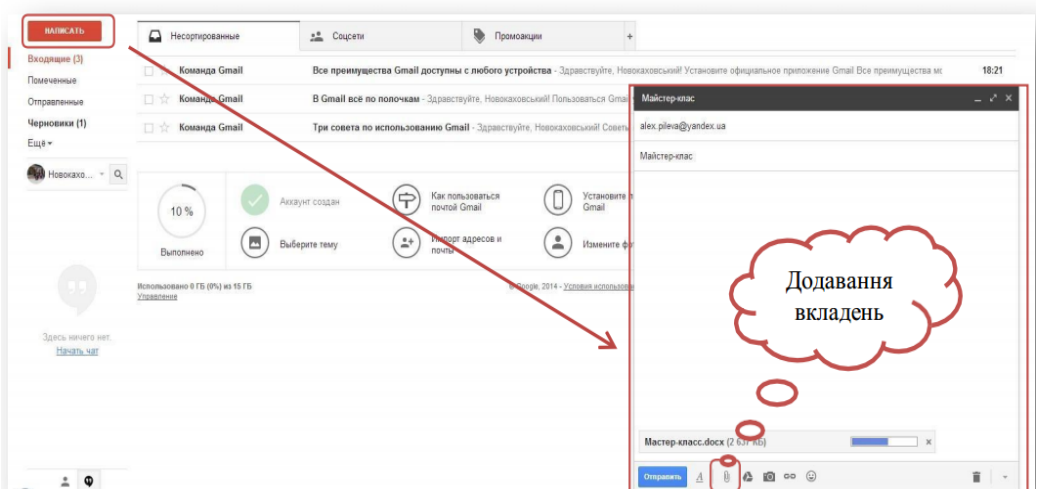


Рис 4.8. Загальний вигляд власної сторінки

Завантаження файлів на Google диск

У відкритому вікні перейдемо до Google Диску (рис. 4.9).

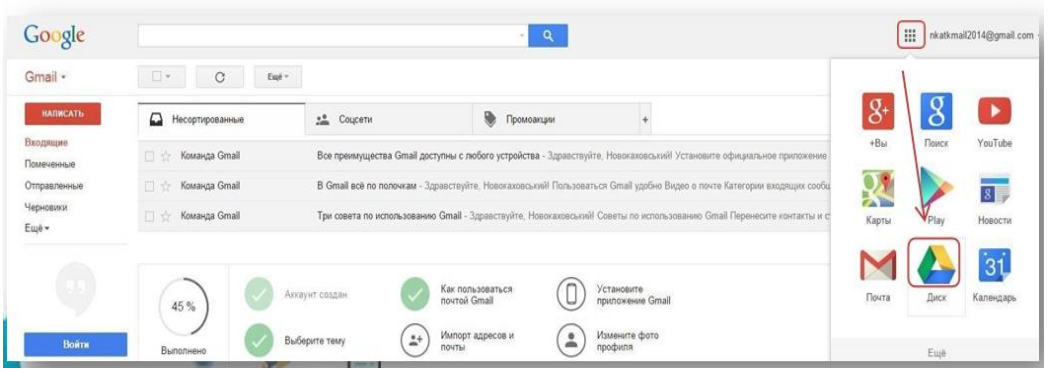


Рис. 4.9. Процес переміщення до Google Диску

4.2. Робота у GOOGLE DOCS створення простих GOOGLE документів з наданням доступу

Алгоритм створення нового документу у через Google Документі

Виконайте наступні дії:

1. Для початку вам потрібен обліковий запис Gmail. Якщо ще не є зареєстрованим користувачем – зробіть це. Відразу після реєстрації ви зможете користуватися сервісом. Для цього перейдіть за посиланням (docs.google.com).

2. Ви потрапите в головні меню. Отут знаходиться список останніх документів, з якими ви працювали, і кнопка «Створити». Натисніть на неї.

Після цього ви потрапите на сторінку, що дуже нагадує MS Word, і зможете працювати з текстом. Загальний вигляд нового документу, що створили (рис 4.10).

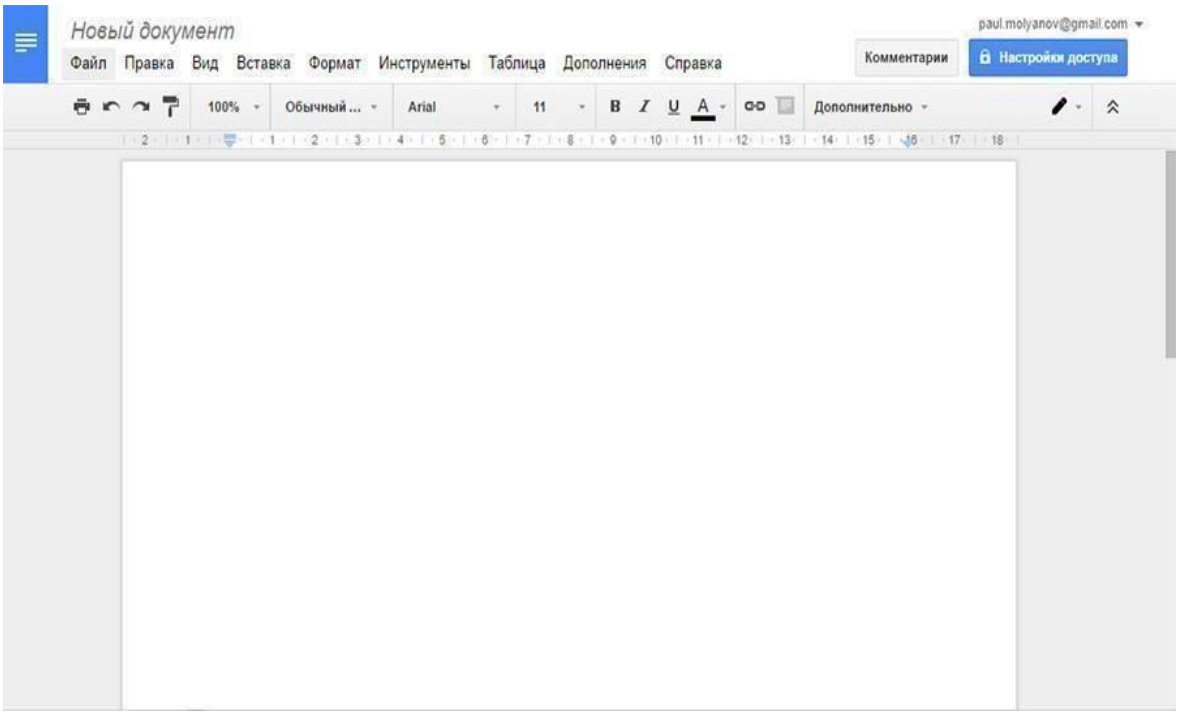


Рис. 4.10. Загальний вигляд нового документу, що створили

Інший спосіб почати роботові – через Google Диск. Він створюється автоматично, як тільки реєструєтеся в Gmail. Потрібно викликати контекстне меню і створіть документ. Вас відразу ж перенесе на робочу сторінку (рис. 4.11).

Якщо ви вже створювали якісь файли – просто відкрийте їх, щоб продовжити роботу. Щоб повернутися в головні меню, клацніть по логотипу Google Docs уверхньому лівому кутку (рис. 4.12).

Алгоритм переглядання нового документу у через Google Документі

Ви можете переглядати файли, що були створені на інших пристроях і в сторонніх програмах (наприклад, Microsoft® Word, Excel или PowerPoint).

Потрібно відкрити *Google Документы*, *Таблицы*, *Презентации* …

Натисніть на потрібний файл. Примітка. Якщо з цим файлом працюють інші користувачі, ви побачите зміни, які зміни вносять.

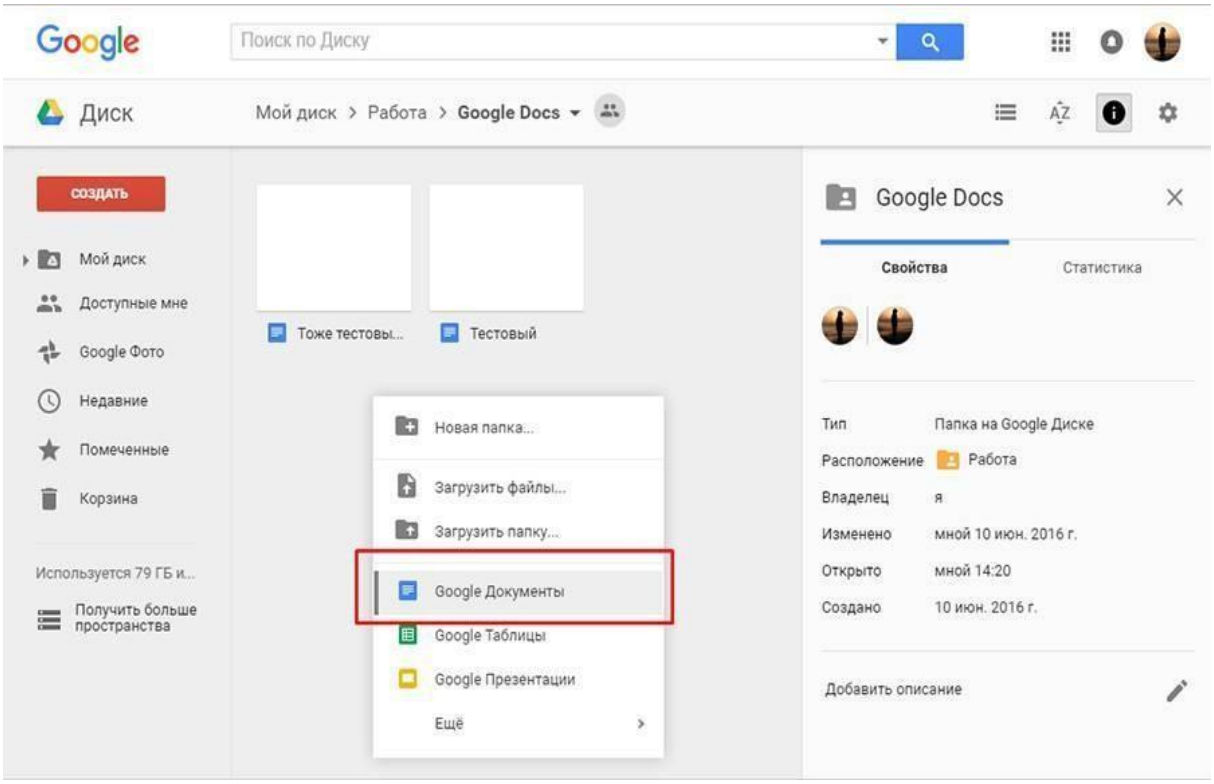


Рис. 4.11. Створення нового документа в Google Docs

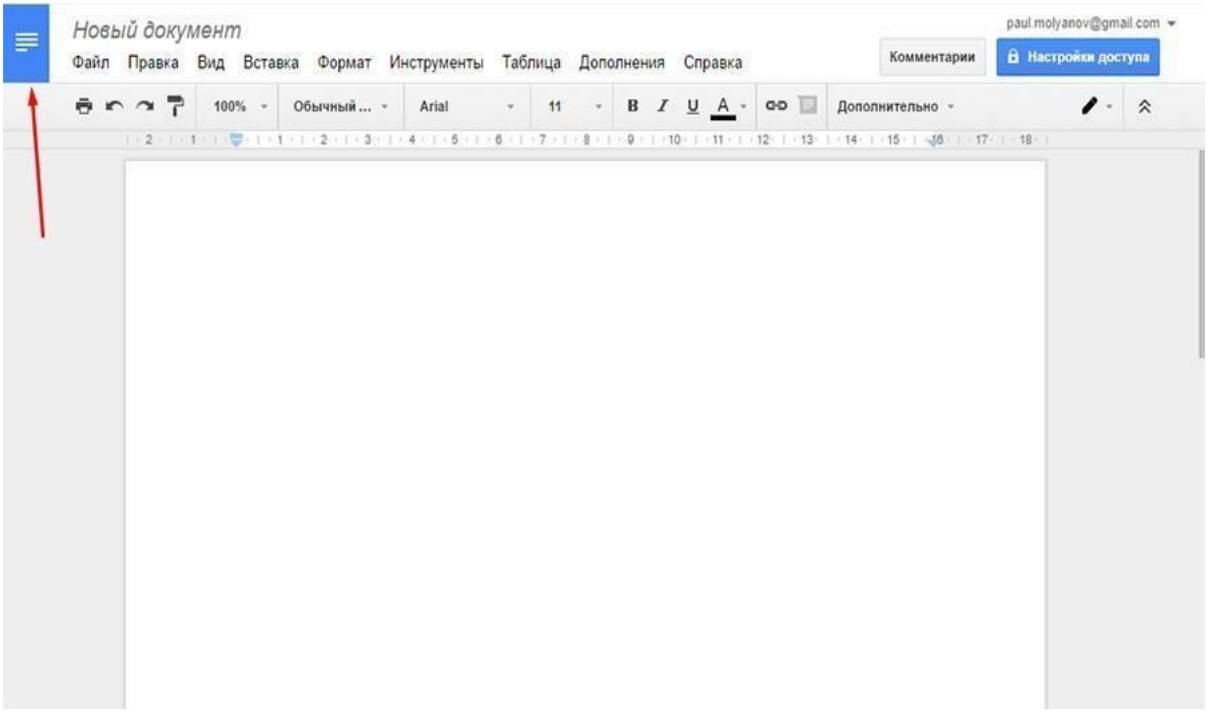


Рис. 4.12. Перехід до головного меню

Алгоритм завантаження файлу з Google Документу (рис. 4.13):

1. Відкрийте Google Документи, на комп'ютері.
2. Відкрийте потрібний файл.
3. У верхній частині екрану натисніть «Файл» «Завантажити як».
4. Виберіть формат, у якому хочете зберегти файл на комп'ютері.

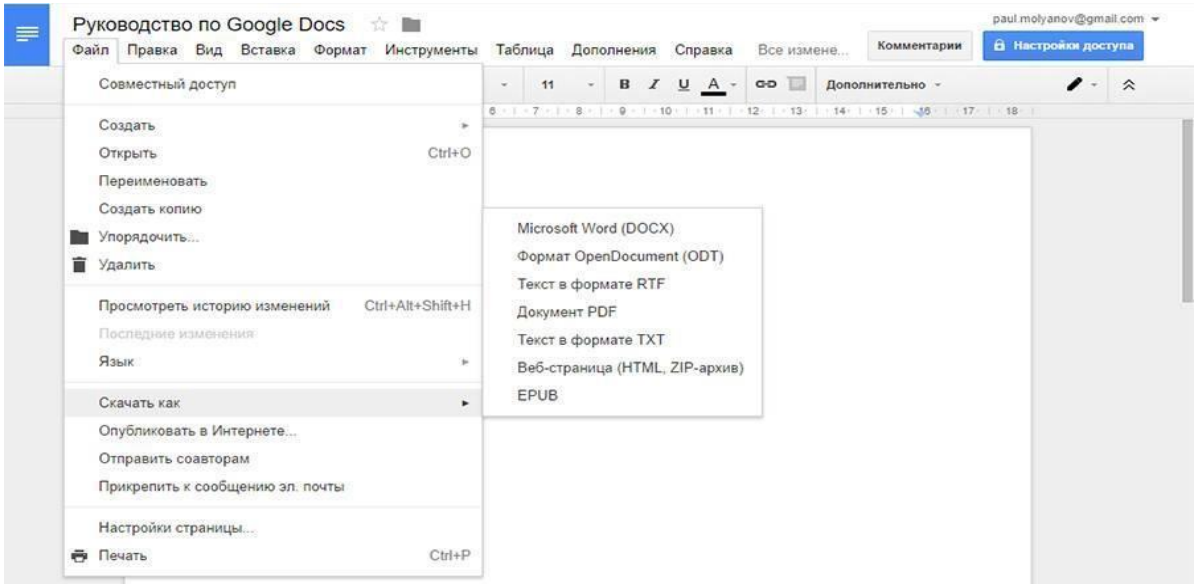


Рис. 4.13. Завантаження файлу з Google Docs

Елементи форматування

Стилі. Шаблони між якими можна швидко перемикатися. Зручно для створення заголовків і форматування скопійованого з зовнішніх джерел тексту. (рис. 4.14).

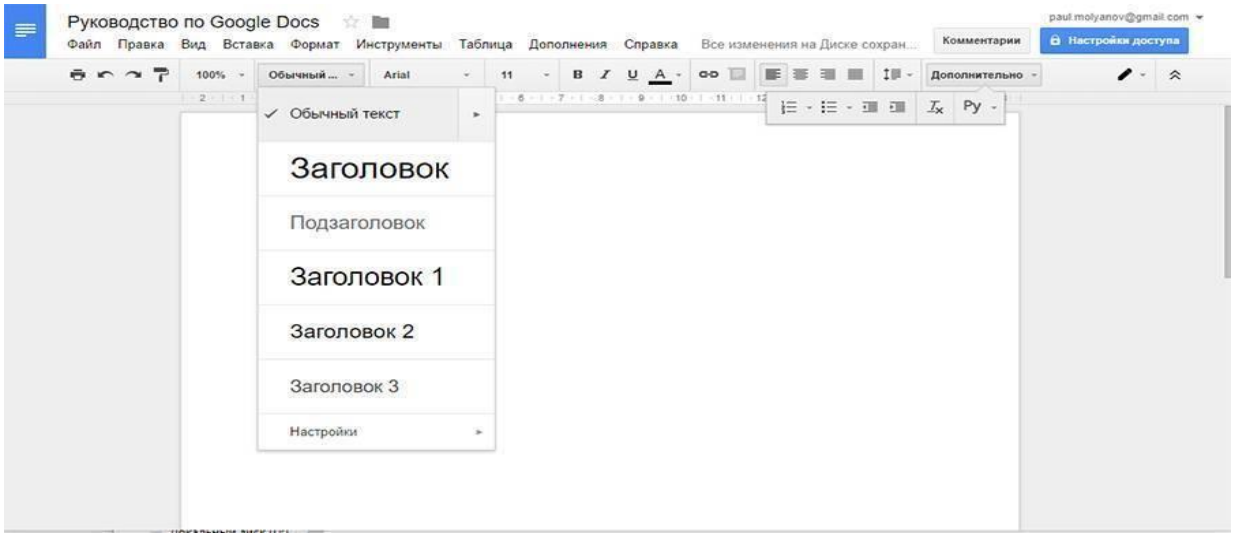


Рис. 4.14. Стилі та заголовки

Шрифт і розмір. За замовчуванням шрифтів трохи, але є можливість підключати нові. *Ефекти і колір.* Жирний, курсив, підкреслення. Відразу вибирається коліртексту і тлу (як би виділення маркером) (рис. 4.15).

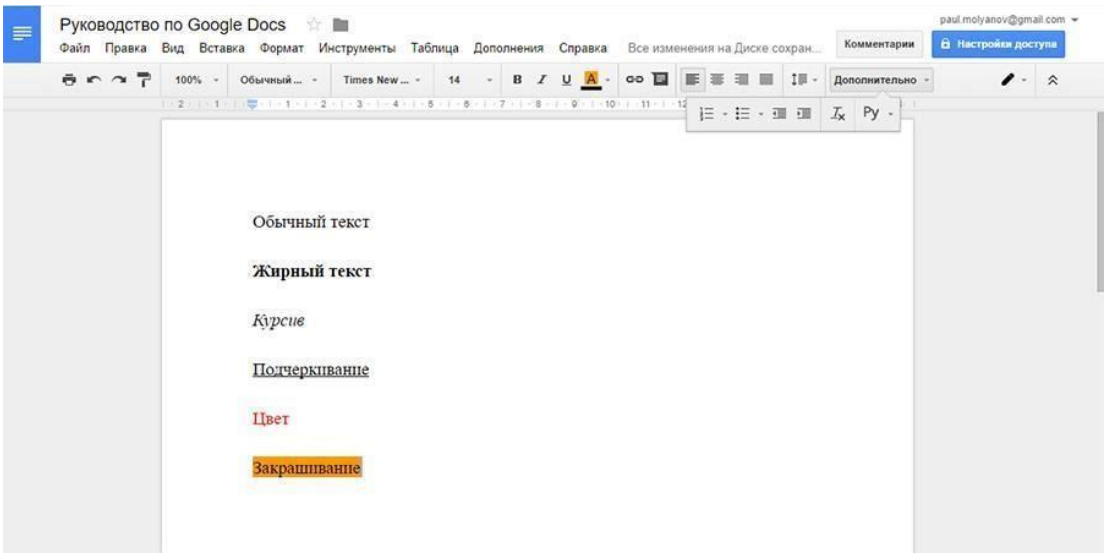


Рис. 4.15. Шрифт і розмір. Ефекти і колір

Вставити посилання. Створює гіперпосилання в документі.

Коментар. Додає замітки й нагадування на полях. Дуже зручно, щоб нічогоне забути.

Списки. Створює нумеровані й маркіровані списки. Відступ. Відстань від краю аркуша до тексту.

Вирівнювання. Текст можна «притиснути» до лівого або правого краю аркуша, розмістити по центру або зробити всі рядки однаковими по ширині. Міжрядковий інтервал. Задає відстань між рядками тексту рис. 4.16.

Очистити форматування. Видаляє всі ефекти з тексту.

Алгоритм виділення фрагменту тексту. Для виконання будь якої операції над частиною тексту, наприклад форматуванням чи видаленням, необхідно цючастину насамперед виділити, а потім робити необхідні операції.

– *Для виділення фрагменту тексту*, що складається з *одного* чи *декількох символів,* необхідно помістити курсор «миші» у качан фрагмента і при натиснутій *лівій* клавіші перемістити покажчик у кінець виділюваного фрагменту, що виділений (зазначимо, що виділення можна такожробити не тільки праворуч, але і навпаки – ліворуч).

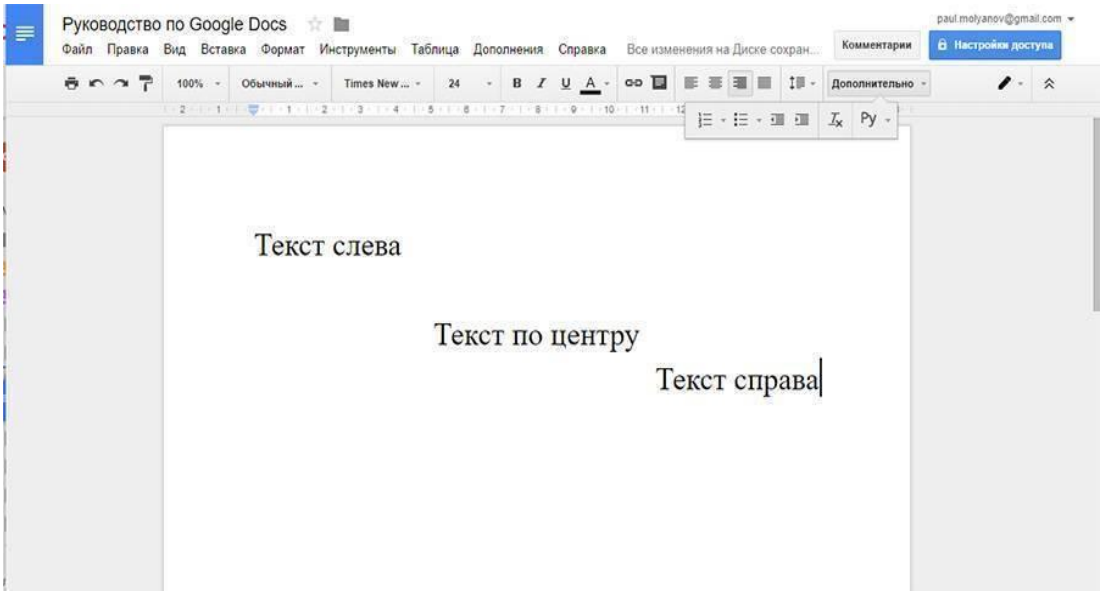


Рис. 4.16. Вирівнювання тексту

– *Для виділення* слова необхідно *двічі* клацнути на ньому *лівою* кнопкою «миші».

– *Для виділення* речення необхідно виконати щиглик на будь-якому символі речення при натиснутій клавіші *Ctrl.*

– *Для виділення* абзацу треба тричі клацнути лівою кнопкою в будь-якому місці абзацу. До речі, так можна вибачимо шляхом перевірити, якові частину тексту охоплює даний абзац, не використовуючи кнопку на вкладці *Главная.*

Алгоритм копіювання фрагмента тексту. Для копіювання фрагмента тексту (у т.ч. і багаторазового) необхідно виділити потрібний фрагмент і викликати команду *Копіювати* (Ctrl+C) у меню *Головна*. У результаті копія виділеного фрагмента буде поміщена в буфер обміну. Потім треба розташувати курсор у тій частині документа, куди потрібно вставити копію фрагмента з буфера. Цю ж копію можна вставити й в інше місце в цьому документі, а також і в інший документ. Викликом команди *Вставити* (Ctrl+V) у меню *Головна* операція копіювання буде виконана.

4.3 Робота у Google docs. Створення структури документа, закладок, колонтитулів та введення спеціальних символів

Для створення документа необхідно зайти в Google та відкрити піктограму «Приложения Google» (рис. 4.17).

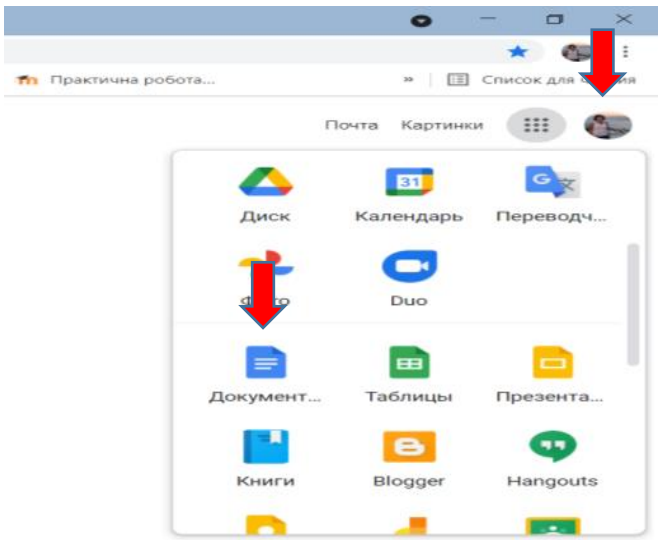


Рис. 4.17. Створення документа (крок 1)

У результаті активації піктограми «Документи» відкриється вікно сервісу (рис. 4.18). Для створення нового документу необхідно натиснути на «+» внизу сторінки.

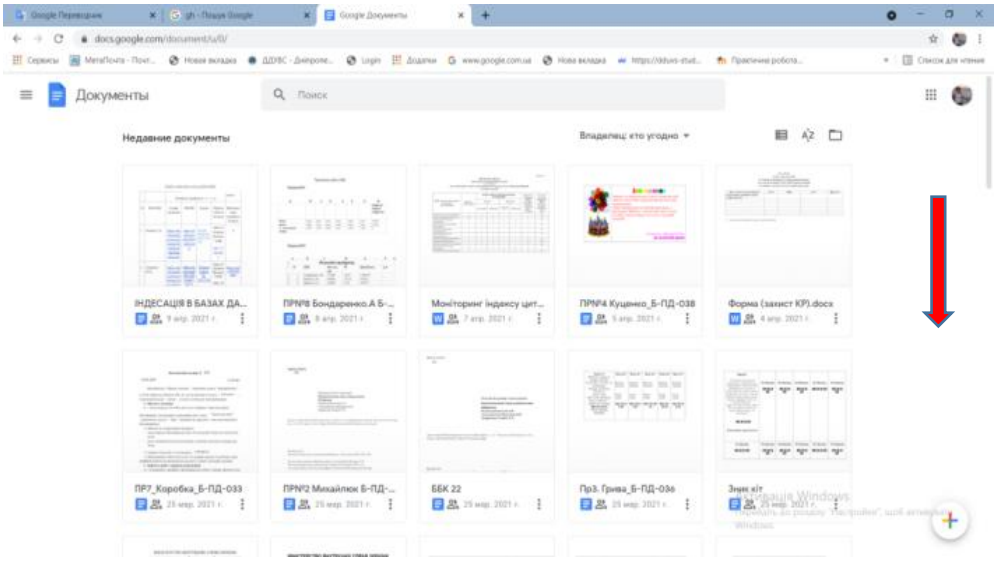


Рис. 4.18. Створення документу (крок 2)

Відкриється документ, що має багато спільного з MS Word (рис. 4.19).

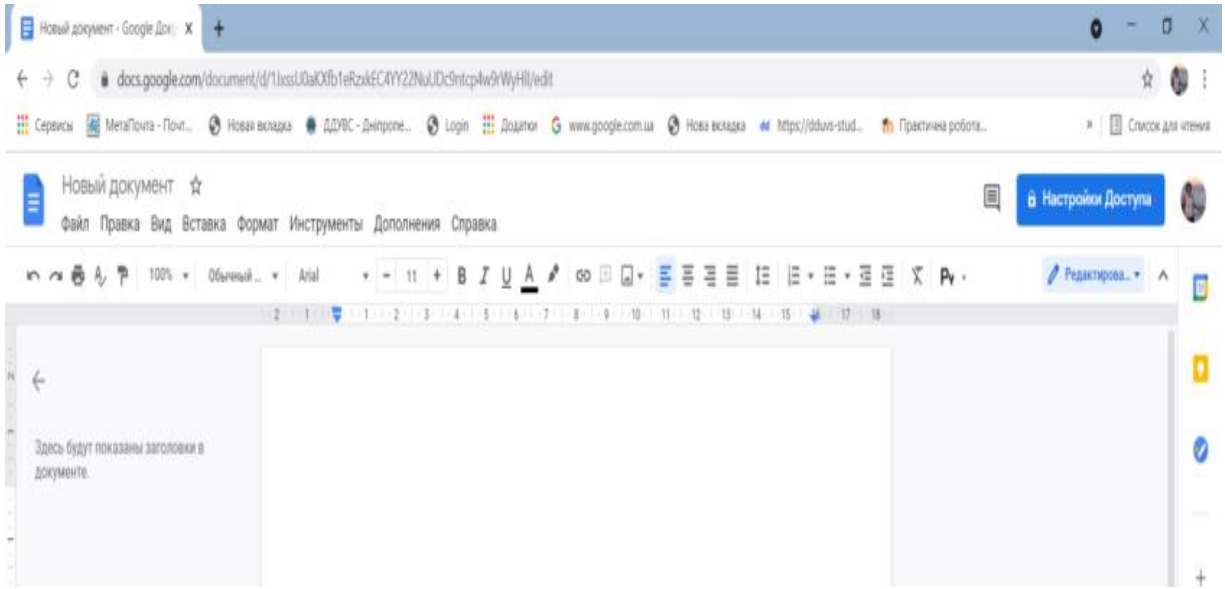


Рис. 4.19. Загальний вигляд документа

Щоб його перейменувати, слід ввести його нову назву. Створений документ автоматично зберігається на Google Диску. Сервіс зберігає всю введену в документ інформацію.

За замовчуванням всі документи зберігаються в кореневий каталог диска. Для того, щоб помістити його в будь-яке інше місце, необхідно виконати команду *Файл/Скачати* та обрати потрібний тип файлу із запропонованого списку (рис. 4.20).

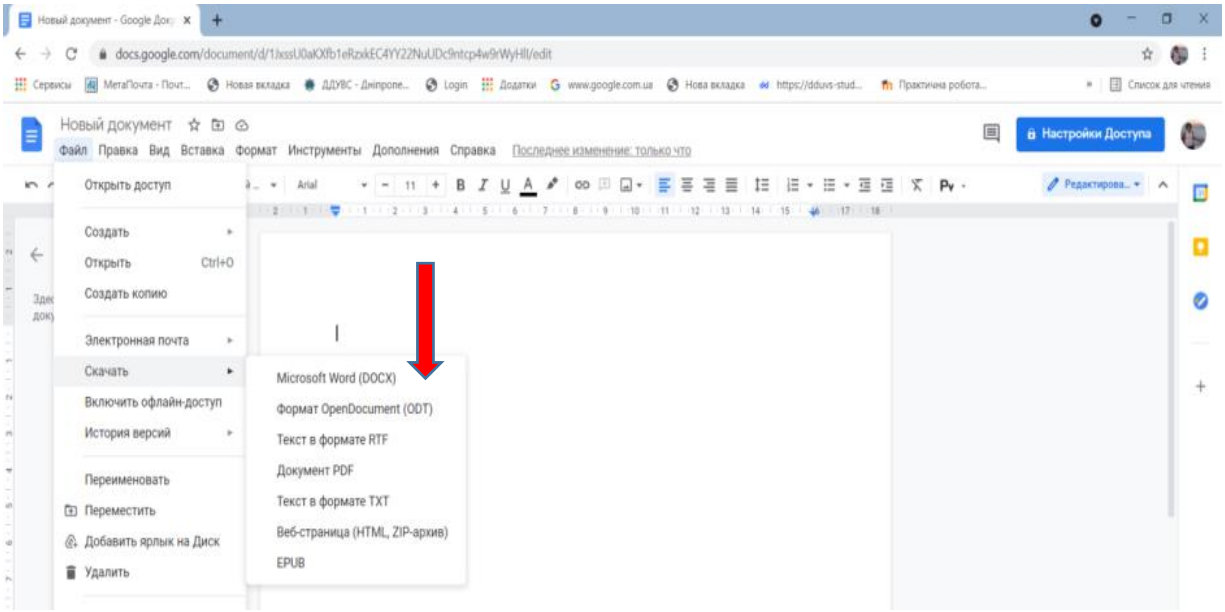


Рис. 4.20. Збереження файлу на комп’ютері

Форматування Google документа.

Для форматування документу існують наступні опції:

– *стилі, шаблони*, між якими можна швидко перемикатися. Зручно для створення заголовків і форматування скопійованого з зовнішніх джерел тексту.

– *шрифт і розмір.* За замовчуванням є достатньо шрифтів, але є можливість підключати нові;

– *ефекти і колір.* Жирний, курсив, підкреслення. Відразу вибирається колір тексту і виділення маркером;

– *вставити посилання.* Створює гіперпосилання в документі, коментар. Додає замітки й нагадування на полях. Дуже зручно, щоб нічого не забути.

– *вирівнювання.* Текст можна «притиснути» до лівого або правого краю аркуша, розмістити по центру або зробити всі рядки однаковими по ширині;

– *міжрядковий інтервал.* Задає відстань між рядками тексту.

– *списки.* Створює нумеровані й маркіровані списки;

– *відступ.* Відстань від краю аркуша до тексту;

– *очистити форматування.* Видаляє всі ефекти з тексту;

– *способи введення.* Викликає різні екранні клавіатури.

Для роботи з текстом використовуємо інструменти головного меню:

– копіювання форматування: необхідно виділити текст та зберегти параметри форматування (шрифт, колір, розмір, вирівнювання). Далі виділити інший текст, щоб застосувати параметри до нього;

– масштаб – наближає й віддаляє текст, не змінюючи розмір його шрифту.

– стилі, шаблони, між якими можна швидко перемикатися. Зручно для створення заголовків і форматування скопійованого з зовнішніх джерел тексту;

– шрифт і розмір;

– ефекти і колір: жирний, курсив, підкреслення. Відразу вибирається колір тексту;

– вставити посилання – створює гіперпосилання в документі;

– коментар-додає замітки й нагадування на полях;

– вирівнювання-текст можна «притиснути» до лівого або правого краю аркуша, розмістити по центру або зробити всі рядки однаковими по ширині;

– міжрядковий інтервал-задає відстань між рядками тексту;

– списки-створює нумеровані та маркіровані списки;

– відступ-відстань від краю аркуша до тексту;

– очистити форматування-видаляє всі ефекти з тексту;

– способи введення-викликає різні екранні клавіатури.

Налаштування параметрів друку службового документу.

Форматування документів, призначених для друку на принтері, виконується в прив’язці до параметрів друкованої сторінки. Тому створення документів цієї категорії необхідно починати з настроювання параметрів сторінки. До таких параметрів належать розміри аркушу й розміри полів.

Для друку документу виконується команда Файл/Друк (рис. 4.21).

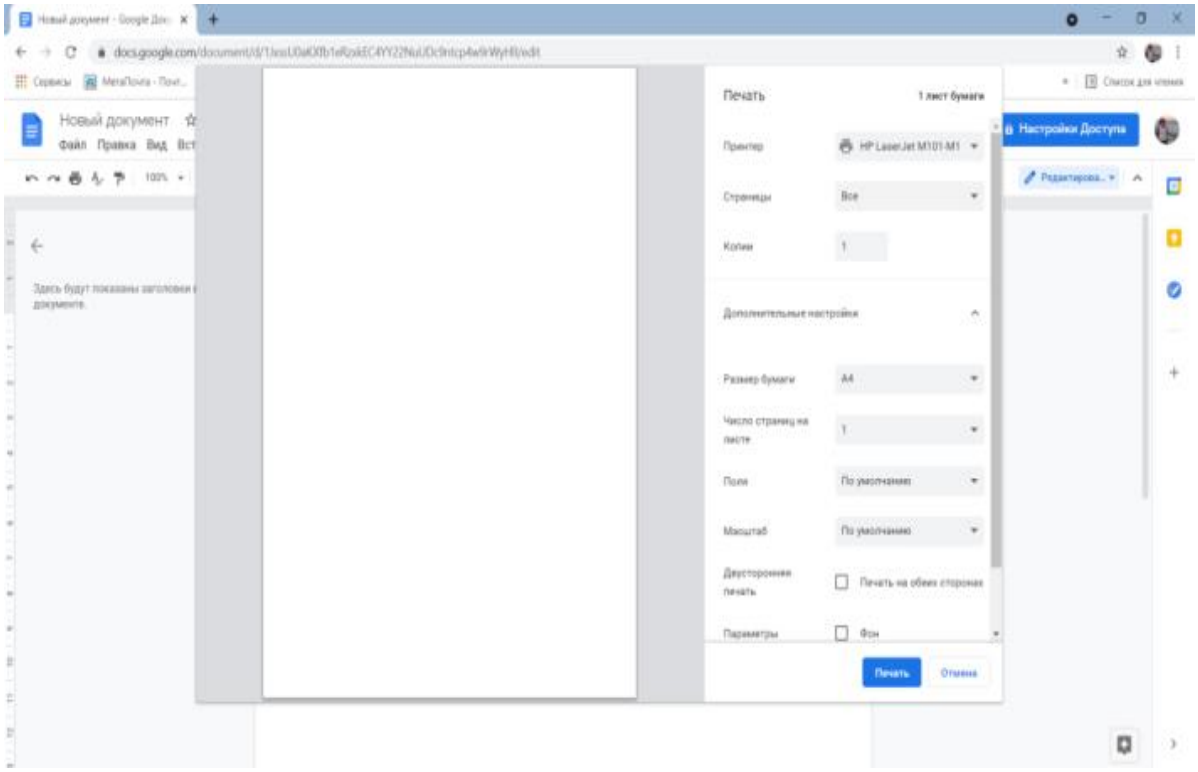


Рис. 4.21. Налаштування друку документа

У вікні обрати :

- тип принтеру;
- кількість сторінок;
- кількість копій друку;
- додаткові параметри: поля, масштаб, параметри сторінки і т.д;
- на вкладці «Розміри паперу» обрати у списку «Розмір паперу пункт А4» (це стандартний формат 210×297 мм). У випадку використання нестандартного формату вибирають пункт «Інший» і за допомогою лічильників «Ширина» і «Висота» задають його параметри;
- на вкладці «Поля» задаються розміри полів: ліве; праве; верхнє; нижнє. Задається орієнтація паперу – «Книжкова» чи «Альбомна». За альбомної орієнтації папір розташовується довгою стороною по горизонталі;
- якщо передбачається двосторонній друк (парні сторінки друкуються на зворотному боці непарних сторінок), то треба поставити прапорець «Двосторонній друк» на вкладці «Поля».

Створення структури документа.

Цей інструмент створює наочну структуру документа, по якій можна швидко перейти до потрібного місця. Для цього необхідно відкрити вкладку «Вид» « Показать структуру документа» рис. 4.22.

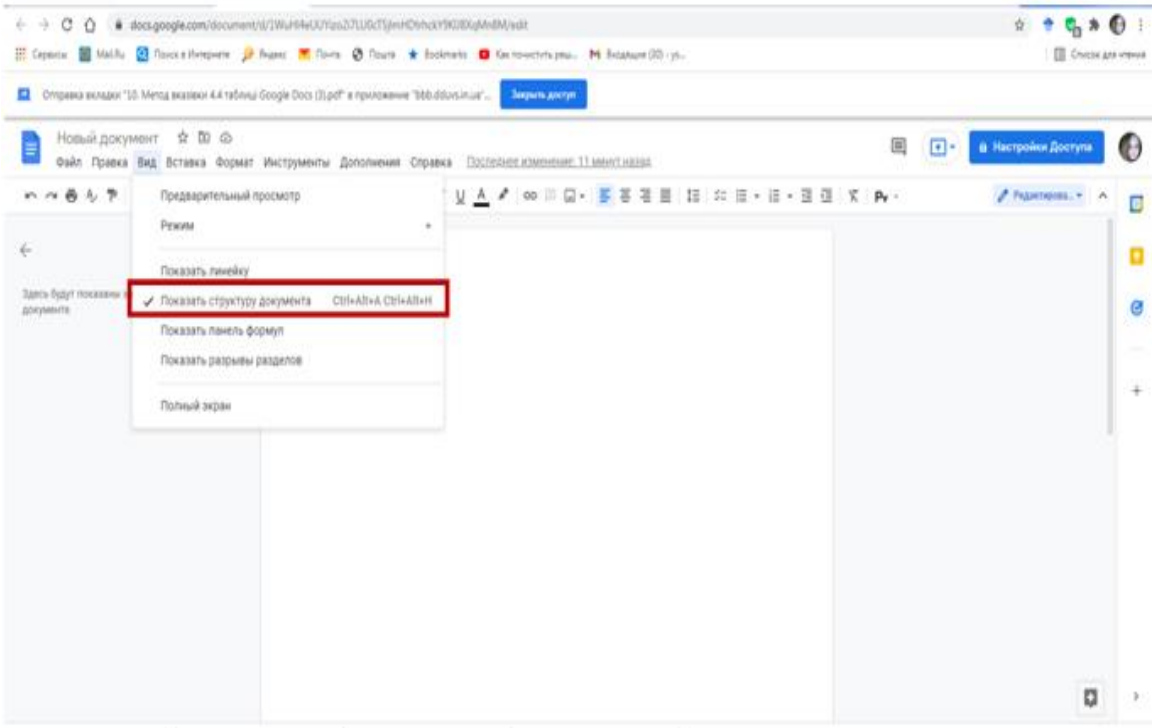


Рис. 4.22. Створення структури Google документа

Для формування структури Google документу потрібно їх оформити. Використав «Меню стилів» рис. 4.23.

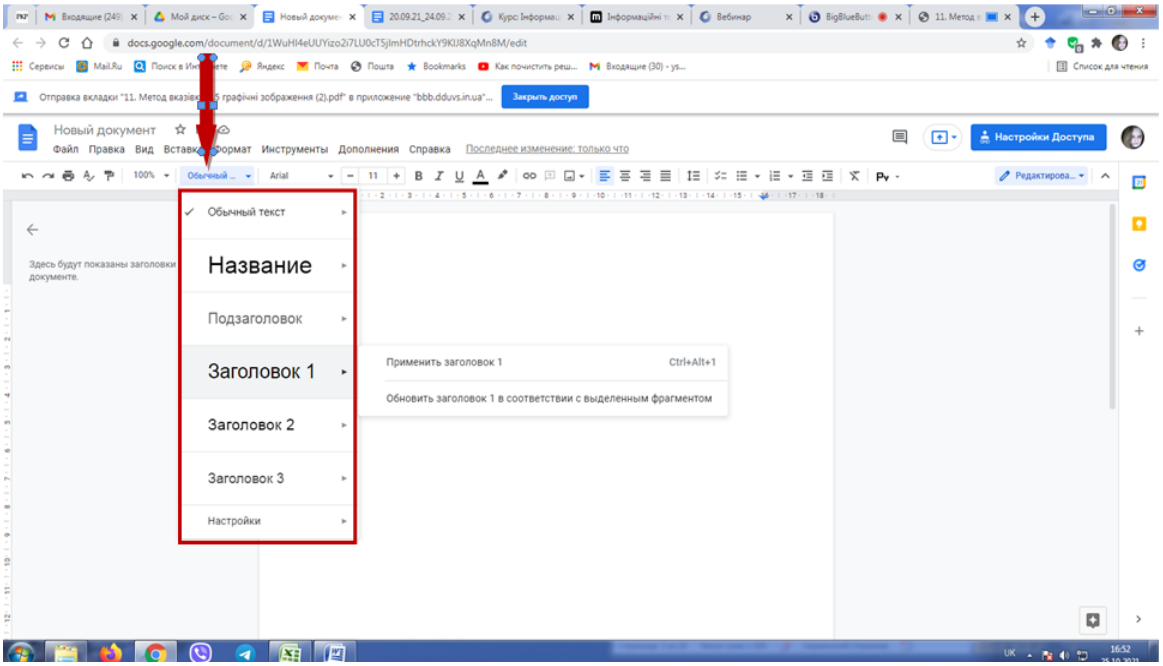


Рис. 4.23. «Меню стилів»

Для цього потрібно (рис. 4.24):

– виділіть заголовок;

– натисніть «Заголовок 1» («меню стилів»);

– виберіть заголовок.

– виділіть підзаголовок і застосуєте до нього стиль: «Заголовок 2»;

– збільшить шрифт заготовка та підзаголовка, він винний бути більше, ніж решта тексту;

– застосуєте до нього напівжирне виділення.

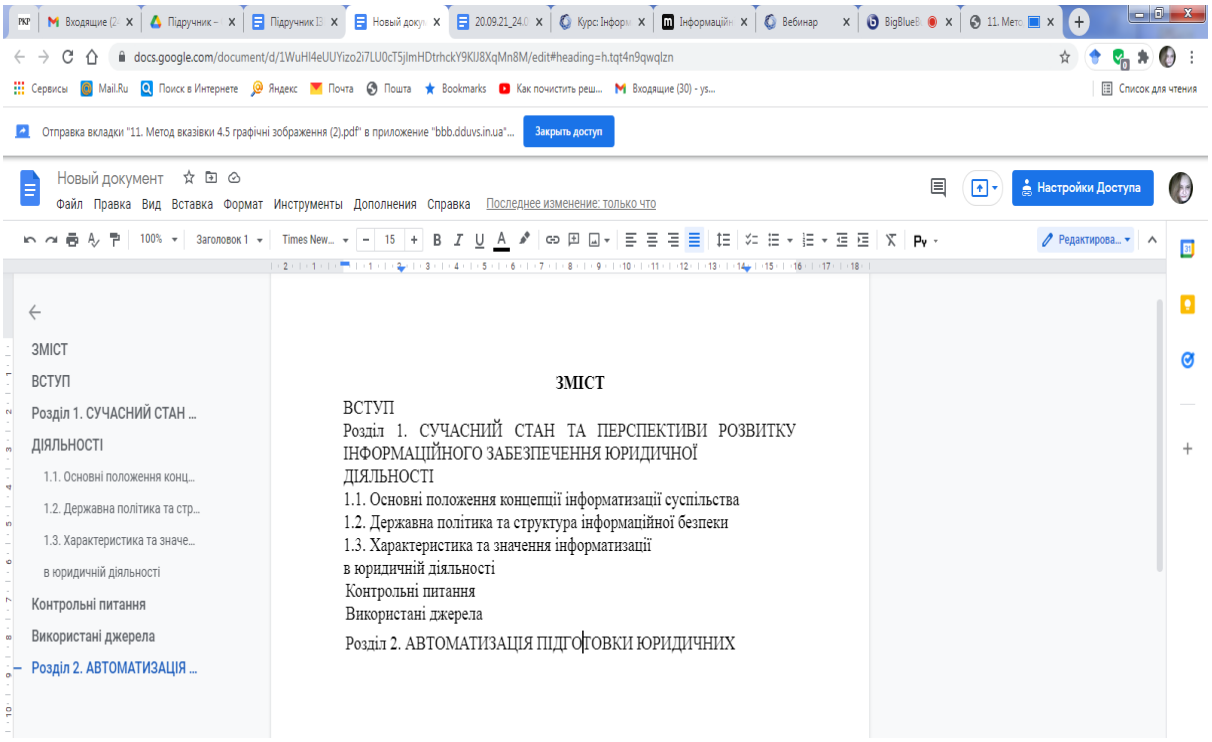


Рис. 4.24. Формування структури Google документа з використанням «Меню стилів»

Структуру документа можна зробити змістом. Для цього потрібно вибрати вкладку «Вставка» та перейти до «Оглавление» рис. 4.25.

Зміст документа можна представити як за номерами сторінок так і за посиланням рис. 4.26 та 4.27.

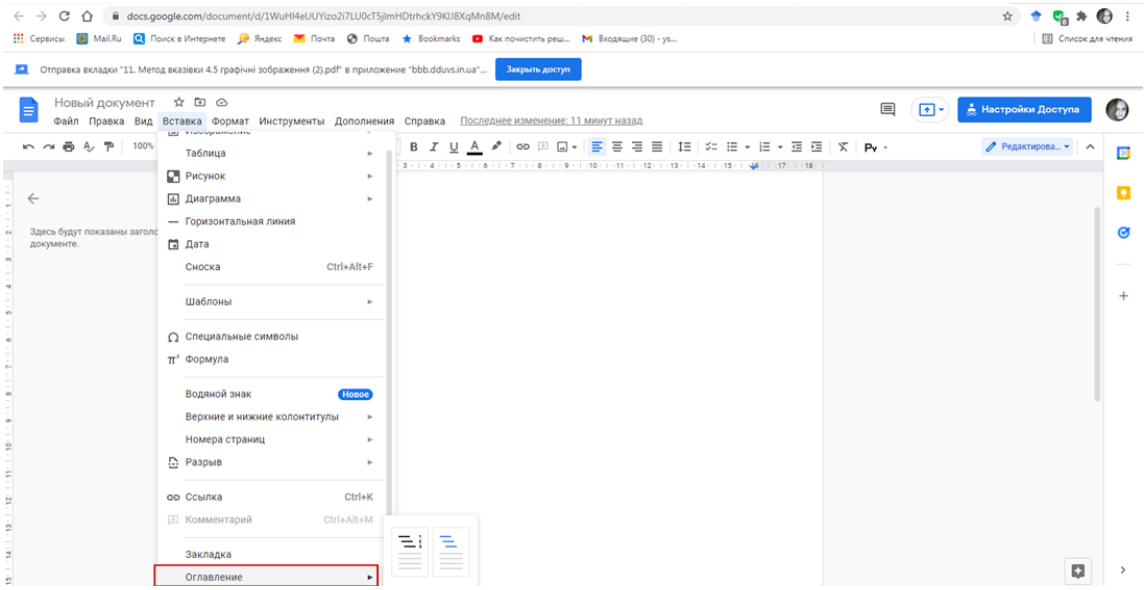


Рис. 4.25. Створення зміст Google документа

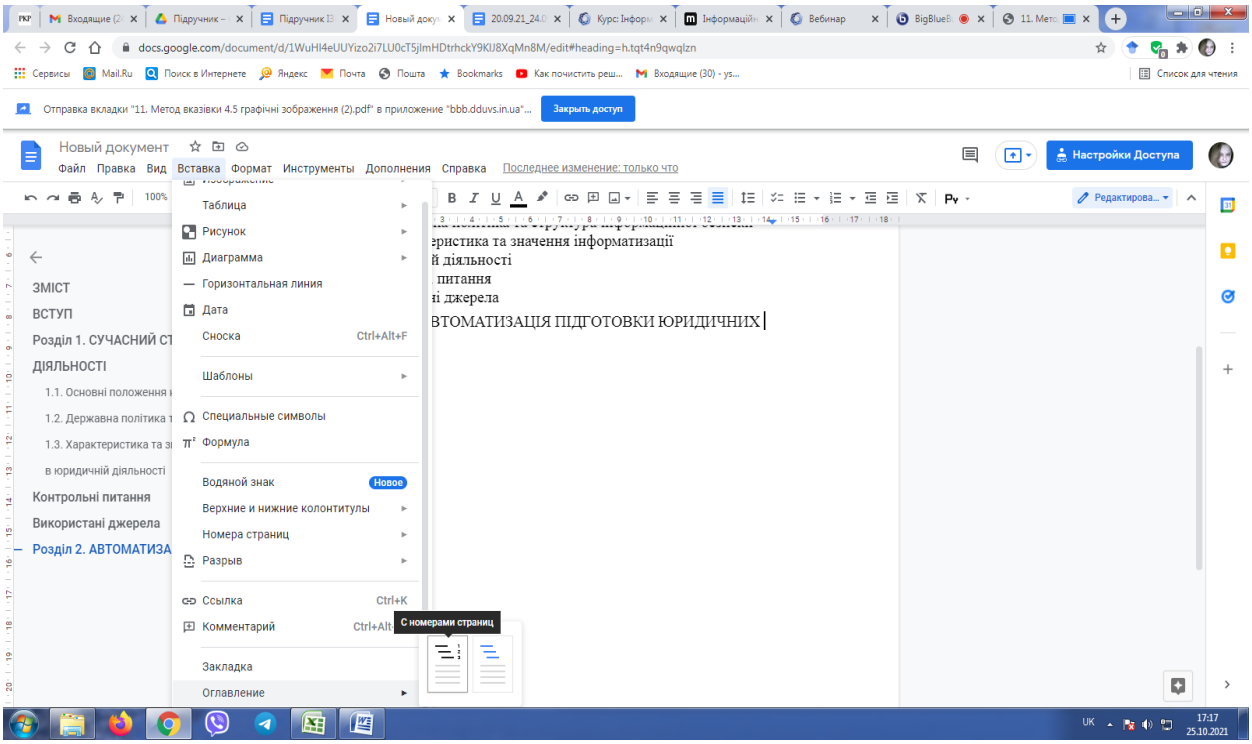


Рис. 4.26. Визначення вигляду «змісту» документа
за номерами та посиланнями

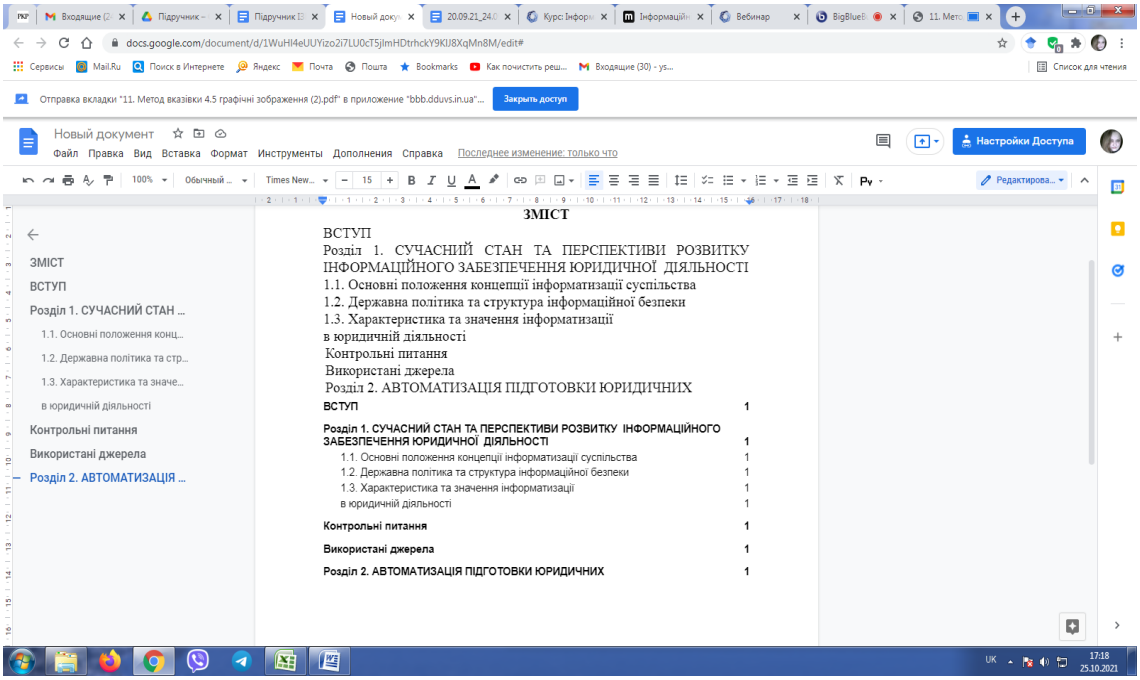


Рис. 4.27. Загальний вигляду «змісту» документа за номерами та посиланнями

Під час внесення змін до «змісту» документу потрібно проводити оновлення «Змісту» рис. 4.28 та 4.29.

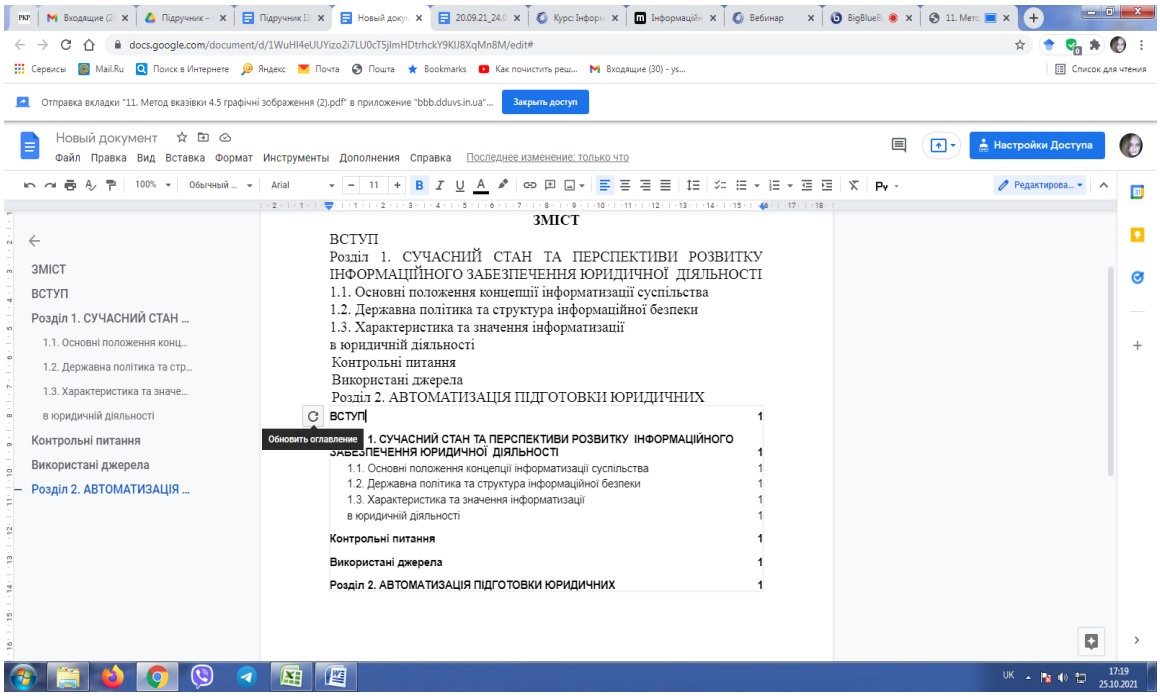


Рис. 4.28. Оновлення «змісту» документа

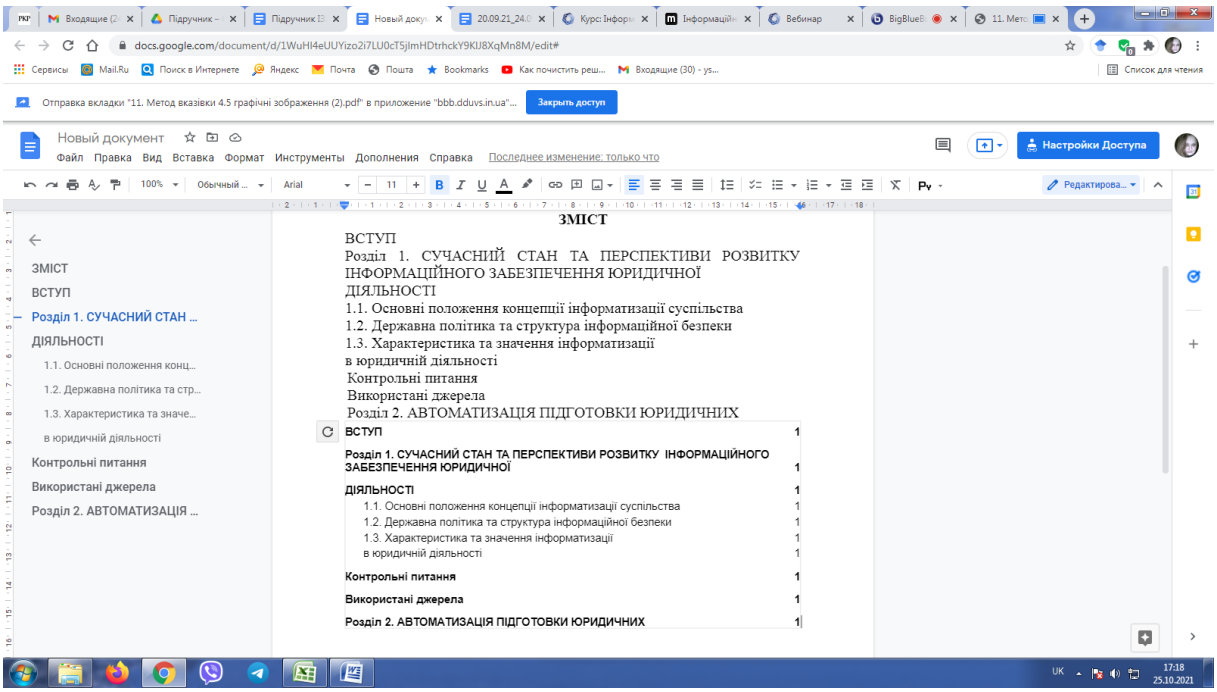


Рис. 4.29. Загальний вигляд «змісту» після оновлення

Створення закладки

Закладка запам’ятовує потрібне вам місце й створює на нього посилання. Її можна відправляти іншим користувачам, так зможуть відразу перейдуть до потрібного фрагмента тексту.

Для створення закладки відкрийте «Вставка» оберіть з меню, яке розкрилося позицію «Закладка», на початку рядка з’явиться невеликий синій прапорець (рис. 4.30).

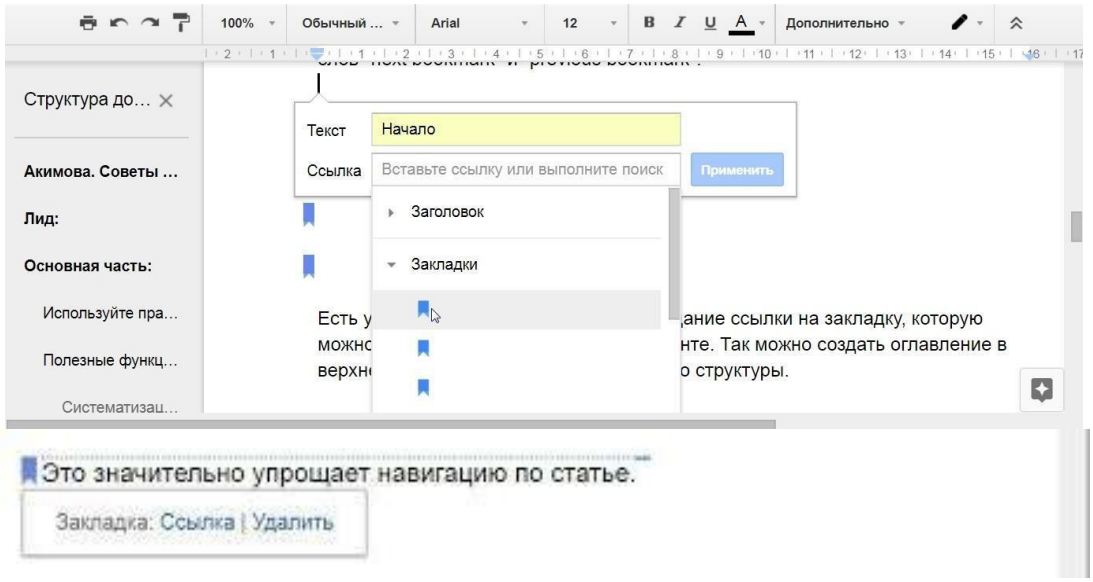


Рис. 4.30. Загальний вигляд позиції «Закладка»

На закладку можна посилатися у тексті документа:

– виберіть місце, куди хочете розмістити посилання;

– натисніть пункт «Посилання», замість URL виберіть одну з закладок уменю, яке випадає;

– введіть текст.

Створення колонтитулу.

Колонтитул – це область (зверху або знизу), загальну для всіх сторінок документа (рис. 4.31). Тут можна вказати інформацію про автора, назву документа, номер сторінки та розмістити посилання і т.п.

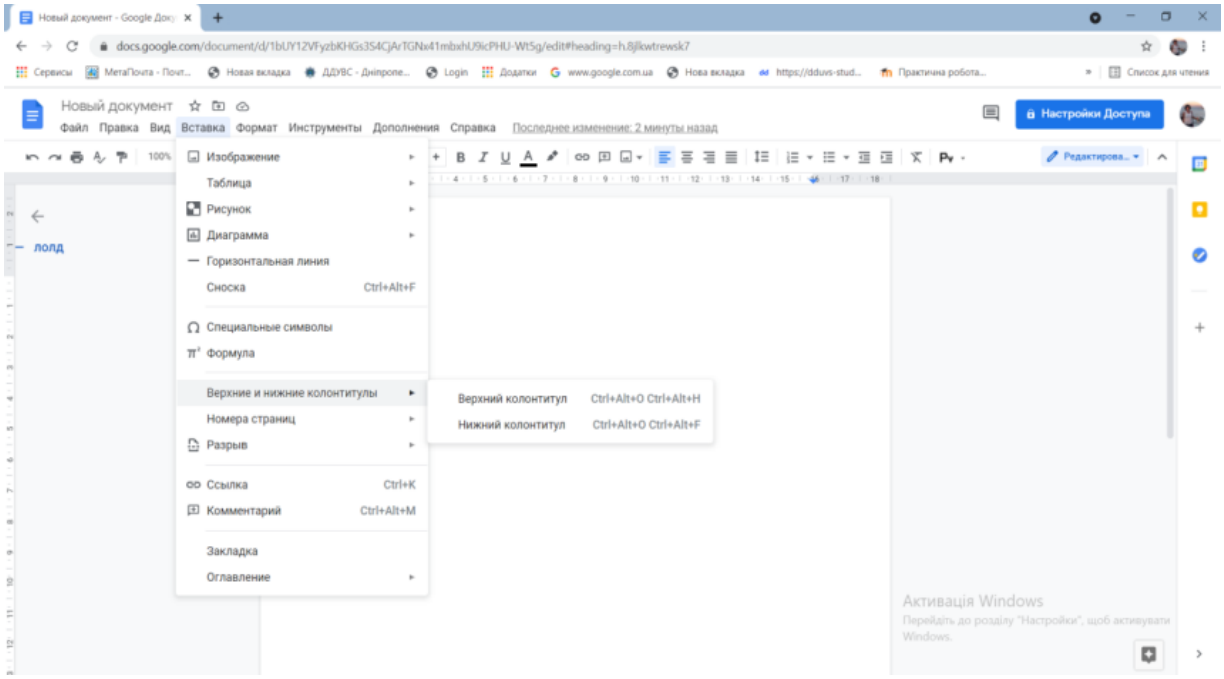


Рис. 4.31. Вставка колонтитулів

Нумерація сторінок.

Нумерацію сторінок документу можна знайти у вкладці *Вставка/Номера сторінок* (рис. 4.32). Google дозволяє 4 варіанта на вибір розміщення номеру: унизу; вгорі; унизу, без першої сторінки; вгорі, без першої сторінки.

За замовчуванням номер перебуває в правому куті колонтитула, але його можна перемістити в будь-яке місце.

Історія змін в Google Docs

Однією з найкращих функцій Google Документів є збереження змін. Переглянути попередні варіанти файлу можна послідовністю команд: *Файл /Історія версій/Дивитись історію версій* (рис. 4.33).

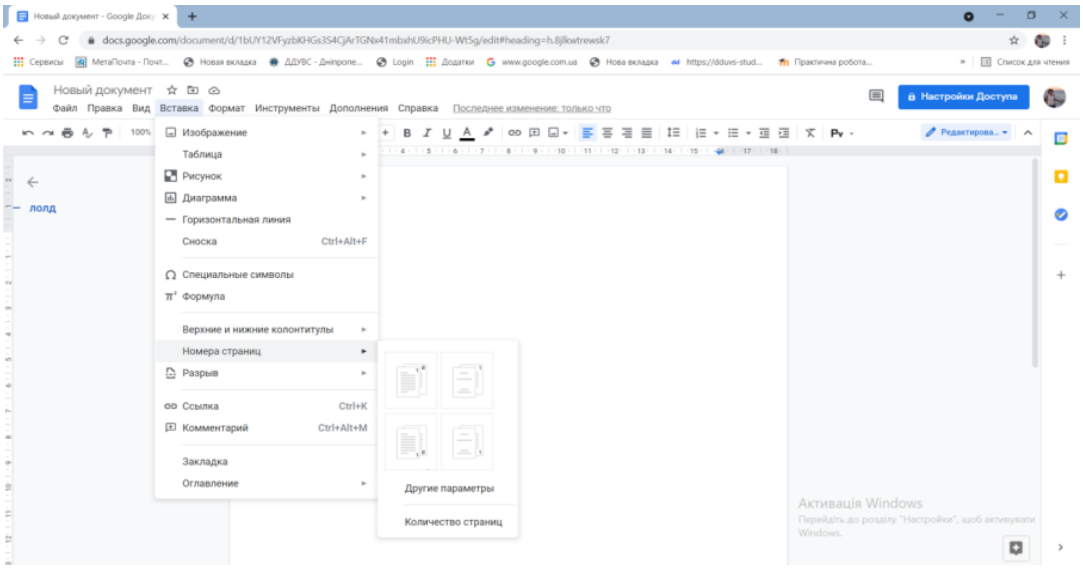


Рис. 4.32. Вставка номера сторінки

Відкриється величезна історія версій документа, у якій можна вибрати будь-який етап і подивитися, чому він відрізняється від поточного тексту. Звідси можна скопіювати вилучені фрагменти чи просто відкотитися до потрібної версії. Можна відновити будь-яку версію.

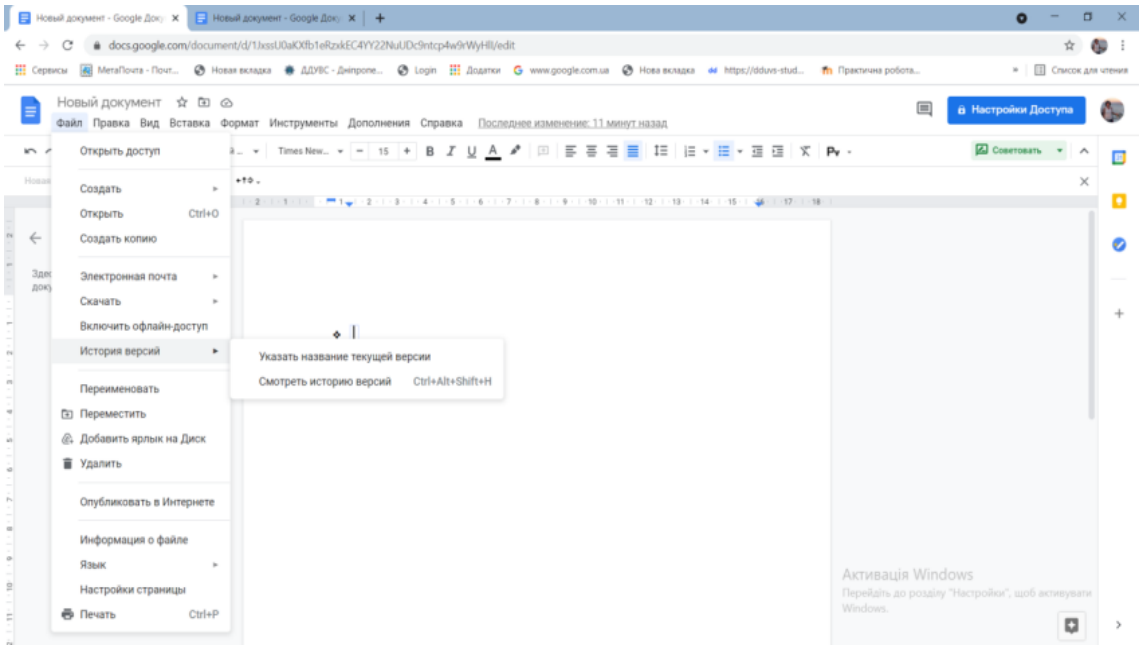


Рис. 4.33. Історія змін

Введення спеціальних символів.

Для відтворення спеціальних символів потрібно зайти до вкладки «вставка» та перейти у розділ спеціальні символи (рис. 4.34).

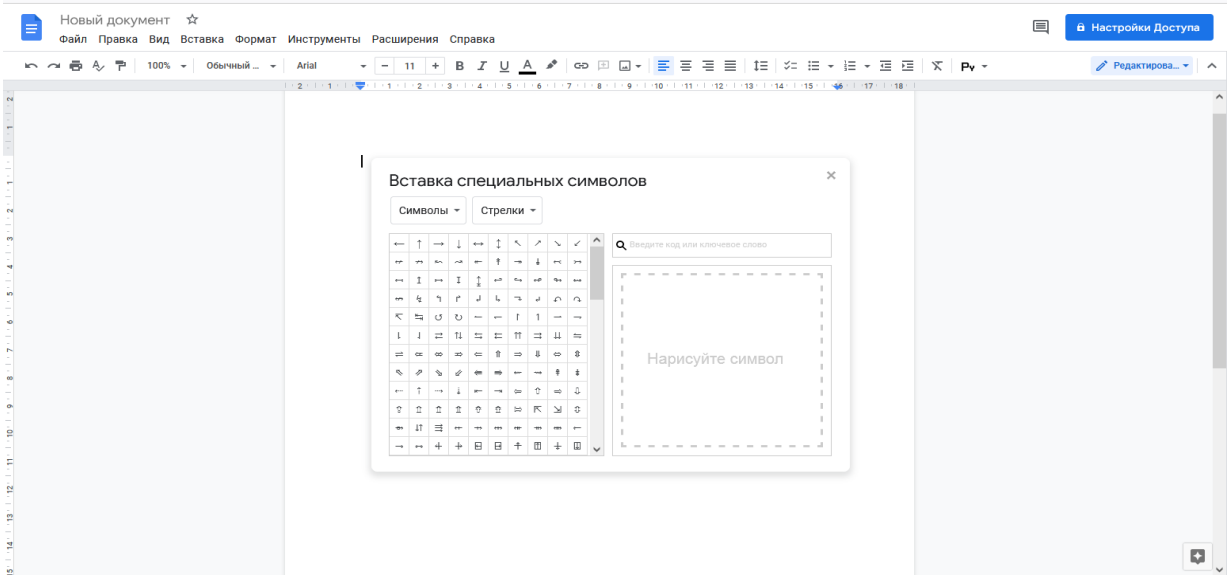


Рис. 4.34. Введення спеціальних символів

Розділ спеціальні символи має у своєму складі дві окремі категорії:

– Символ; Стрілки.

Ці дві категорії мають свої меню (рис. 4.35 та 4.36). Якщо потрібно знайти необхідний символ необхідно поперемінно змінювати категорії. Наприклад символ Видавництва знайдемо у категорії «Символ» – «Символ», у категорії «Стрілки» – «Прочие» рис. 4.37.

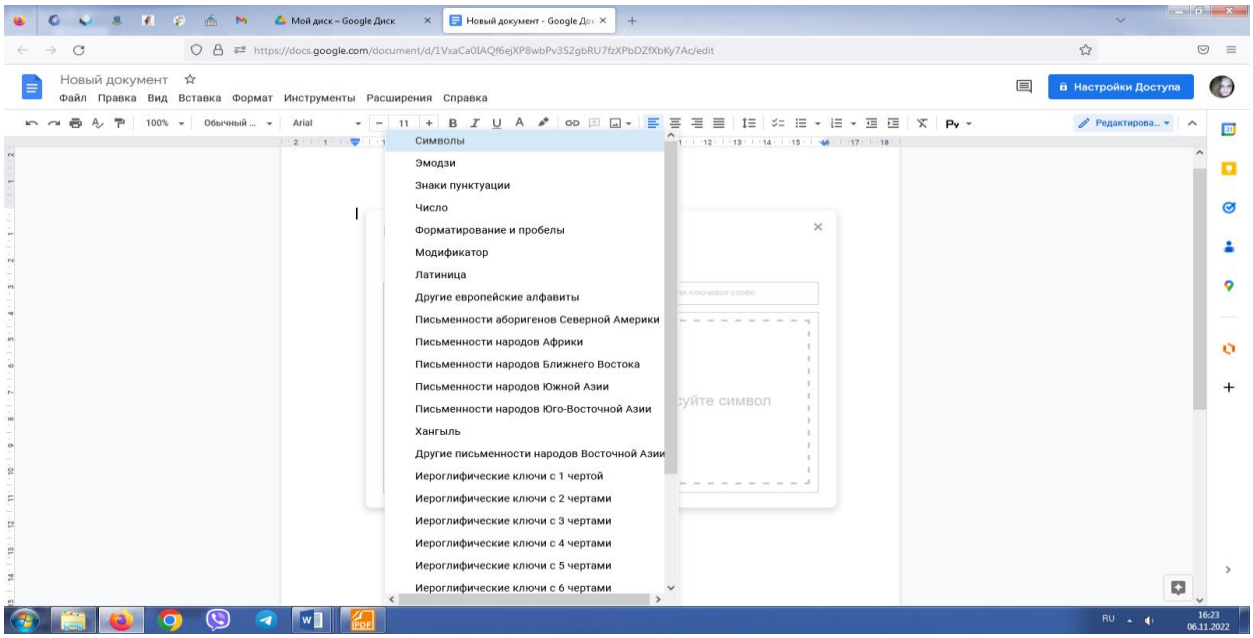


Рис. 4.35. Загальний вигляд категорії «Символ»

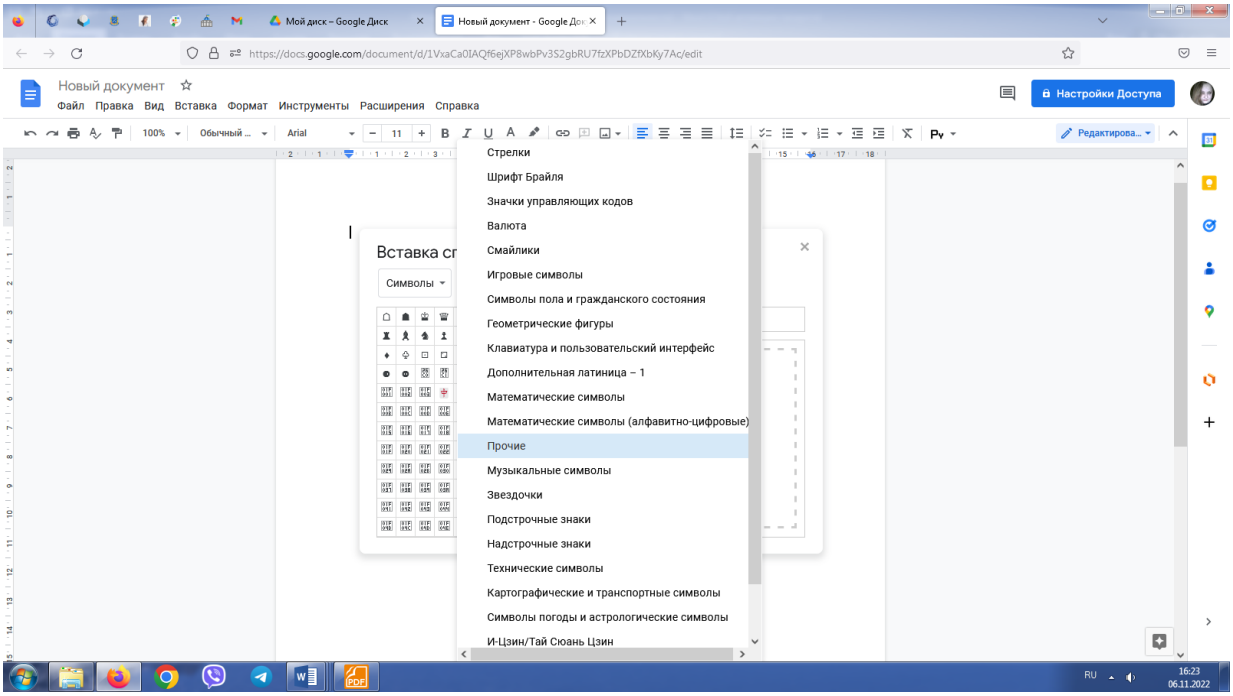


Рис. 4.36. Загальний вигляд категорії «Стрілки»

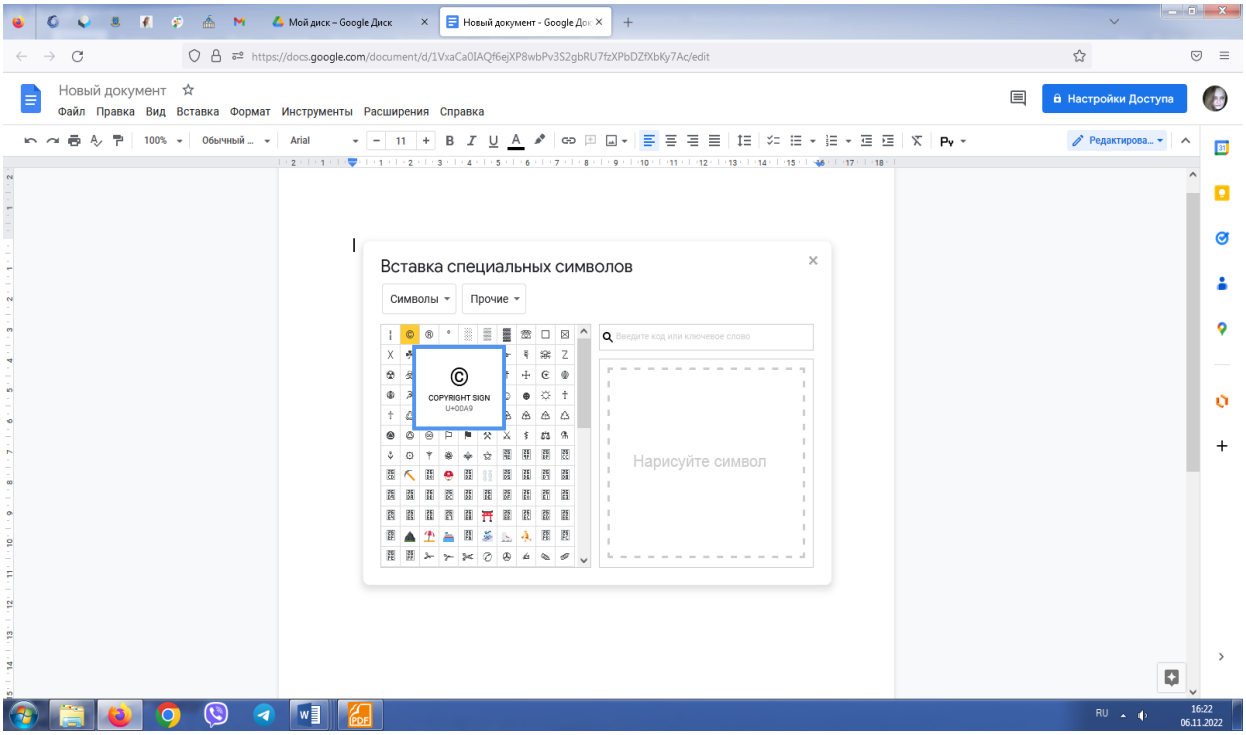


Рис. 4.37. Визначення символу «Видавництво»

4.4. Робота у Google docs. Створення таблиці та її форматування, а також пошук та редагування зображення

Робота з таблицями

Таблиці використовуються для представлення найрізноманітнішої числової і текстової інформації, схильної до упорядкування за одним чи кількома критеріями. Google Docs має великий набір інструментів для побудови і форматування таблиць, що дозволяє будувати дуже складні таблиці з будь-яким оформленням. У вкладці «Вставка» виберіть пункт «Таблиця». На сітці, що з'явився, можна задати кількість стовпців і рядків (рис. 4.38).

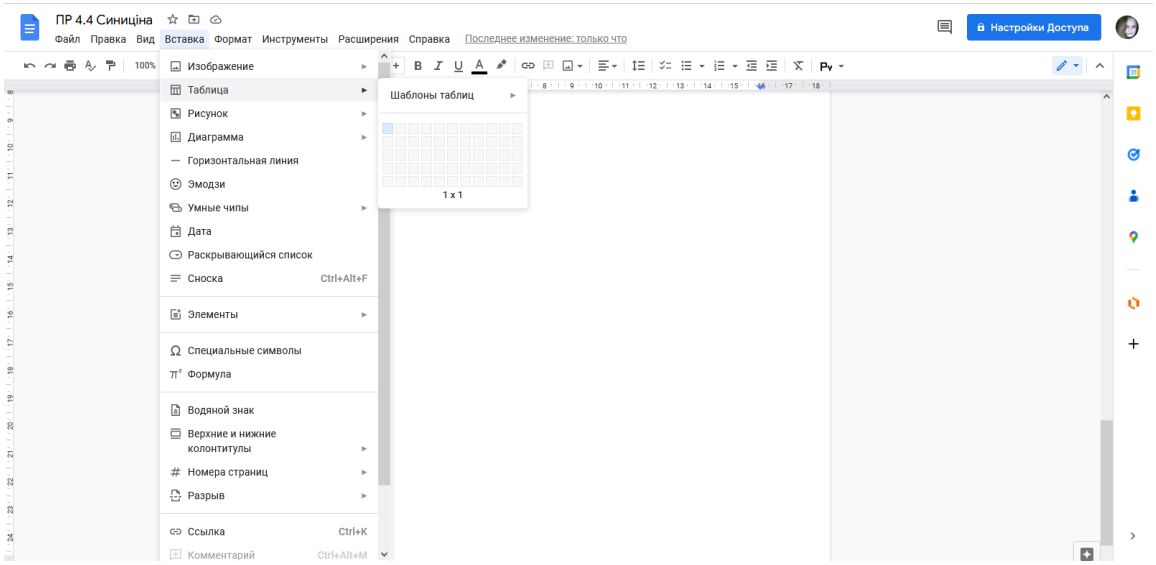


Рис. 4.38. Створення таблиці

Тепер можливе заповнення комірок таблиці текстом, цифрами та зображеннями. Якщо потрібно створити додаткові рядок або стовпець, кликніть ПКМ у таблиці й у контекстному меню виберіть «Вставити» (рис. 4.39).

Аналогічним образом віддаляються непотрібні елементи (рис. 4.40).

Також можливе поєднання декількох комірок в одну. Для цього потрібно їх виділите, викликати контекстне меню правої клавішею миші та обрати «Об'єднати комірки» або «Поділити комірку» (рис. 4.41).

Для того щоб змінити розміри рядка або стовпця – наведіть курсор на лінію й перетягнете її в потрібну сторону.

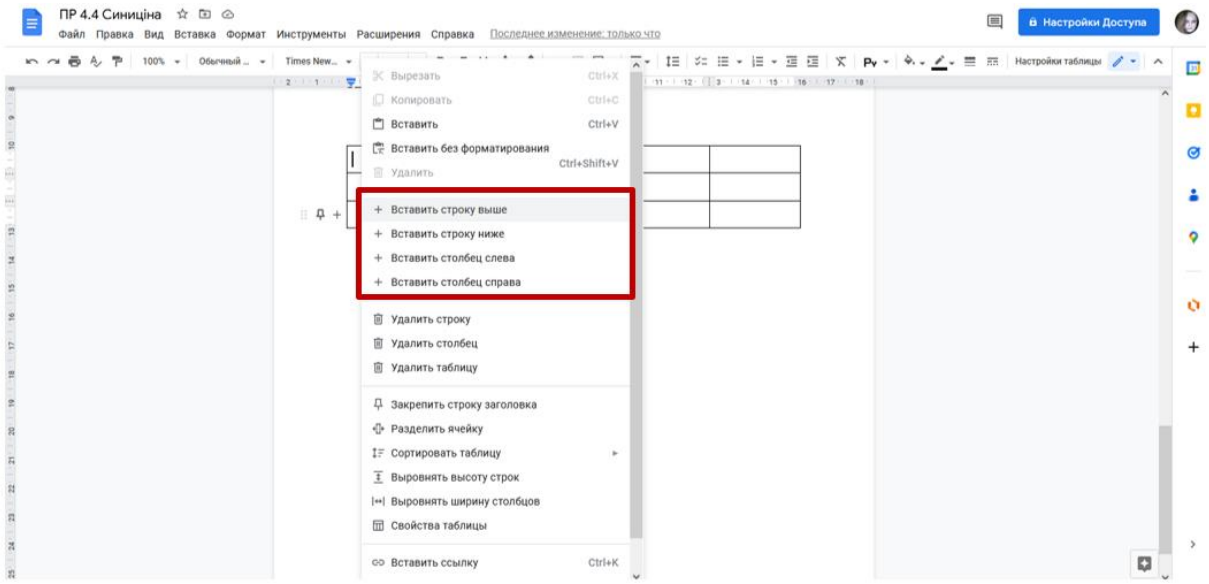


Рис. 4.39. Створення додаткових рядків і стовбців у таблиці

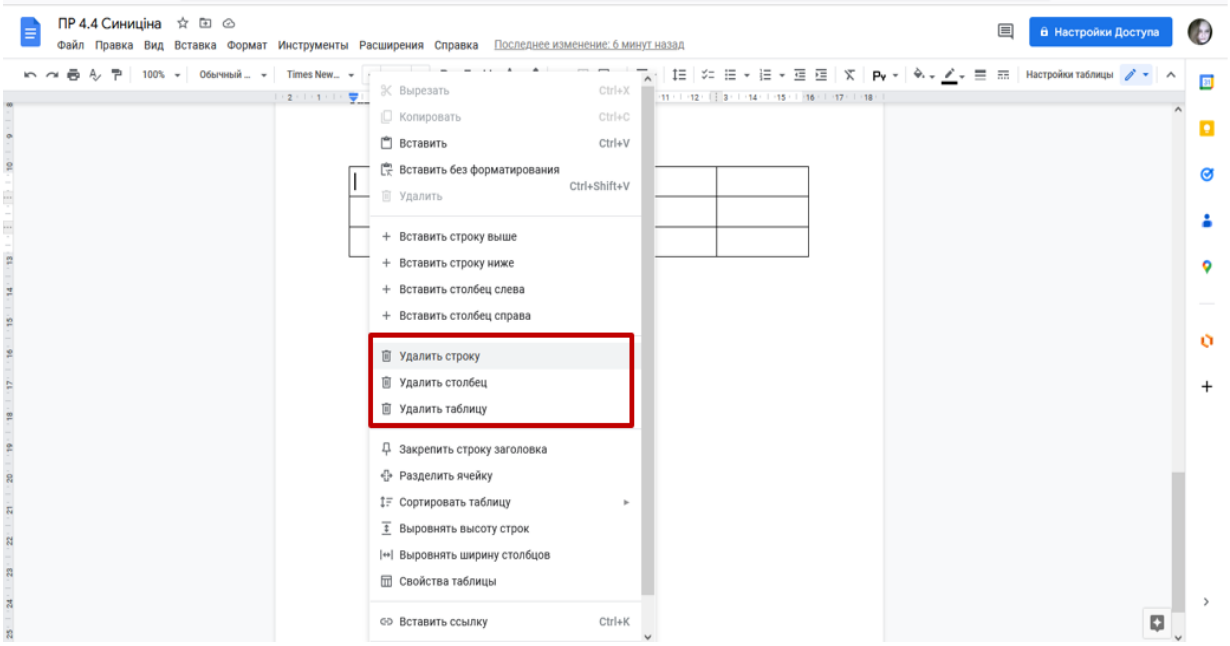


Рис. 4.40. Видалення зайвих рядків і стовбців у таблиці

Форматування таблиці також можливо проводити за допомогою вкладки «Формат» (рис. 4.42).

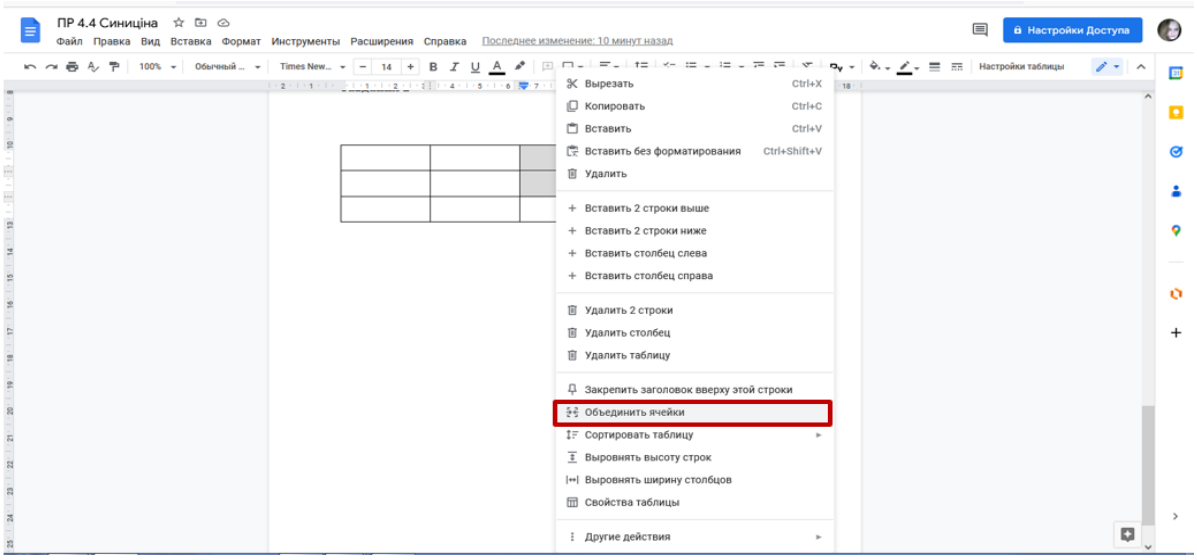


Рис. 4.41. Об’єднання комірок у таблиці

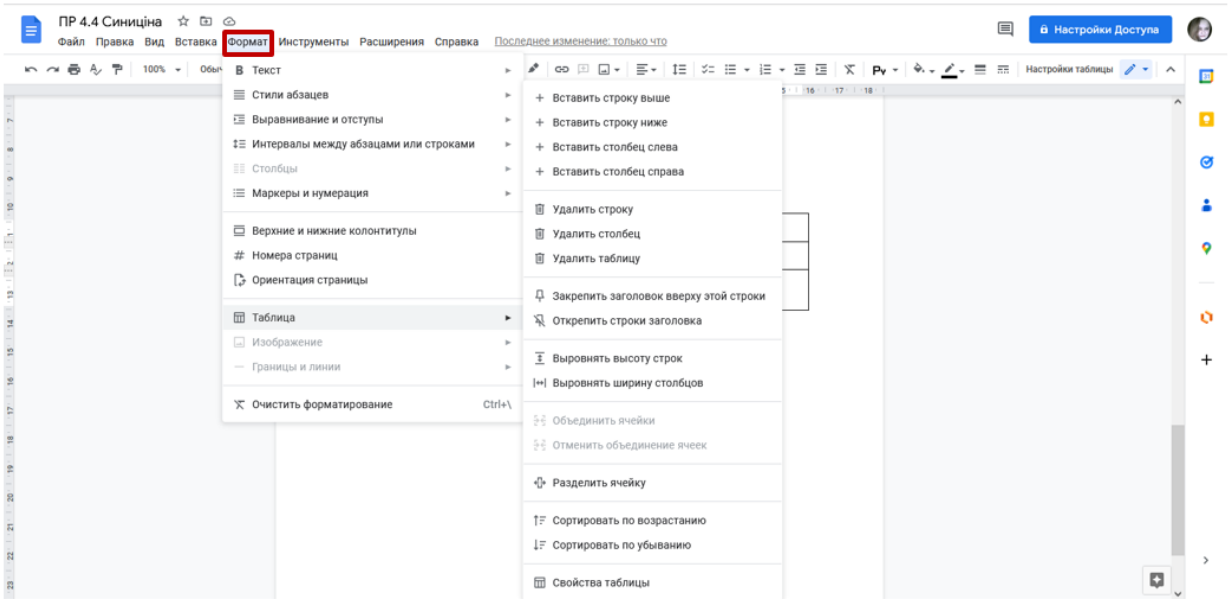


Рис. 4.42. Форматування таблиці за допомогою вкладки «Формат»

Стилізувати таблицю та зробити її більш наочної можливо за допомогою використання додаткових кнопок (рис. 4.43).

Колір тіла – зафарбовує обрані комірок;

Колір границь – задає колір ліній навколо обраних комірок.

Ширина границь – міняє товщину (жирність) ліній. Якщо обрати 0 пт – границі навколо комірок будуть невидимі.

Стиль – змінює вид границь (пряма, пунктир, крапки).

Якщо виділити одну або кілька клітинок – у правому верхньому куті з'явиться стрілка-значок-стрілка. Він викликає меню, у якому можна виділити певні лінії, а не всі підряд.

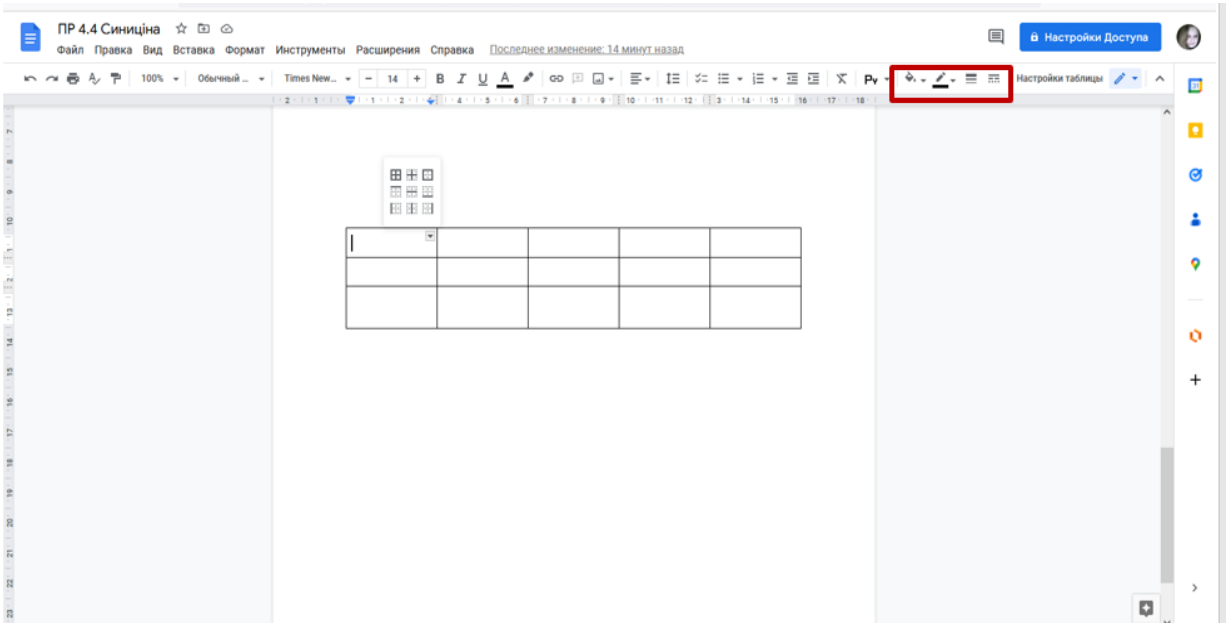


Рис.4.43. Додаткове форматування таблиці

Можливі варіанти форматування таблиці наведено на рис. 4.44.

Рис. 4.44. Додаткові варіанти щодо форматування таблиці

Налаштовувати формати та вигляд таблиці, можна, скориставшись командою контекстного меню *Властивості таблиці*. За цієї можливості можна задати вирівнювання, відступи, розміри комірки і параметри ліній границь (рис 4.45, 4.46).

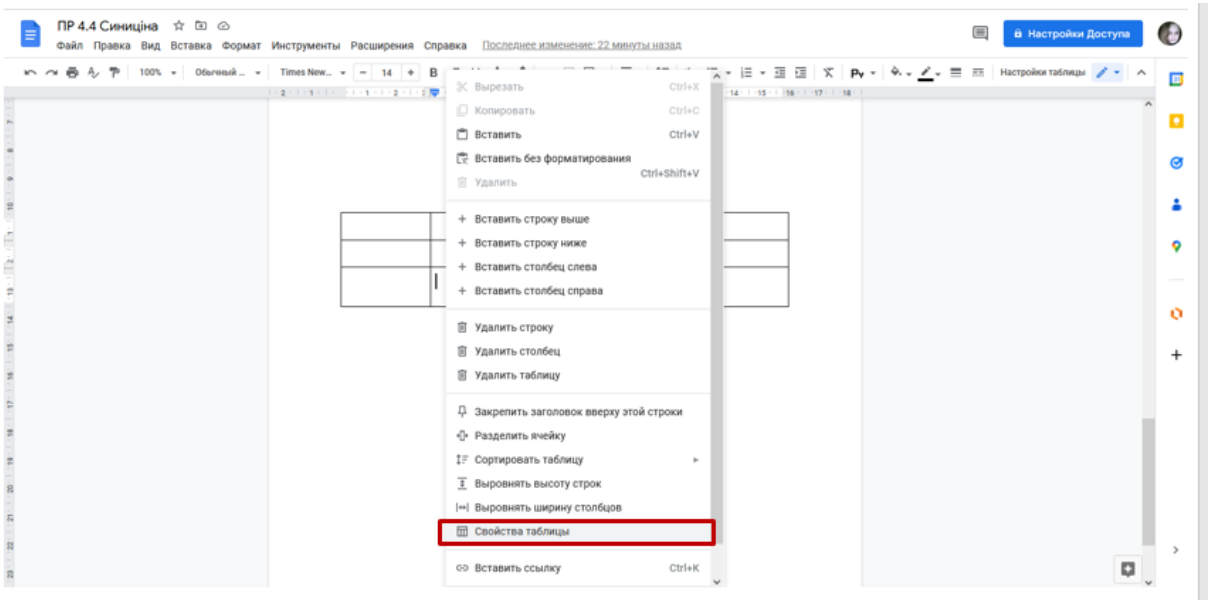


Рис. 4.45. Загальний вигляд контекстного меню з визначенням кнопки «Властивості таблиці»

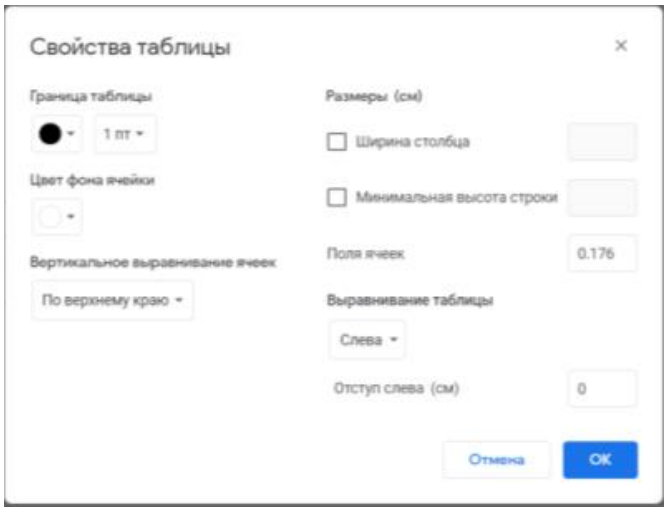


Рис. 4.46. Налаштування таблиці

Якщо виділити всю таблицю й натиснути клавішу Del – ви вилучите тільки вміст комірок. Видалити таблицю можна командою «Видалити таблицю» у контекстному меню.

Вставка зображень в документ або в таблицю

Будь-яке зображення можна вставити в документ або таблицю шляхом(рис. 4.47):

– стандартного копіювання картинки;

– завантаження з комп’ютера;
– пошук в інтернеті;
– добавити з Google Диску;
– добавити з Google Фото
– вставити посилання;
– зробити знімок.

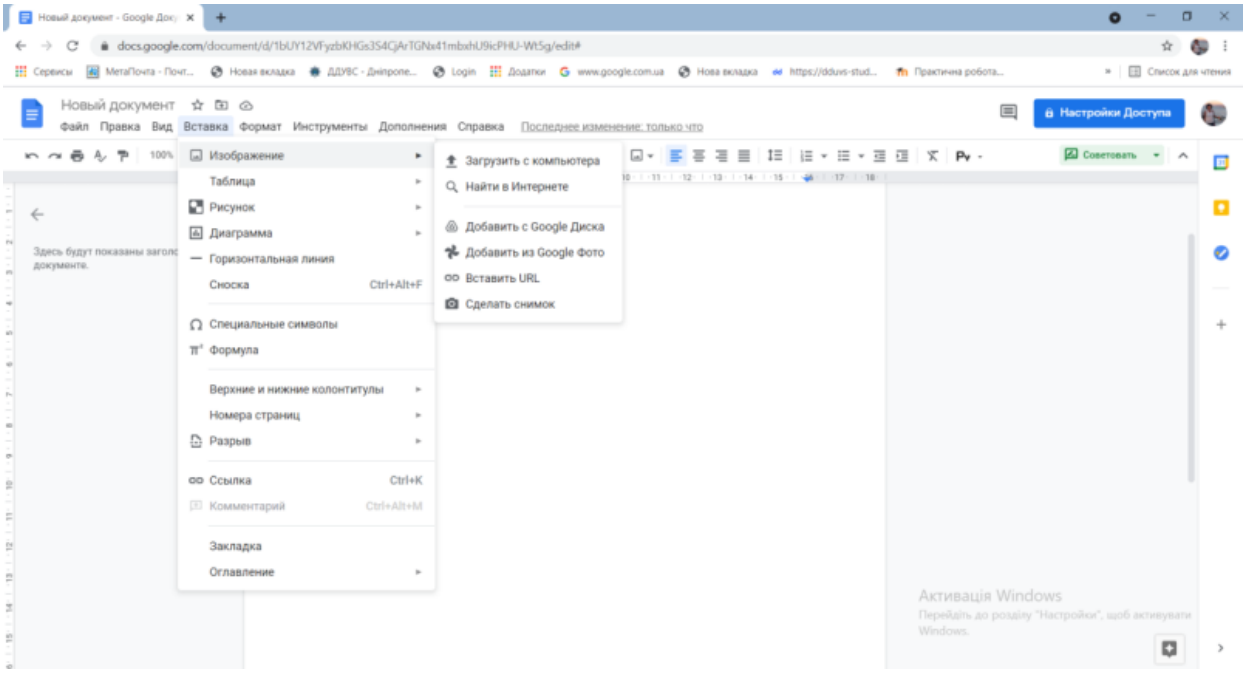


Рис. 4.47. Вставка зображення через меню

Якщо активувати зображення на робочому листі документа з’явиться два контекстних меню (рис. 4.48):

За першим можливо: форматування зображення: можна копіювати, переставляти, зробити гіперпосиланням, вирівнювати по потрібному краю аркуша або за центром за розміщенням відповідно робочого листа, корегування розміру, повороту та кнопка «параметри зображення».

За другим, відповідно, вкладка «Параметри зображення» здійснити корегування розмірів, здійснити поворот зображення, здійснити перенос тексту «обтікання тесту» (У середині тексту, наверх тексту, за текстом), скорегувати колір зображення, змінити прозорість, яскравість, контрастність і поміняти передачу кольору.

У Google Docs можна обрізати картинки, відкидаючи непотрібні частини. У контекстному меню обрати пункт *Обрізка* і за допомогою

рамок указати область, яку потрібно залишити.

Подвійне клацання по картинці теж викликає рамку для обрізки.

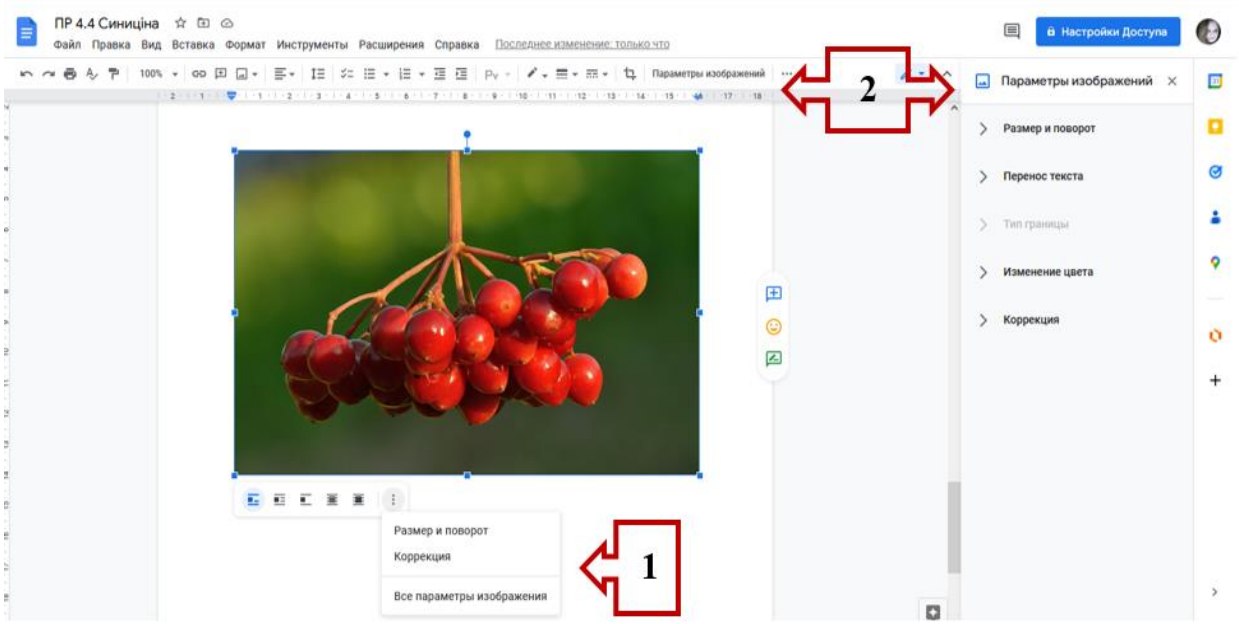


Рис. 4.48. Налаштування параметрів зображення

4.5. Робота у Google docs. Створення рисунка, його форматування та редагування

Вставка рисунків.

Вставка рисунків – це інструмент, яким можна створювати наочні схеми, карти, додавати підписи й стрілки до зображень. Це невеликий графічний редактор усередині Google Docs.

Створення нового об’єкта можливе командами Вставка/Рисунок. У вікні, що відкриється, можна рисувати фігури, писати текст і додавати зображення за допомогою команд, що знаходяться на панелі інструментів.

На панелі інструментів «Рисунок» має наступні команди:

– «Вибрати» – дозволяє виділити об’єкти, щоб їх переміщати, редагувати й видалення;

– «Лінія» – дозволяє рисувати прямі й криві лінії, стрілки й роздільники.

– «Фігура» – дозволяє рисувати геометричні фігури, стрілки, винесення й математичні символи.

– «Текстове поле»-усередині більшості фігур автоматично створюється текстове поле, у якому відтворити текст. Параметри тексту

задаються у вкладці «Додатково».

– «Зображення» – дозволяє завантажувати в редактор картинку, з використанням зображення на комп'ютері, на Google Диску, зробити знімок з веб-камери, указати URL або скористатися пошуком.

– «Дії» – вкладка з корисними інструментами: групування, вирівнювання, поворот, збереження.

Щоб відредагувати вже створений рисунок, треба його активувати та виконати команду «Змінити».

Рисунки – інструмент, яким можна створювати наочні схеми, додавати написи й стрілки до зображень. Це невеликий графічний редактор усередині Google Docs.

Щоб створити новий об'єкт, відкрийте закладку «Вставка» і оберіть пункт «Рисунок» (рис. 4.49).

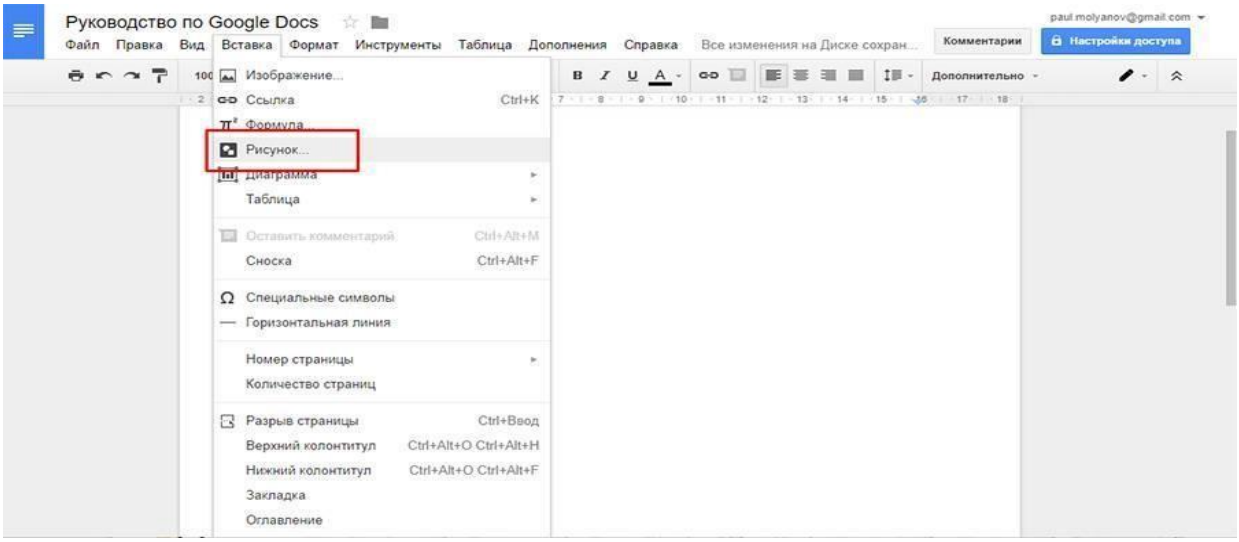


Рис. 4.49. Загальний вигляд вкладки «Вставка» пункт «Рисунок»

У вікні, що відкрилося, можна малювати фігури, писати текст і додавати зображення (рис. 4.50).

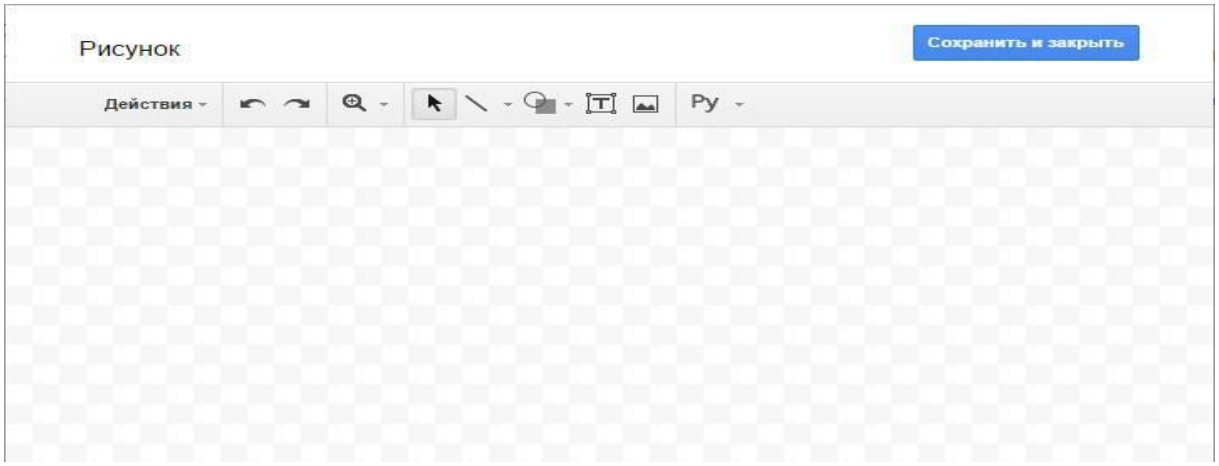


Рис. 4.50. Загальний вигляд вікно створення рисунка

Лінія. Дозволяє створювати прямі й криві лінії, стрілки й роздільники (рис. 4.51).

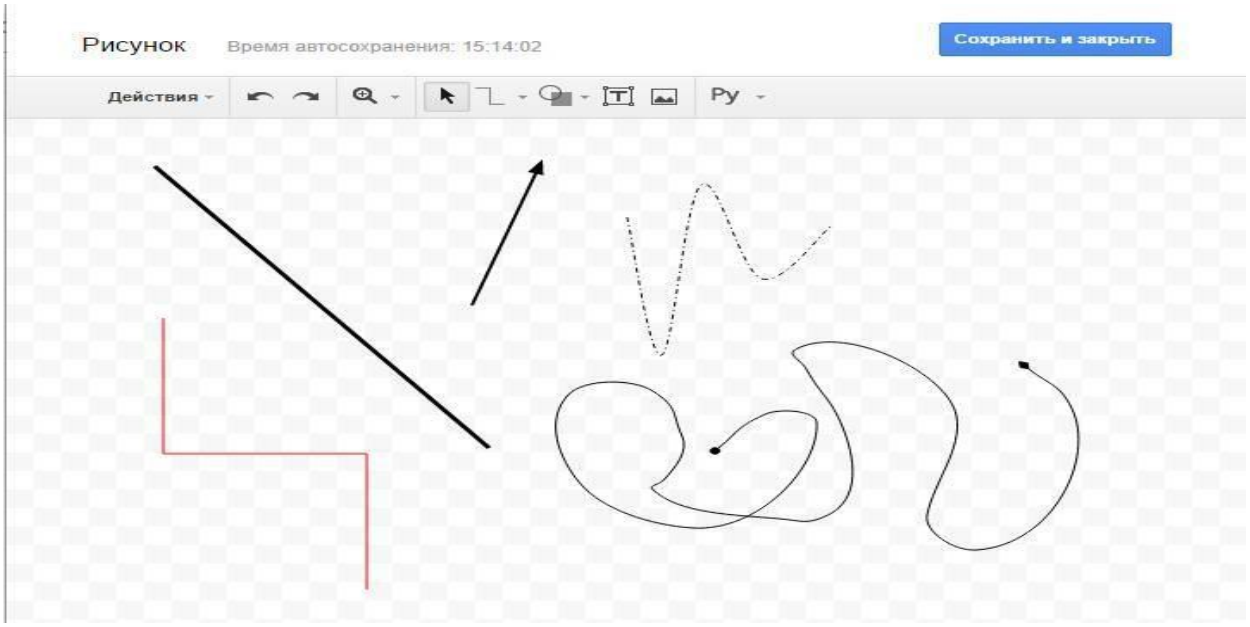


Рис. 4.51. Інструмент створення ліній

Якщо виділити вже нарисовану лінію, можна змінити її товщину, колір, стиль (суцільна, пунктир), додати мітки на кінцях (наприклад, стрілки) (рис. 4.52).

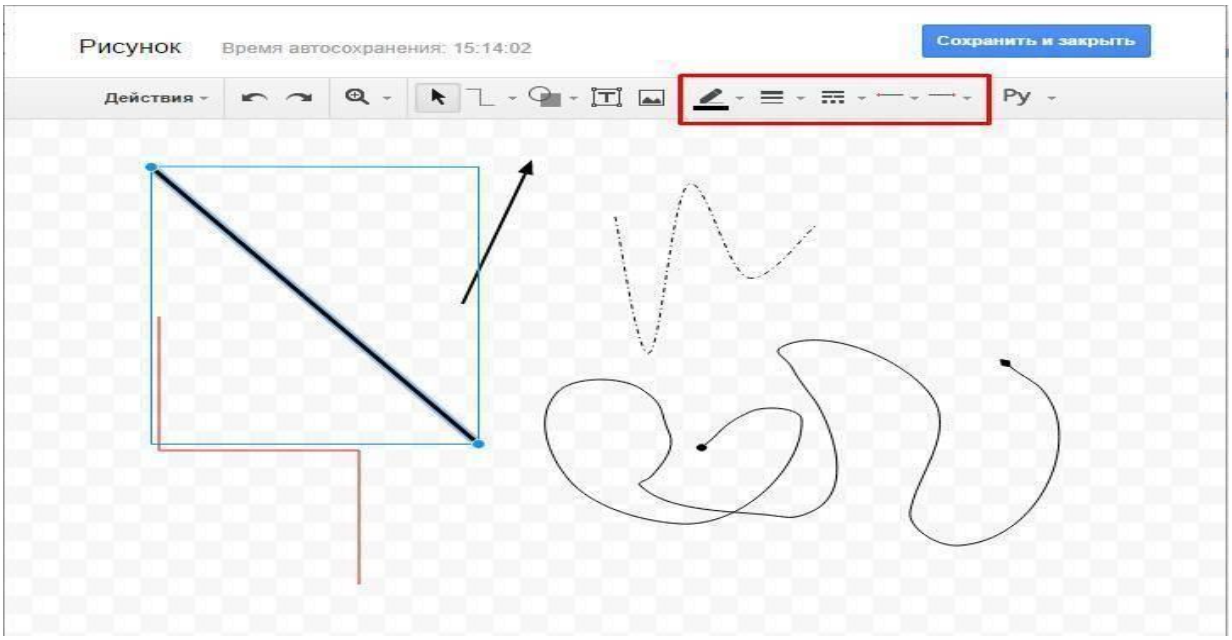


Рис. 4.52. Створені лінії можна редагувати

Фігура. Дозволяє створювати геометричні фігури, стрілки, винесення й математичнісимволи.

Усередині більшості фігур автоматично створюється текстове поле, у якому можна вводити текст написати (рис. 4.53).

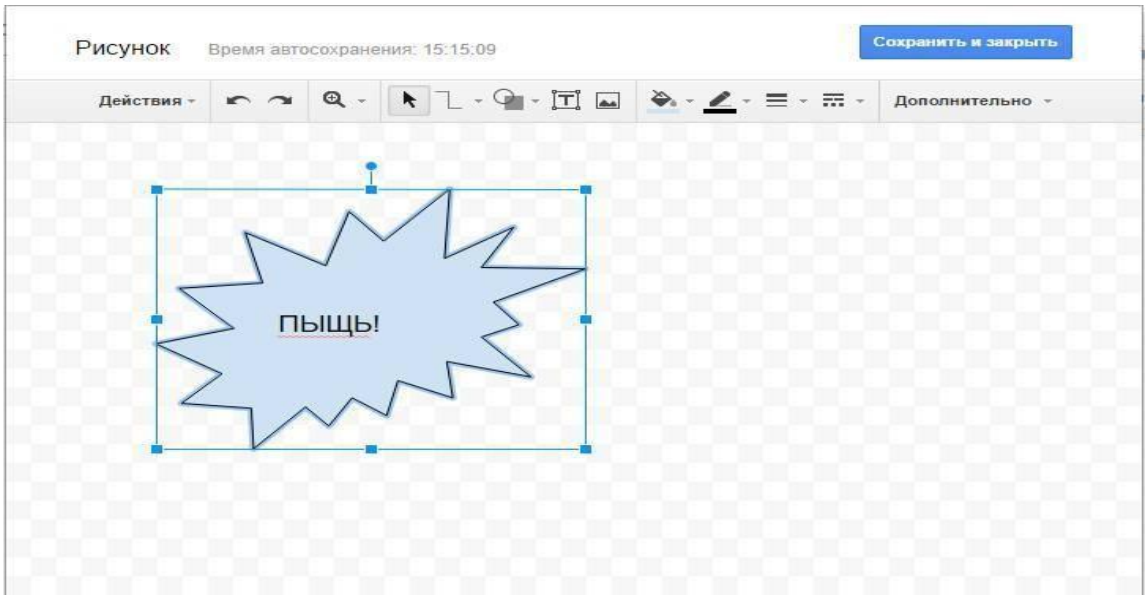


Рис. 4.53. Усередині більшості фігур
автоматично створюється текстове поле

Текстове поле. Дозволяє створювати область, у якій можна вводити текст. Параметри тексту задаються у вкладці «Додатково» (рис. 4.54).

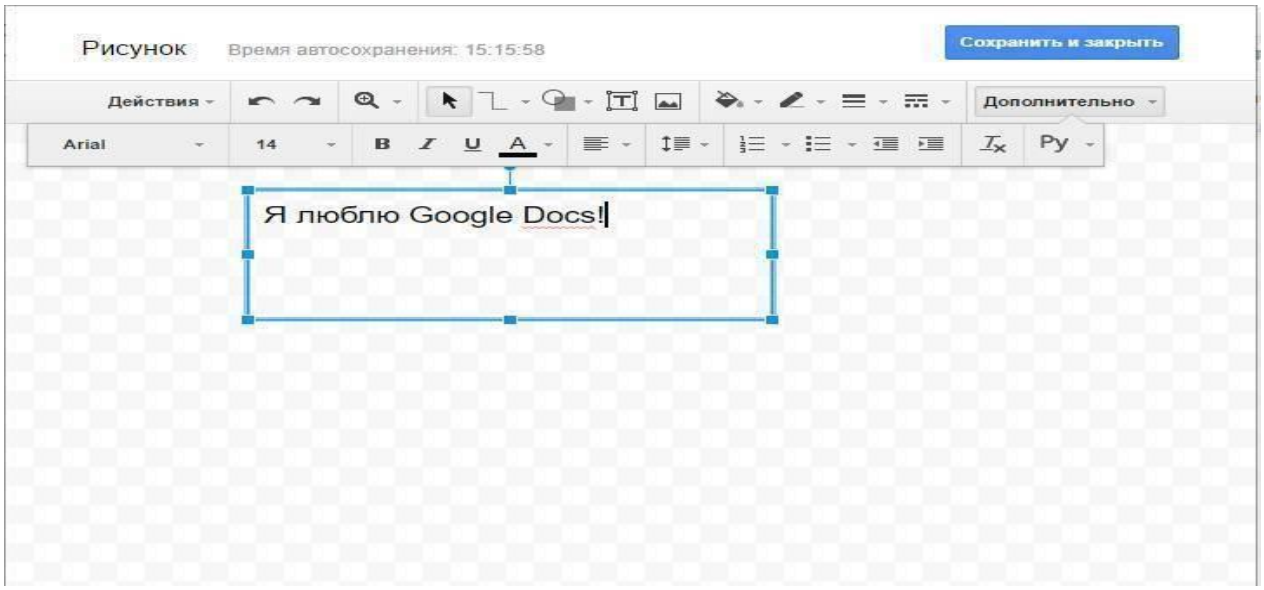


Рис. 4.54. Загальний вигляд текстового поля

Зображення. Дозволяє завантажувати у редактор картинку. Можна використовувати зображення, які знаходяться на комп'ютері, на Google Диску, зробити знімок з веб-камери, указати URL (посилання) або скористатися пошуком.

Дії. Вкладка з корисними інструментами: групування, вирівнювання, поворот, збереження (рис. 4.55).

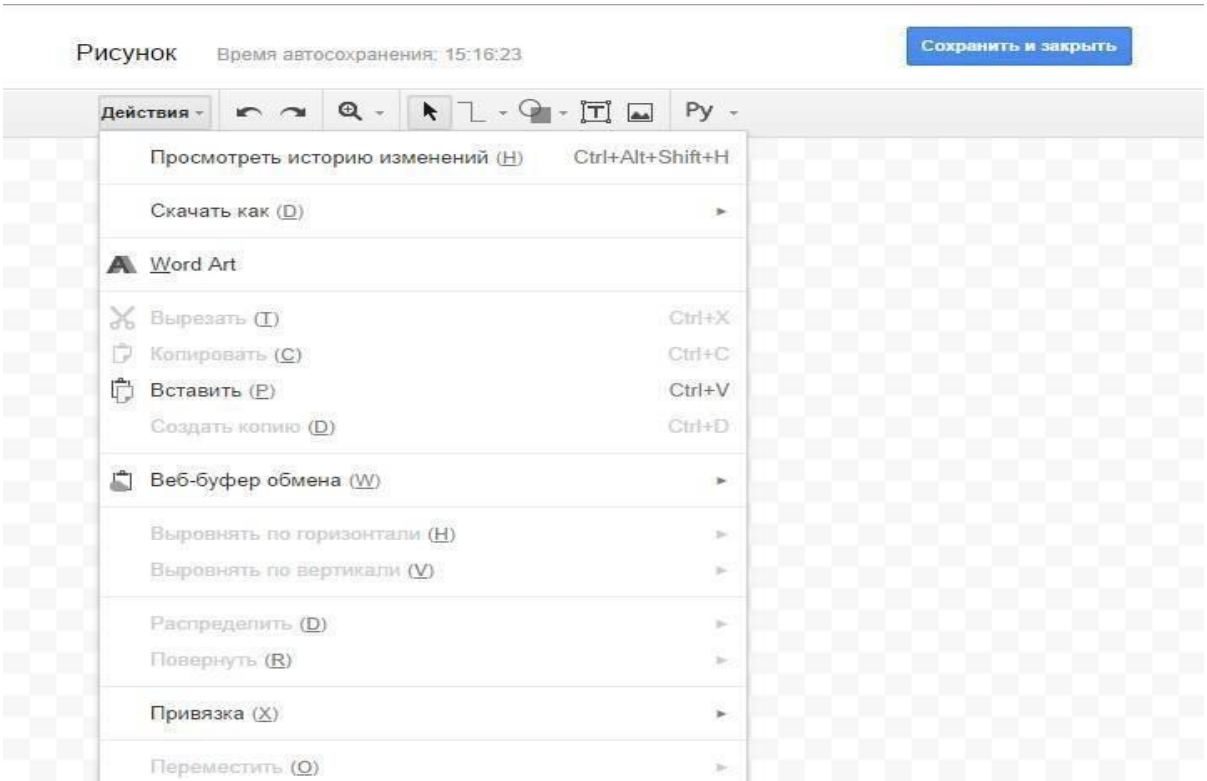


Рис. 4.55. Загальний вигляд вкладки «Дія»

У вкладці «Дія» є інструмент Word Art, який створює текст із заливанням і контурами. У Google Docs установлений шрифт Impact. Це значить що можна створювати меми в парі кліків. Завантажили картинку, додали Word Art текст, зберегли.

Якщо ви прагнете зберегти малюнок на локальному диску, відкрийте вкладку «Дія», натисніть «Скачати як» та виберіть потрібний формат (рис. 4.56).

Якщо рисунок потрібно відтворити у самому документі потрібно кликнути по кнопці «Зберегти та закрити», яка знаходить у верхньому правому куті (рис. 4.57).

Щоб відредагувати вже створений рисунок потрібно його виділити й натиснути «Змінити».

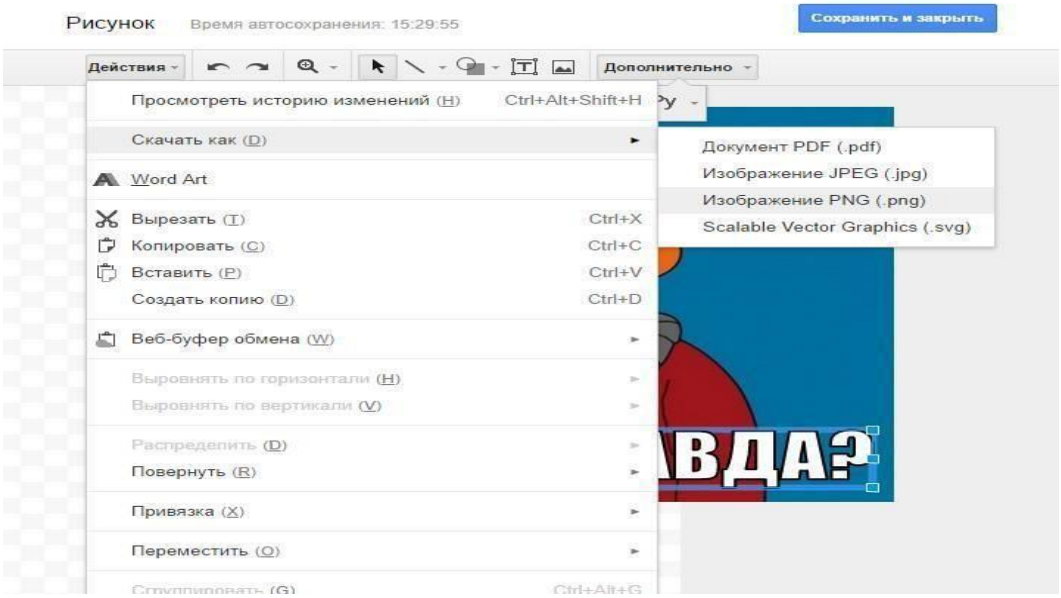


Рис. 4.56. Збереження рисунка

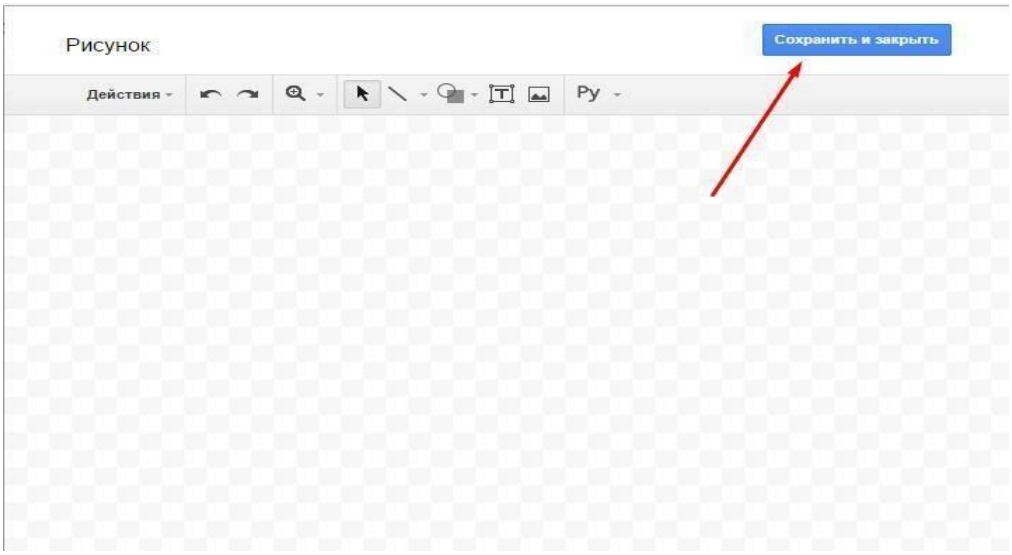


Рис. 4.57. Етап збереження рисунка в документі

4.6. Надання посилання на документ

Для цього потрібно:

Натиснути правою клавішею миші на створену папку та вибрати меню, яке випадає «Открыть доступ» (рис. 4.58).

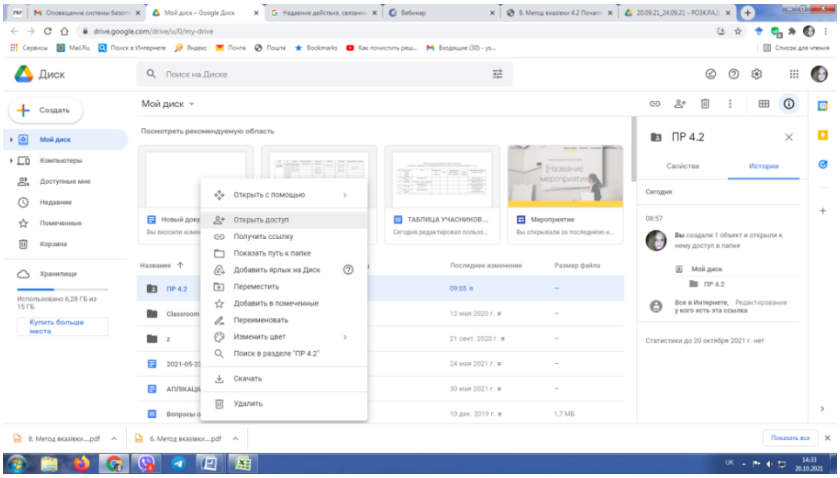


Рис. 4.58. Надання доступу «Меню»

На екрані з’явиться додаткове вікно. У цьому вікні потрібно вибрати яким чином буде надаватися допуск до папки, яку Ви створили: вибирати кнопку «Изменить» (рис. 4.59).

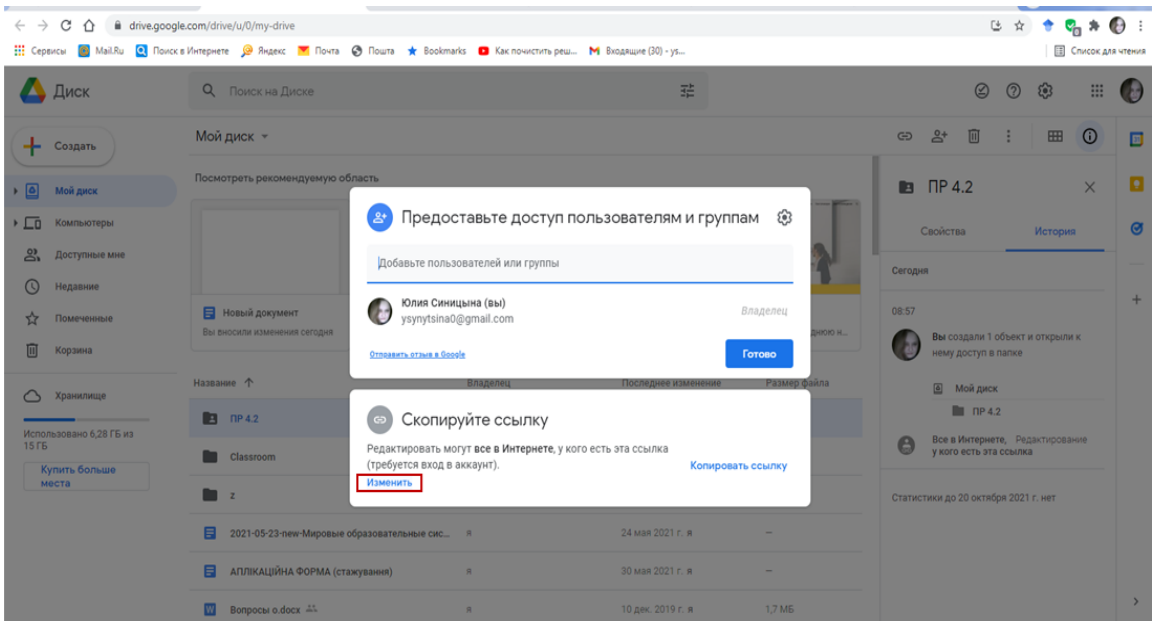


Рис. 4.59. Вибір способу надання доступу до папки (документа)

Вікривається вікно «Скопируйте ссылку», де потрібно вибрати доступ до вашої папки (документа). Із меню, що випадає, обираємо «Редактор» рис. 4.60.

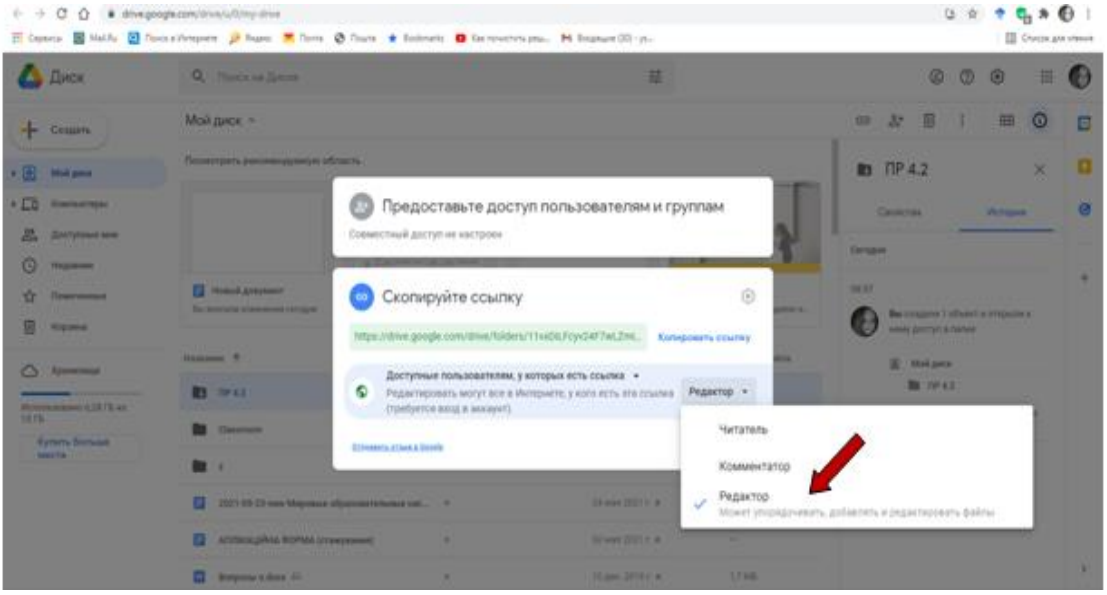


Рис. 4.60. Вибір управління доступом

Заключним етапом є копіювання посилання рис. 4.61.

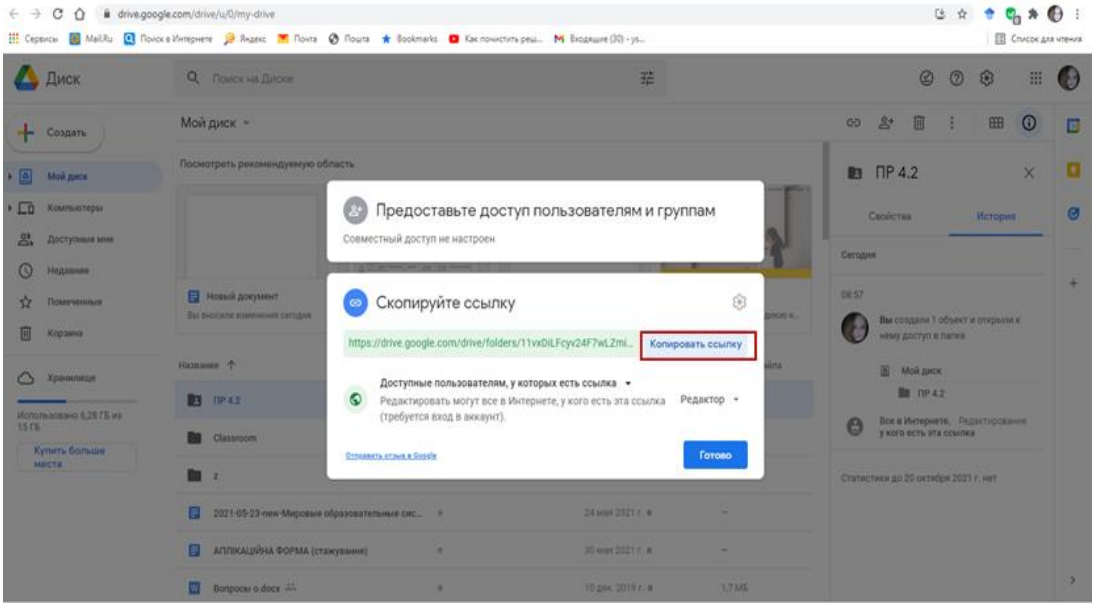


Рис. 4.61. Копіювання посилання на папку (документ)
у якому надано доступ викладачеві

Прикріплення посилання до МІА «Освіта», СУДН «Moodle».

Для цього потрібно зайти до папка ПР 4.2 Завантажити роботу. Зберегти зміни. Після виконаних дій з’явиться кнопка «Коментарі» (рис. 4.62).

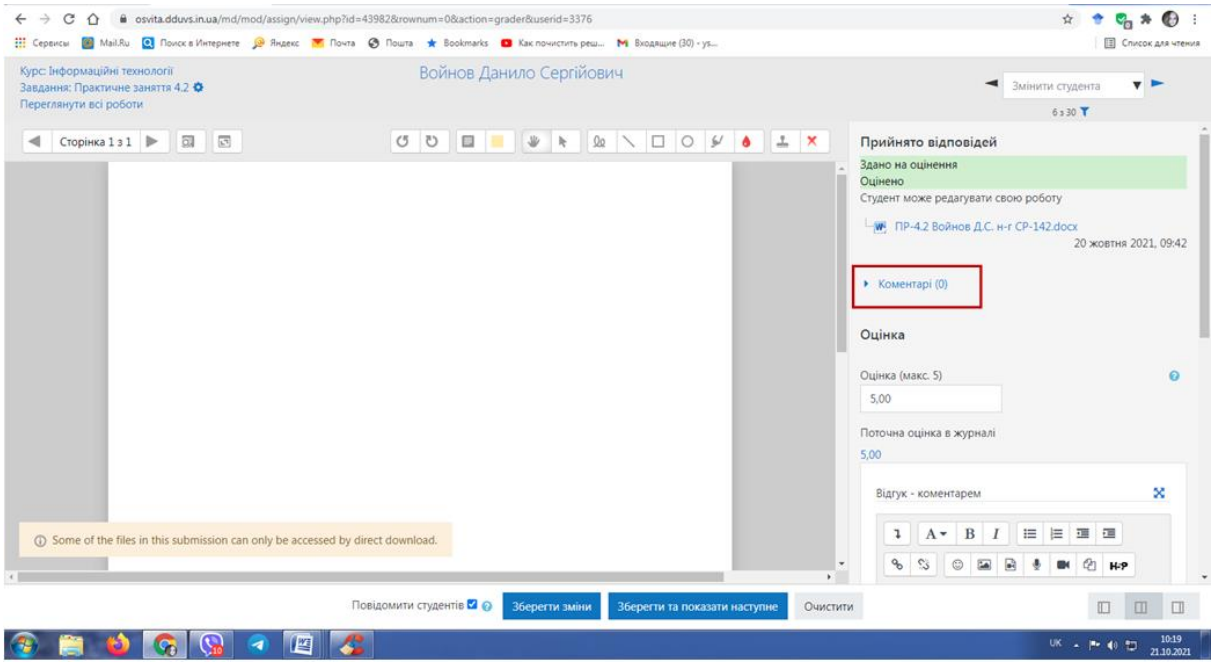


Рис. 4.62. Кнопка «Коментарі»

Потрібно натиснути на кнопку «Коментарі» для її активації. Після виконаних дій відкриється вікно, де можна вставити посилання на гугл папку (документ) (рис. 4.63).

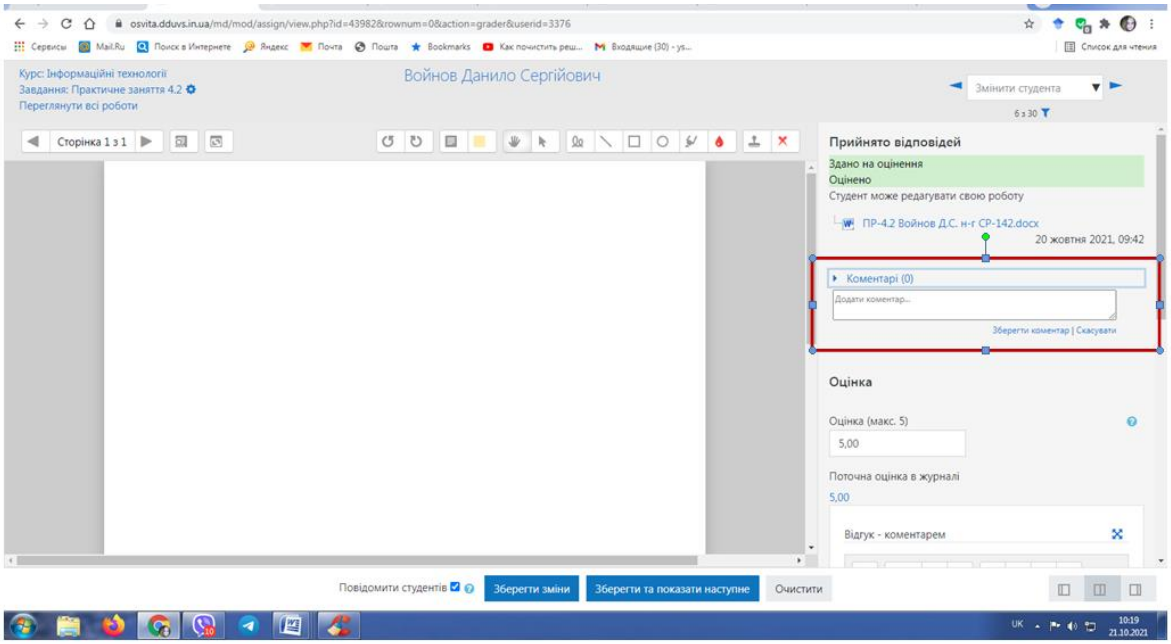


Рис. 4.63. Активація кнопки «Коментарі»

Та натиснути кнопку «зберегти коментар» (рис. 4.64).

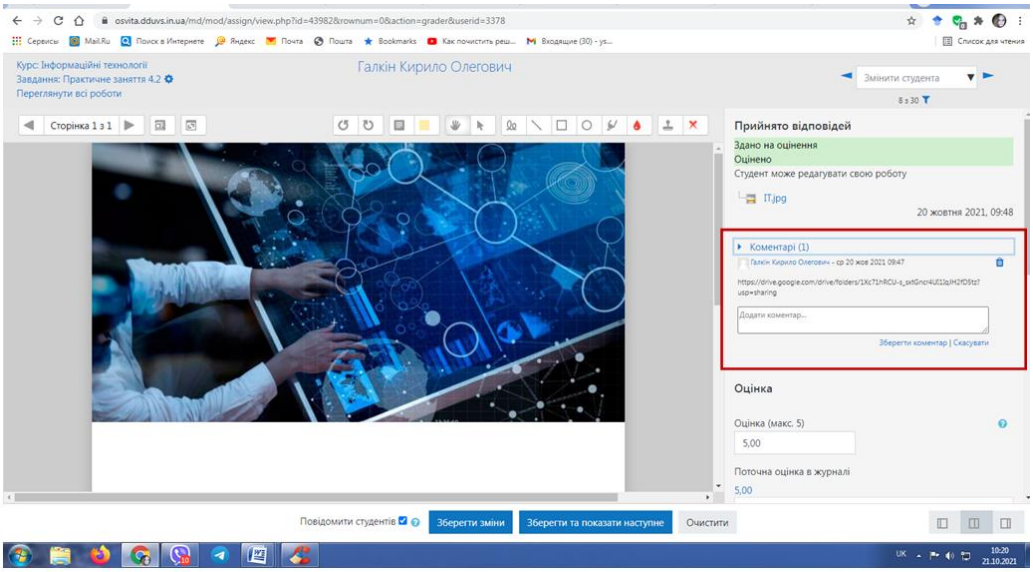


Рис. 4.64. Загальний вигляд вірного надання посилання на Google папку (документ)

Практичні завдання

Завдання № 1

1. Створити свій аккаунт у Google.
2. Створити нову папку на Google Диску з назвою «Інформаційні технології – П.І.Б.».
3. Створити у папці «Інформаційні технології – П.І.Б.» наступні файли:

a) Google Документ;
b) Google Таблиця;
c) Google Презентація;
d) Google форму

Скориставшись наведеними шаблонами.

4. Зробити скриншот зображення на вашому екрані та завантажити до МІА «Освіта»

Завдання № 2

1. Створіть на Google Диску папку «ПР … – ПІБ – ваше прізвище» і збережіть документи у цій папці.
2. Відкрийте *Google Документи*. У вікні нового документа наберіть текст:

Правила створення та використання надійних паролів

При створенні облікового запису в соціальних мережах, реєстрації в інтернет-магазинах або додатках у смартфонах, необхідно вказувати пароль – так працює будь-яка система авторизації. Конфіденційність приватних даних захищена ненадійно, якщо пароль є нестійким до зламу. Безліч людей нехтують власною безпекою та встановлюють прості паролі, які хакери без зусиль можуть зламати менше ніж за секунду. Для прикладу, у рейтинг найуживаніших паролів, який щорічно складає компанія Nord Security, постійно потрапляють такі комбінації як 123456, qwerty, password, фрази на кшталт iloveyou або власні імена (перевірити, чи немає у переліку вашого пароля, можна тут: https://nordpass.com/most-common-passwords-list/).

Надійний пароль – один з основних способів захисту для будь-якого облікового запису. Тому найважливіше правило, якого слід дотримуватися: що він складніший, то краще.

Під надійними паролями слід розуміти такі, що:

– складаються з не менш як 8 символів;

– включають літери (у верхньому і нижньому регістрі), цифри та спеціальні символи;

– не містять персональної інформації (наприклад: дати народження своєї та своїх близьких, номерів телефонів, номерів та серій документів, що посвідчують особу, номерів власного автотранспорту, банківської картки, адреси реєстрації), а також фраз зі щоденного вжитку (назв книг, відомих цитат, текстів пісень);

– не використовуються в будь-яких інших облікових записах та потребують негайної зміни у разі підозри щодо їх компрометації.

Для захисту облікових записів ефективно використовувати парольні фрази. (набір слів, зашифрованих користувачем). Наприклад, оберіть будь-яку фразу – рядок із вірша, пісні, книжки тощо. Видаліть пробіли та замініть деякі літери цифрами, спецсимволами, переведіть певні букви у верхній регістр.

Для створення складних паролів також можна використовувати сервіси генерації паролів.

Завдання № 3

1. Наберіть наведений текст перших трьох статей «Закону України про інформацію» (прийнятий в 1992 р.) як один абзац і потім розбийте його на чотири абзаци, які починаються статтями. Виділіть назву кожної статті. Для всіх абзаців встановіть відступ ліворуч в 3 одиниці. Проведіть форматування тексту вирівнювання «по ширине», шрифт Times New Roman 14, міжрядковий інтервал 1,5.

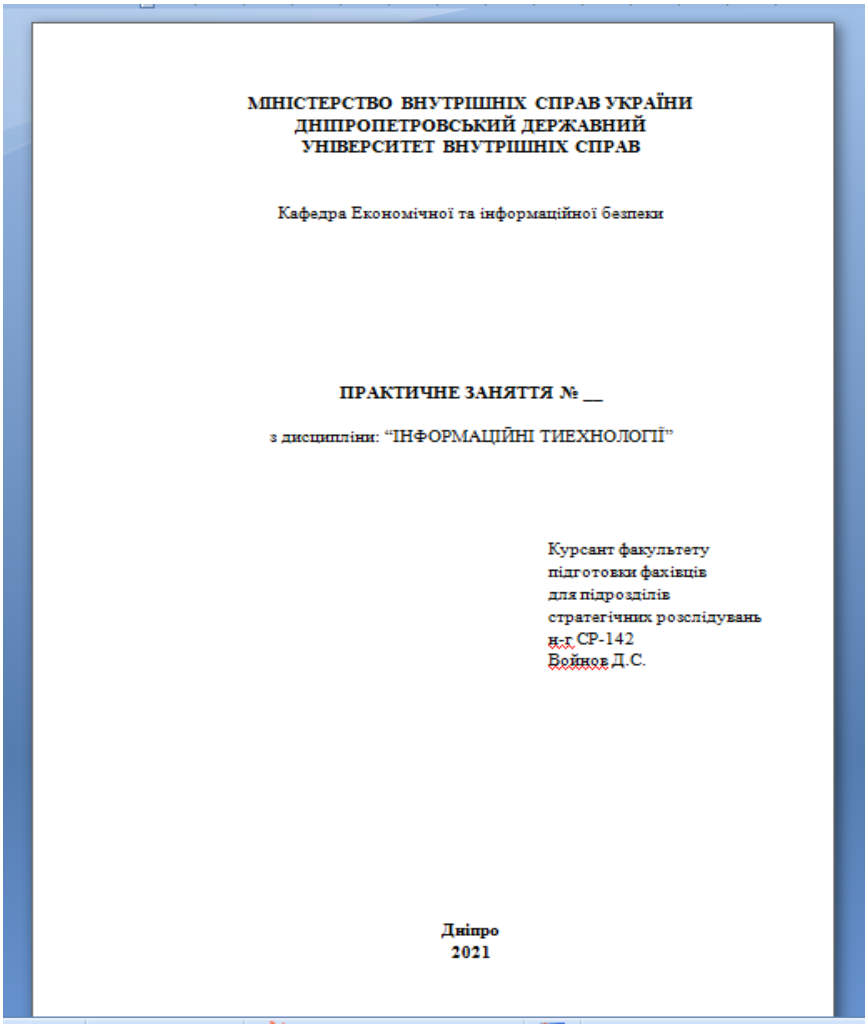
2. Виконати копіювання й потім вставку 1-го абзацу документу:
– у кінець вихідного тексту;
– у новий документ;
3. Виконати вирізку 2-го абзацу вихідного тексту і його вставку:
– у кінець вихідного тексту;
– у новий документ;

Завдання № 4

1. У папці створіть наступний документ рис. 4.16.
2. Установіть параметри сторінки: поля сторінки, рівні відповідно: праві поле – 1 см, ліве –3 см, верхнє й нижнє поле – по 2,0 см; Відстані від краю доколонтитула – по 1 див.

Текст до завдання № 3.

Стаття 2. *Об'єкти захисту в системі Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.* ***Стаття 3.*** *Суб'єкти відносин Суб'єктами відносин, пов'язаних із захистом інформації в системах, є: володільці інформації; власники системи; користувачі; спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи. На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі – розпоряднику системи.* ***Стаття 4.*** *Доступ до інформації в системі. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації. Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством. У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.* ***Стаття 5.*** *Відносини між володільцем інформації та власником системи Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом. Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.*


МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ
УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра Економічної та інформаційної безпеки

ПРАКТИЧНЕ ЗАНЯТТЯ № __

з дисципліни: "ІНФОРМАЦІЙНІ ТИЕХНОЛОГІЇ"

Курсант факультету
підготовки фахівців
для підрозділів
стратегічних розслідувань
н-г СР-142
Войнов Д.С.

Дніпро
2021

Рис. 4.16. Зразок для виконання

Завдання № 5

1. Скопіюйте текст наведений нижче на окрему сторінку вже створенного Google документу.
2. Створіть структуру документу застосував відповідні стилі тексту.
3. Створіть «ЗМІСТ з номерами сторінок» для відтвореного Вами тексту, використав вкладку «Оглавление».
4. Створіть «ЗМІСТ за посиланням» для відтвореного Вами тексту, використав вкладку «Оглавление».
5. Збережіть документ у форматі *.docx.
6. Надайте доступ на перегляд і редагування викладачеві
7. Збережіть посилання на гугл документ у вкладці «коментарі».

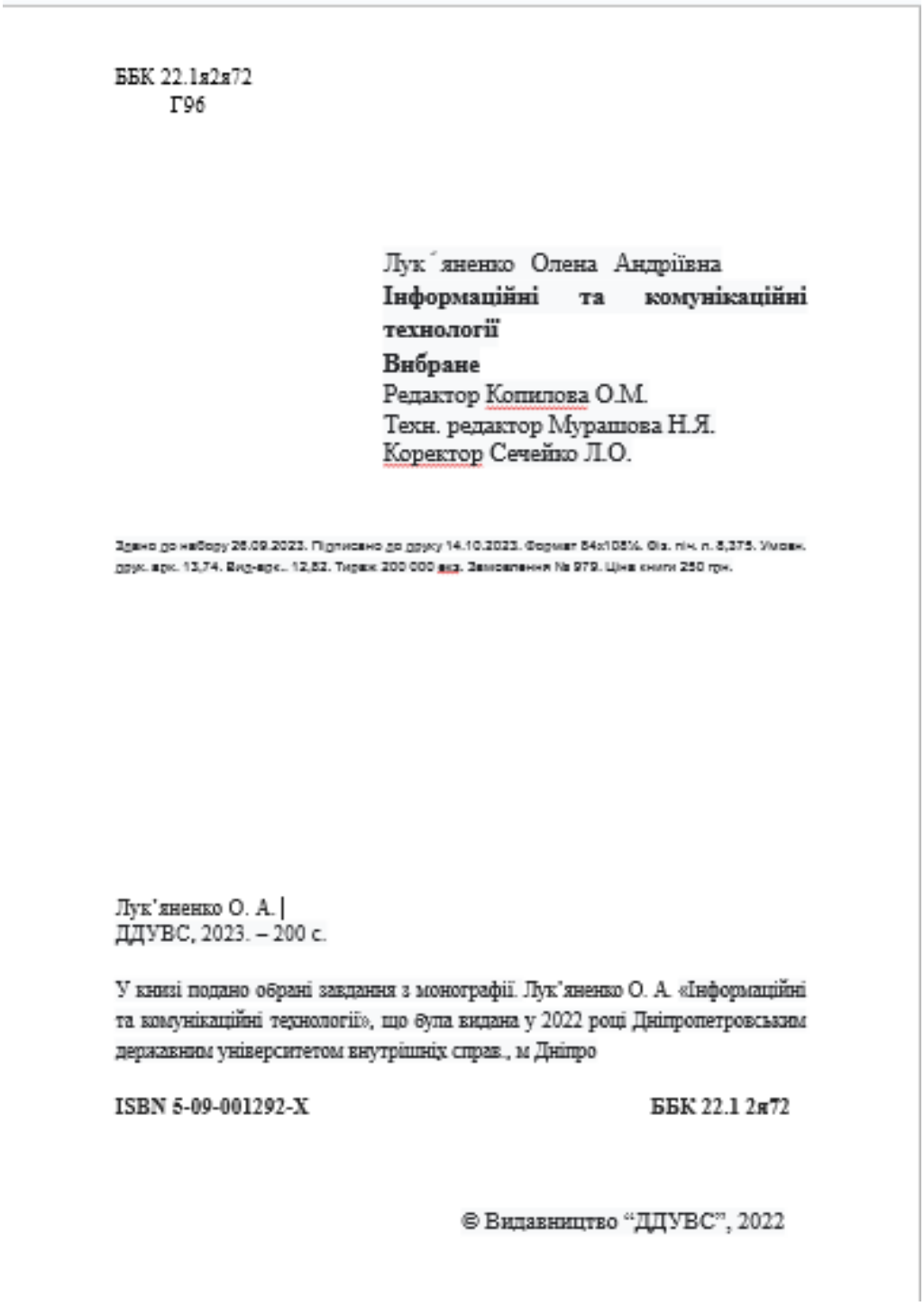
ЗМІСТ

Завдання № 6

1. Створіть на Google Диску новий Google Документ «ПР .. – ПІБ – ваше прізвище».
2. Установіть параметри сторінки відповідно: праве поле – 2 см, ліве –3 см, верхнє й нижнє поле – по 2,5 см.
3. У вікні нового документа Наберіть наступний текст українською мовою, розтягнувши його на сторінку.
4. Виконайте всі формати абзаців і символів: вирівнювання; ліві і праві відступи; відстані між абзацами; тип, розмір та стилі шрифтів; інтервали між символами.
5. Створити верхній та нижній колонтитули з таким текстом:

Верхній: ББК 22.1я2я72
Г96.

6. Нижній: © Видавництво «ДДУВС», 2023.
7. Замініть у завданні рядок «Лукяненко Олена Андріївна» на свої П.І.Б.



ББК 22.1я2я72
Г96

Лук´яненко Олена Андріївна
Інформаційні та комунікаційні технології
Вибране
Редактор Копилова О.М.
Техн. редактор Мурашова Н.Я.
Коректор Сечейко Л.О.

Здано до набору 26.09.2023. Підписано до друку 14.10.2023. Формат 84x108¼. Фіз. піч. л. 8,375. Умовн. друк. арк. 13,74. Вид-вих.. 12,82. Тираж 200 000 вид. Замовлення № 979. Ціна книги 250 грн.

Лук'яненко О. А. |
ДДУВС, 2023. – 200 с.

У книзі подано обрані завдання з монографії. Лук'яненко О. А. «Інформаційні та комунікаційні технології», що була видана у 2022 році Дніпропетровським державним університетом внутрішніх справ., м Дніпро

ISBN 5-09-001292-X ББК 22.1 2я72

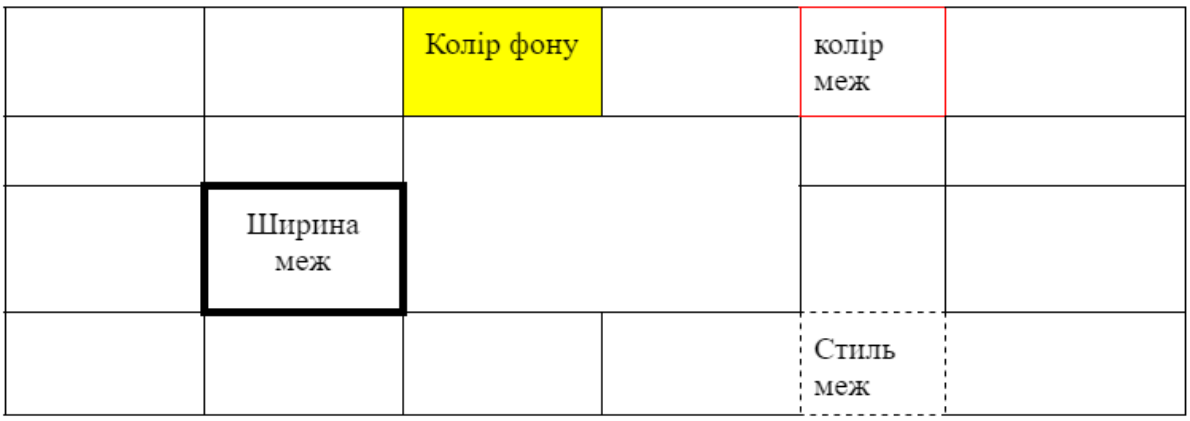
Завдання № 7

1. За допомогою сервісу Google Doc створити новий документ з назвою «ПР … – ПІБ».

2. Загальне: створити структуру документу таким чином, щоб кожне наступне завдання починалося з нового листа, використавши вкладу «Вставка» «Розрив сторінки».

3. Створити таблицю та виконати необхідні дії (теоретична частина «Робота з таблицями» за наведеним зразком.

Зразок



Завдання № 8

1. Створити таблицю, заповнити її текстом, як вказано за прикладом. За допомогою пошукової системи знайти картинки, що відповідають на загадки. Знайдені рисунки вставити у комірки таблиці напроти загадок.

Загадки	
Через воду він проводить, А сам з місця вік не сходить.	
	По полю ходить, жне, косить, Зерно молотить, хліба не просить.
І червона, й соковита, Та гірка вона все літо. Припече мороз – вона Стала добра й смачна.	
	На городі нога стоїть, На нозі голова висить. Куди сонце повертається, Туди голова нахиляється.
Спритний майстер у стрибках: На деревах, по гілках. Вся руда, пухнастий хвіст, Рідний дім для неї – ліс.	
	Не ставок і не ріка, Мох росте і осока. Там земля – неначе тісто, Що воно за дивне місце?

У нашої бабусі Сидить дід в кожусі, Проти печі гріється, Без води умиється.	
	Найрідніша, наймиліша, Всіх вона нас пестить, тішить, Завжди скрізь буває з нами. Відгадайте, хто це?..
Олена зелена, Не сіяна, не саджена, Хто доторкнеться, Той обпечеться.	
	Сонечко в траві зійшло, Усміхнулось, розцвіло, Згодом стало біле-біле І за вітром полетіло.
Неначе паровоз, гуде, Шумить, кипить, і пара йде, Смачний заварює нам чай. Хто ж він такий? От відгадай.	

Приклад виконання

Завдання 2

Загадки	
Через воду він проводить, А сам з місця вік не сходить.	
	По полю ходить, жне, косить, Зерно молотить, хліба не просить.
І червона, й соковита, Та гірка вона все літо. Припече мороз – вона Стала добра й смачна.	

Завдання № 9

1. Скопіювати довільно текст.
2. Знайти в Інтернеті зображення «комп’ютер», вставити декілька зображень, відповідно розташував їх різними варіантами обтікання тестом: всередині тексту, поверх тексту, за текстом, у тексті.
3. Знайти в інтернеті зображення «комп’ютер» та відтворити наступні дії над зображенням:

– змінити розмір малюнка, призначивши масштаб, рівний 40% від його вихідноївеличини;
– змінити яскравість зображення;
– змінити контрастність зображення;
– встановити заливання жовтим кольором.

Приклад виконання

Таблиці використовуються для представле ної числової і
текстової інформації, схильної до упорядкуван ома критеріями.
Google Docs має великий набір інструментів для ння таблиць,
що дозволяє будувати дуже складні таблиці з будь-яким оформленням.
У вкладці «Вставка» виберіть пункт «Таблиця». На сітці, що з'явився, можна задати кількість стовпців і рядків Скопіювати довільно текст.

Знайти в інтернеті зображення «комп'ютер», вставити декілька зображень, відповідно розташував їх різними варіантами обтікання тестом:
всередині тексту, поверх тексту, за текстом, у тексті.

Знай ти в інтернеті зображення «комп'ютер» та відтворити наступні дії
над зображенням:
змінити розмір малюнка, призначивши масштаб, рівний 40% від його
вихідної величини;
змінити яскравість зображення;
змінити контрастність зображення;
встановити заливання жовтим кольором

Завдання № 10

1. За допомогою сервісу Google Doc створити новий документ із назвою «ПР 4.5 – ПІБ».
2. Загальне: створити структуру документу таким чином, щоб кожне наступне завдання починалося з нового листа, використавши вкладу «Вставка» «Розрив сторінки».
3. Відтворити документ об’єктом такого змісту:

Вказівки до виконання:

Щоб оформити документ представленим чином, потрібно:

– вставити в документ 3 об’єкти, а саме:

✓ автофігуру Вертикальний сувій,

✓ картинку з файлу-малюнок або фото,

✓ текст «Вітаю», оформлений за допомогою WordArt;

– Згрупувати вставлені три об’єкти в єдиний один об’єкт;

– Повернути об’єкт.

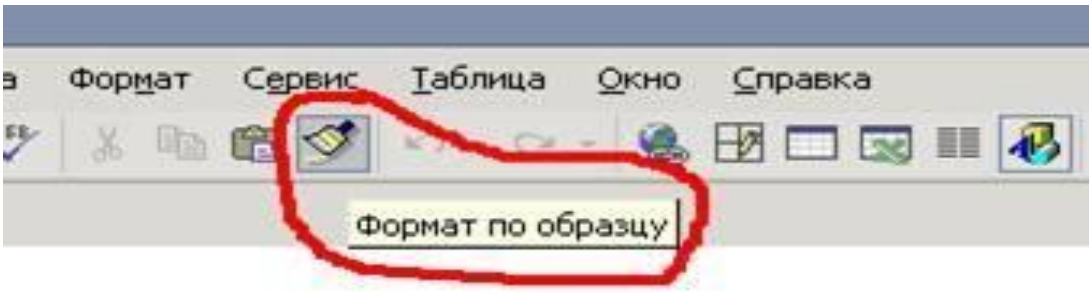
Для того щоб вставити в документі автофігуру, можна використовувати панель інструментів Вставка/Фігури/Вертикальний свиток.

Далі вставити надпис за допомогою WordArt.

Щоб згрупувати три вставлених об’єкта, необхідно спочатку виділити їх. Щоб виділити кілька об’єктів одночасно, необхідно клацнути лівою клавішею миші по ним по черзі, утримуючи клавіші Shift. Щоб виділені об’єкти згрупувати, вибираємо команду контекстного меню Угруповання/Групувати:

Завдання № 11

1. На новій сторінці створіть об’єкт, що містить наступний фрагмент екрану:



Вказівки до виконання:

Щоб помістити фрагмент екрану в документ як вставленого об’єкта необхідно:

Натиснути на клавіатурі клавішу PrnSc, тим самим стан екрану буде скопійовано в буфер обміну;

Відкрити будь-який графічний редактор, наприклад Paint, і вставити вміст буфера в новий документ графічного редактора за допомогою,наприклад, команди меню вікна Paint Правка-Вставити;

Провести обробку документа, тобто за допомогою інструменту Олівець або Пензлик обвести необхідний фрагмент червоним кольором, а потім виділити оброблений фрагмент і скопіювати його в буфер обміну

Завдання № 12

1. На новому листі оформіть «Запрошення» наступним чином:

Вказівки до виконання:

Щоб оформити документ представленим чином необхідно:

– сформувати самостійно текст запрошення;
– вставити в запрошення картинку,
– відкоригувати розмір картинки,
– розмістити картинку на сторінці певним чином по відношенню дотексту.
– для реквізитів обов’язково використати бібліотеку спеціальних символів:

–

Контрольні питання

1. Надайте визначення поняття «Хмарні обчислення».
2. Надайте пояснення моделі, відомої як послуга SaaS.
3. Назвіть та охарактеризуйте відомі Вам сервіси Google.
4. Проаналізуйте переваги та недоліки використання.
5. Як настроїти розміри полів сторінки?
6. Як змінити орієнтацію сторінки?
7. Як настроїти міжрядковий інтервал?
8. Що таке абзацний відступ і як його змінити?
9. У яких одиницях виміряється висота шрифту і як її змінювати?
10. Як вставити номера сторінок документа, починаючи з другої сторінки?
11. Які існують варіанти розташування номерів сторінок?
12. Як об’єднати два існуючих тексти в одному документі?
13. Як два розташованих один за одним абзаци одного документа об’єднати в один абзац?
14. У чому полягає режим «розмітка сторінки»?
15. Навіщо потрібний режим «попередній перегляд»?
16. Як настроїти розміри полів сторінки?
17. Як змінити орієнтацію сторінки?
18. Як настроїти міжрядковий інтервал?
19. Що таке абзацний відступ і як його змінити?
20. У яких одиницях виміряється висота шрифту і як її змінювати?
21. Як вставити номера сторінок документа, починаючи з другої сторінки?
22. Які існують варіанти розташування номерів сторінок?
23. Як об’єднати два існуючих тексти в одному документі?
24. Як два розташованих один за одним абзаци одного документа об’єднати в один абзац?
25. У чому полягає режим «розмітка сторінки»?
26. Який алгоритм створення «Змісту» Google докоменту»? Які види змісту бувають?
27. Що таке «Закладка» у Google документі? Як її налаштувати?
28. Яким чиному формується структура Google документу?
29. Як алгоритм створення колонтитулів у Google документу?
30. Де знаходяться спеціальні символи в Google документі?
31. Де зберігаються документи при роботі з сервісом Google Docs?

32. Які режими доступу до документу можливі в сервісі Google Docs?

33. Відтворіть алгоритм дій зі створення таблиці.

34. Яким чином можливо змінити види границь комірки?

35. Яким чином здійснюється заливка кольором комірки?

36. Видворіть алгоритм дій зі вставки зображення у Google Документі.

Джерела до розділу 4

1. Інформаційні системи та технології: підручник / кол. авт.; ред. В. Б. Вишня. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2021. 296 с.

2. Гриценко В. Використання сервісу Google Disk для управління освітніми процесами. В. Гриценко. Науково-практична інтернет-конференція (XII Хмурівські читання) з проблеми «Технологія фахової майстерності: сучасний інструментарій вчителя. URL : http://www.kspu.kr.ua/ua/ntmd.

3. Офісні технології: навч. посібник. /О. Г. Трофименко, Ю. В. Прокоп, Н. І. Логінова, Р. І. Чанишев. Одеса: Фенікс, 2019. 207 с.

4. Литвинова С. Г. Хмарні технології як засіб розбудови інноваційної школи. URL : https://virtkafedra.ucoz.ua/ el_gurnal/pages/vyp14/Litvinova.pdf.

5. Спеціальна техніка в правоохоронній діяльності : навч. посібник / Ю. П. Синиціна, С. О. Прокопов, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 244 с.; іл. ISBN 978-617-8032-47-0.

6. Методичний навігатор Електронний ресурс: URL : https://sites.google.com/a/lyceum2.cv.ua/metodicnij-navigator/google-servisi.

Розділ 5
СТВОРЕННЯ ЮРИДИЧНИХ БАЗ ДАНИХ НА ОСНОВІ ОНЛАЙН СЕРВІСУ GOOGLE SHITS

5.1. Використання географічної діаграми онлайн сервісу Google Таблиці в правоохоронній діяльності

Сьогодні все більше число спеціалістів у різних областях використовує у процесі своєї професійної діяльності Google таблиці (Google Sheets), і цьому є логічне пояснення, адже, на відміну від звичного MS Excel, цей інструмент має цілий ряд переваг, які на практиці можуть грати ключову роль. До них можна віднести наступні: безкоштовність; можливість сумісної роботи одночасно з одним й тим самим файлом; автоматичне збереження; збереження історії версій; можливість встановлення автоматичного імпорту даних зі сторонніх джерел тощо.

Як і в Google документах, почати роботу з Google таблицями можна, просто маючи свій Google акаунт та посилання на https://docs.google.com. Тут за допомогою головного меню (рис. 5.1) слід обрати безпосередньо роботу з таблицями (рис. 5.2).

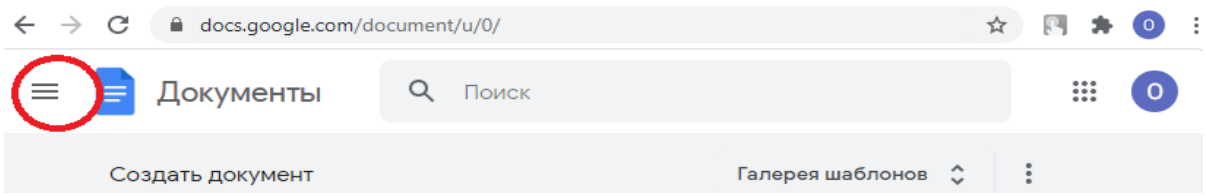


Рис. 5.1. Головне меню

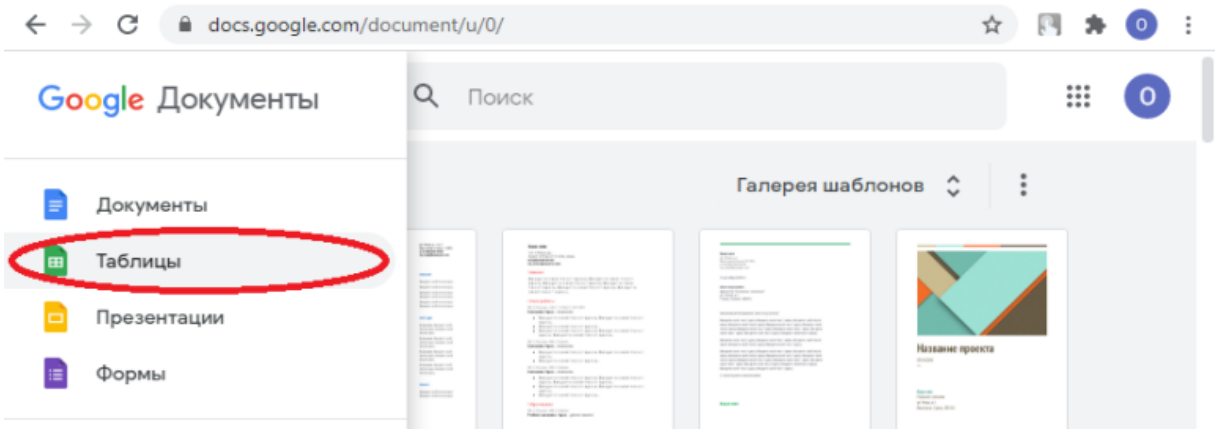


Рис. 5.2. Вибір роботи з таблицями

Вибір вкладинки «Пустой файл» дозволяє перейти безпосередньо до роботи з новою Google таблицею, яка за своїм дизайном багато в чому нагадує програмне середовище MS Excel (рис. 5.3).

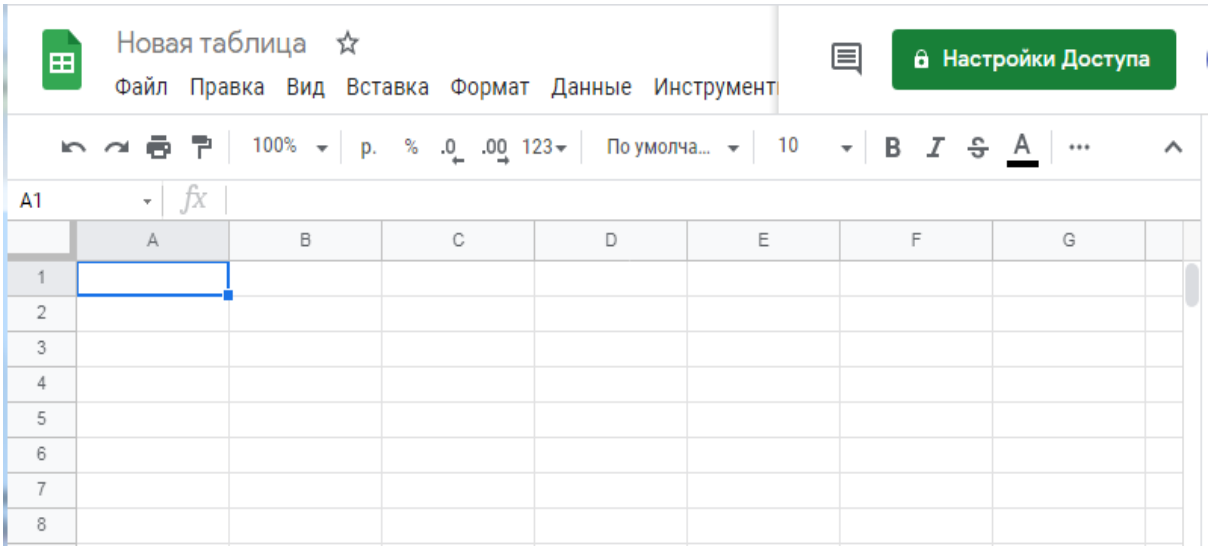


Рис. 5.3. Пуста сторінка Google Sheets

Ще один варіант створення Google таблиць – використання Google диску. Для цього необхідно активізувати кнопку «Створити» та обрати розділ «Google таблиці» (рис. 5.4.)

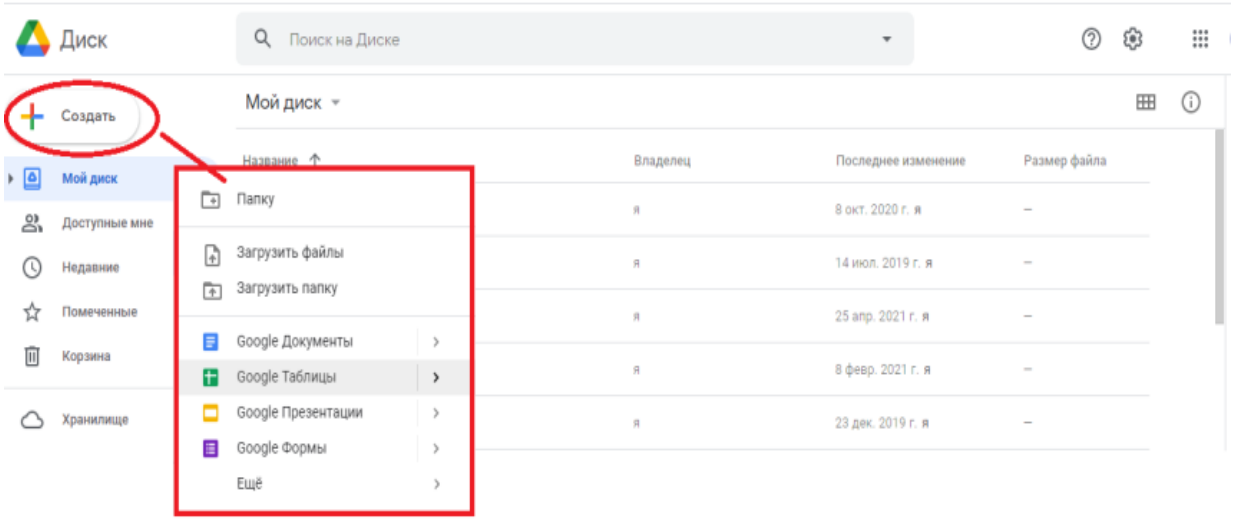


Рис. 5.4. Створення Google таблиці

Оскільки Google таблиці автоматично зберігають всю інформацію, в меню «Файл» немає кнопки «Зберегти», але є можливість закачати Google таблиці одразу у декількох найбільш розповсюджених розширеннях (рис. 5.5) – «*.xlsx», «*.ods», «*.pdf» тощо.

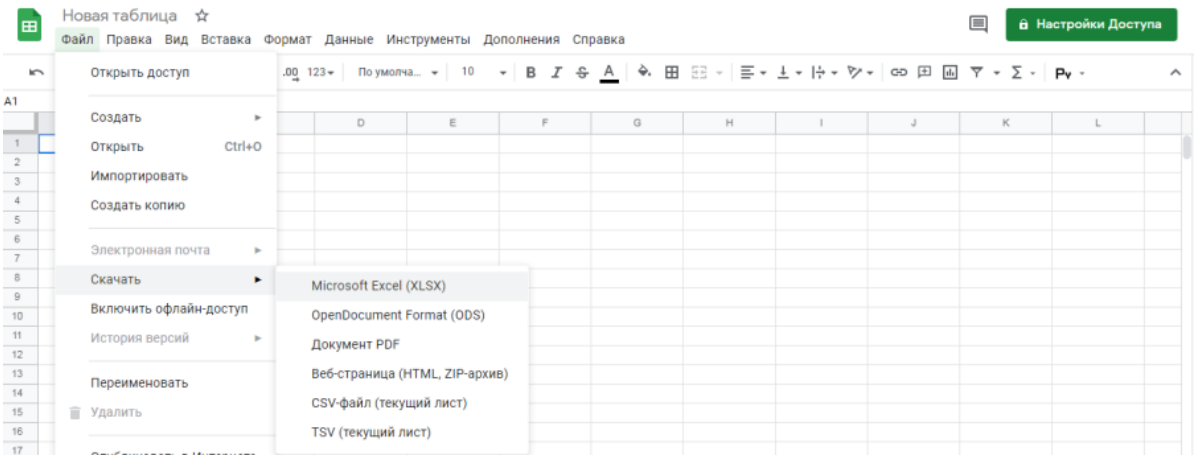


Рис. 5.5. Формати збереження Google таблиці

За замовчуванням Google таблиці зберігаються на Google диску з ім’ям «Нова таблиця». Для зміни назви можна скористатися або відповідним рядком зверху безпосередньо у самій таблиці (рис. 5.6), або контекстним меню на початковій сторінці Google таблиць (https://docs.google.com/spreadsheets).

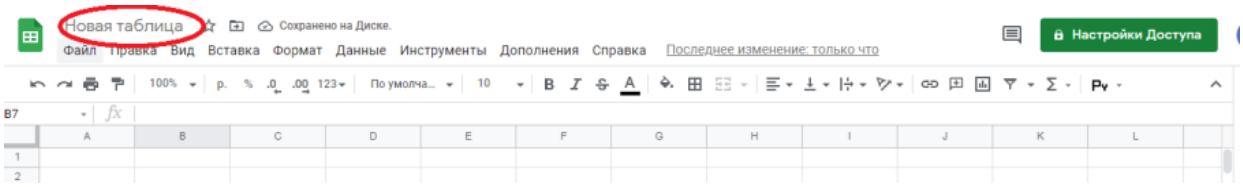


Рис. 5.6. Перейменування Google таблиці

Як зазначалося вище, однією з важливих особливостей роботи з документами за допомогою Google таблиць є можливість одночасного користування одним й тим самим файлом. Для використання такої можливості необхідно надати доступ до документу відповідній людині. Це можна зробити завдяки кнопці «Настойка доступа», яка виділена зеленим кольором на відповідному рядку на головному екрані, або ж у меню «Файл» вибрати кнопку «Відкрити доступ» (рис. 5.7).

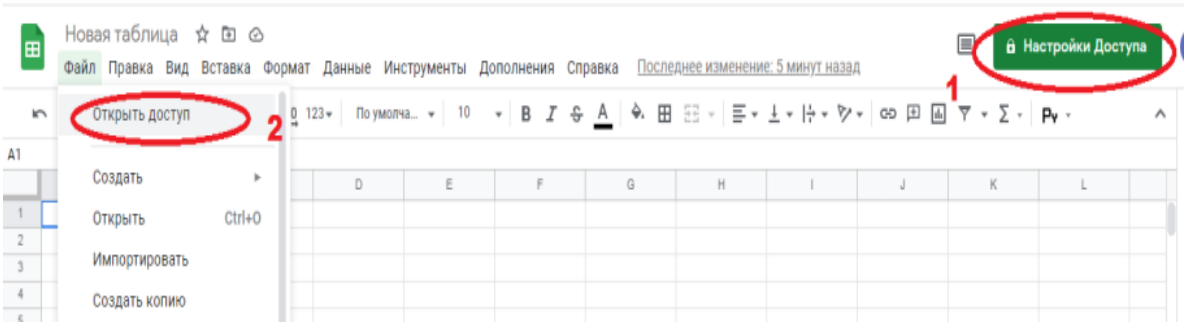


Рис. 5.7. Доступ до Google таблиці

Створення таблиці в Google Sheets

Зовнішній вигляд Google таблиць дуже схожий на таблиці MS Excel (рис. 5.8). Тут є панель для вводу імені таблиці (рис. 5.8, 1), рядок меню для основних дій (рис. 5.8, 2), панель з основними елементами керування типу «Відмінити дію» чи «Роздрукувати» (рис. 5.8, 3). Присутня можливість зміни масштабу (рис. 5.8, 4), форматування чисел (рис. 5.8, 5), тексту (рис. 5.8, 6) та зовнішнього виду комірок (рис. 5.8, 7).

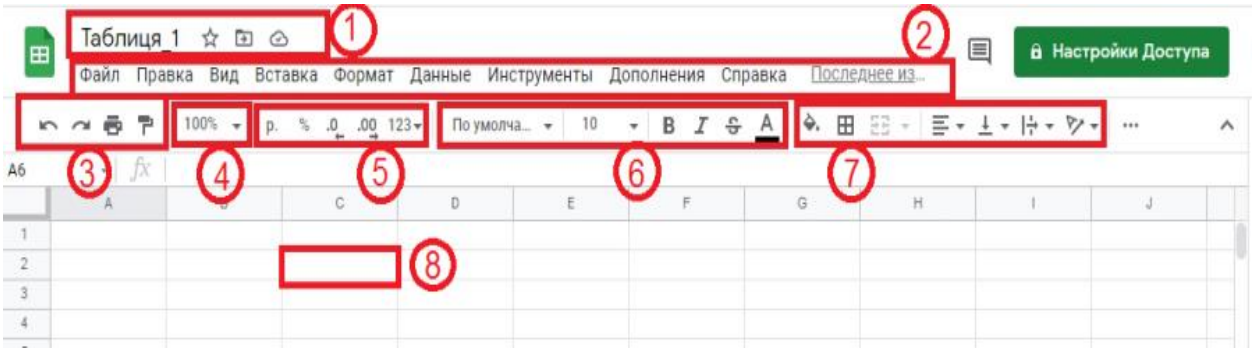


Рис. 5.8. Основні елементи інтерфейсу

Нумерація комірок в Google таблицях побудована таким самим чином, як і у MS Excel: наприклад, комірка, яка розташована на перетині другого рядка та стовпця «С», буде мати назву «С2» (рис. 5.8, 8).

Для вводу початкових даних достатньо клацнути на відповідну комірку та ввести потрібну інформацію. Для переходу між комірками, окрім миші, можна користуватися також клавішами зі стрілками та кнопкою «Tab».

Форматування таблиці в Google Sheets

Наступним логічним кроком після додавання даних до таблиці буде їх форматування. Перше, з чим необхідно працювати – це ширина комірок. Змінити їх розмір можна двома способами: або вручну, просто натиснувши курсором на границі назви стовпця та рухаючи вправо і вліво (рис. 5.9, 1), або в автоматичному режимі, тобто за допомогою кнопки «Формат» на панелі інструментів та кнопки «Змінити розмір стовпця» (рис. 5.9, 2).

Після цього не зайвим буде наступне: відцентрувати розташування тексту в комірці та (за необхідністю) дозволити перенос слів. Вирівнювати дані в комірці можна за допомогою вкладинки «Формат» та кнопки «Вирівняти» (рис. 5.10). Перенос тексту в комірці відбувається за допомогою тієї ж вкладники та кнопки «Пернос тексту» (рис. 5.11).

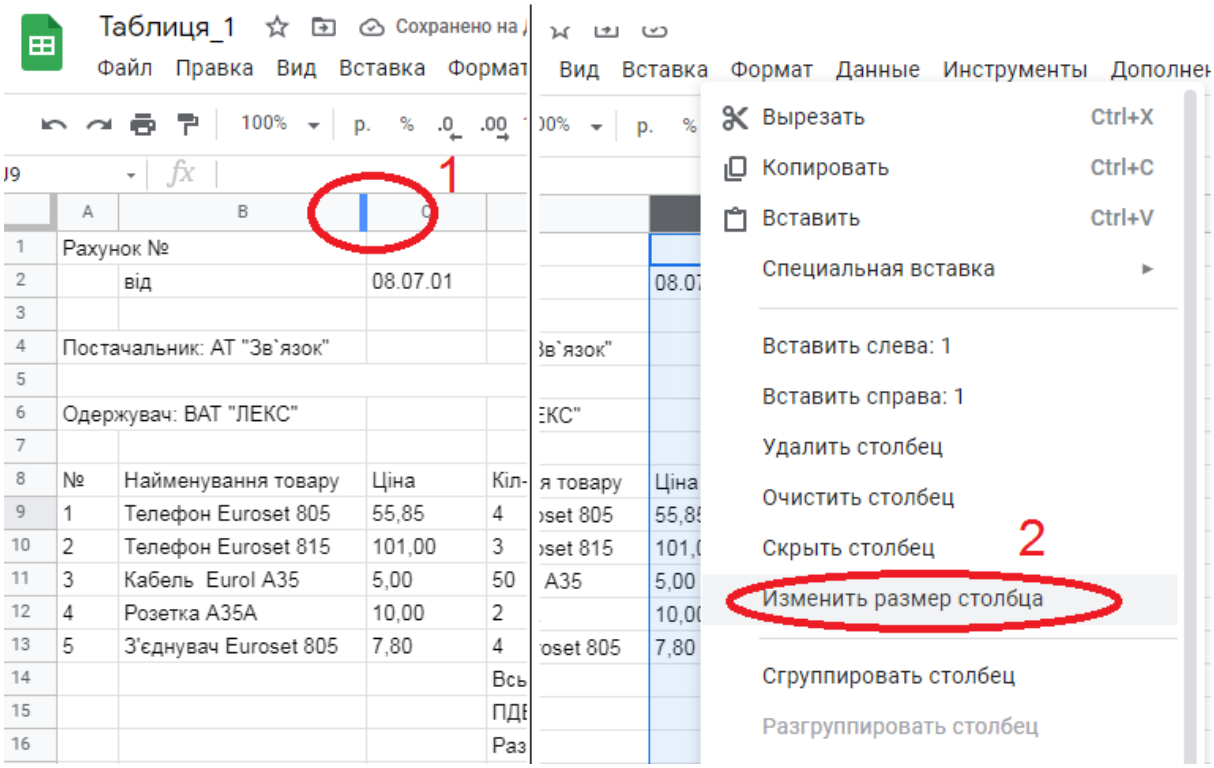


Рис. 5.9. Зміна ширини комірки

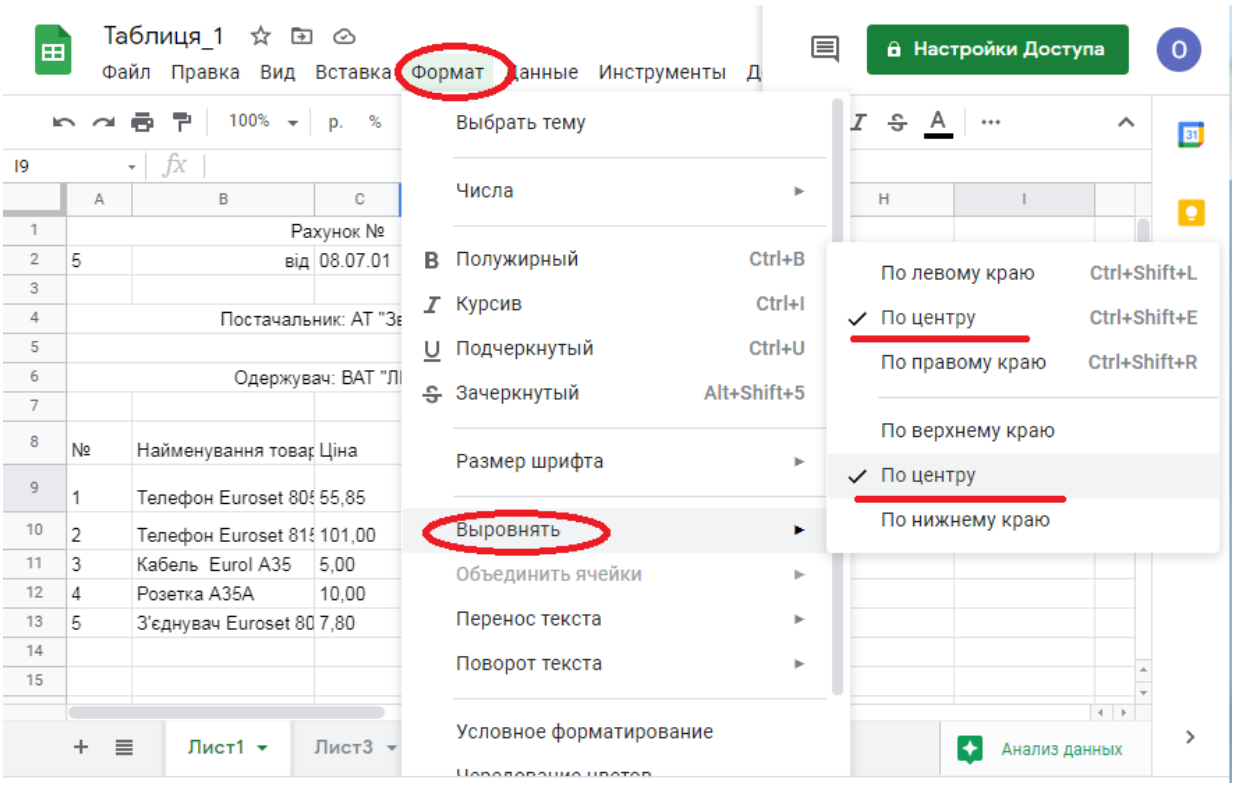


Рис. 5.10. Вирівнювання даних

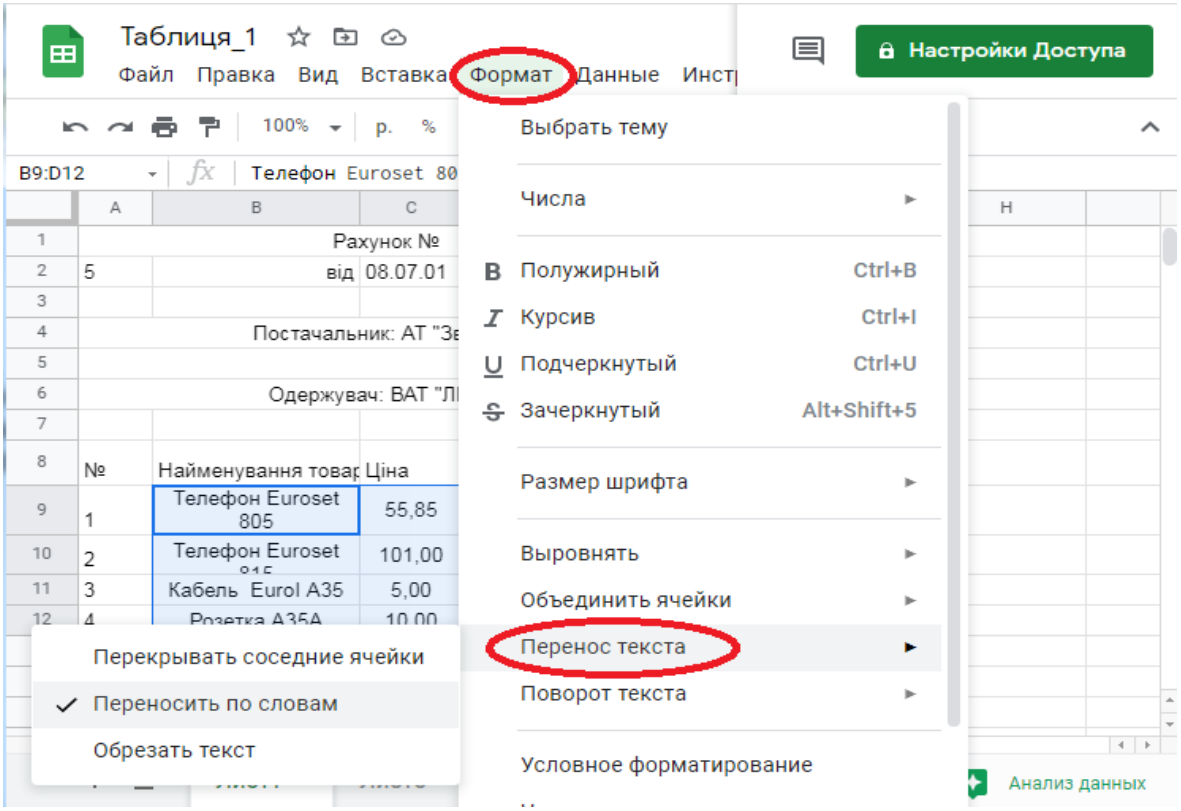


Рис. 5.11. Перенос тексту в комірці

Наступною важливою можливістю форматування тексту є об’єднання декількох комірок в одну. Для цього необхідно виділити всі комірки, які підлягають об’єднанню, та натиснути кнопку «Об’єднати комірки» (рис. 5.12, 1). Використавши додатково центрування тексту, можна отримати центрування не тільки в комірці, але й на всьому листі (рис. 5.12, 2).

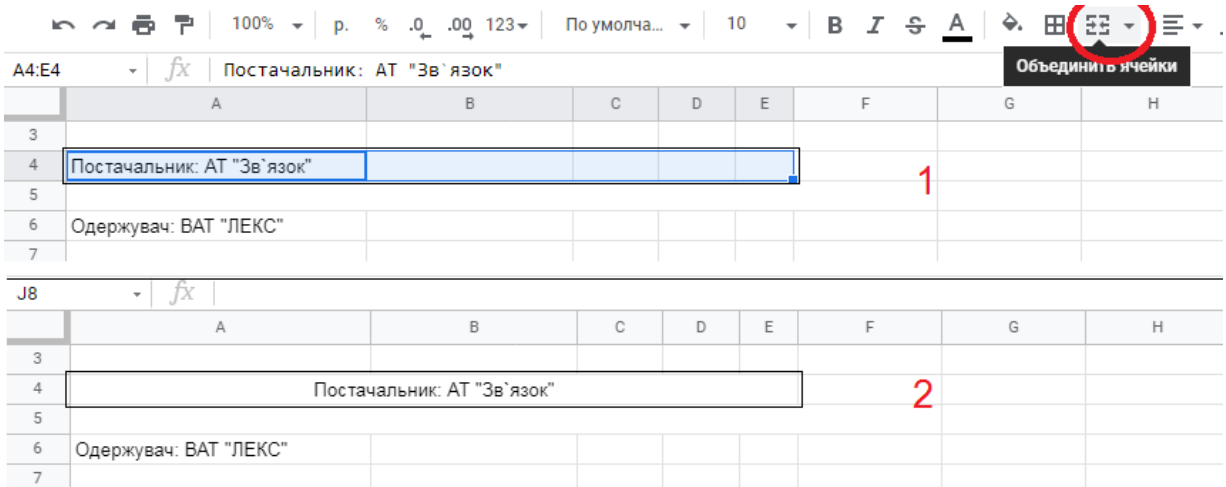


Рис. 5.12. Об’єднання комірок

Створення Діаграми

Наступною важливою особливістю Google таблицях є можливість графічного зображення даних – діаграм. Для створення діаграми необхідно обрати ту область таблиці, в якій зазначені ті дані, що підлягають відображенню, та скористатися вкладкою «Вставка» та кнопкою «Діаграма» (рис. 5.13, 1) або кнопкою «Вставити діаграму» (рис. 5.13, 2).

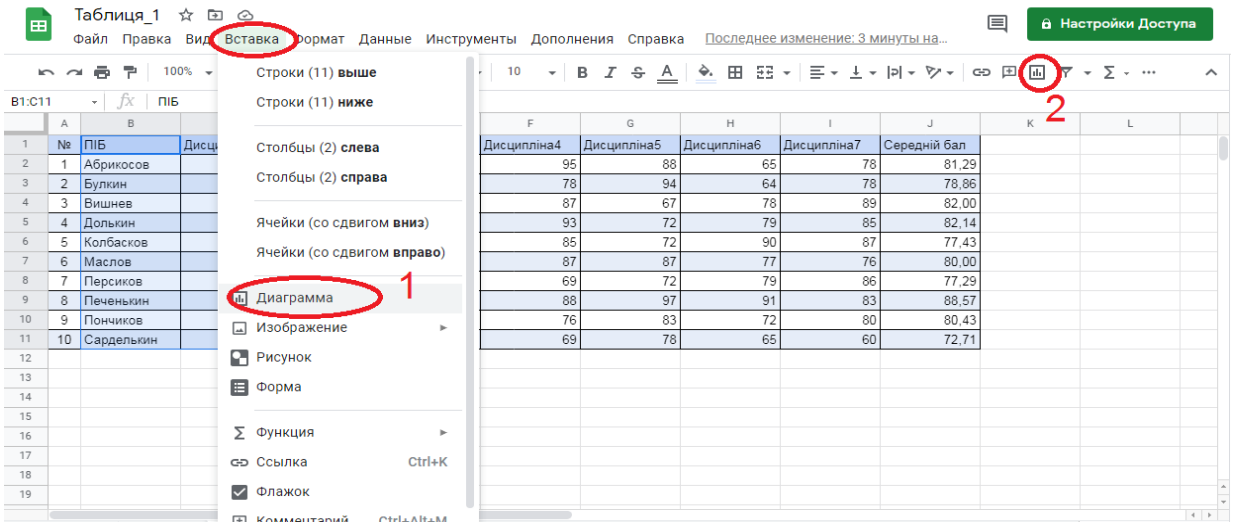


Рис. 5.13. Вставка діаграми

За допомогою додаткової форми Google таблицях дозволяють обирати: тип діаграми, наявність накопичування, діапазон даних, підпис осей тощо (рис. 5.14).

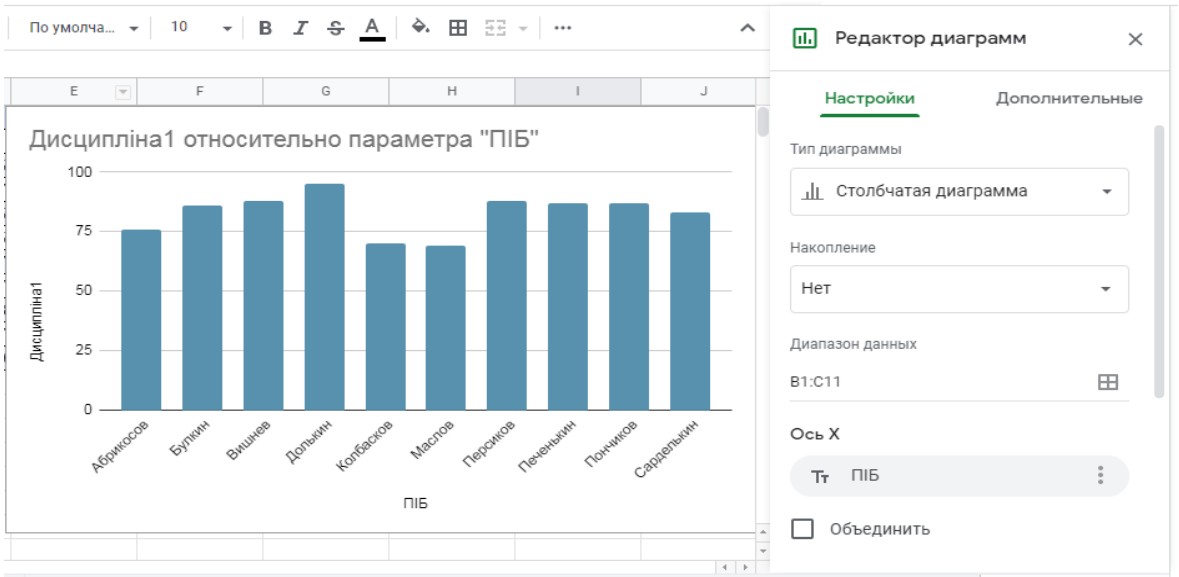


Рис. 5.14. Налаштування параметрів діаграми

Цікавою особливістю діаграм у Google таблицях є наявність, окрім стандартних графіків, гістограм та кругових діаграм, всіляких специфічних типів діаграм: «Карти» та інше.

Вкладка «Додатково» редактору формул (рис. 5.15) дозволяє налаштовувати такі параметри, як колір фону діаграми, стиль та колір ліній чи стовпців, назву діаграми та підписи осей, легенду, горизонтальні та вертикальні поділи тощо.

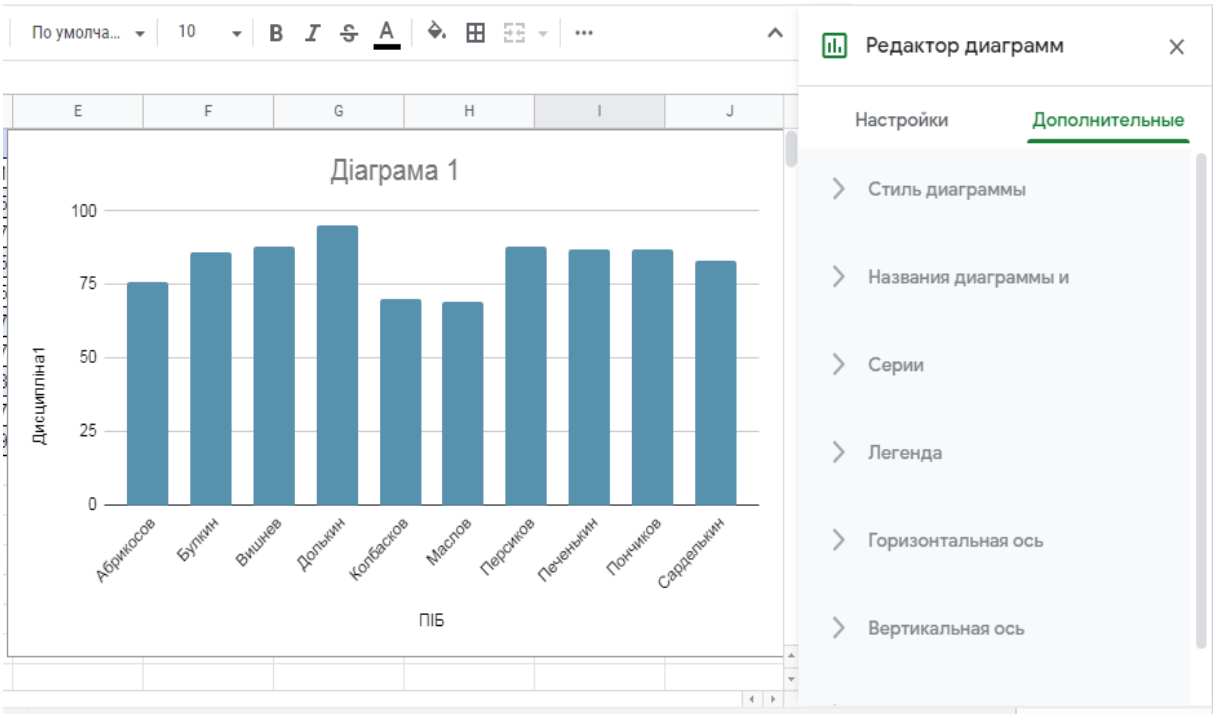


Рис. 5.15. Додаткові параметри діаграми

Зверніть також увагу, що, крім додаткової форми для налаштування, сама діаграма має контекстне меню, яке відкривається за допомогою натиснення кнопки з трьома точками (рис. 5.16). Саме це меню надає можливість перемістити створену діаграму на окремий лист за допомогою кнопки «Перемістити на окремий лист» або видалити з листа за допомогою кнопки «Видалити».

Окрім того, в тому випадку, якщо створену таблицю разом з діаграмами необхідно закачати, сама діаграма завантажується окремо від файлу Google таблицях – за допомогою кнопки «Закачати» та в результаті вибору відповідного формату файлу (рис. 2.16).

Дані для створення діаграми «Карта» повинні виглядати наступним чином: в першому стовпці – назви країн або міст в англійській або українською мовах, а в другому – кількісні значення, що характеризують регіон по якомусь параметру (рис. 5.17).

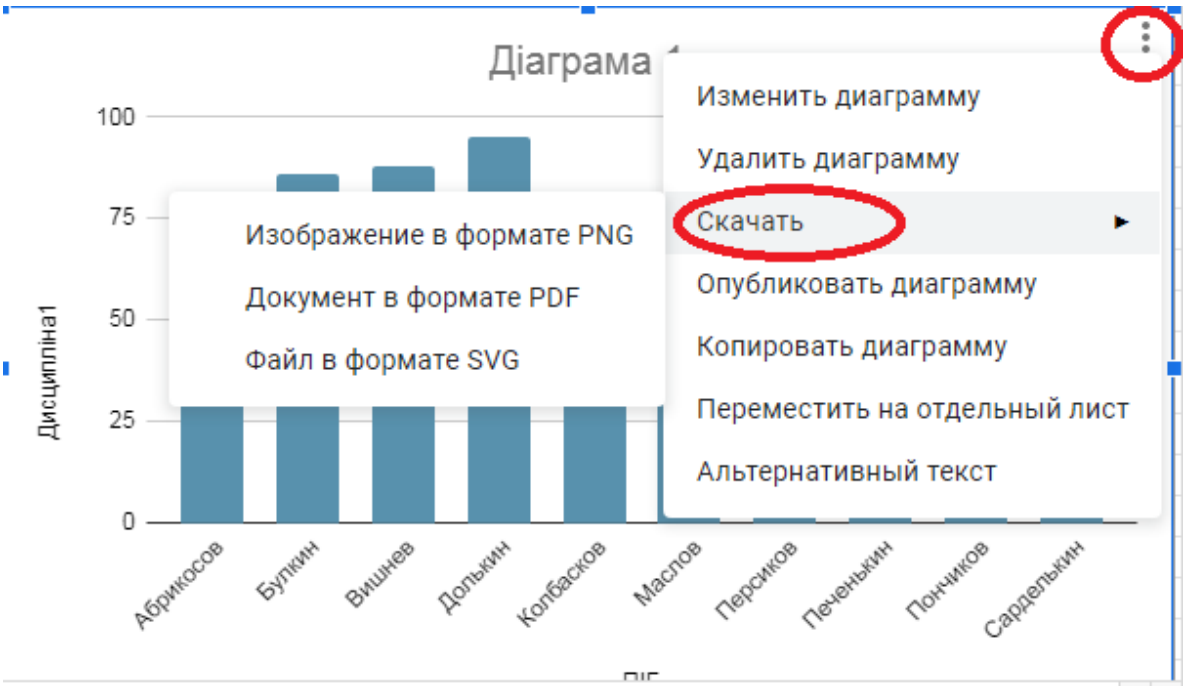
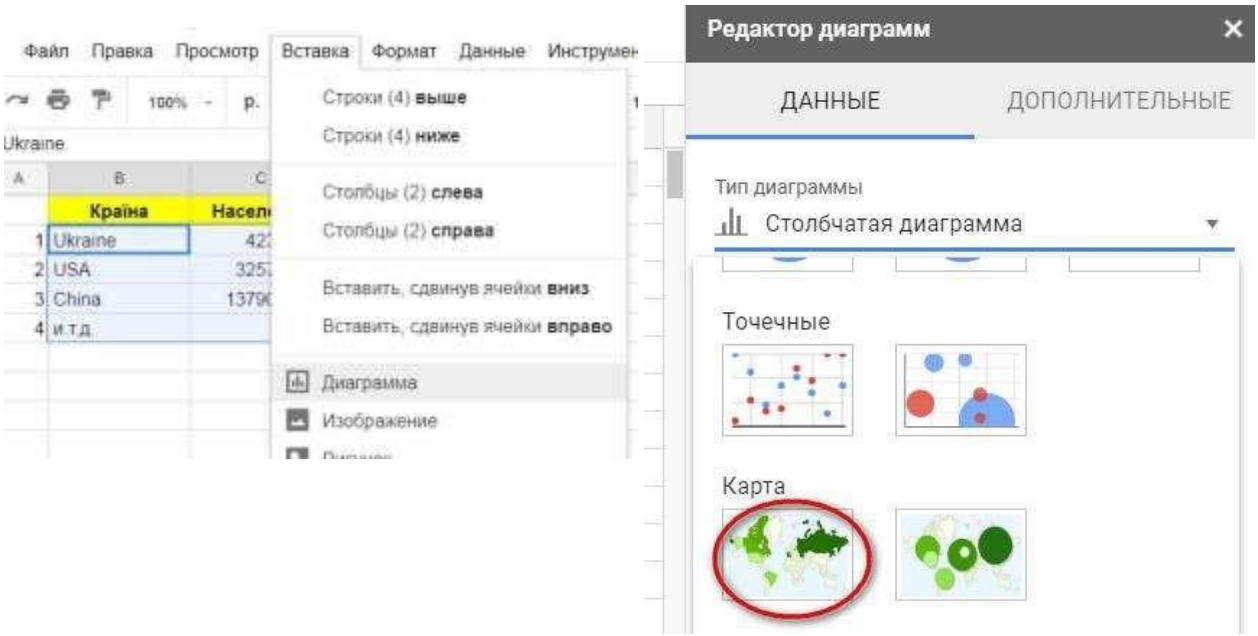


Рис. 5.16. Меню діаграми

	A	B	C
1		**Країна**	**Населення**
2	1	Ukraine	42346263
3	2	USA	325719178
4	3	China	1379000000
5	4	и.т.д.	
6			
7			

Рис. 5.17. Загальний вигляд електронної бази даних, отриманих за допомогою пошуку в Інтернеті

Виділіть весь діапазон, зайдіть в меню **Вставити** та оберіть вкладку **Діаграма** (рис. 5.18, а):



а **б**

Рис. 5.18. Етапи створення географічної карти

В **Редакторі** на вкладці **Типи діаграм** виберіть **Карту** (рис. 5.8, б). У вкладці **Додатково Географія** виберіть регіон **Земний**. Кольори ви можете змінити за бажанням:

Карта з виділеними країнами по населенню (рис. 5.19):

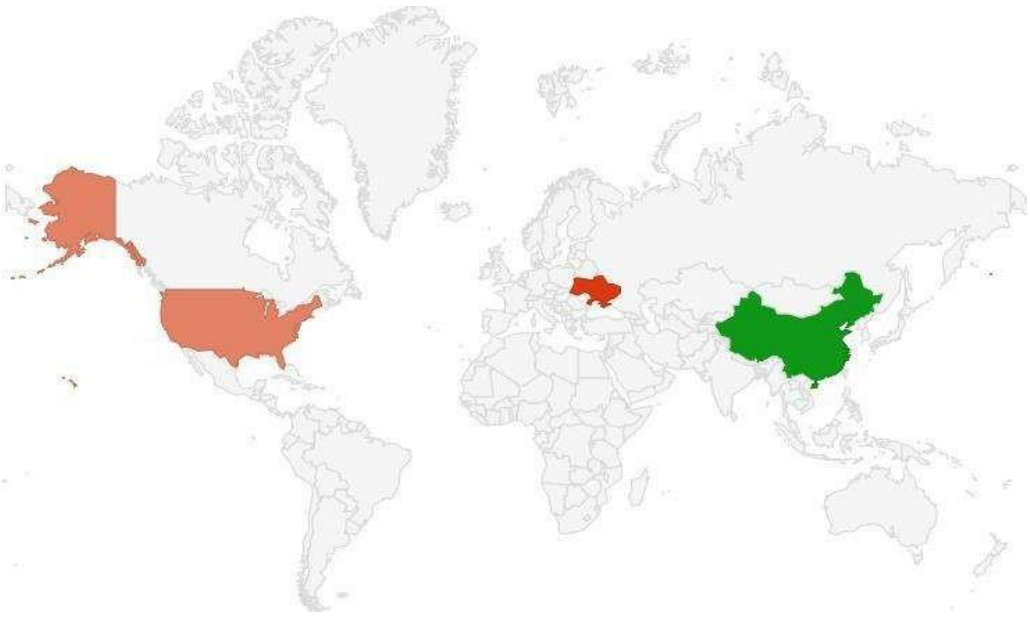


Рис. 5.19. Загальний вигляд діаграми – Географічна карта

5.2. Робота з текстовими функціями онлайн сервісу Google

Використання текстових функцій має велике значення для підготовкиюридичних документів.

В Google таблицях існує цілий ряд вбудованих функцій, які ставлять собі за мету полегшення життя користувача. Для виклику тієї чи іншої функції можна скористатися одним з наступних способів: або за допомогою меню «Вставка» та вкладники «Функція» (рис. 5.20, 1), або за допомогою кнопки «Функції» (рис. 5.20, 2).

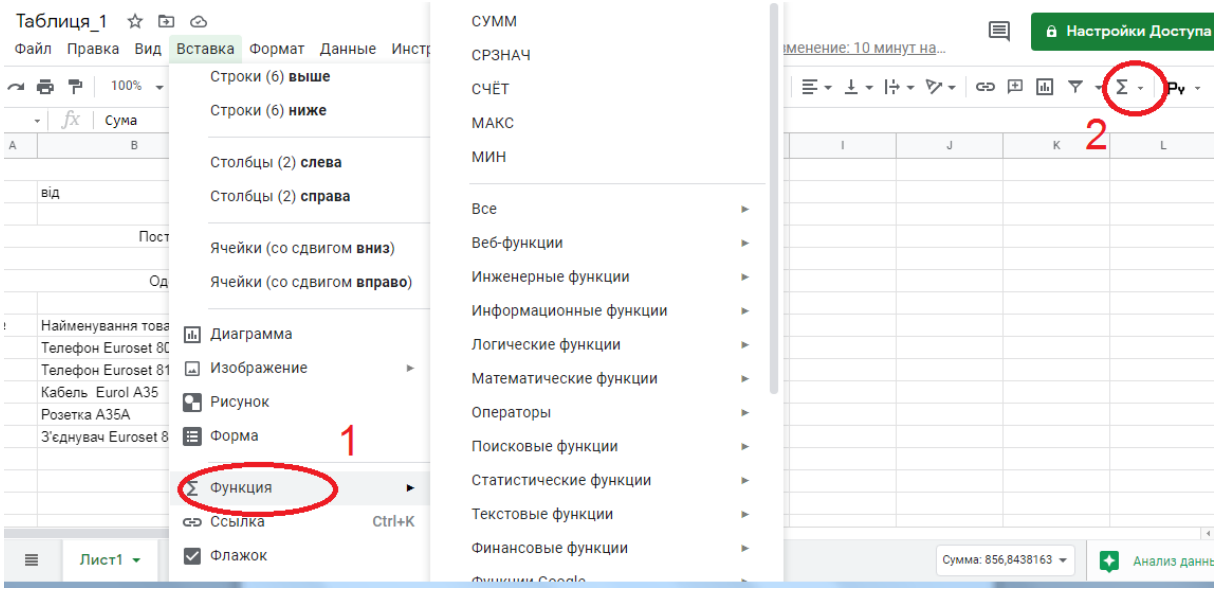


Рис. 5.20. Виклик функції

У цій роботі ми розглянемо основні текстові функції.

Назви та призначення текстових функцій:

TRIM (СЖПРОБЕЛЫ) – видаляє зайві пробіли між словами, а також пробіли до першого й останнього слова в тексті. Формула залишає лише по одному пробілу між словами. Єдиний аргумент — можна вказати текст у лапках прямо в самій формулі, але на практиці таке чи навряд знадобиться.

UPPER (ПРОПИСН) і LOWER (СТРОЧН) міняють регістр тексту на верхній і нижній відповідно. У них теж один аргумент.

Функція LEN (ДЛСТР) визначає довжину тексту. Ураховуються всі символи, включаючи пробіли. Її можна використовувати як формулу масиву. У такому випадку вдасться порахувати суму довжин текстів із цілого діапазону клітинок.

Функція FIND визначає позицію входження слова або символу

втексті (в Excel є два аналоги – ЗНАЙТИ враховує регістр, ПОШУК – немає). Перший аргумент – текст, який ми шукаємо; другий – клітинка з текстом, у якому будемо шукати; третій — необов'язковий – аргумент: позиція початку пошуку. Шукати можна не з початку. У прикладі слово «кефір» у вихідному тексті стоїть на 266-й позиції.

Функція SUBSTITUTE (ЗАМІНИТИ) міняє в тексті одне слово (символ,текст) на інше. Наприклад, функція нижче:

=SUBSTITUTE(«пробіг я марафон за 3:15»;»3:15»;»2:55») видасть такий приємний результат: пробіг я марафон за 2:55.

Функція TEXT (ТЕКСТ) потрібна в тих випадках, коли за допомогою формул ви становите текстову фразу, у якій використовуються числові значення або дати із гнізд вашої таблиці.

У прикладі: =«сьогодні «&B13

видає дату в невідформатованому вигляді*, тобто як число: сьогодні 42413А функція TEXT (ТЕКСТ):

=«сьогодні «&TEXT(B14;»DD/MM/YYYY»)

=«сьогодні «&ТЕКСТ(B14;»DD/MM/YYYY»)

дозволяє одержати гарний результат: сьогодні 13/02/2016.

Функції LEFT (ЛЕВСИМВ) і RIGHT (ПРАВСИМВ) вирізують ізтексту (перший аргумент) певна кількість знаків (другий аргумент).

=LEFT(«Слово»;3) = Сло

=ЛЕВСИМВ(«Слово»;3) = Сло

Примітка. В Google Таблицях, як і в Excel, дати зберігаються в пам'яті як звичайні числа – починаючи з 1, де 1 = 31.12.1899. Наприклад, 42736 =

01.01.2017.

Функція MID (ПСТР) вирізує з тексту задану кількість символів,починаючи з певної позиції (другий аргумент):

=MID(«Машина»;3;2) = ши

=**ПСТР(«Машина»;3;2) = ши.**

Практичні завдання

Завдання № 1

Створити електрону таблиці з назвою «ПР 5.1 – ПІБ.

Усі завдання виконати на одному листі у онлайн сервісі Google таблицях.

Скачати документ у форматі *.XLSX та завантажити до МІА: Освіти.

Завантажити посилання на Google документ у «Коментарі».

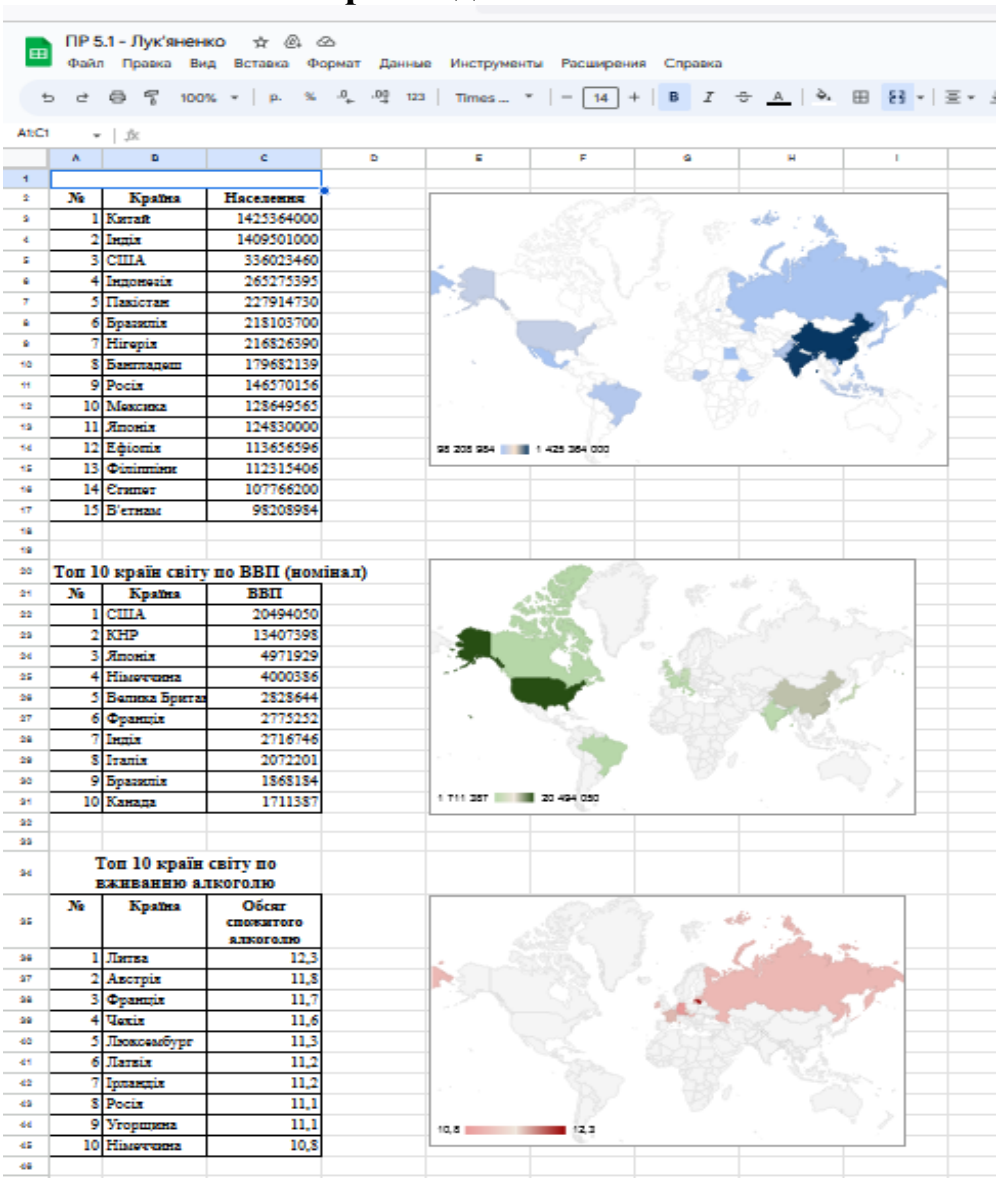
1. Створити карту топ 15 країн по населенню, з кольорами від світлого до темного (темний колір найбільше населення, світлий найменше).

2. Створити топ 10 країн світу по ВВП (номінал) на душу населення, з кольорами від світлого до темного (темний колір найбільше ВВП, світлий найменше).

3. Створити карту топ 10 країн світу по вживанню алкоголю, з кольорами від світлого до темного (темний колір найбільше вживання, світлий найменше).

4. Створити карту ТОП 5 країн світу по вживанню наркотичних речовин (кокаїну), з кольорами від світлого до темного (темний колір найбільше вживання, світлий найменше).

Приклад виконання



№	Країна	Населення
1	Китай	1425364000
2	Індія	1409501000
3	США	336023460
4	Індонезія	265275395
5	Пакістан	227914730
6	Бразилія	218103700
7	Нігерія	216826390
8	Бангладеш	179682139
9	Росія	146570156
10	Мексика	128649565
11	Японія	124830000
12	Ефіопія	113656596
13	Філіппіни	112315406
14	Єгипет	107766200
15	В'єтнам	98208984

Топ 10 країн світу по ВВП (номінал)

№	Країна	ВВП
1	США	20494050
2	КНР	13407398
3	Японія	4971929
4	Німеччина	4000386
5	Велика Британ	2828644
6	Франція	2775252
7	Індія	2716746
8	Італія	2072201
9	Бразилія	1868184
10	Канада	1711387

Топ 10 країн світу по вживанню алкоголю

№	Країна	Обсяг спожитого алкоголю
1	Литва	12,3
2	Австрія	11,8
3	Франція	11,7
4	Чехія	11,6
5	Люксембург	11,3
6	Латвія	11,2
7	Ірландія	11,2
8	Росія	11,1
9	Угорщина	11,1
10	Німеччина	10,8

Завдання № 2

Створити електрону таблиці з назвою «ПР … – ПІБ.

Усі завдання виконати на одному листі у онлайн сервісі Google таблиця.

Скачати документ у форматі *.XLSX та завантажити до МІА:Освіти.

Завантажити посилання на Google документ у «Коментарі»:

1. Створити електронну таблицю (рис. 5.21) з наступними стовбцями:

1) назва функції;

2) вихідний текст;

3) текст після застосування функції (клітинка з формулою) – Підсумок;

4) текст самої функції.

Функція	Вихідна	Підсумок	Формула
TRIM	текст з зайвими проблемами	текст з зайвими проблемами	=СЖПРОБЕЛЫ(I30)
UPPER	текст	ТЕКСТ	=ПРОПИСН(I31)
LOWER	ТЕКСТ	текст	=СТРОЧН(I32)
LEN	визначає довжину тексту	23	=ДЛСТР(I34)
ARRAYFORM	можна як формулу масиву	23,00	=СУММ(ДЛСТР(I30:I35))
FIND	у цьому тексті є слово КЕФІР	24	=НАЙТИ("КЕФІР";I37)
SUBSTITUTE	його б змінити на МОЛОКО	у цьому тексті є слово МОЛОКО	=ПОДСТАВИТЬ(I37;"КЕФІР";"МОЛОКО")
TEXT	21.11.2022	сьогодні44886	="сьогодні"&I41
	21.11.2022	сьогодні21/11/2022	="сьогодні"&ТЕКСТ(I42;"DD/MM/YYYY")
LEFT	машина	маши	=ЛЕВСИМВ(I45;4)
RIGHT	машина	шина	=ПРАВСИМВ(I46;4)
MID	машина	ши	=ПСТР(I47;3;2)

Рис. 5.21. Скріншот виконання умов завдання

2. Відредагувати вихідний текст з використанням текстових функцій.

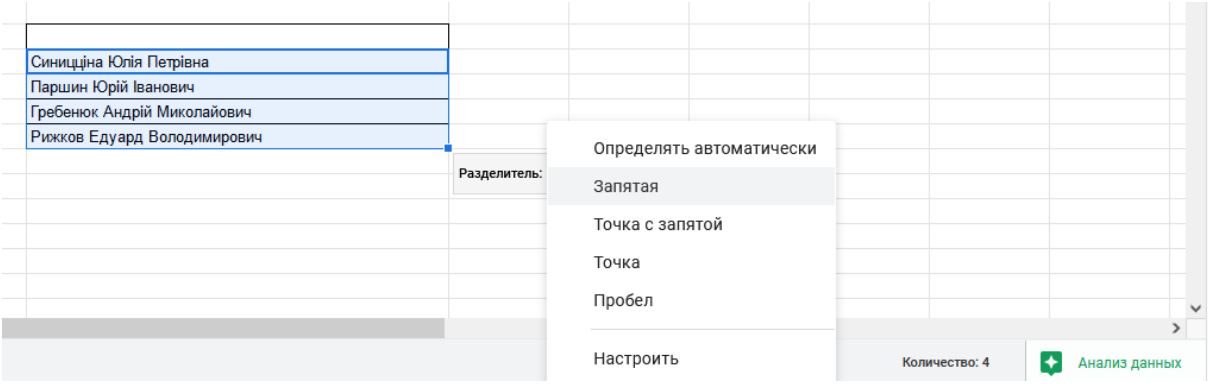
Завдання № 3

1. У трьох різних комірках написати ПІБ повністю (рис. 5.22).

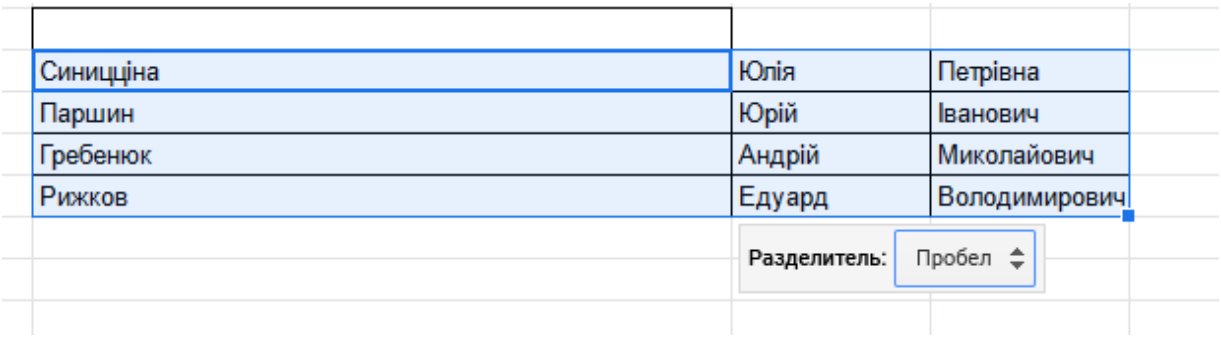
Синицціна Юлія Петрівна
Паршин Юрій Іванович
Гребенюк Андрій Миколайович
Рижков Едуард Володимирович

Рис. 5.22. Приклад виконання завдання 2

2. Розділити прізвищу, імена та по батькові з одному у стовпці на три стовбця. Для цього виділимо дані, у вкладці «Дані» потрібно обрати пункт «Розділити текст на стовбці» та вибрити роздільник у списку, що з’явився (у нашому випадку роздільник — Пробіл) (рис. 5.23).



а

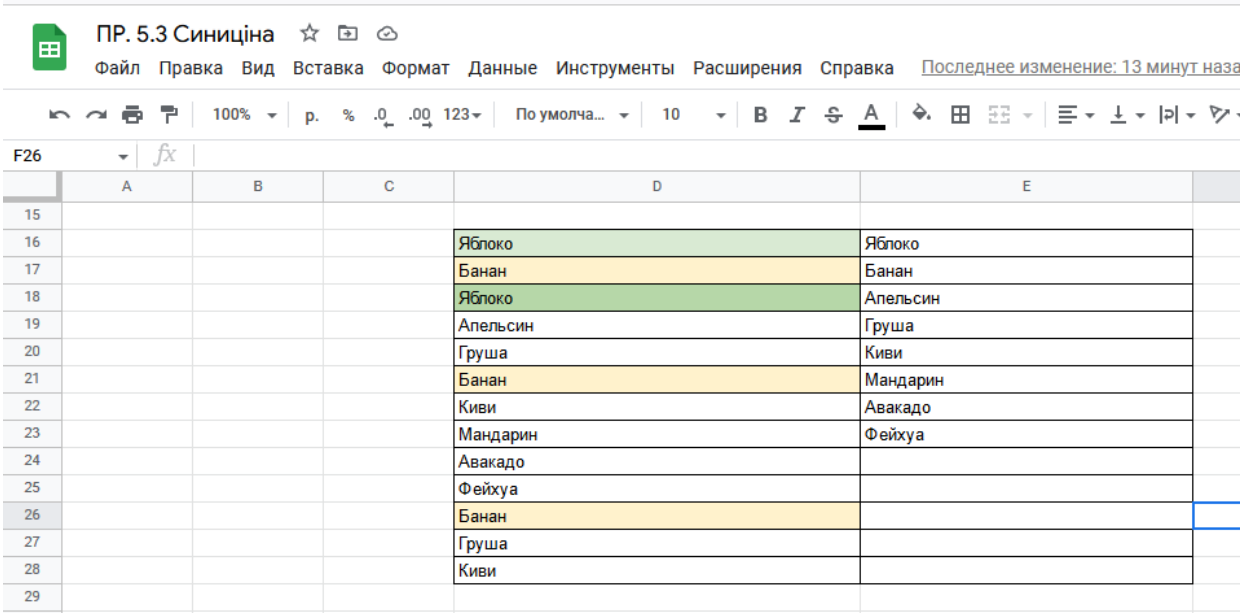


б

Рис. 5.23. Процес поділу тексту за стовбцями

Завдання № 4

1. Створити з вихідного списку, список що містить тільки унікальні значення, використав функцію UNIQUE, єдиний аргумент якої – вихідний список (рис. 5.24).
2. Вихідний список можна сформувати самостійно.



	D	E
16	Яблоко	Яблоко
17	Банан	Банан
18	Яблоко	Апельсин
19	Апельсин	Груша
20	Груша	Киви
21	Банан	Мандарин
22	Киви	Авакадо
23	Мандарин	Фейхуа
24	Авакадо	
25	Фейхуа	
26	Банан	
27	Груша	
28	Киви	

Рис. 5.24. Створення унікального списку
за допомогою функції UNIQUE.

Контрольні питання

1. З яким розширенням можна завантажити Google таблицю?
2. Назвіть головну особливість та перевагу використання Google таблиці у порівнянні з Excel.
3. Назвіть основні елементи інтерфейсу Google таблиць.
4. Опишіть основні можливості зміни формату комірок.
5. Опишіть процес додавання діаграми до Google таблиць.
6. Опишіть процес зміни розміру стовбців (строк).
7. Опишіть, яким чином можна зберегти діаграму.
8. Опишіть, яким чином можна таблиці додати границі.
9. Опишіть, яким чином нумерують комірки в Google таблицях
10. Яким чином можна імпортувати файли до Google таблиці?
11. Яким чином можна надати доступ до своєї таблиці?
12. Яким чином розпочати роботу з Google таблицями?
13. Яким чином, можна перенести текст в межах однієї комірки на

наступну строку?

14. Які типи файлів імпортуються до Google таблиці?

15. Яким чином можна поділити текст за різними стовбцями у Google таблиці?

16. Яку текстову функцію застосувати щоб відтворити унікальний текст?

17. Яку текстову функцію застосувати щоб виправити текст з невірно набраним регістром?

18. Яку текстову функцію застосувати щоб порахувати кількість символів у фразі?

19. Для яких цілей застосовують **Функцію SUBSTITUTE (ЗАМІНИТИ)** ?

20. Для яких цілей застосовують **Функцію TEXT (ТЕКСТ)** ?

21. Для яких цілей застосовують **Функції LEFT (ЛЕВСИМВ) і RIGHT (ПРАВСИМВ)**?

22. Для яких цілей застосовують **Функцію MID (ПСТР)**?

23. Для яких цілей застосовують **Функцію UPPER (ПРОПИСН) і LOWER (СТРОЧН)**?

24. Для яких цілей застосовують Функцію **LEN (ДЛСТР)**?

Джерела до розділу 5

1. Інформаційні системи та технології: підручник / кол. авт.; ред. В. Б. Вишня. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2021. 296 с.

2. Інформаційне забезпечення юридичної діяльності: підручник / кол. авт.; ред. В. Б. Вишня. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. 240 с.

3. Технічна підтримка ресурсів корпорації Google. URL : https://support.google.com/docs/topic/9054603?hl=ru&ref_topic =1382883.

4. Google Sheets проти Microsoft Excel – Які відмінності? URL : https://uk.gadget-info.com/google-sheets-vs-microsoft-excel-what-are-differences.

5. Посібник для початківців по Google Таблицях. Електронний ресурс: https://apcaglobal.com/uk/11752-the-beginner8217s-guide-to-google-sheets.html.

6. Посібник з формули Google Sheets. Електронний ресурс:https://ukr.4meahc.com/google-sheets-formula-tutorial-99639.

Розділ 6
СТВОРЕННЯ ПРЕЗЕНТАЦІЙ У MS POWER POINT

6.1. Призначення, можливості й особливості використання презентацій. види та типи презентацій

Однією з потужних програм для побудови презентацій є PowerPoint. Ця програма дозволяє навіть не дуже обізнаному у галузі інформаційних технологій користувачу створювати мультимедійні презентації.

Презентація (від англ. *Presentation* — представлення, вистава) — це набір картинок-слайдів на будь-яку тему, файл якого має спеціальний формат. Ці слайди міститять довільну текстову, графічну, відеоінформацію, анімацію, стереозвук (як синтезований, так і записаний з мікрофона).

Презентації можуть використовуватись у будь-яких сферах діяльності, як от навчання, дослідницька діяльність, аналітична робота правоохоронних підрозділів та інше.

Розглянемо види презентацій, їх поділяють на :

- із сценарієм;
- інтерактивні;
- автоматичні.

Презентація зі сценарієм

Це звичайна презентація зі слайдами, яка доповнюється засобами показу кольорової графіки й анімації, титрами, що переміщуються по екрану. Присутня можливість під час демонстрації вносити зміниї. Цей вид презентацій належить до найрозповсюдженіших мультимедійних презентацій.

Можливість використання анімаційного тексту разом з анімаційними діаграмами, графіками та ілюстраціями дозволяє слухачам швидше та глибше засвоїти запропанований матеріал та сприяє кращому запам’ятовуванню інформації. Коментує слайди, як правило, лектор.

Інтерактивна презентація

Вона надає можливість вибору користувачем певного матеріалу з запропанованого. Користувач приймає рішення, який матеріал для нього важливий, і здійснює вибір на екрані потрібного об'єкта. Тобто затребується інформація, яка цікава користувачам презентації.

Інтерактивні презентаційні програми в даному випадку керують подіями. Презентаційна програма виконує дію після активації на певному об'єкті екрану.

Інтерактивна презентація дає змогу здійснювати пошук потрібної інформації, заглиблюючись в неї настільки, наскільки це передбачено розробником презентації. Наприклад, користувач починає вивчати матеріал, використовуючи можливість поглибленого ознайомлення за допомогою натискання на певні гіперпосилання.

Як правило інформація може подаватися:

- графічно;
- у текстовому вигляді;
- за допомогою анімації або відеокліпів;
- читанням тексту «від розробника»
- використанням звукових ефектів.

Для інтерактивної презентації характерним є можливість користувача самостійно обирати цікавий на його думку матеріал.

Автоматична презентація

Це найбільш досконалий інформаційний продукт. Дана презентація налаштована на демонстрацію в автоматичному режимі, може бути розміщена на будь-яких носіях.

Відповідно до сфери застосування розрізняють такі *типи презентацій*:

- торгові,
- маркетингові,
- корпоративні,
- навчальні.

Розглянемо навчальні презентації. Вони призначені для допомоги лектору забезпечити зручне і наочне подання навчального матеріалу.

Навчальні презентації поділяються на такі *види*:

- *презентації-семінари* (ознайомлення з новою технікою; освітні презентації; порівняльний аналіз продукції, що випускається; огляд поточного стану ринку; навчання студентів, надомних працівників; презентації для споживачів, у тому числі потенційних);
- *презентації для самоосвіти* (інтерактивні системи, за

допомогою яких можна здобути відомості про товар, компанію, ринок, конкурентів тощо, включаючи самий додаток, у середовищі якого здійснюється перегляд матеріалу);

– *презентації-порадники* (поради викладачу або лектору, як ефективніше провести презентацію);

– *презентації для клієнтів корпорацій* (навчальні диски та тематичні порадники, які розсилаються за замовленням споживачів).

6.2. Планування презентації та стилі її демонстрації. Вимоги щодо структури, змісту й оформлення навчального матеріалу

Планування презентацій

Для планування презентації важливий аналіз послідовності відображення матеріалу, логічно продумані питання, практичні приклади використання навчального матеріалу. Для створення презентації необхідно дотримуватись наступних вимог:

– точність визначення мети, про що ви хочете розповісти;

– врахування особливості слухачів презентації;

– ретельно продумати сценарій презентації, який використовувати текст, зображення, звуки та інші елементи, що супроводжують слайди.

Категорично забороняється перенасичуватив презентацію великою кількістю інформації, графічних зображень та анімаційних ефектів, які лише відвертають увагу слухачів від змісту презентації.

Також під час планування презентаціїї необхідно вибрати тему та призначення презентації, спосіб її демонстрації, розробити сценарій презентації та скласти зміст усіх слайдів, їх стиль та оформлення.

Демонстрація презентацій

За структурою презентації поділяються на *лінійні* та *розгалужені.*

Презентації лінійної структури створюються для послідовного викладання матеріалу з використанням мультимедійних засобів. Вони мають містити лише текстову інформацію та зображення.

Презентації з гіпертекстовими посиланнями мають ***розгалужену структуру,*** їх доцільно застосовувати для узагальненні й систематизації знань та у визначенні рівня отриманих знань навчального матеріалу.

По можливості можна представити готову презентацію колегам-рецензентам та врахувати їхні случні зауваження в разі вашої

згоди з ними.

До побудови презентації та змісту матеріалу необхідно дотримуватись наступних вимог:

– викладайте матеріал стисло, з максимальною інформативністю тексту;

– використовуйте слова і скорочення, вже знайомі аудиторії;

– інформацію подавайте блоками (кейсами);

– використовуйте короткі та змістовні заголовки, марковані та нумеровані списки;

– висновки, визначення виділяйте великими літерами шрифтом і розташовуйте у лівому верхньому куті екрана зверху слайда

– другорядну інформацію бажано вміщувати внизу сторінки;

– кожному кейсу потрібно відвести окремий слайд;

– для ілюстрації важливих положень застосовуйте діаграми, схеми;

– графічні зображення мають підкреслювати основні текстові положення;

– придавайте підвищену увагу методичним матеріалам для виконання завдань: їх чіткість, лаконічність, однозначність;

– інформацію на слайдах потрібно обов’язково перевірити щодо відсутність орфографічних, граматичних і стилістичних помилок.

Необхідно приділяти увагу на врахування фізіологічних особливостей людини у сприйнятті кольорів, які можна поділити на:

– ***стимулюючі*** (теплі) кольори сприяють збудженню й діють як подразники (у порядку спадання інтенсивності впливу: червоний, оранжевий, жовтий);

– ***дезінтегруючі*** (холодні) кольори заспокоюють, викликають сонливий стан (у тому самому порядку: фіолетовий, синій, блакитний, синьо-зелений, зелений);

– ***нейтральні*** кольори: світло-рожевий, жовто-зелений, коричневий;

– ***поєднання двох кольорів*** — кольору знака і кольору фону — суттєво впливає на зоровий комфорт, причому деякі пари кольорів не тільки стомлюють зір, а й можуть спричинити стрес (наприклад: зелені символи на червоному фоні);

– найкраще поєднання кольорів шрифту і фону: білий на темно-синьому, чорний на білому, жовтий на синьому;

– кольорова схема має бути єдиною для всіх слайдів;

– будь-який фоновий малюнок втомлює очі та знижує ефективність сприйняття інформації;

– чіткі, яскраві малюнки, що швидко змінюються, легко вловлює підсвідомість, вони швидко запам'ятовуються;

– будь-який другорядний об'єкт, що рухається (анімований), знижує якість сприйняття матеріалу, відволікає, порушує динаміку уваги.

Розглянемо загальні правила використання шрифтів текстових процесорів для презентації:

Кожен шрифт має своє змістове навантаження, а саме: напівжирний шрифт використовується для назви розділів презентації; *курсив* –для логічного наголосу, наприклад для визначень, правил та іншого; звичайний – для відображення основної інформації.

Неприпустимо використання понад трьох різних шрифтів на одному слайді, це призводить до втоми слухачів.

Математичні формули рекомендується відображати Times New Roman, причому всі змінні — *курсивом,* а решта — дужки, знаки математичних дій, назви функцій (sin, cos, sign тощо) — звичайним шрифтом.

Вибір шрифтів для презентації

Вибираючи шрифти, слід керуватися такими відомостями:

– Вибраний шрифт визначає вплив повідомлення на слухачів. Для консервативної аудиторії та серйозних повідомлень обирайте класичний шрифт (наприклад, Times New Roman); для радісних повідомлень «веселий» шрифт (наприклад, Comic Sans MS).

– Шрифти з зарубками (Times New Roman і Bookman) легко читаються, тому їх використовують для друку великих обсягів тексту. Шрифти без зарубок (Arial і Verdana) простіші, тому вони краще виглядають у заголовках та колонтитулах.

– Щоб забезпечити легкість читання, колір тексту потрібно зробити контрастним відносно кольору фону. Напівжирний шрифт і курсив використовується лише для виділення – часте використання послаблює їх ефективність.

6.3. Створення презентації

Елементи слайдової презентації

Основними елементами слайдової презентації є *слайди, нотатки* та *заголовки.*

Слайди складаються з наступних елементів, таких як: заголовки, текст слайда, графічні об'єкти (організаційні діаграми, об'єкти WordArt, рисунки, автофігури, таблиці, діаграми, тощо), елементи мультимедіа (відеокліпи, звукові кліпи з файлів чи дикторські тексти), дата, час, нижній колонтитул, номер слайда, кнопки керування процесом демонстрації.

Для створення презентації в Microsoft PowerPoint необхідно виконати наступні дії:

- вибір стилю оформлення за допомогою різноманітних шаблонів оформлення;
- додавання нових слайдів та їх вмісту;
- вибір розмітки слайдів;
- використання ефектів анімації під час демонстрації слайдів.

Створення слайдів

Щоб створити довільну кількість слайдів у PowerPoint необхідно на меню *Главная* групи *Слайды* натиснути клавішу *Создать слайд* (рис. 6.1) або стати нижче створеного слайду у режимі *Слайди* та за допомогою контекстного меню вибрати команду *Создать слайд* (рис. 6.2) або стати лівою кнопкою між створеними слайдами та натиснути клавішу Enter (рис. 6.3).

Застосування макетів

Для створених слайдів можна до них застосувати доцільний макет: на меню *Главная* групи *Слайди* натиснути клавішу *Макет* та вибрати необхідний макет (рис. 6.4).

Оформлення дизайну слайдів

Для оформлення дизайну створених слайдів у меню *Дизайн* групи *Темы* вибраємо потрібний дизайн (рис. 6.5).

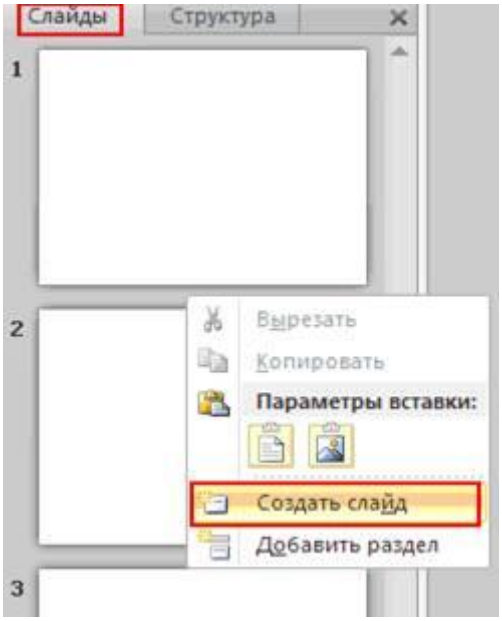


Рис. 6.2. Процес створення слайду за допомогою контекстного меню

Рис. 6.3. Процес створення слайду за допомогою клавіші Enter

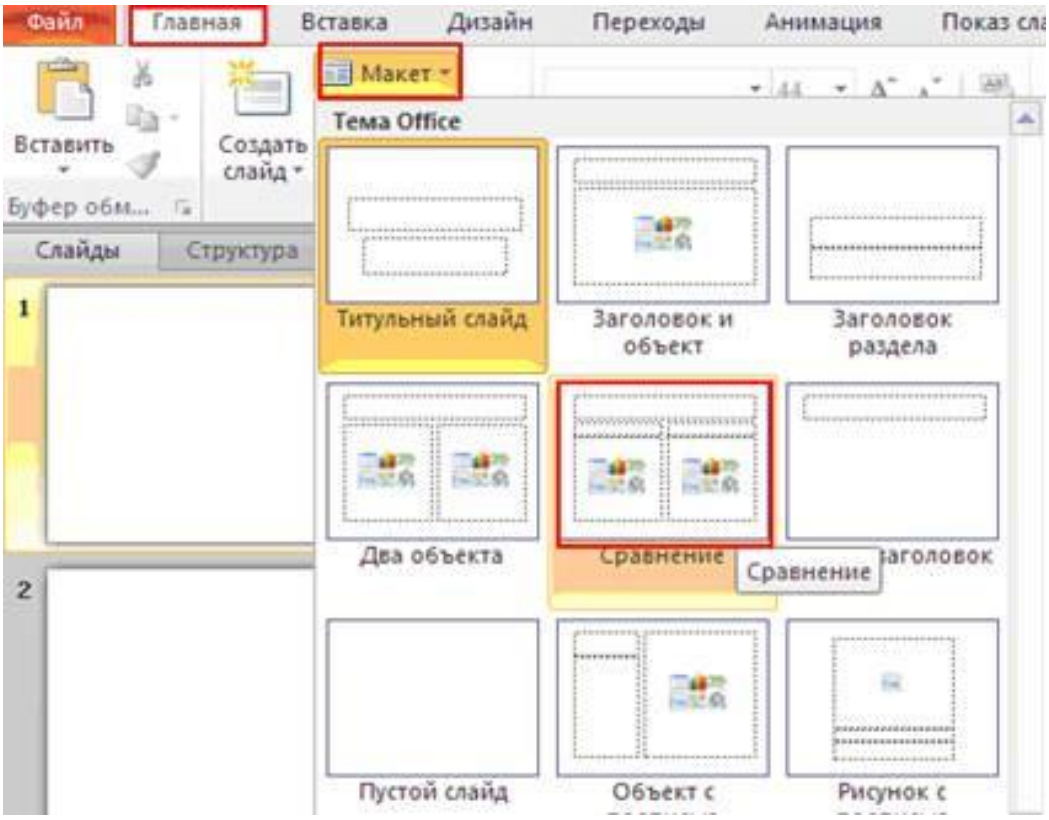


Рис. 6.4. Приклад макету до слайдів

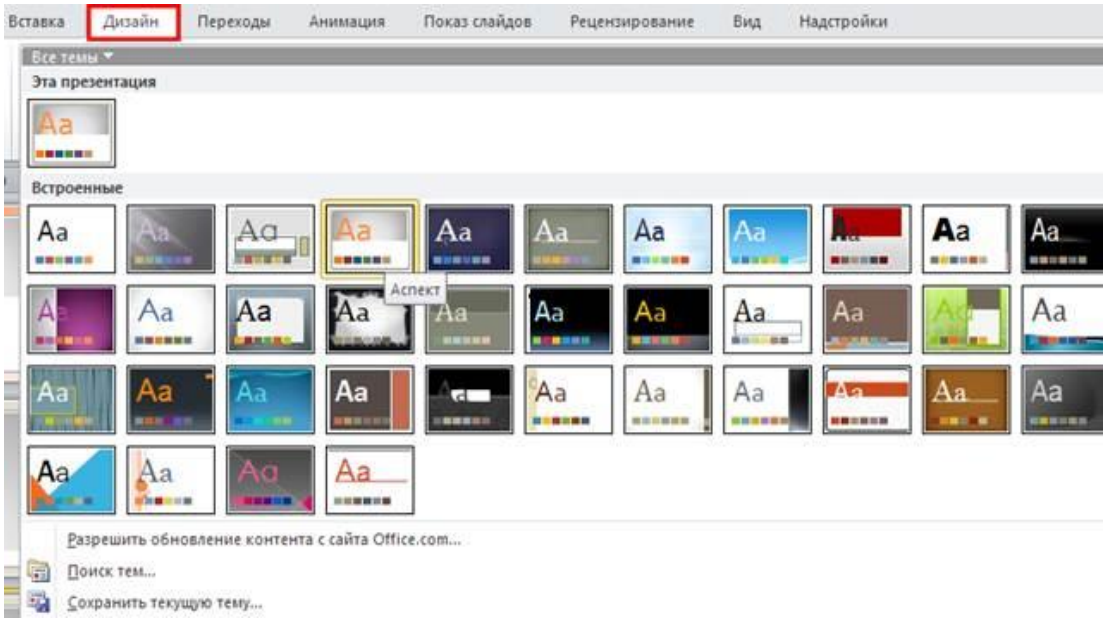


Рис. 6.5. Вибір необхідного дизайну до слайдів

Існує можливість самостійного створення фону: у меню ***Дизайн*** групи ***Фон*** натиснути клавішу ***Стили фона*** та вибрати команду ***Формат фона***, де можна вибрати суцільну заливку, градієнтну заливку, застосувати рисунок або текстуру узорну заливку, … (рис. 6.6).

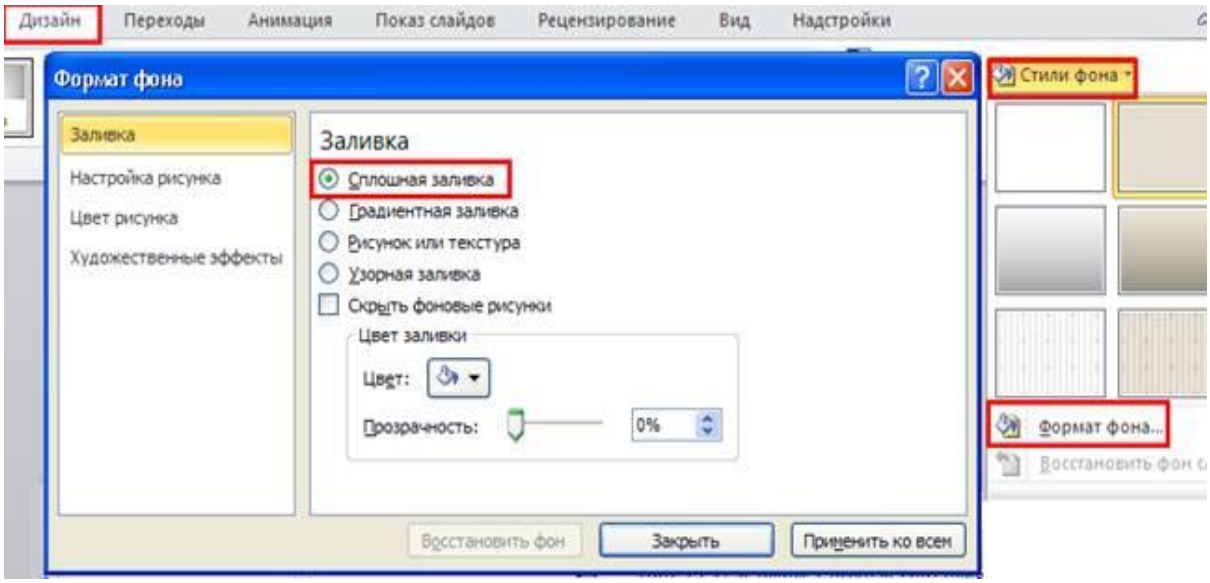


Рис. 6.6. Самостійне створення фону слайду

Режими відображення слайдів

Використовуються наступні режими відображення слайдів:

– режим слайди (вкладка ***Слайди***) (рис. 6.7),

– режим структура (вкладка ***Структура***) (рис. 6.7),

– режим сортувальника слайдів (вкладка *Вид* кнопка ***Сортировщик слайдов*** (рис. 6.8).

–

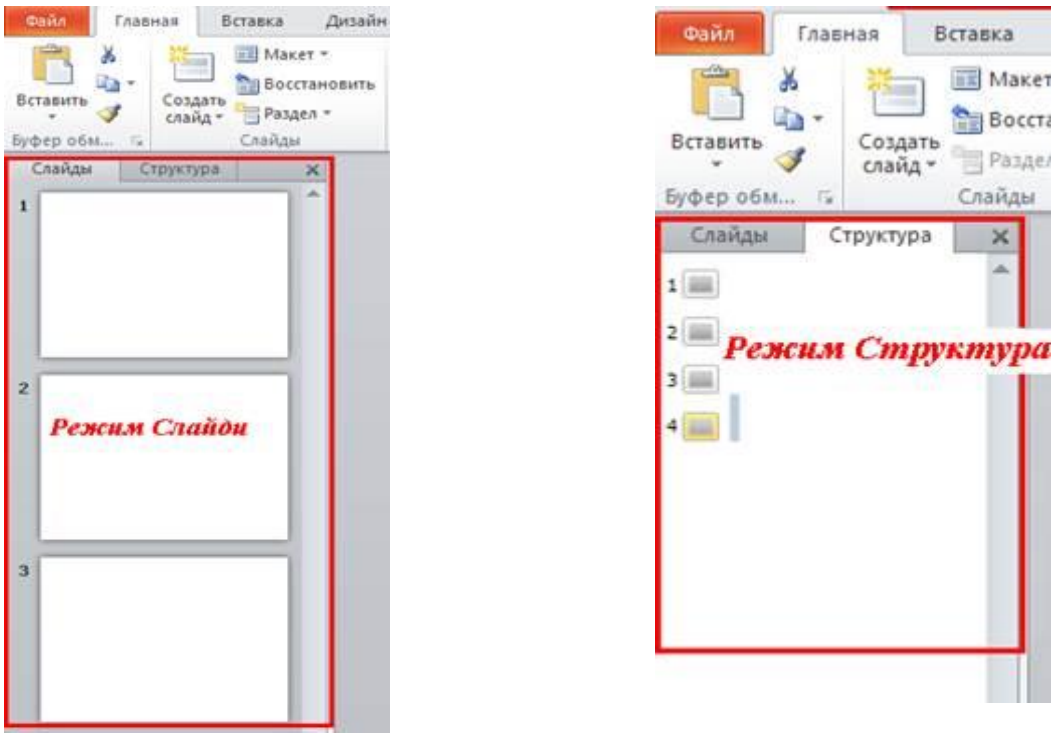


Рис. 6.7. Режими слайдів: Структура та Слайди

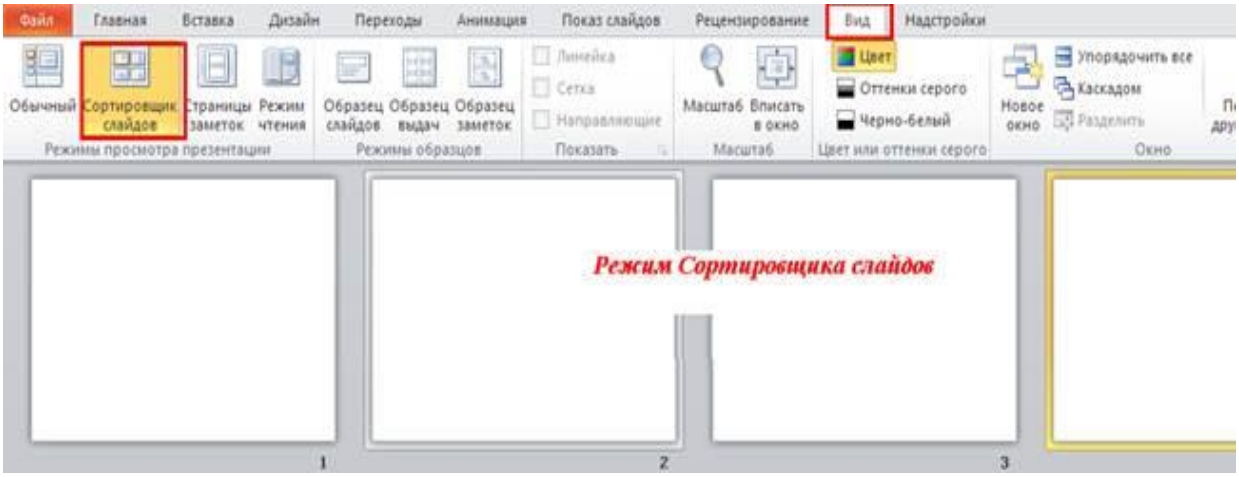


Рис. 6.8. Режим Сортировщика слайдов

6.4. Анімаційні ефекти. показ слайдів. налаштування дії

Слово анімація має прозору етимологію і буквально означає «оживлення».

Розглянемо поняття анімації в PowerPoint це видозміна об’єктів на слайді. Використання анімаційних ефектів надає презентації динамічності, а також може підкреслювати та акцентувати увагу слухача на основних та важливих інформаційних посилах презентації, дозволяють краще сприймати необхідну інформацію.

Анімаційні ефекти використовуються під час зміни слайдів або для появи та відображення об’єктів слайда.

Анімаційні ефекти зміни слайдів (переходи)

1. Анімаційний ефект під час переходу до наступного слайду активують шляхом натиснатискання вкладки *Переходы* групи *Переход к этому слайду* та вибравши потрібний перехід. Також, можна задати параметри ефектів переходів, а саме: справа, зверху, знизу, зліва, .. (кнопка *Параметры эффектов*).

Для визначенняти тривалісті кожного переходу між слайдами використовується кнопка *Длительность* вкладки *Переходы* групи *Время показа слайдов* (рис. 6.10):

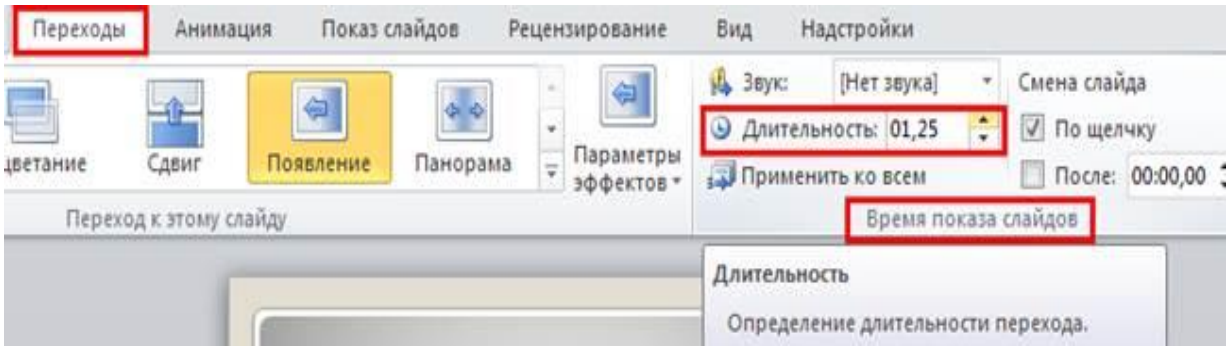


Рис. 6.10. Меню тривалісті переходів між слайдами

Анімація тексту й об’єктів

До будь-якого об’єкта слайда (тексту, рисунків, таблиць тощо) можна застосувати той чи інший анімаційний ефект.

Перед застосовуванням анімаційного ефекту, необхідно вибрати ті об’єкти, які будуть рухатись, запланувати порядок їх появи під час демонстрації, а також визначитись з тим, який саме анімаційний ефект буде застосований у процесі їх появи на слайді та під час виходу зі слайда.

Для додавання ефектів анімації до презентації необдно зробити наступні дії:

1. У звичайному режимі відкрийте слайд, до об’єктів якого потрібно застосувати анімацію.
2. Виберіть об’єкт, до якого потрібно застосувати анімацію.
3. У меню ***Анимация*** групи ***Анимация*** виберіть відповідну анімацію (рис. 6.11).

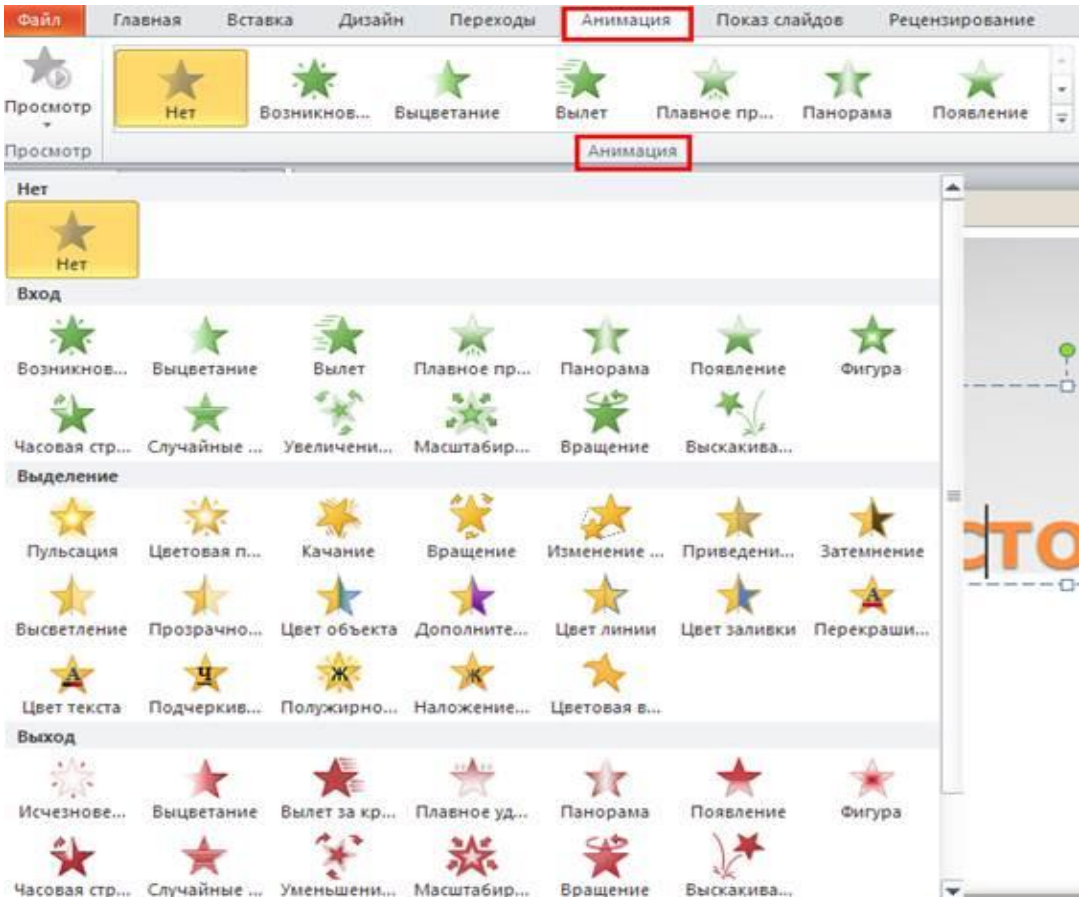


Рис. 6.11. Меню застосування анімації до об’єктів слайду

До обраної анімації можливо використовувати параметри ефектів, а саме: напрямок, послідовність, … . Це можна зробити використавши клавішу ***Параметры эффектов*** групи ***Анимация*** вкладки ***Анимация*** (рис. 6.12):

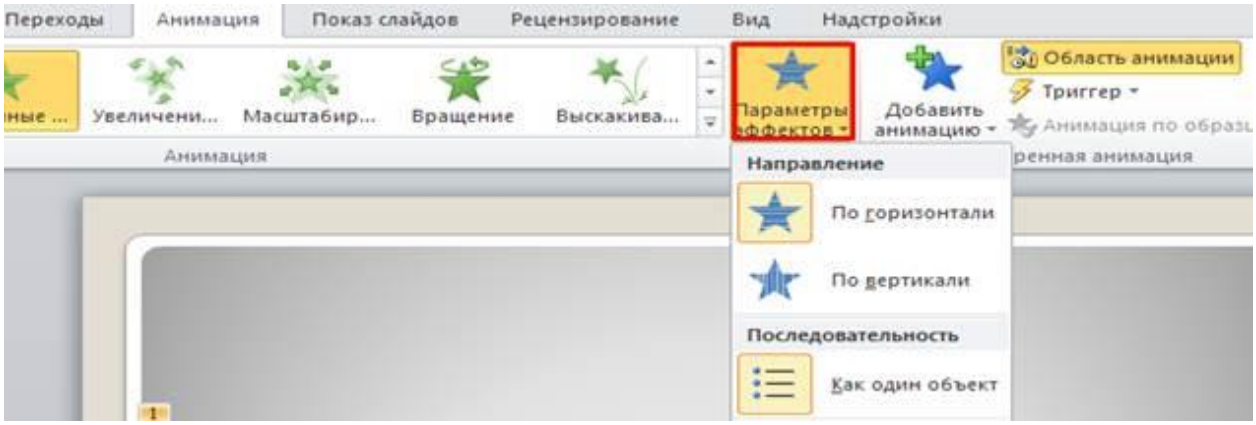


Рис. 6.12. Меню параметрів ефектів

Таким же чином для додавання анімації до об’єктів слайду застосовується кнопка ***Добавить анимацию*** (рис. 6.13). Можна застосовувати анімацію для появи об’єкта на слайді (***вход***), зникнення (***выход***), виділення (***выделение***), шляхів переміщення об’єкту (***пути перемещения***) (рис. 6.13):

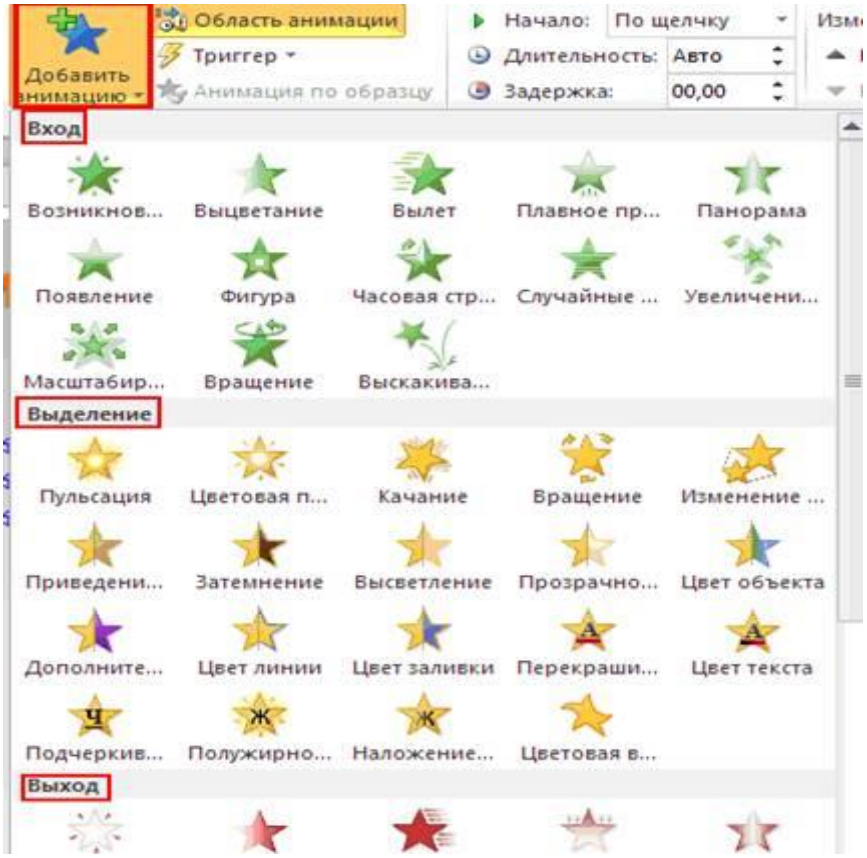


Рис. 6.13. Меню анімації до об’єктів слайду
з допомогою кнопки Добавить анимацию

Кнопка ***Область анимации*** вкладки ***Анимация*** застосовується для задання порядку відображення анімації на відповідних об’єктах.

Демонстрація презентації

Для демонстрації слайдів у меню ***Показ слайдів*** групи ***Начать показ слайдов*** вибраємо потрібну клавішу (рис. 6.14): ***С начала*** (або натиснути функціональну клавішу **F5**), ***С текущего слайда*** (або натиснути комбінацію клавіш **Shift + F5**), ***Широковещательный показ слайдов, Произвольный показ.***

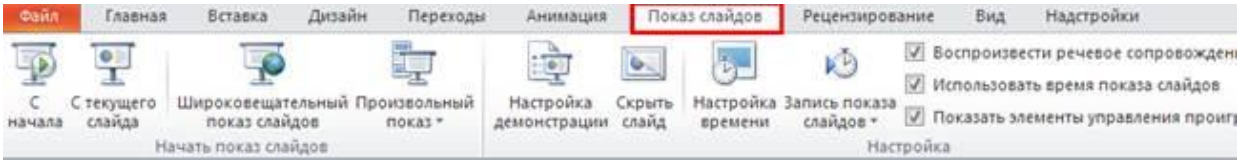


Рис. 6.14. Меню «Показ слайдів»

Для переходу від слайду до слайду також можна використовувати і клавіатуру: клавіша <Page Down> спричиняє перехід на наступний слайд, а клавіша <Page Up> – на попередній. Таку ж дію роблять клавіші стрілок або клавіші <N> (Next – наступний) і <P> (Previous – попередній). Клік по наявній в лівому куті кнопці також розкриває *Контекстне меню*, в якому можна вибрати потрібну команду (рис. 6.15).

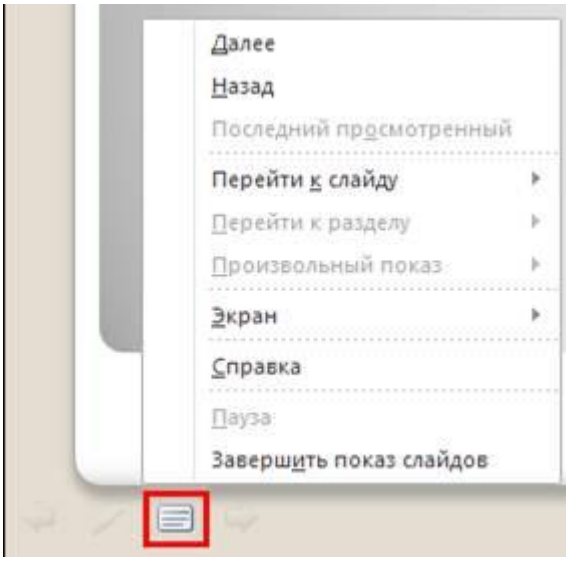


Рис. 6.15. Кнопка виклику контекстного меню в режимі показу слайдів

Контекстне меню дозволяє виконати під час показу слайдів усякого роду допоміжні дії. Меню застосовується для показу прихованих слайдів. Можна також перейти відразу до потрібного слайду за допомогою команди ***Перейти к слайду*** та вибрати потрібний слайд. Команда ***Перо*** (рис. 6.16) переводить мишу в режим малювання – тобто дає можливість зробити на слайді деякі необхідні позначки вже під час демонстрації презентації – наприклад, підкреслити або обвести ключове поняття або іншим чином виділити потрібний фрагмент слайду і навіть зробити додатковий напис. А активація клавіші <**Esc**> або щиглик мишею на останньому слайді завершують показ слайдів. Використовується можливість закінчення демонстрації презентації спеціальним порожнім слайдом або слайдом з будь-якою заставкою і завершуючим написом.

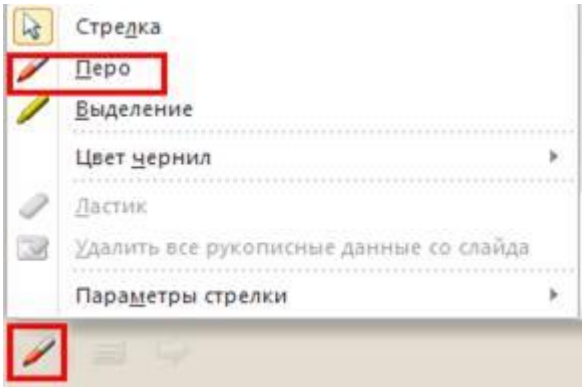


Рис. 6.16. Кнопка Пера під час показу слайдів

Застосування ефекту «Прихований слайд» під час показу слайдів

Слайд презентації можна призначати як «прихований» за допомогою вкладки ***Показ слайдов*** **групи** ***Настройка*** **кнопкою** ***Скрыть слайд*** (рис. 6.17).

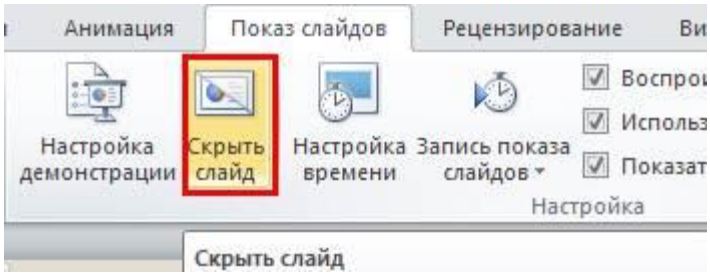


Рис. 6.17. Меню Прихованого слайду

У меню **Слайди** такі слайди позначаються перекресленим номером слайда. Такі слайди не виводяться на екран за звичайного перегляду презентації. Для показу цих слайдів в процесі презентування необхідно вибрати в контекстному меню **Перейти до слайда** у запропонованому списку прихований слайд. Номери прихованих слайдів відображаються в круглих дужках (рис. 6.18). Використовуючи цей ефект можемо розробити додаткові матерали для презентації, які можуть бути продемонстровані або пропущені під час презентування. Прихований слайд залишається у файлі, навіть якщо він був прихованим під час показу презентації.

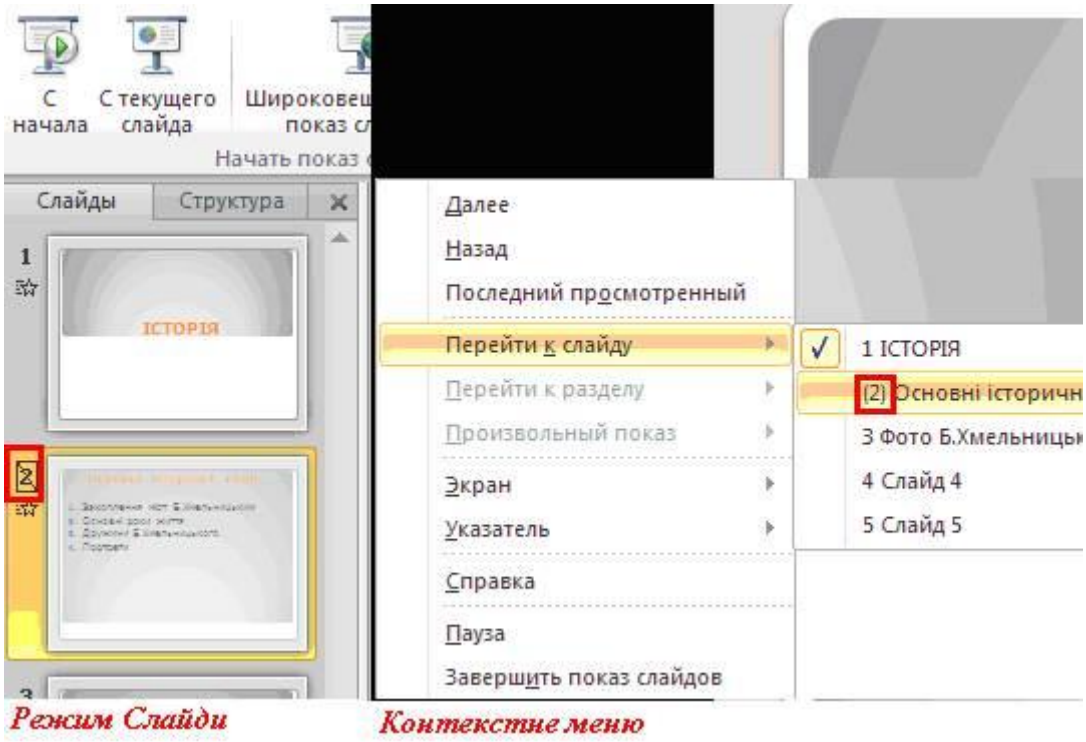


Рис. 6.18. Меню прихованих слайдів у режимі Слайди

Для відновлення прихованих слайдів використовується контекстне меню на цьому слайді, на якому необхідно вибрати повторно команду ***Скрыть слайд*** (рис. 6.19).

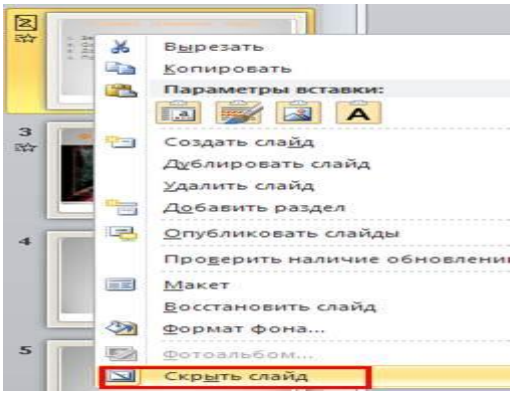


Рис. 6.19. Кнопка Приховати слайд

Широкоекранний показ слайдов

Він використовується для демонстрації слайдів віддаленим глядачам, які використовують для перегляду веб-браузер. Для цього у меню ***Показ слайдов*** групи ***Начать*** *показ слайдов* натисніть клавішу ***Широковещательный показ слайдов***.У діалоговому вікні, що відкриється вибираємо команду ***Начать широковещательный показ*** та у наступному вікні, що з'явиться ввести адресу своєї електронної пошти та пароль для трансляції (рис. 6.20).

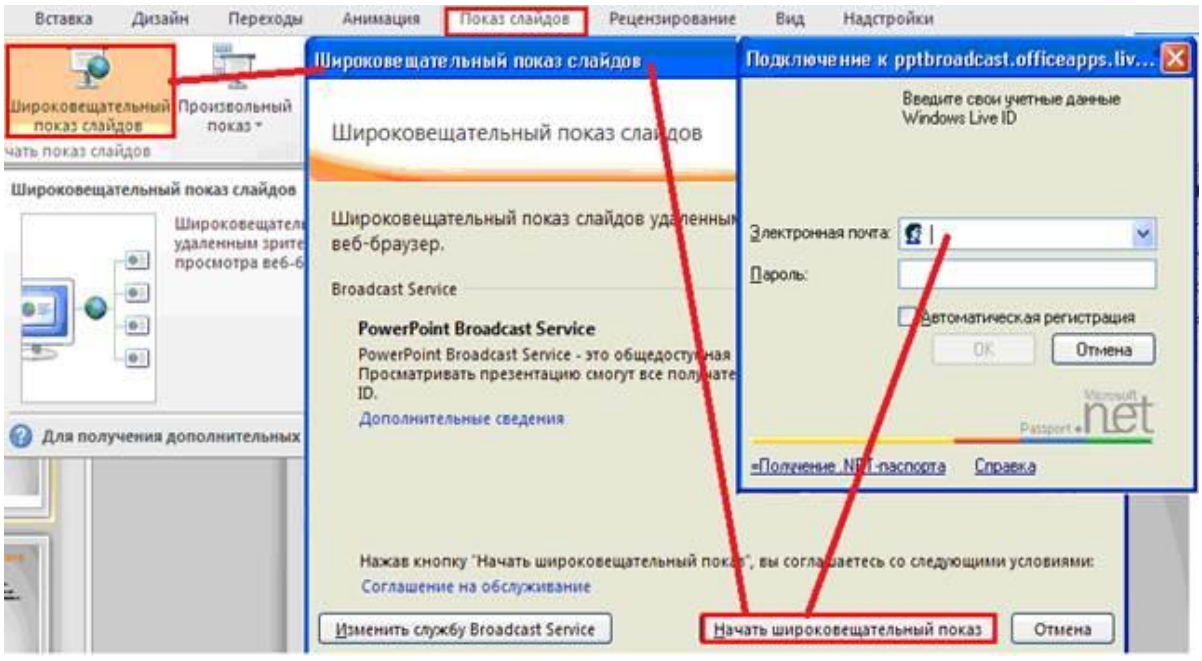


Рис. 6.20. Режим показу Широковещательный показ слайдов

Довільний показ слайдів

Одну й ту саму презентацію можна налаштувати для різних аудиторій, створивши довільні покази. Довільний показ – це слайди, що згруповані у презентацію, які можна демонструвати незалежно від

усього показу, або групи слайдів у презентації, на які створено гіперпосилання.

Для визначення довільного показу необхідно зробити наступні дії:

1. У меню ***Показ слайдів*** групи ***Начать показ слайдов*** виберіть клавішу ***Произвольный показ*** та у вікні, що з'явиться, натисніть клавішу ***Создать***.

2. У вікні ***Задание произвольного показа*** в області ***Слайды презентации*** виберіть слайди, які потрібно додати до запланованого довільного показу, і натисніть клавішу ***Добавить***. Додані слайди можна вилучати зі списку, виділивши їх та натиснувши на клавішу ***Удалить***.

3. Для виділення декількох слайдів використовується натиснута клавіша **Ctrl**, утримуючи яку, по черзі вибераються необхідні слайди.

4. Дя зміни порядку демонстрації слайдів, активуйте слайд у списку ***Слайды произвольного показа*** та перемістіть його у списку вгору або вниз, натиснувши відповідну стрілку.

5. Введіть ім'я в полі ***Имя произвольного показа*** та натисніть клавішу **ОК**.

6. Для створення наступних довільних показів, які містять вибрані слайди з презентації, повторіть кроки з 1 по 5.

Розглянемо можливість створення ***рукописних приміток під час демонстрації презентації***

Підтримка рукописних даних надає такі можливості:

– створення нотаток і позначення певних місць на слайдах, що буде видно аудиторії під час проведення презентацій та дозволить звернути увагу на необхідний об'єкт;

– повторне використання рукописних нотаток із щоденника Microsoft Windows;

– внесення рукописних позначок до презентацій Microsoft PowerPoint та їх редагування;

– створення рукописних чернеток слайдів і документів;

– надсилання рукописних повідомлень електронною поштою.

Уведення рукописних позначок під час демонстрації презентації

Упродовж показу презентації можна робити позначки від руки в будь-якому місці слайда за допомогою пера або миші, змінивши вказівник на ручку або інструмент виділення на панелі інструментів *Показ слайдів*.

Задля стварення рукописних приміток під час демонстрації презентації потрібно:

1. На панелі інструментів ***Показ слайдів***, що з'являється в режимі

показу слайдів у лівому нижньому кутку, клацніть стрілку вказівника (або під час презентації скористайтеся контекстним меню, що викликається натисканням правої кнопки миші). Виберіть ***Цвет чернил*** та команду ***Перо*** або ***Выделение*** (рис. 6.21).

2. Необхідно ввести рукописні дані на слайді за допомогою пера або миші.

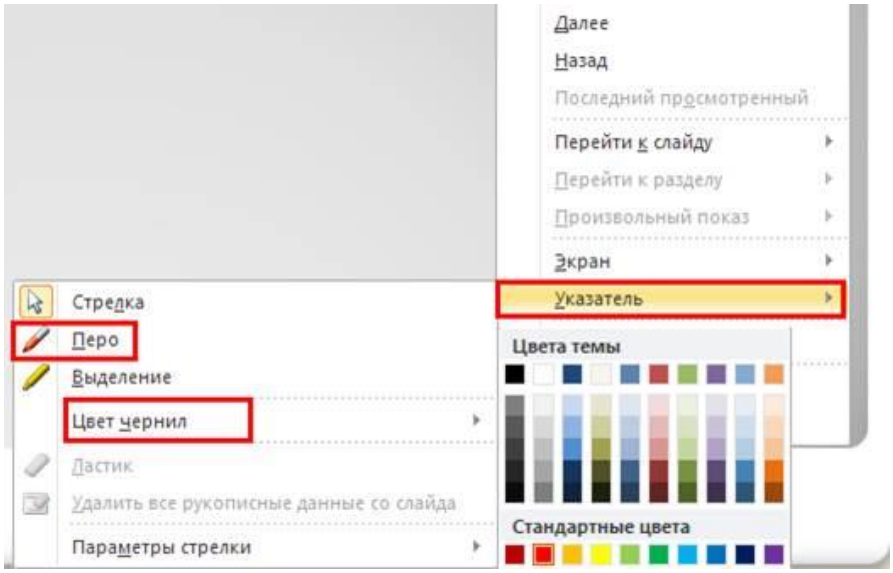


Рис. 6.21. Меню рукописних приміток

Вилучення рукописних даних

1. На панелі інструментів ***Показ слайдів*** клацніть стрілку вказівника, а потім виберіть пункт ***Гумка (Ластик)***.

2. Протягніть гумку по рукописних даних, які потрібно вилучити (рис. 6.22).

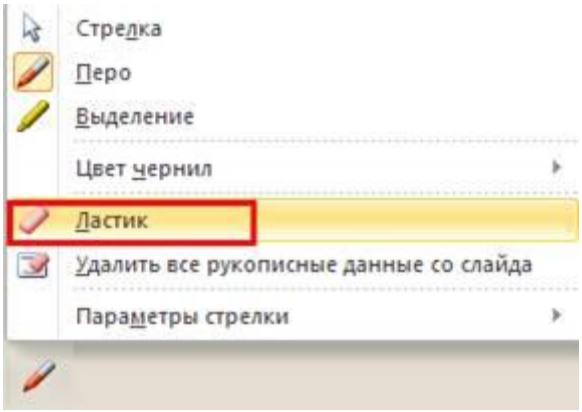


Рис. 6.22. Кнопка «Гумка»

Для переходу на інший слайд, не виходячи з режиму рукописного введення, натисніть одну із кнопок переходу зі стрілками (назад, вперед) на панелі інструментів *Показ слайдів*.

Якщо протягом показу презентації було додано рукописні дані під час закриття показу слайдів виводиться запит про збереження або вилучення доданих рукописних даних. У разі вибору вилучення рукописних даних, вони не зберігаються і відновити їх неможливо.

У разі збереження рукописних даних, вони будуть доступні під час редагування презентації в режимах ***Обычный***, ***Сортировщик слайдов*** та наступній демонстрації презентації в режимі ***Показ слайдів***.

Налаштування дії (демонстрація)

Демонстрація активується командою вкладки ***Показ слайдов*** групи ***Настройка*** кнопкою ***Настройка демонстрации*** (рис. 6.23), де можна задавати *режими показу слайдів* (автоматичний або що керується доповідачем), налаштовувати *параметри показу* (з анімацією або без неї, з звуковим супроводом або ні, неперервний показ або ні), *показ слайдів* (усіх, або вибрати з … по …), *зміна слайдів* (вручну, за часом):

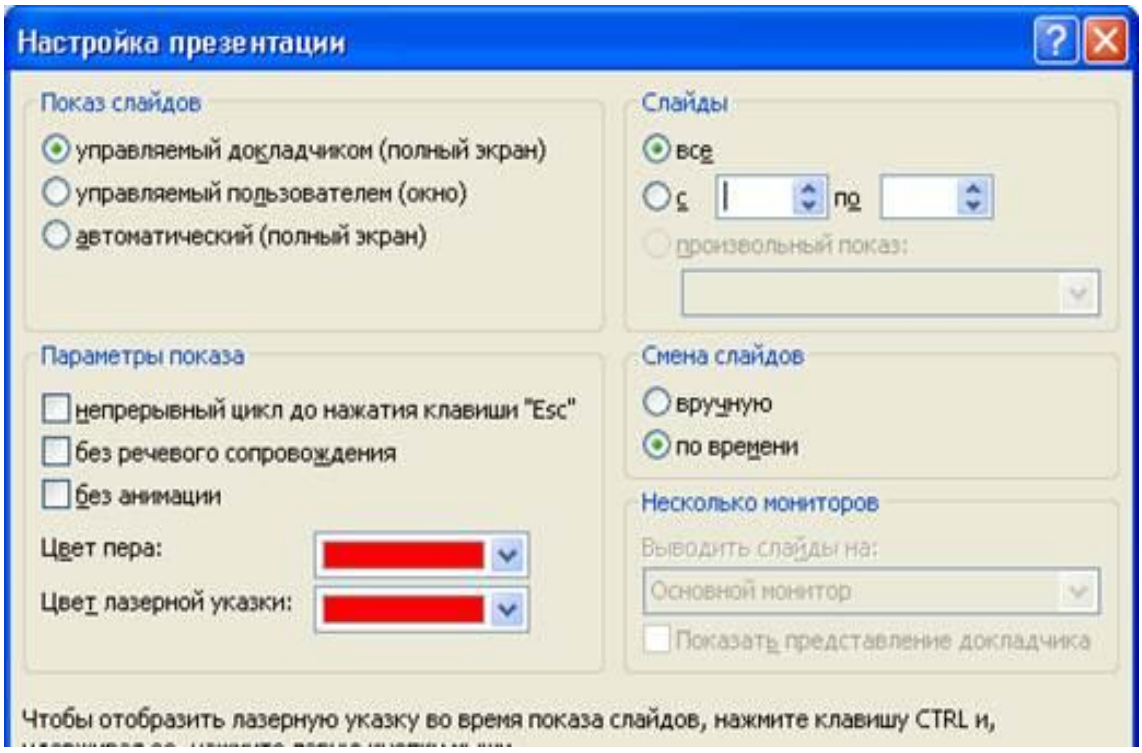


Рис. 6.23. Налаштування демонстрації

Також використовується команда ***Настройка времени*** презентації, що знаходиться на меню ***Показ слайдов*** (рис. 24).

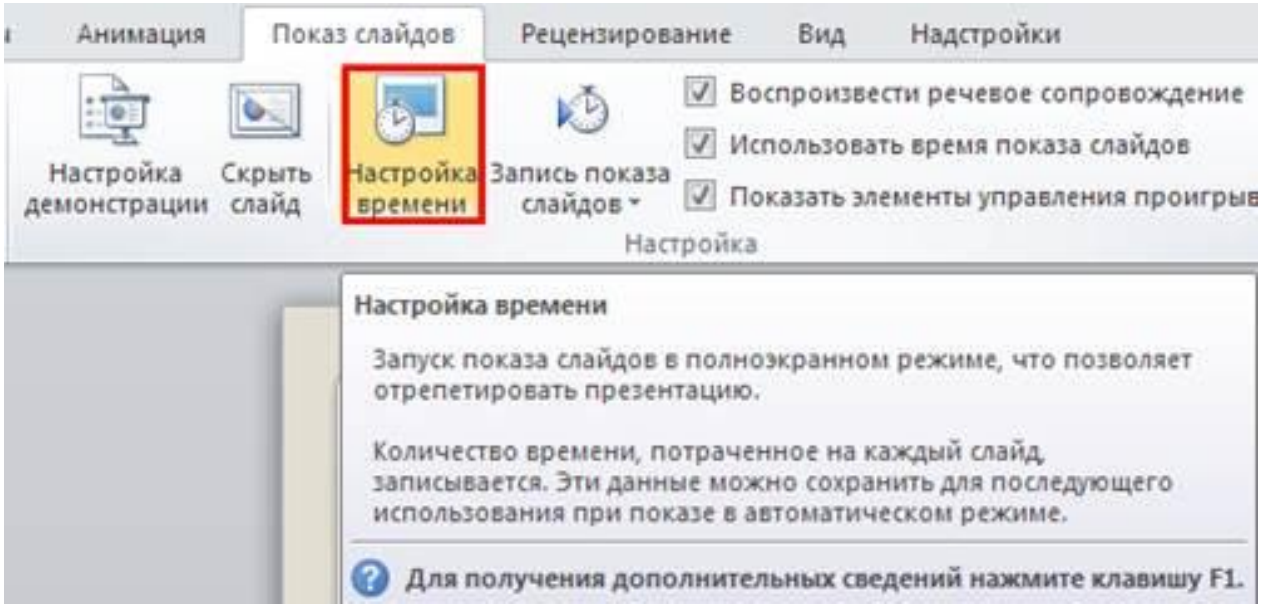


Рис. 6.24. Налаштування часу

Під час настроюваннянеобхідно робити щиглик лівою кнопкою миші в розрахованому для показу темпі. Цей темп буде збережено у процесі автоматичного показу надалі (рис. 6.25).

Рис. 6.25. Задання часу у режимі показу слайдів

Після настроювання часу вибираємо автоматичний режим показу слайдів за допомогою кнопки ***Настройка демонстрации***: вкладка ***Показ слайдов*** групи ***Настройка*** (рис. 6.25).

6.5. Графіка, аудіо- й відеооб’єкти в мультимедійних презентаціях

Імпорт інформації і об’єктів

Для введення інформаціїі та об’єкт у слайд,насамперед, потрібно вибрати необхідний макет до слайду. Для цього натискаємо у меню ***Главная*** групи ***Слайды*** меню ***Макет*** та активуємо необхідий макет, наприклад, ***Заголовок и объєкт*** (рис. 6.26).

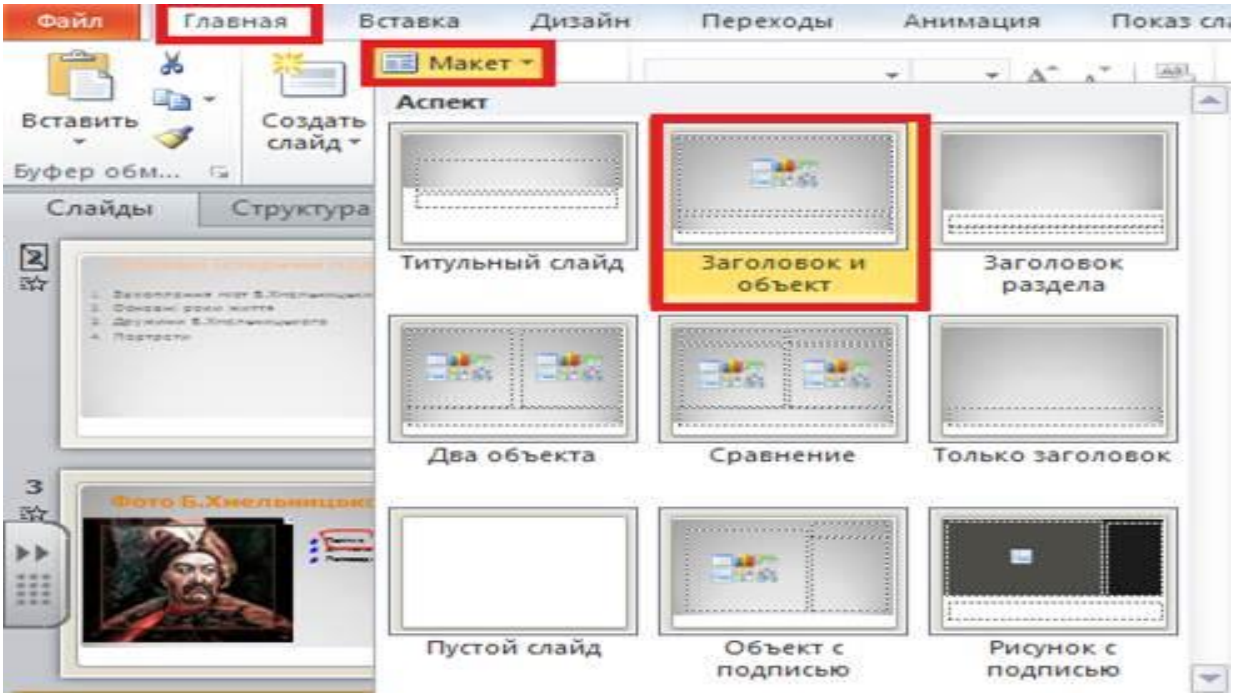


Рис. 6.26. Опис активації макету слайду для об’єктів

У разі необхідності рамку для заголовку слайду можна видалити шляхом її виділення та натиснувши клавішу **<Delete>.**

Додавання об’єкта WordArt

У якості заголовків слайдів рекомендуємо використовувати фігурний текст WordArt. Для виконання активуємо меню ***Вставка*** групи ***Текст*** натискаємо клавішу ***WordArt*** та вибраємо шаблон (рис. 6.27).

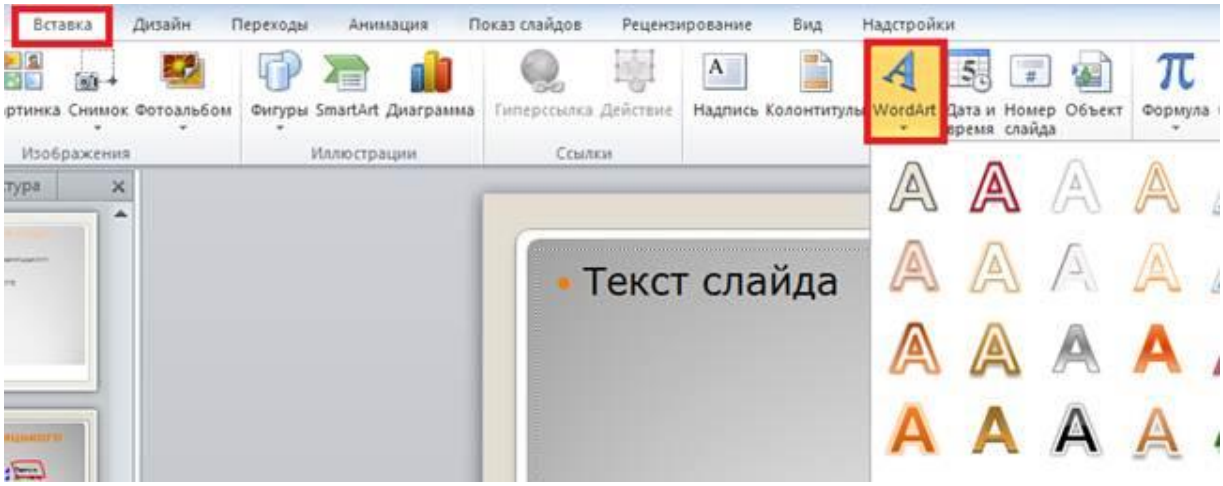


Рис. 6.27. Приклад додавання об’єкта WordArt

Далі з об’єктом ***WordArt*** можна виконувати наступні дії за допомогою меню ***Формат***, а саме: можна змінювати заливку і контур фігури, використовувати ефекти фігур, заливку і контур тексту, використовувати текстові ефекти, переміщувати вперед і назад, вирівнювати, повертати і т.д.

Так само додаються з меню ***Вставка*** різноманітні фігури (рис. 28), надписи (рис. 6.29), малюнки (рис. 6.30).

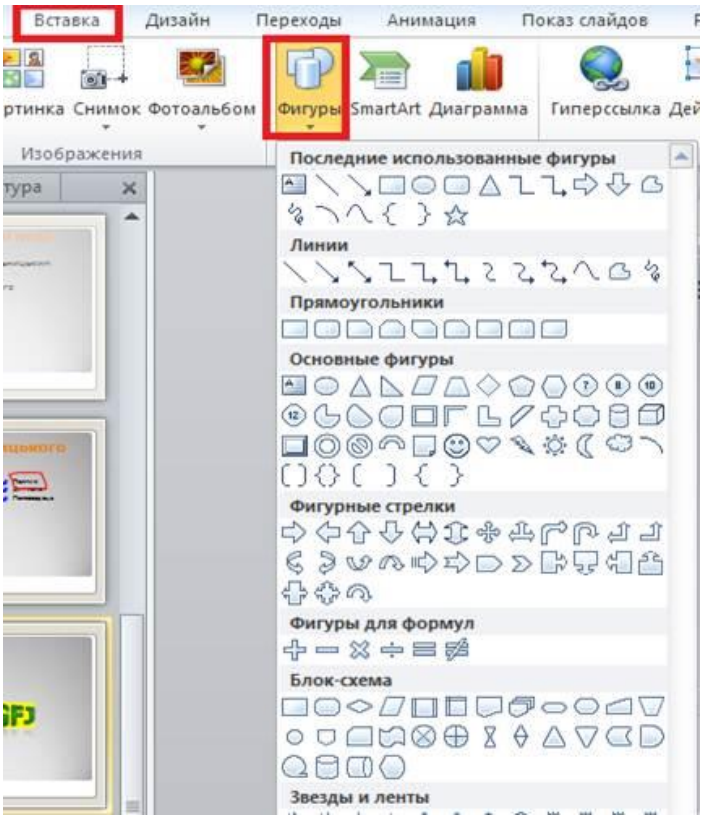


Рис. 6.28. Приклад додавання фігур до слайдів презентації

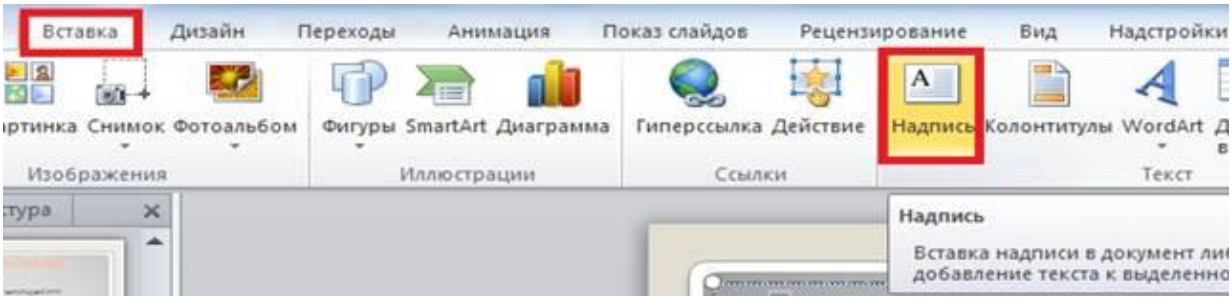


Рис. 6.29. Додавання надписів до слайдів презентації

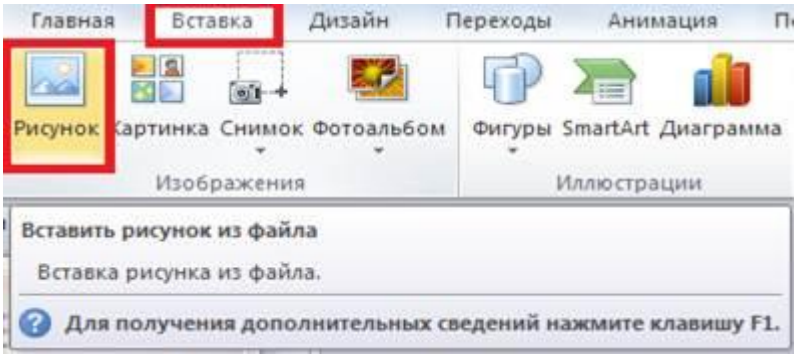


Рис. 6.30. Приклад додавання малюнків до слайдів презентації

Розглянемо процес додавання картинок. Длядодавання графічного об’єкту (картинки з колекції Microsoft Office або додані з мережі Інтернет чи будь-якого носія інформації), вибираємо у меню ***Вставка*** групи ***Изображения*** клавішу ***Картинка*** (рис. 6.31).

Кліпи можна швидко та легко знаходити за допомогою меню **Картинки/Колекція кліпів**.

Колекція кліпів (Microsoft) містить малюнки, фотографії, звуки, відео й інші мультимедійні файли.

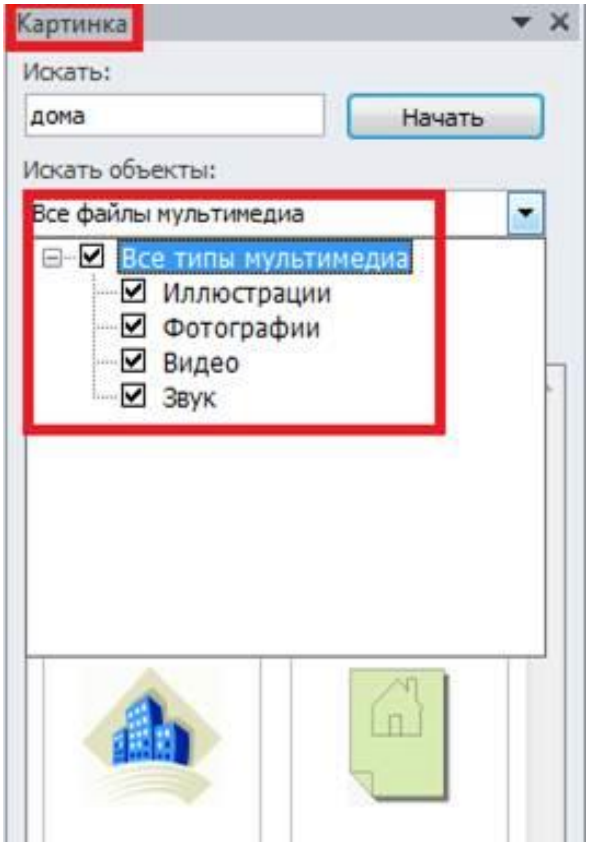


Рис. 6.31. Приклад додавання картинки із колекції кліпів

Далі розглянемо процес додавання таблиці у слайд, для цього слід виконати наступні дії: вибрати необхідний макет до слайду, потім активувати кнопку ***Вставить таблицу*** та вибрати відповідну розмірність даної таблиці (кількість стовпців та рядків таблиці) (рис. 6.32).

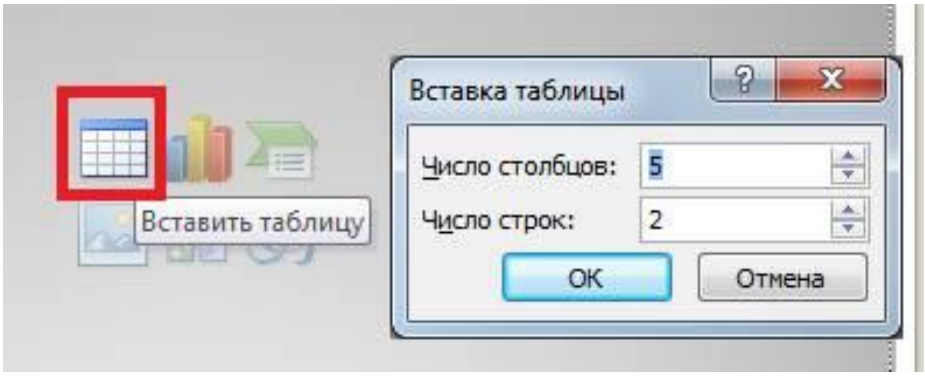


Рис. 6.32. Приклад додавання таблиці до слайдів презентації

Додавання діаграм

Для цього вибираємо необхідний макет до слайду, далі натискаємо кнопку діаграми, після чого з'явиться вікно вставки діаграми (рис. 6.33).

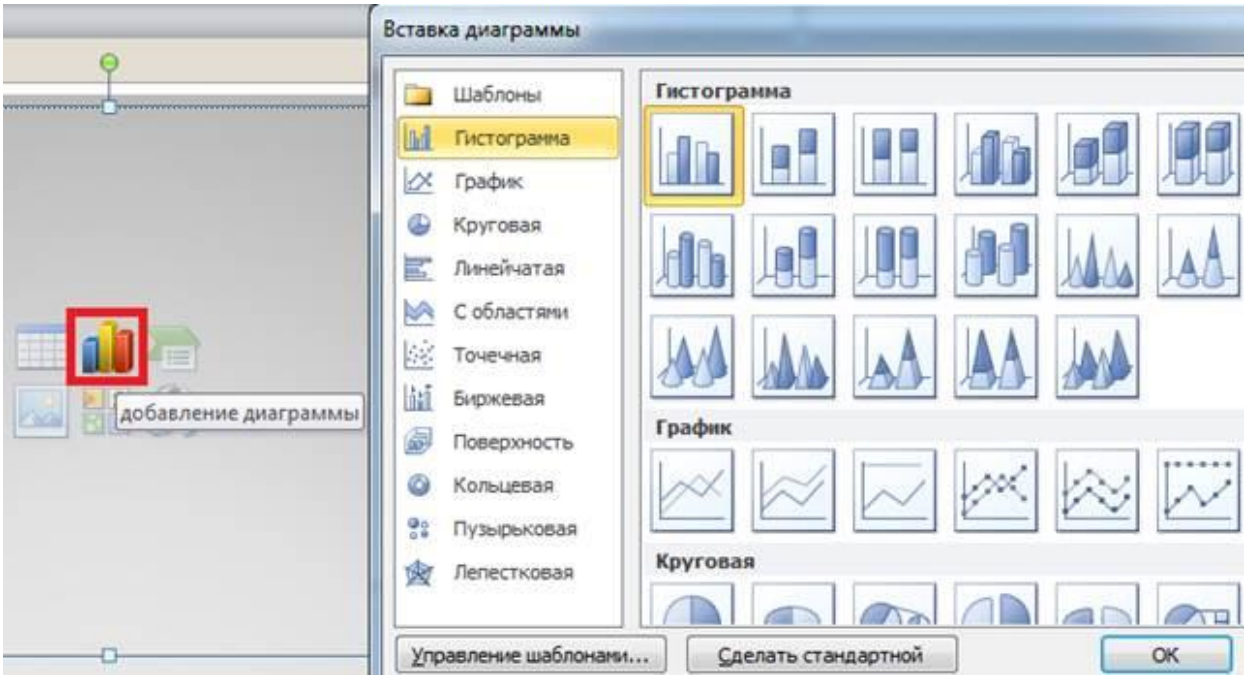


Рис. 6.33. Процес додавання діаграми до слайдів презентації

Після цього потрібно У меню, що з'явилося, слід вибрати тип діаграми, що активує меню таблиці даних (Excel) та область самої діаграми. У вікні таблиці даних потрібно вставити дані вашої діаграми, що автоматично відобразяться в області діаграми.

Змінювання типу діаграм, даних діаграм і т.д. здійснюється за допомогою меню ***Конструктор***.

З допомогою меню ***Макет*** існує можливість роботи з назою діаграми, осі, змінювати дані легенди діаграми, підписувати дані, осі, виконувати необхідні дії з таблицею даних, сіткою, фоном, і т.д.

Розглянемо порядок дій із додавання об'єктів ***SmartArt*** до слайдів презентації. Для цього вибраємо необхідний макет, далі натискаємо кнопку об'єкта ***SmartArt***, з'являється вікно ***Выбор рисунка SmartArt***, у якому вибраємо необхідний тип об'єкта SmartArt (рис. 6.34).

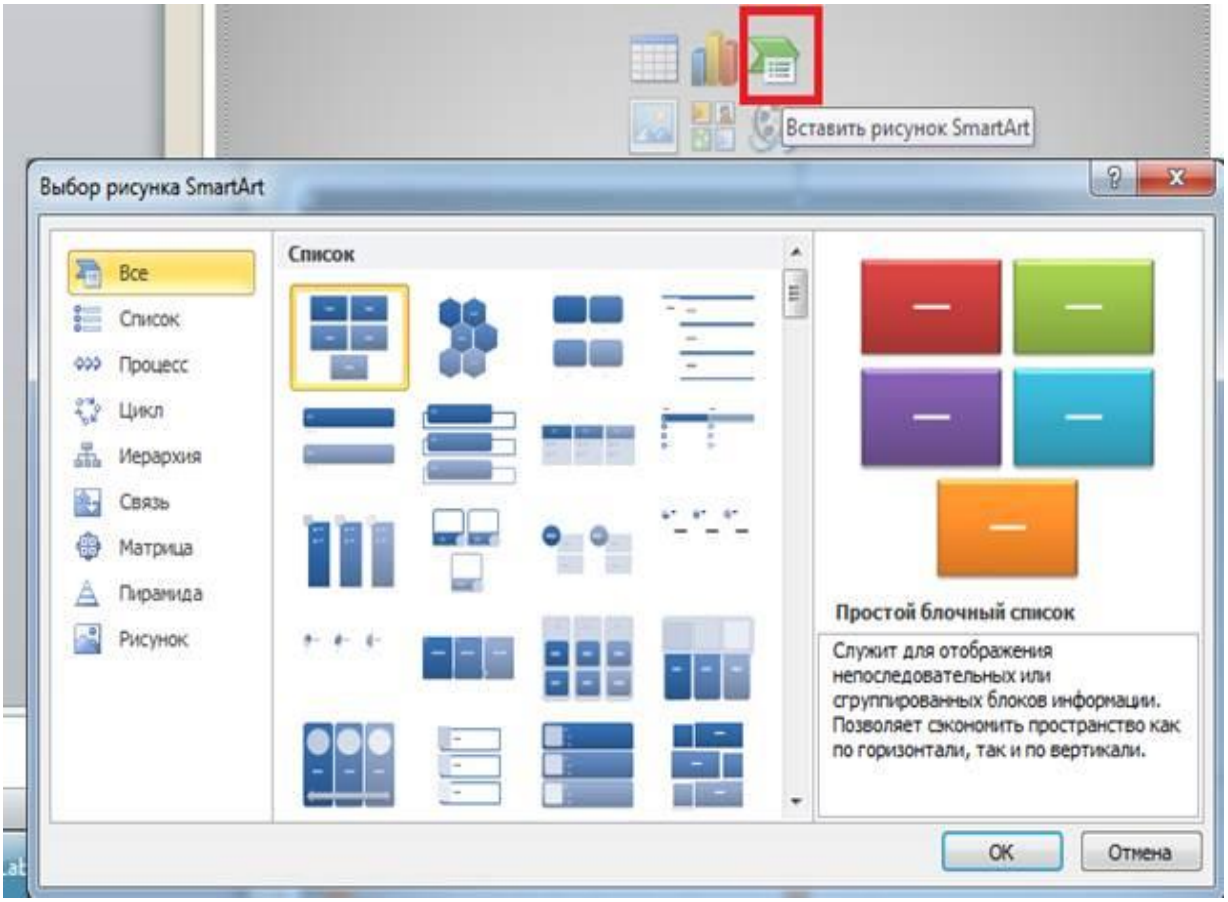


Рис. 6.34. Приклад додавання *об'єктів SmartArt* до слайдів презентації

Взагалі, з об'єктами *SmartArt* можна виконувати такі дії, як додавання фігури, змінювати макет, видозмінювати напрям справа наліво, здійснювати переміщення відповідної фігури донизу чи вгору, змінювати колір, друкувати текст у середині фігури, форматувати текст та ін.(рис. 6.35).

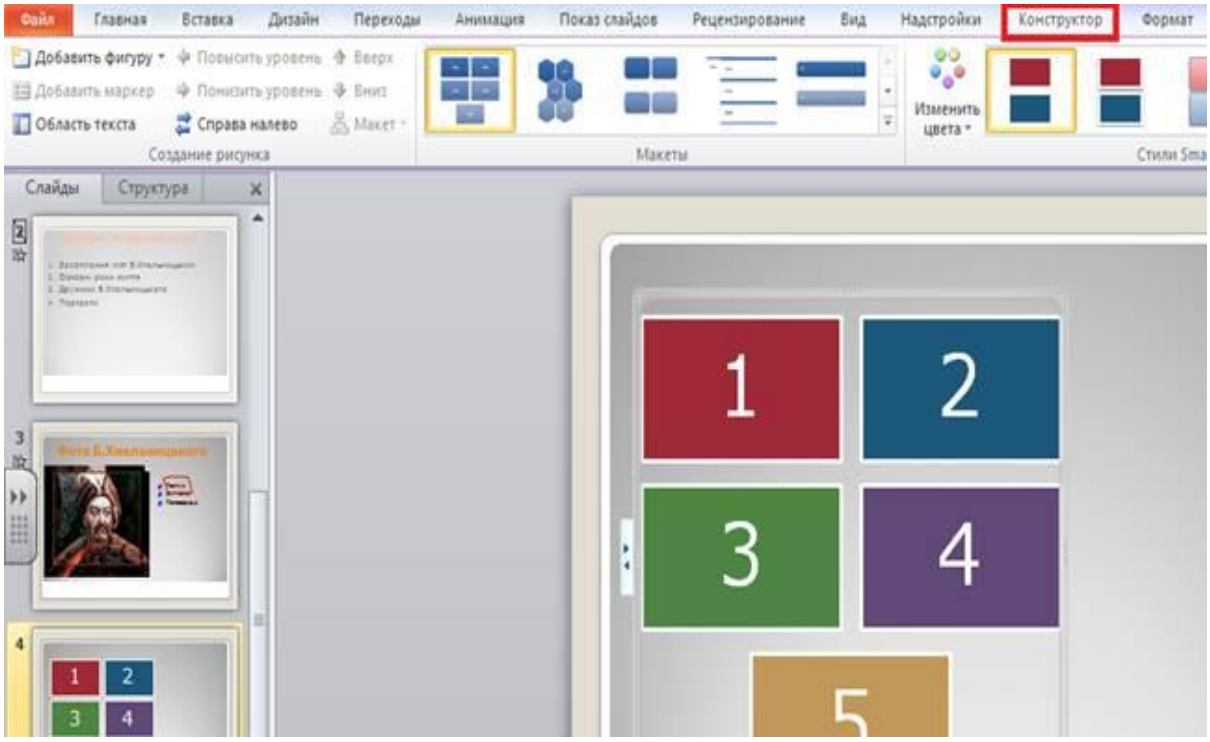


Рис. 6.35. Приклад використання вкладки Конструктор
для редагування об’єкта SmartArt

Групування об’єктів

Для групування об’єктів, що складаються з різних фігур, створених за допомогою вкладки ***Вставка*** кнопкою ***Фигуры*** виникає потреба їх згрупування. Для цього потрібно виконати наступні дії:

1. Виділіть об’єкти, які необхідно згрупувати. Натисніть клавішу Ctrl і не відпускаючи її клацніть на всіх об’єктах, що мають бути згруповані.
2. У меню ***Формат*** натисніть клавішу ***Группировать*** і виберіть команду ***Группировать*** (рис. 36).

Для розгрупування об’єктів необхідно виділити групу, яку необхідно розгрупувати, у меню ***Формат*** натисніть клавішу ***Группировать*** та виберіть команду ***Разгруппировать*** (рис. 6.36).

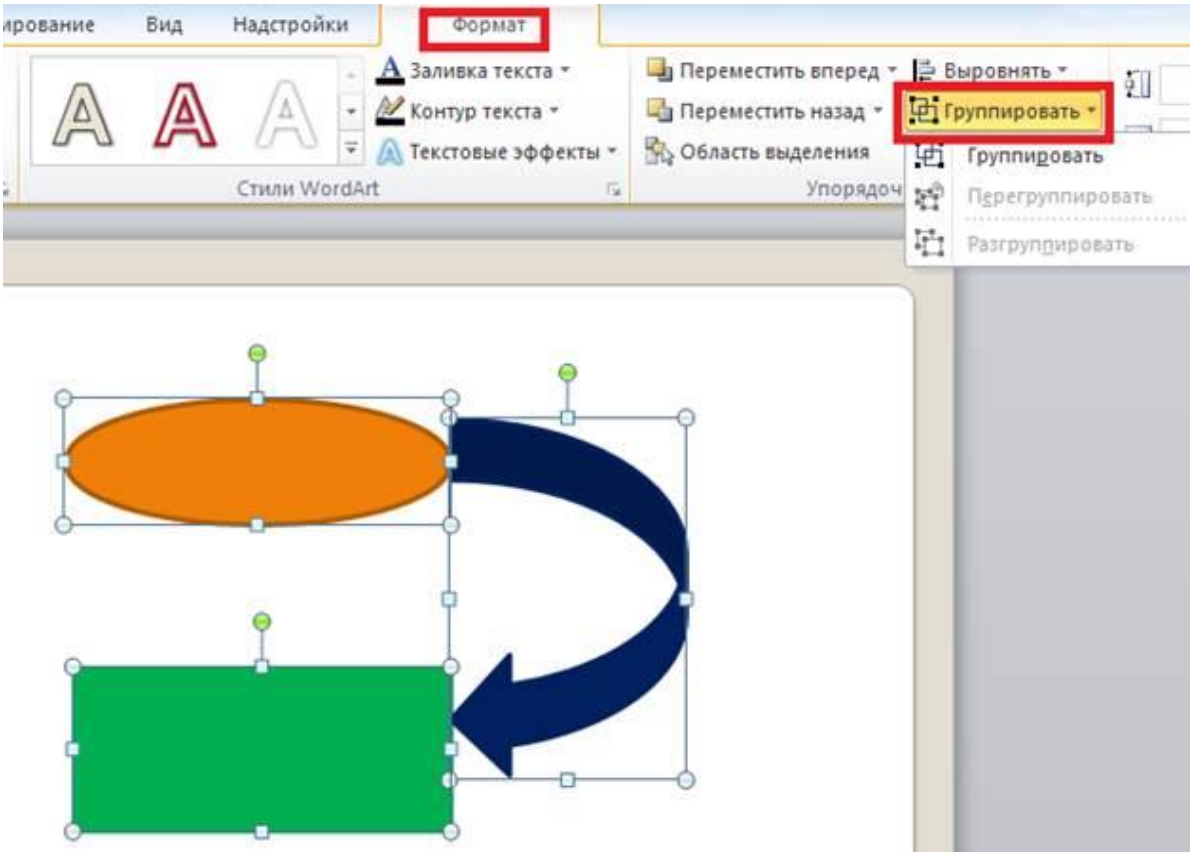


Рис. 6.36. Приклади групування та розгрупування об’єктів

До слайду можна вводити текст до рамки для тексту, а фотокартки – додавати- в рамку для об’єкту. Після чого введені елементи як об’єкти будуть розсунуті по полю слайду.

Озвучення слайдів

Існує декілька способів додавання звуків із файлів. У меню **Вставка** групи ***Мультимедиа*** натисніть кнопку ***Звук*** та виділяємо команду ***Звук из файла*** (рис. 6.37), обираємо потрібну папку, де розміщені звукові файли.

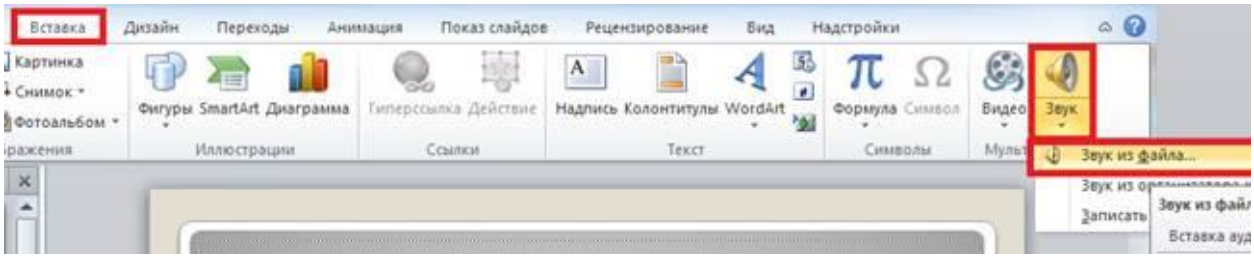


Рис. 6.37. Приклад додавання звуку з файлу

Наступним способом додавання звуків є використання організатора кліпів. У меню ***Вставка*** групи ***Мультимедиа*** натисніть клавішу ***Звук*** та виберіть команду ***Звук из организатора клипов***. (рис. 37). У підменю, що з'явиться, вводимо ключову інформацію для пошуку звуку.

Для запису звуку у меню ***Вставка*** групи ***Мультимедиа*** натисніть клавішу ***Звук*** та виберіть команду ***Записать звук***. З'явиться вікно звукозапису (рис. 37). Там потрібно натиснути клавішу *Запись* (червоний кружечок) та записати виголошений звук (у мікрофон). Наприкінці натиснути клавішу ***Стоп*** (чорний квадратик). Можна прослухати, що вийшло, в разі задовільного результату натискаємо кнопку ***ОК***.

Для додавання універсальних звуків PowerPoint *у* меню ***Переходы*** групи ***Время показа слайдов*** натисніть клавішу ***Звук*** та виберіть відповідний вид звуку, можна обрати тип ***непрерывно*** (рис. 6.38).

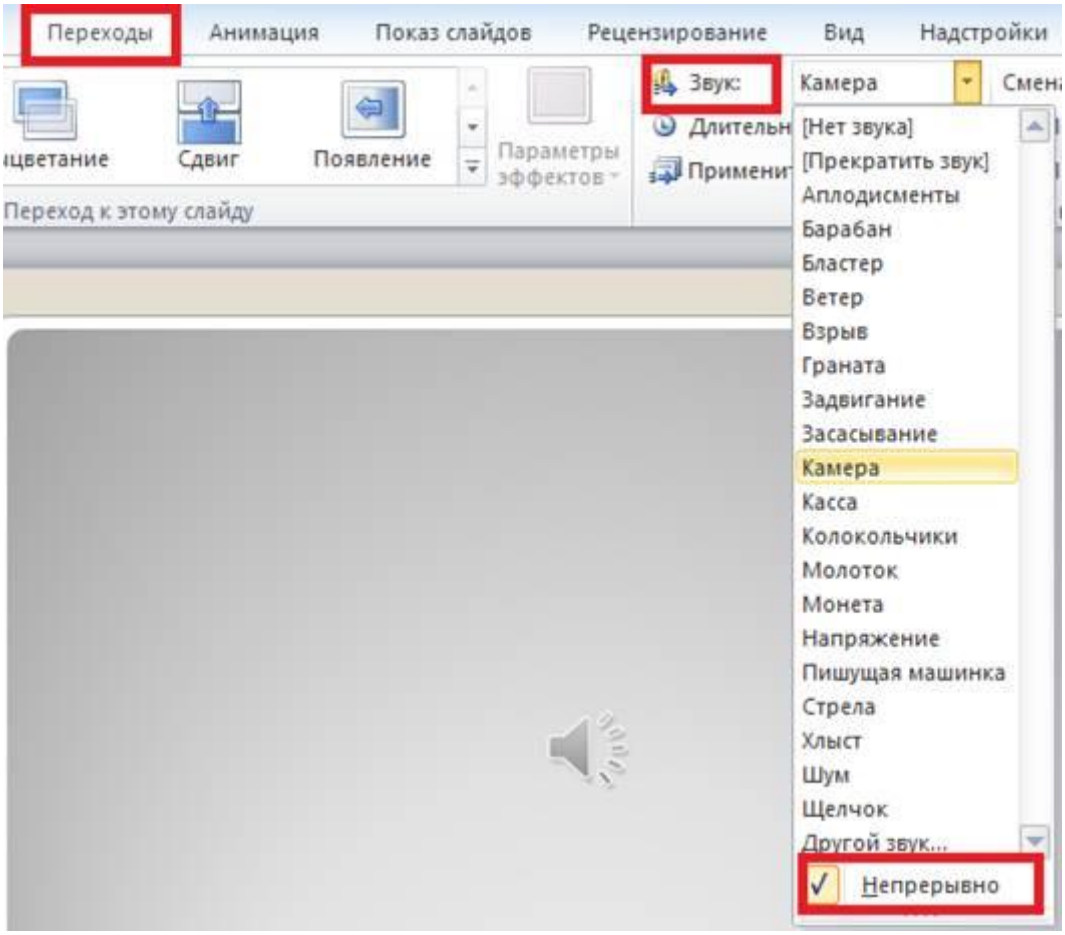


Рис. 6.38. Приклад додавання універсальних звуків PowerPoint

Додавання відео

Програма PowerPoint має можливість використовувати у презентаціях відеокліпи різних форматів.

Існує декілька способів додавання відеоматеріалів до презентацій. Для додавання відео з оболонки PowerPoint необхідно *у* меню ***Вставка*** групи ***Мультимедиа*** активувати клавішу ***Видео*** та перейти до пункту ***Видео из организатора клипов*** (рис.6.39).

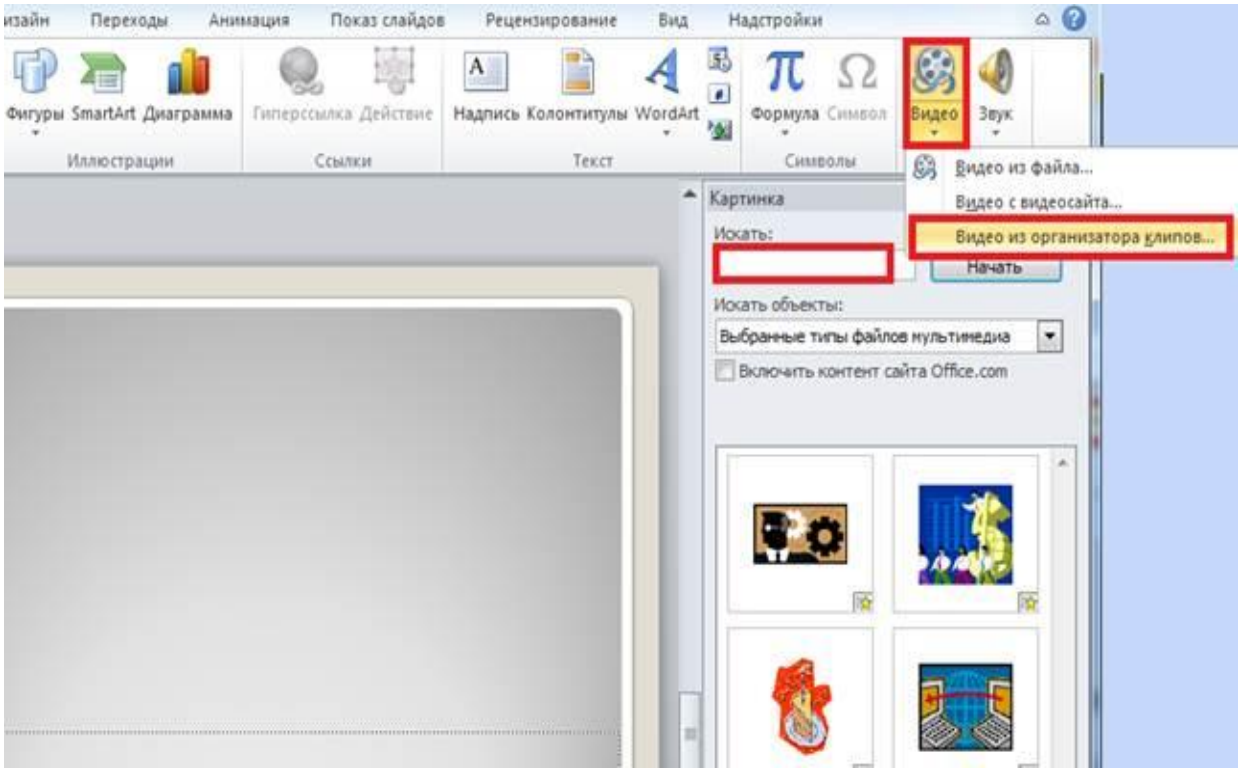


Рис. 6.39. Приклад додавання відеокліпу (відео PowerPoint)

Для додавання відео з веб-сайта необхідно виконати наступні дії – меню ***Вставка*** групи ***Мультимедиа*** натисніть клавішу ***Видео*** та виберіть команду ***Видео с видеосайта*** (рис. 39). Так само для *додавання відео з будь-якого файлу* виберемо команду ***Видео из файла*** та завантажуємо у презентацію.

Процес додавання відеокліпу та його необхідні налаштування виконуються аналогічно діям зі звуковим кліпом.

6.6. Інтерактивність мультимедійної презентації. Формати збереження та упаковка слайдів

Додавання гіперпосилань

Для інтерактивності презентації використовуються вставки гіперпосилань. За їх допомогою можна організовувати переходи на визначений файл, документ або слайд, який може знаходитись, як на комп'ютері, так і у мережі Інтернет.

Для додавання гіперпосилання, необхідно виконати наступні дії:

– Виділити об'єкт, за яким буде закріплено гіперпосилання (наприклад, фрагмент тексту (слово), рисунок або вставлена фігура).

– Виконати команди: вкладка Вставка групи Ссылки кнопка Гиперссылка (рис.6.40) або викликати контекстне меню та вибрати команду Гиперссылка (рис. 6.41).

– Вибрати потрібний тип гіперпосилання та необхідні параметри, що описані далі.

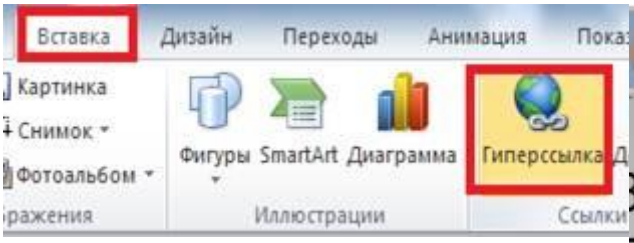


Рис. 6.40. Приклад додавання гіперпосилання з допомогою вкладки Вставка

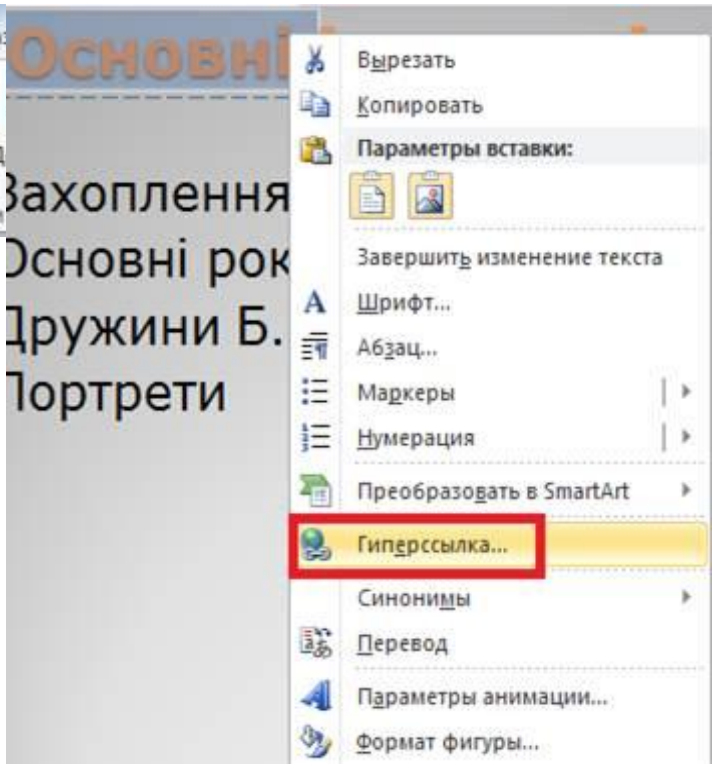


Рис. 6.41. Приклад додавання гіперпосилання з допомогою контекстного меню

Для побудови гіперпосилання на файл або веб-сторінку, необхідно:

– У вікні ***Вставка гиперссылки*** натиснути значок *Связать с* ***файлом, веб-страницей***.

– У списку папок вибрати папку (у нашому випадку Рабочий стол), де знаходиться необхідний файл, та виділити ім'я файла або увести URL-адресу сайту, на який створюється гіперпосилання, наприклад: www.google.com (рис. 6.42).

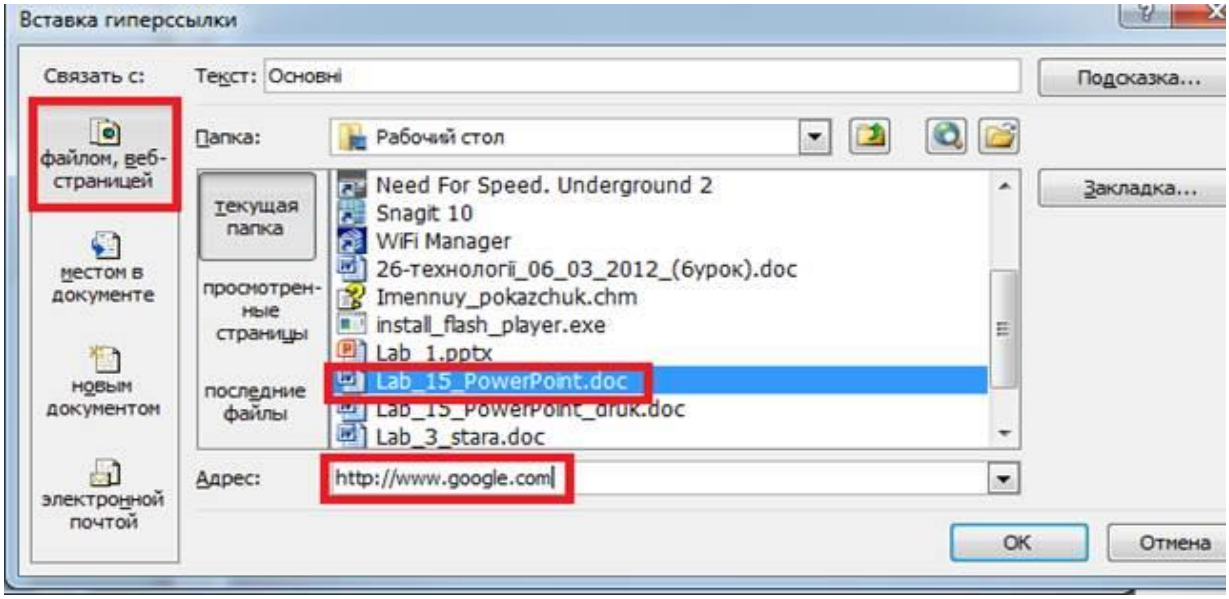


Рис. 6.42. Приклад додавання гіперпосилання на файл або веб-сторінку

Для створення гіперпосилання на слайд у мультимедійній презентації необхідно: ***Вставка гиперссылки***

– у меню натиснути кнопку *Связать с* ***местом в документе***;

– вибрати у списку слайд, до якого потрібно перейти, наприклад на слайд 3, що має заголовок «Фото Б. Хмельницького» (рис. 43). Цей слайд повинен бути прихованим.

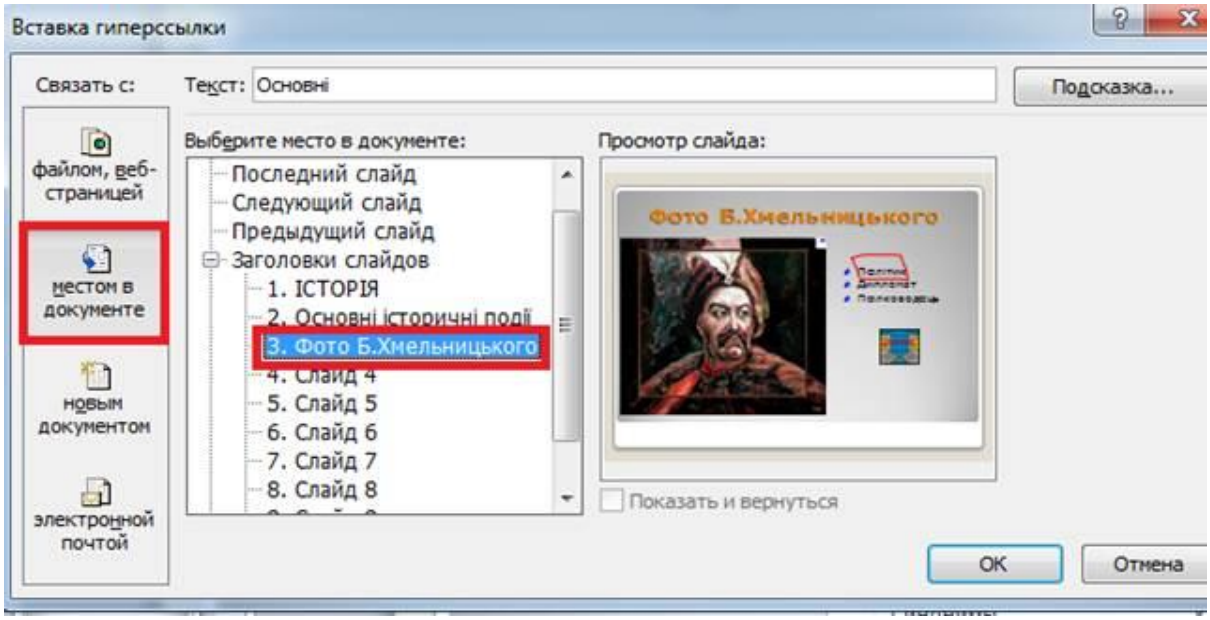


Рис. 6.43. Приклад додавання гіперпосилання на слайд у презентації

Задля створення гіперпосилання на певний слайд з іншої презентаці, необхідно виконати наступні дії:

– виділити текст або об’єкт, що має представляти гіперпосилання, та натиснути клавішу ***Гиперссылка***;

– в області *Связать с* натиснути значок ***файлом, веб-страницей***;

– знайти і виділити презентацію зі слайдом, на який має вказувати посилання;

Файл, на який здійснюється посилання, обов’язково розміщується в одній папкці з файлом презентації.

Для створення гіперпосилання на електронну адресу, необхідно:

– виділити текст або об’єкт, що має представляти гіперпосилання, та натиснути клавішу Гиперссылка;

– в області Связать с натиснути значок электронной почтой;

– вписати адресу потрібної електронної пошти (рис. 6.44).

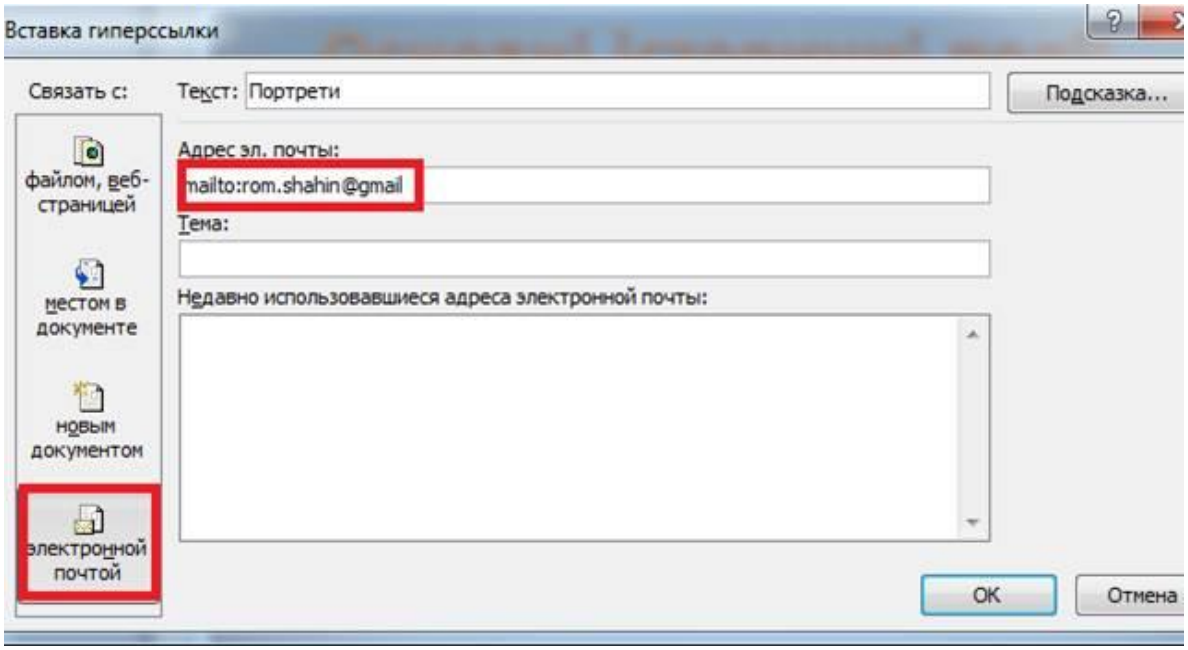


Рис. 6.44. Додавання гіперпосилання на електронну адресу

Формати збереження презентацій розмістимо у вигляді таблиці:

Тип файла	Розширення	Використовується для збереження
Презентація	PPTX	Звичайної презентації Microsoft PowerPoint
Метафайл Windows	WMF	Слайда у формі малюнка
Малюнок у форматі GIF (File Interchange Format)	GIF	Слайда у формі малюнка для використання на web-сторінках
Малюнок у форматі JPEG (File Interchange Format)	JPG	Слайда у формі малюнка для використання на web-сторінках
Структура, RTF	RTF	Вмісту презентації у вигляді документа структури
Шаблон оформлення	POT	Презентації у вигляді шаблону
Демонстрація PowerPoint	PPSX	Презентація, яка завжди відкриватиметься в режимі показу слайдів
Web-сторінка	HTM; HTML	Web-сторінка у формі папки з HTM-файлом і всіма допоміжними файлами
Web-архів	MHT; MHTML	Web-сторінка у формі одного файла, який містить усі допоміжні файли

У разі необхідності збереження презентації у форматі, відмінному від .pptx, виконуються наступні дії: у меню *Файл* вибираємо команду ***Сохранить как…*** . Обираємо папку для збереження презентації, вводимо ім’я файлу та вибираємо його тип. Наприклад: ***Демонстрация PowerPoint*** *(*.ppsx)* та натиснути клавішу ***Сохранить***.

Практичні завдання

Мета практичного заняття: набути та удосконалити навички роботи з програмою підготовки та створення презентацій MS PowerPoint щодо створення презентацій мультимедійного змісту, з таблицями, графіками та побудова блок-схем.

Навчальні засоби :

– персональні комп'ютери;
– програмна оболонка MS PowerPoint.

Сценарій :

Курсантиі розміщуються за персональними комп'ютерами та виконують практичне завдання зі створення презентації «***Моя професія – поліцейський»***:

1 слайд – заголовок, хто укладач, красива градієнтна заливка жовто-блакитна), контрастний напис.

Автоматичний перехід до наступного слайду (10 секунд).

2 слайд – напис вгорі, малюнок внизу.

Ручний перехід до наступного сайту.

3 слайд – анімована напис вгорі, відео внизу (запуск анімації і відео автоматизований).

Автоматичний перехід до наступного слайду (після показу відеоролика).

4 слайд – вставка аудіоролика (запуск по клацанню миші).

Автоматичний перехід до наступного слайду.

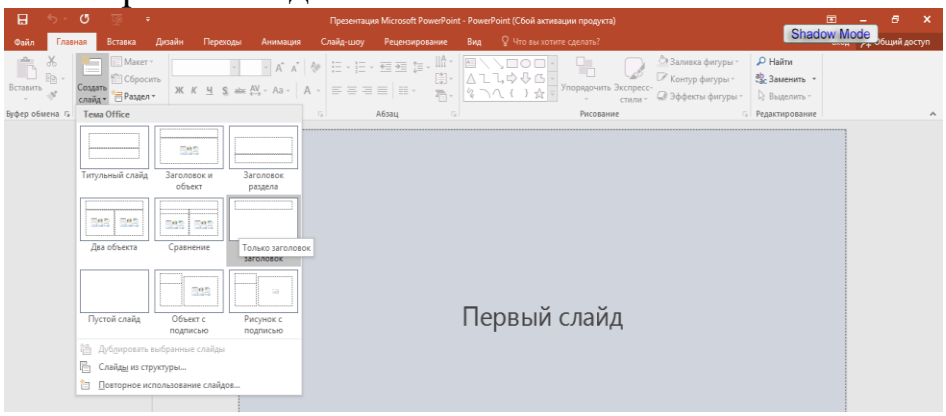
5 слайд – побудова блок-схеми.

Ручний перехід до наступного сайту.

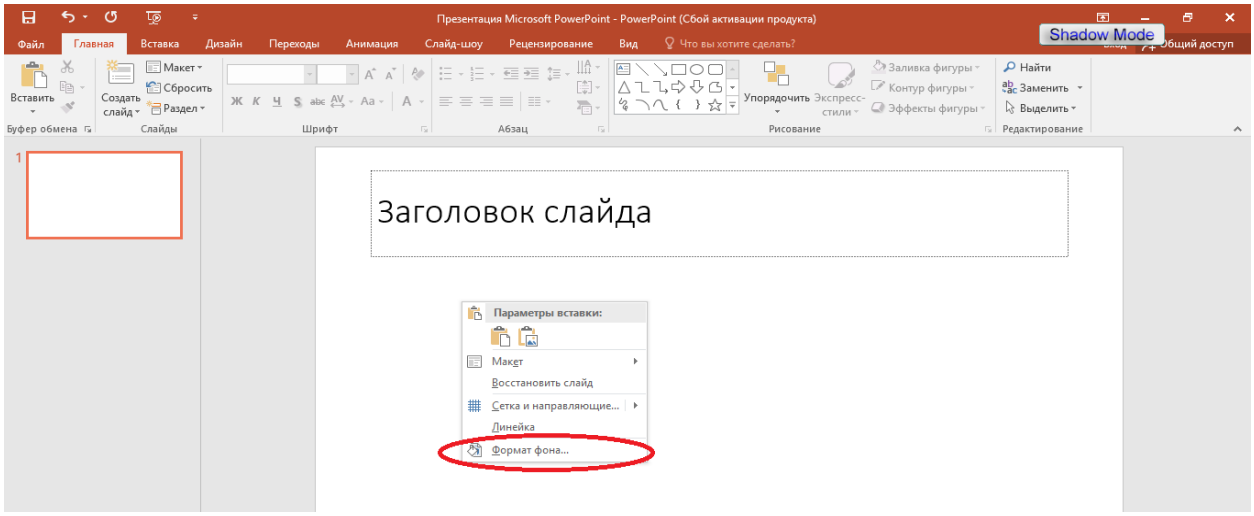
6 слайд – вставка діаграм.

Покрокова інструкція виконання практичних вправ:

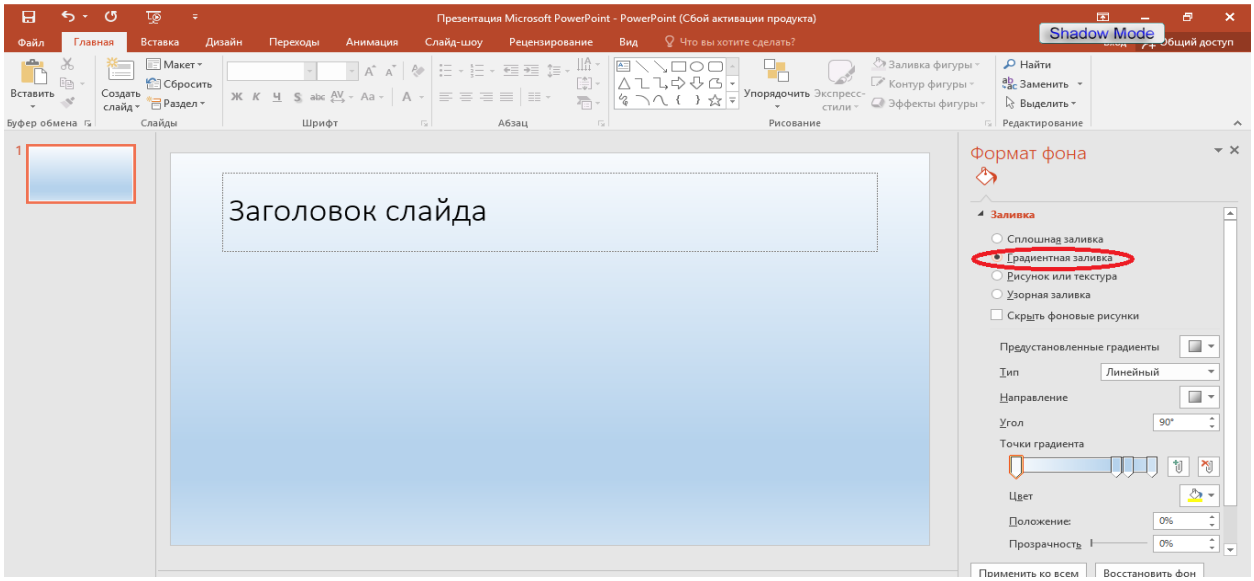
1. Створити слайд ss шаблонів



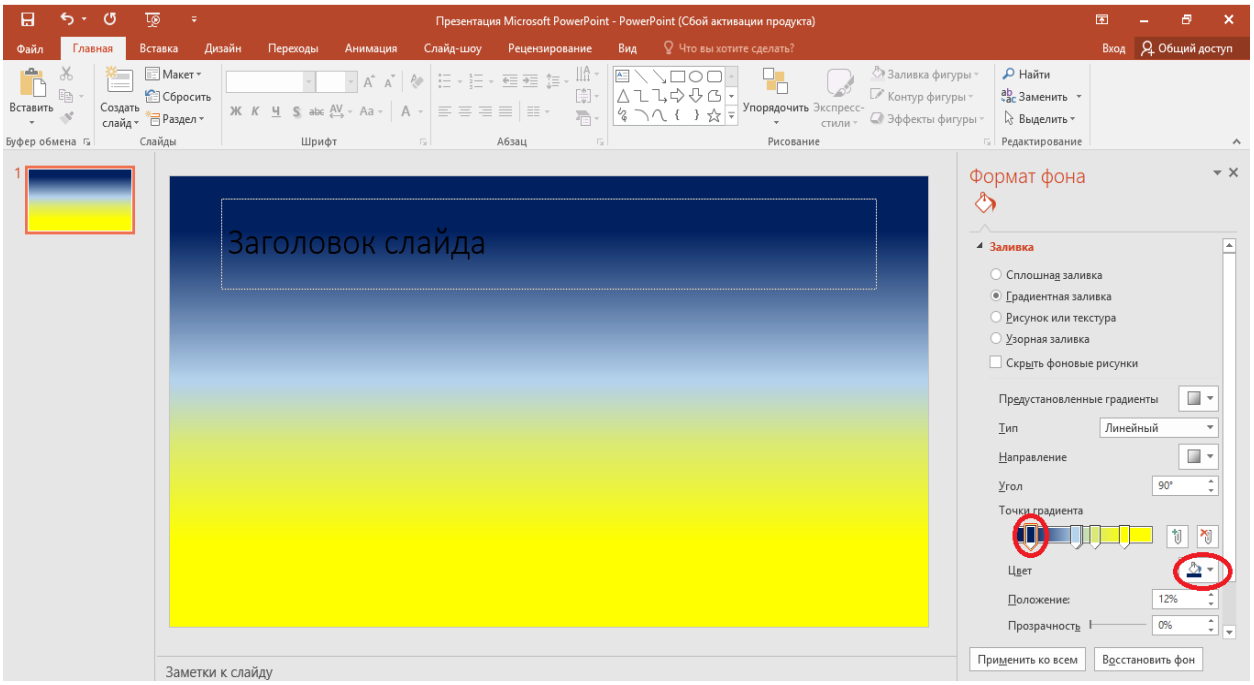
Градієнтна заливка: 1. Клацнути правою клавішою миші на слайді;



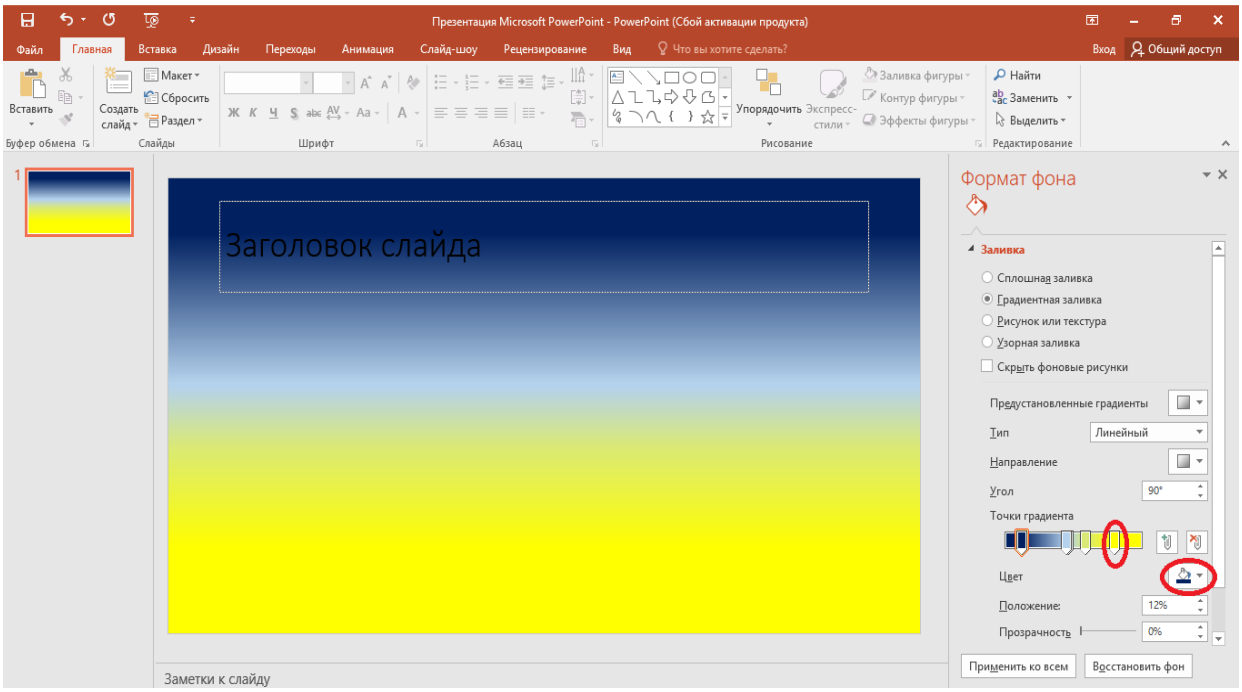
Обрати лівою кнопкою миші **формат фона**, потім ставимо перемикач на градиентную заливку.



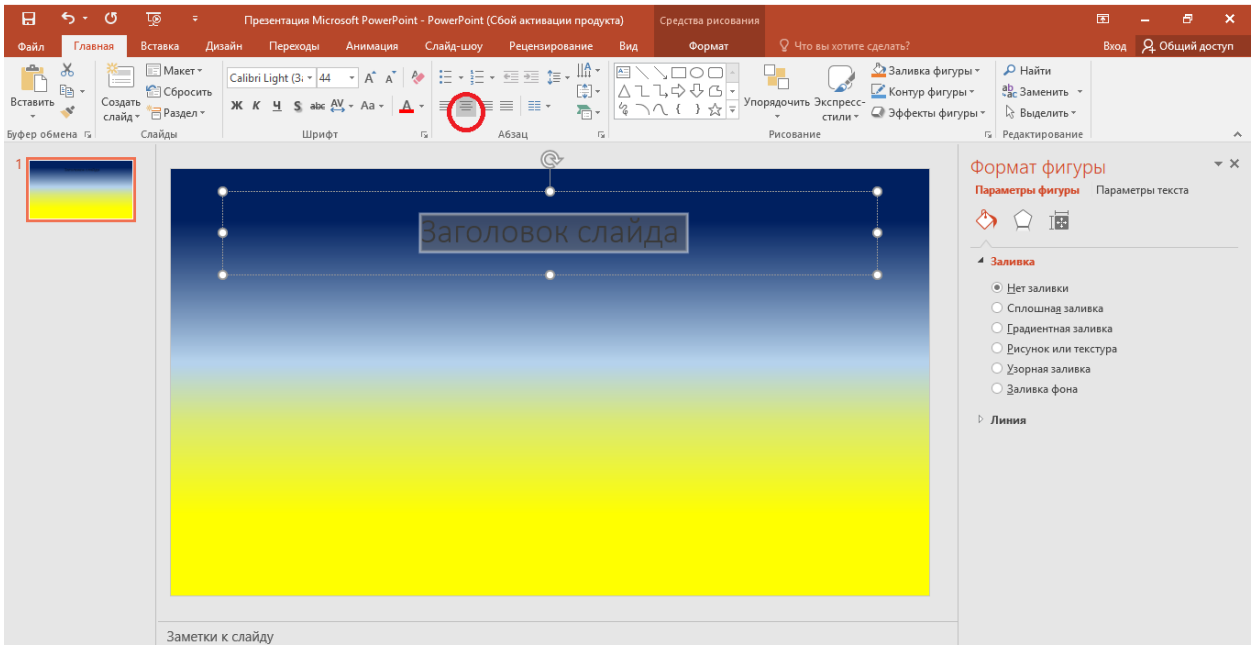
Зверху обираємо синій колір,

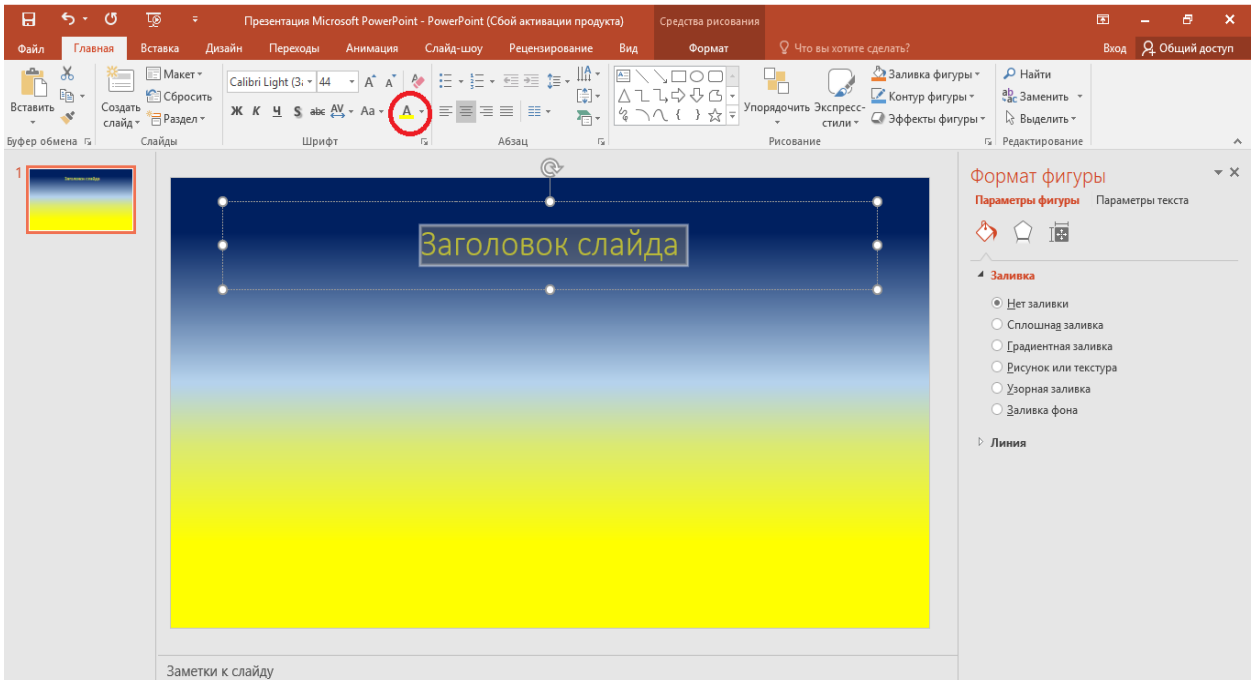


Знизу обираємо жовтий колір.

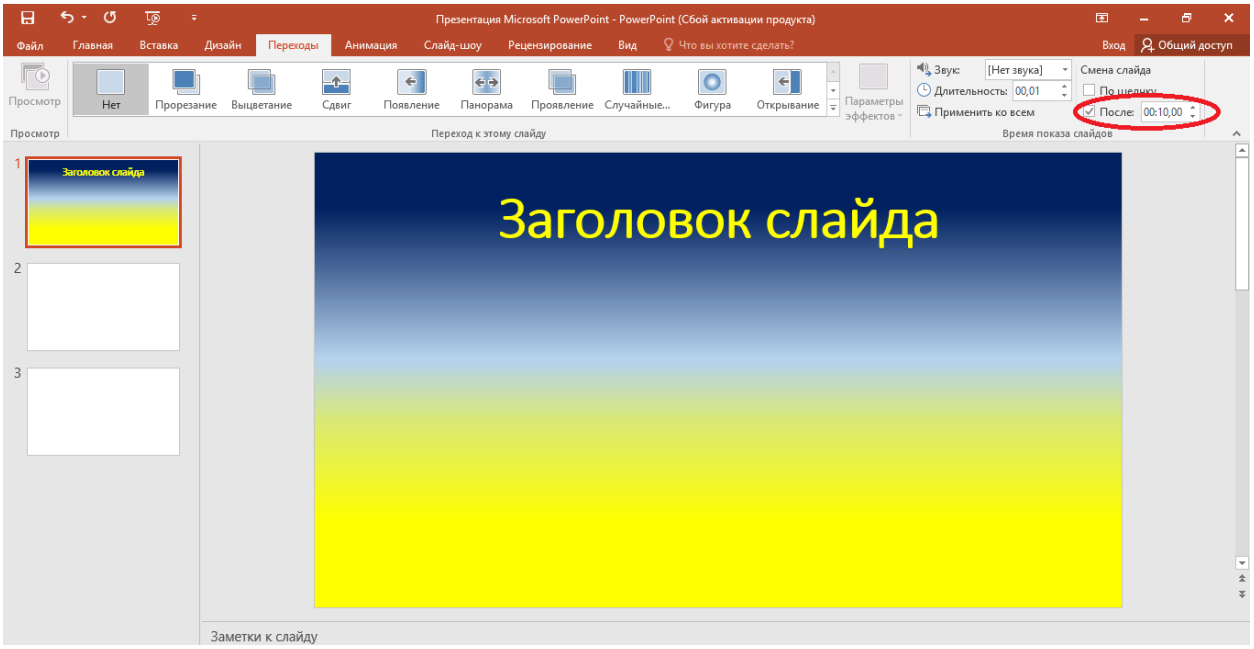


У заголовці слайда пишемо необхідну інформацію, та міняємо колір текста на жовтий (виділяємо текст, позиціонуємо текст по центру, робимо його жовтим). На жовтому фоні відповідно текст синього коліру.

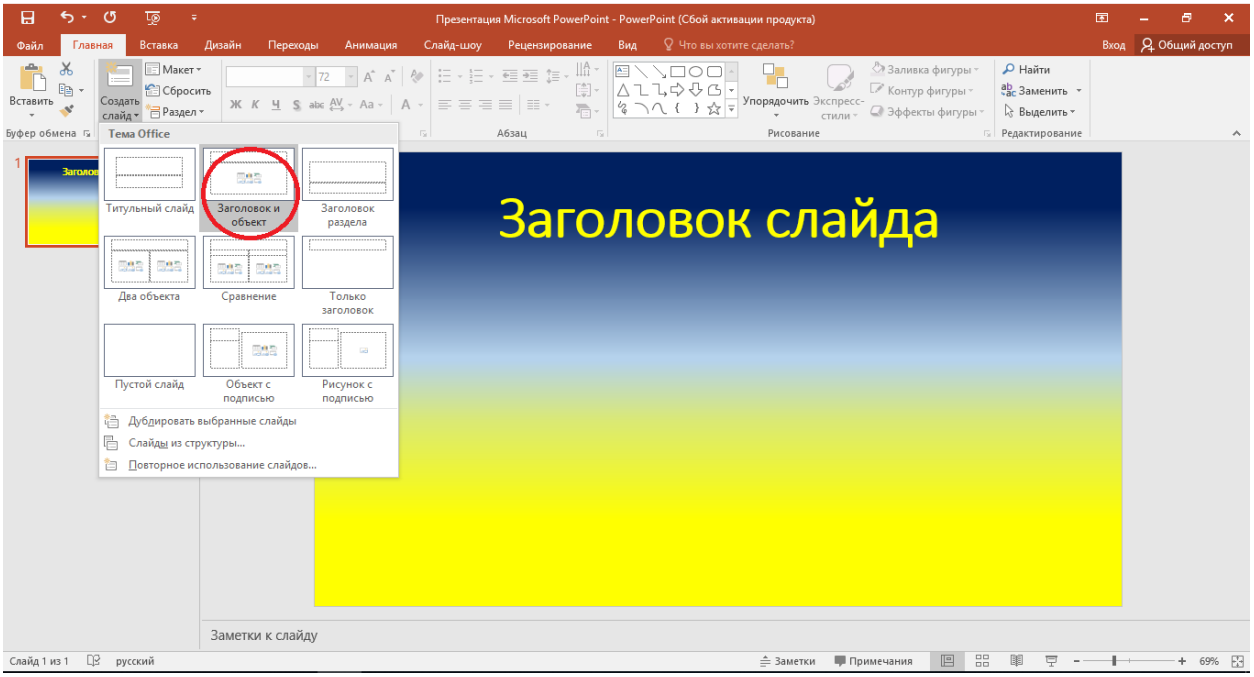


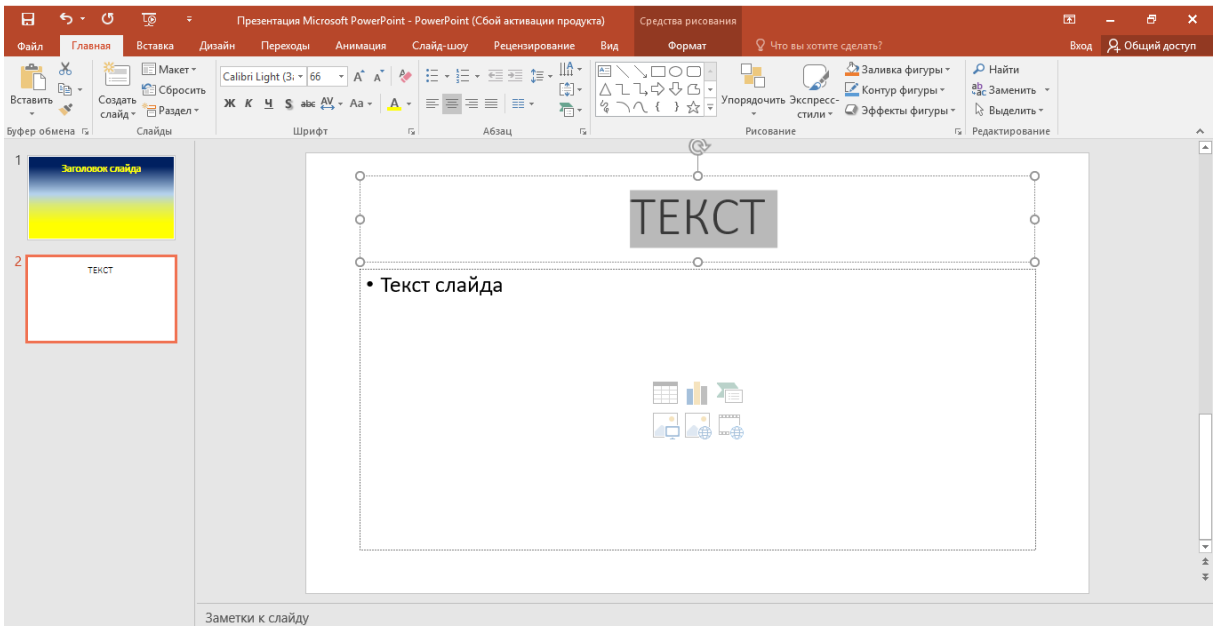


Налаштовуємо перехід на наступний слайд

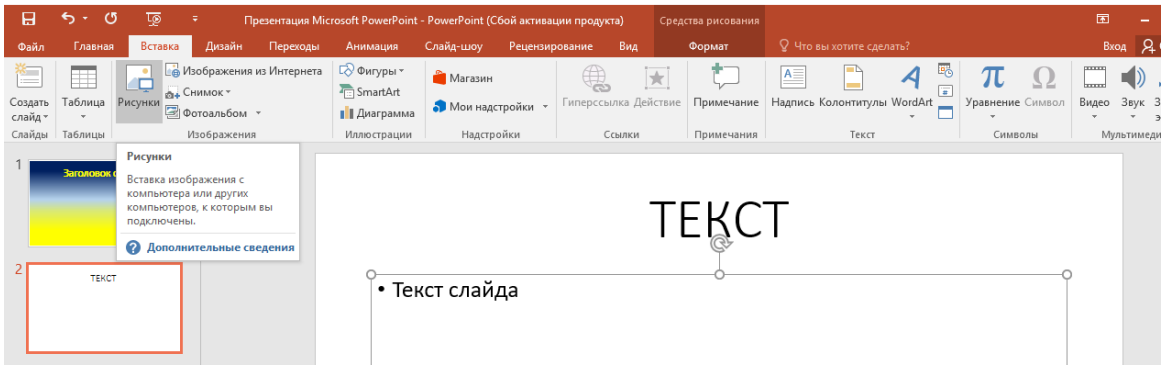

Презентация Microsoft PowerPoint - PowerPoint (Сбой активации продукта)
Заголовок слайда
Заголовок слайда
Заметки к слайду

2-й слайд

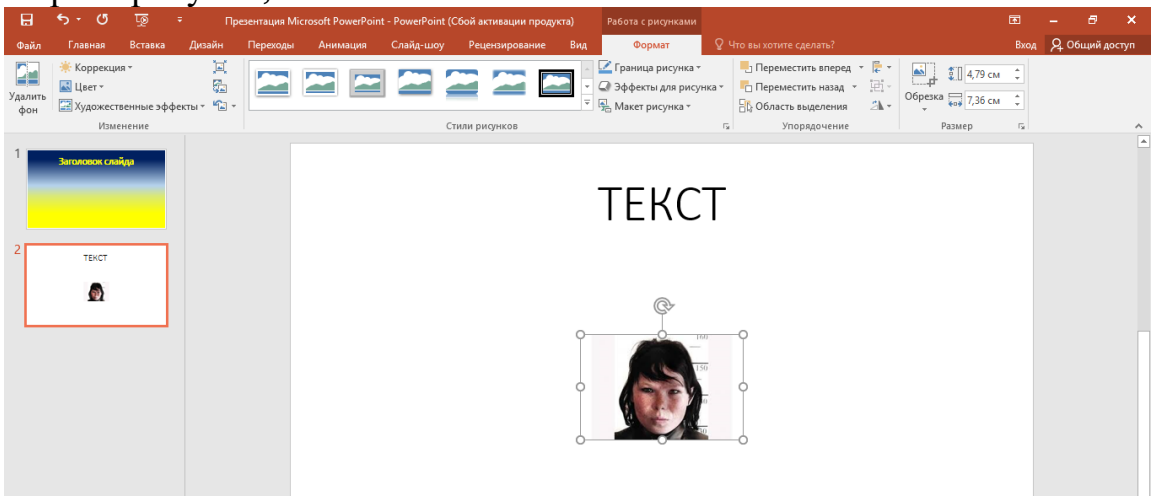

Презентация Microsoft PowerPoint - PowerPoint (Сбой активации продукта)
Тема Office
Титульный слайд
Заголовок и объект
Заголовок раздела
Два объекта
Сравнение
Только заголовок
Пустой слайд
Объект с подписью
Рисунок с подписью
Дублировать выбранные слайды
Слайды из структуры...
Повторное использование слайдов...
Заголовок слайда
Заметки к слайду



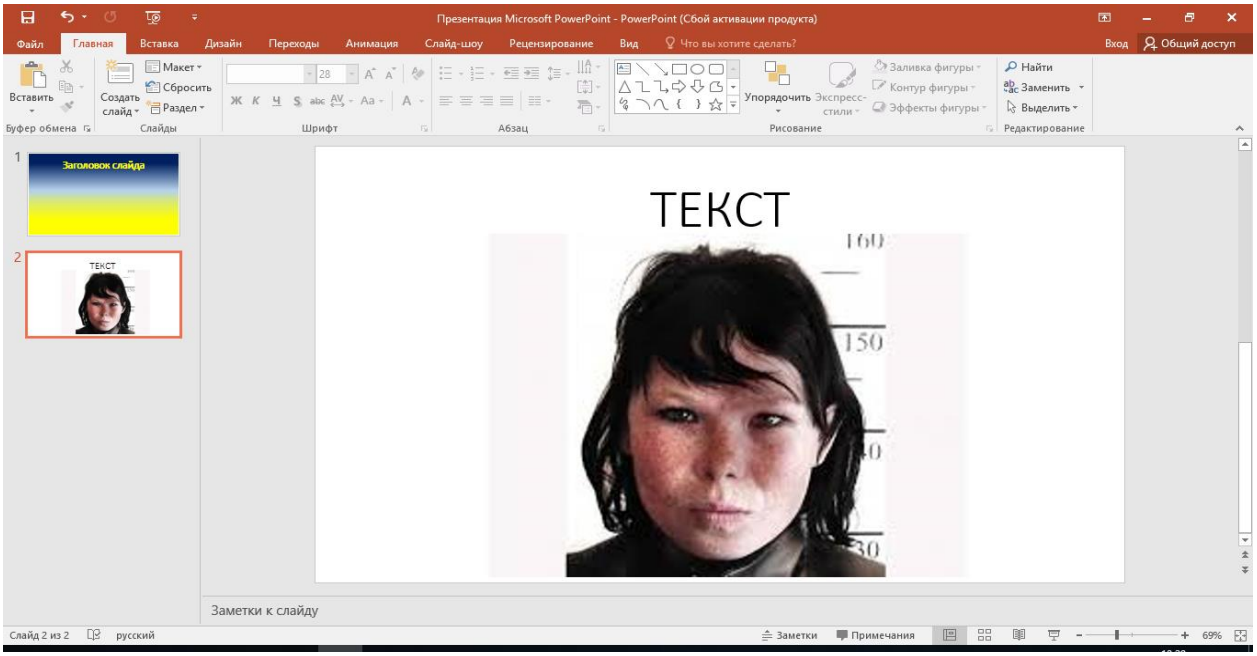
Вставка рисунка:



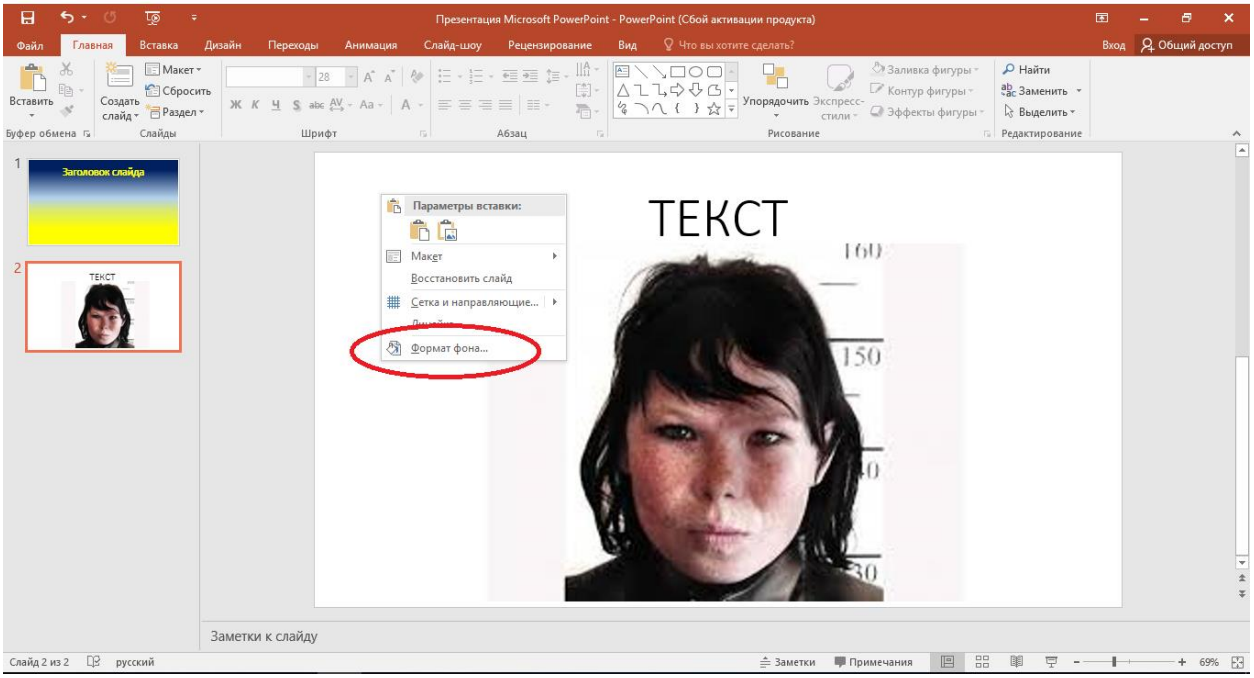
Обрати рисунок;

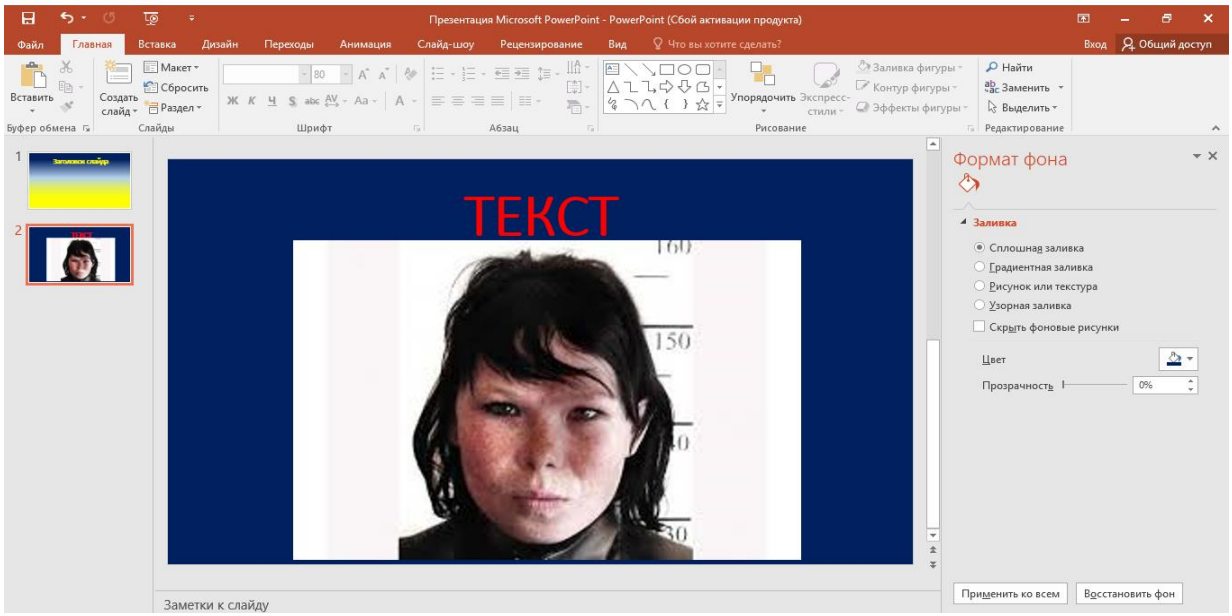


Потягнути курсором миші за кути (де є маленькі кола), щоб змінити розмір рисунка.

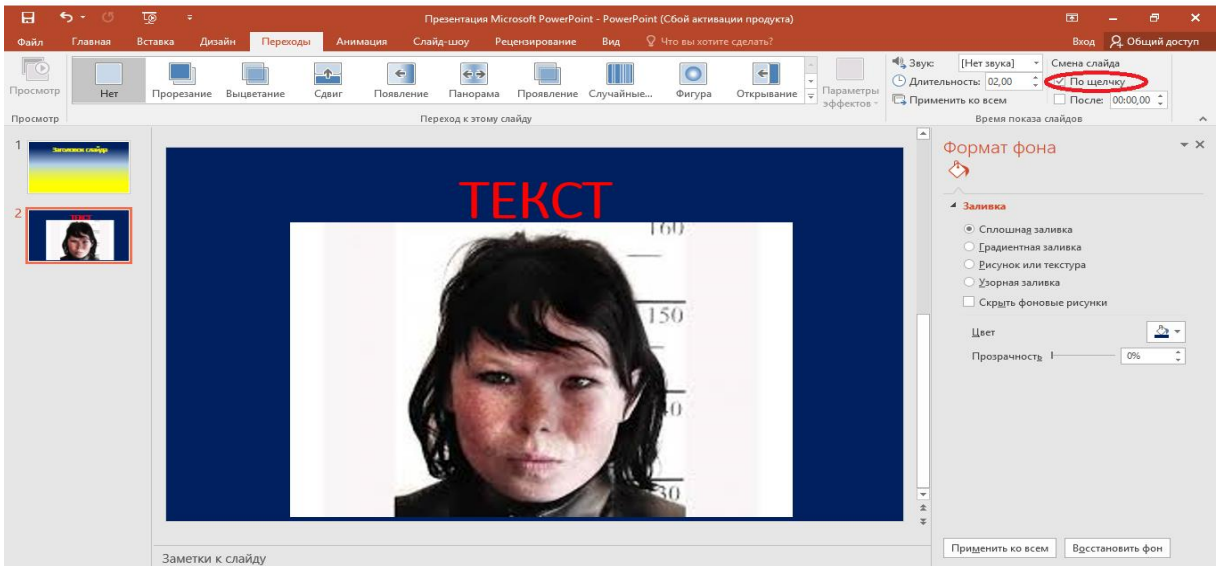


Можливо ще змінити фон слайду (через контекстне меню).

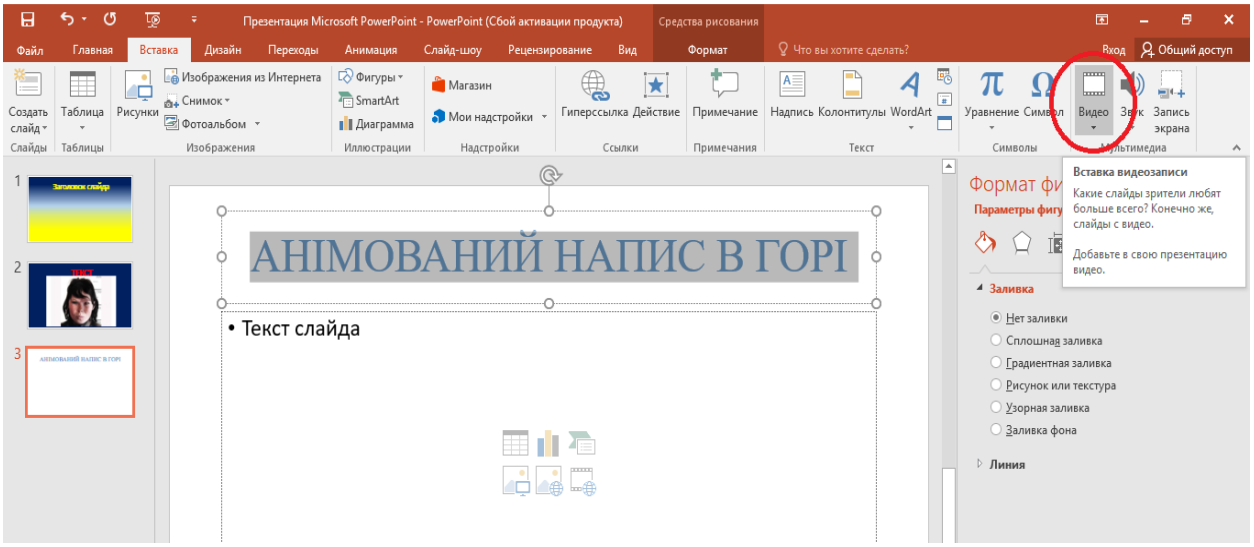




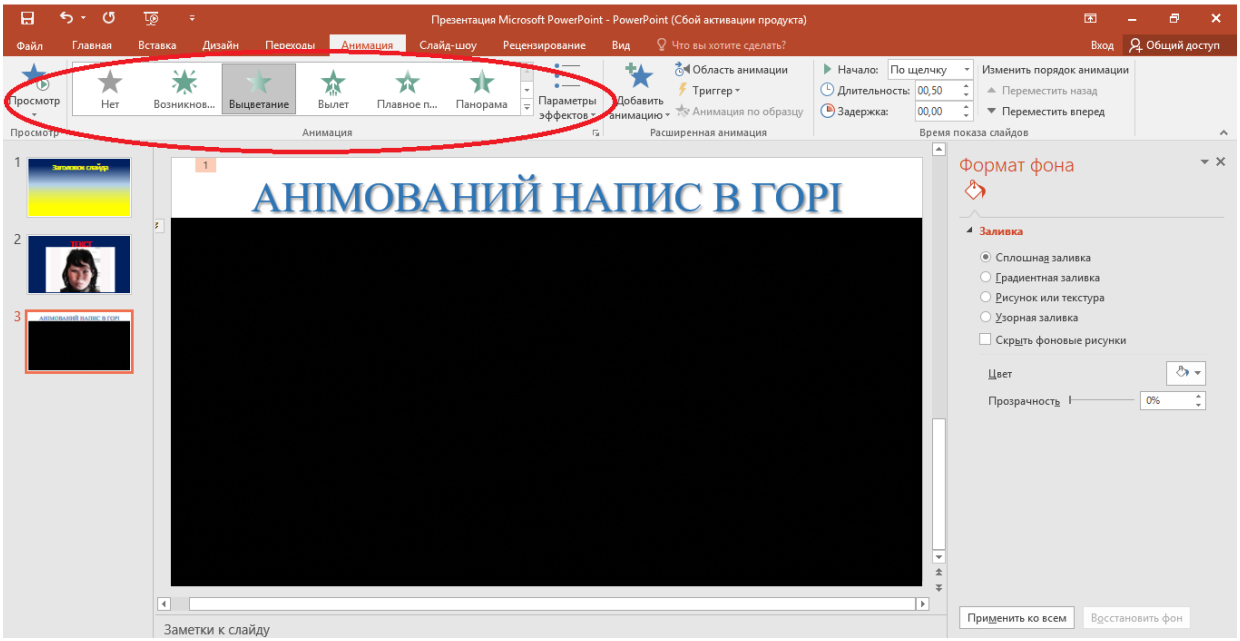
Налашлтувати перехід на наступний слайд



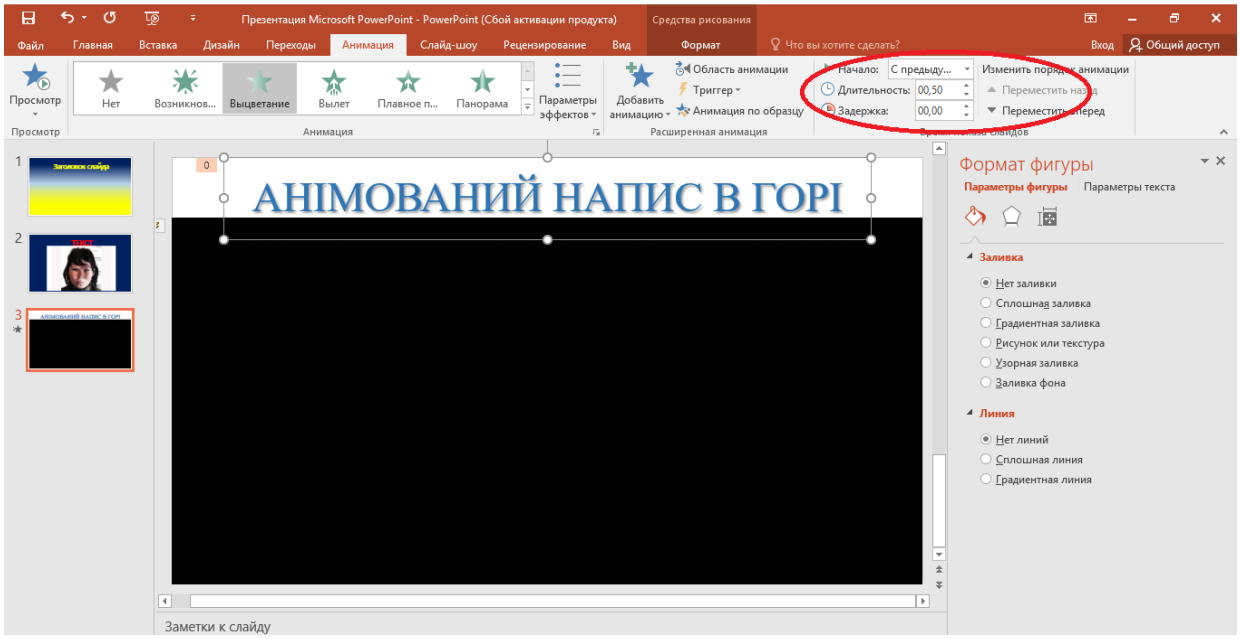
Слайд. Зверху повинен бути текст. Вставка відео.



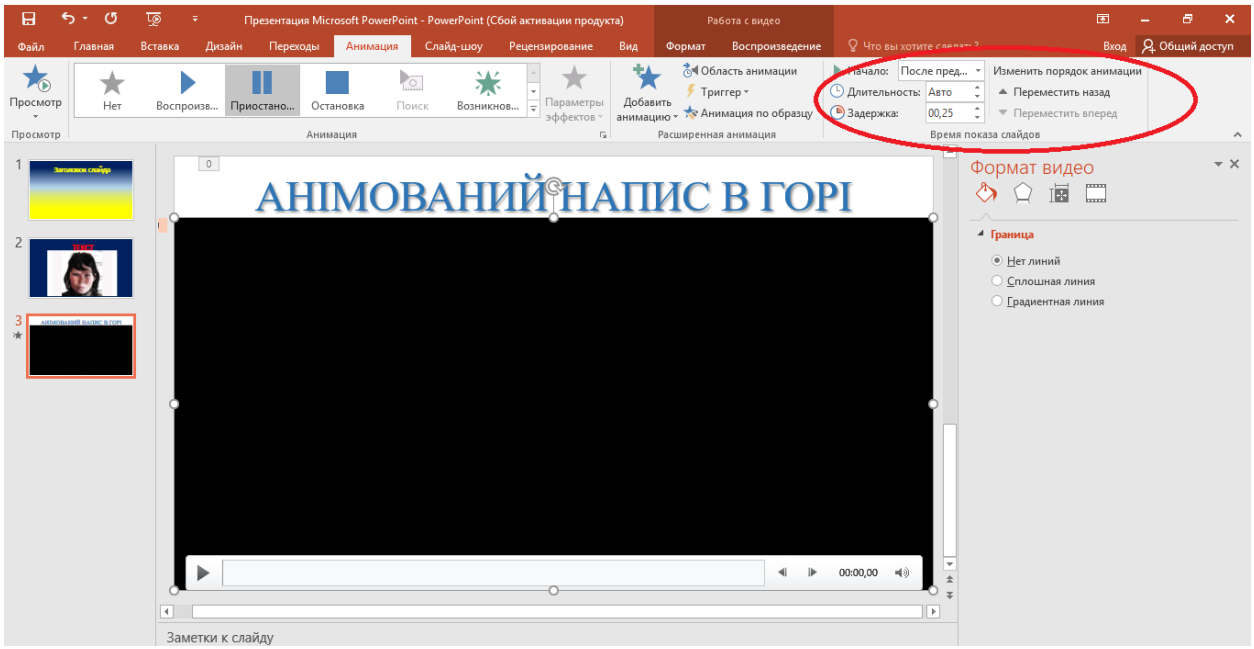
Налаштування анімації:

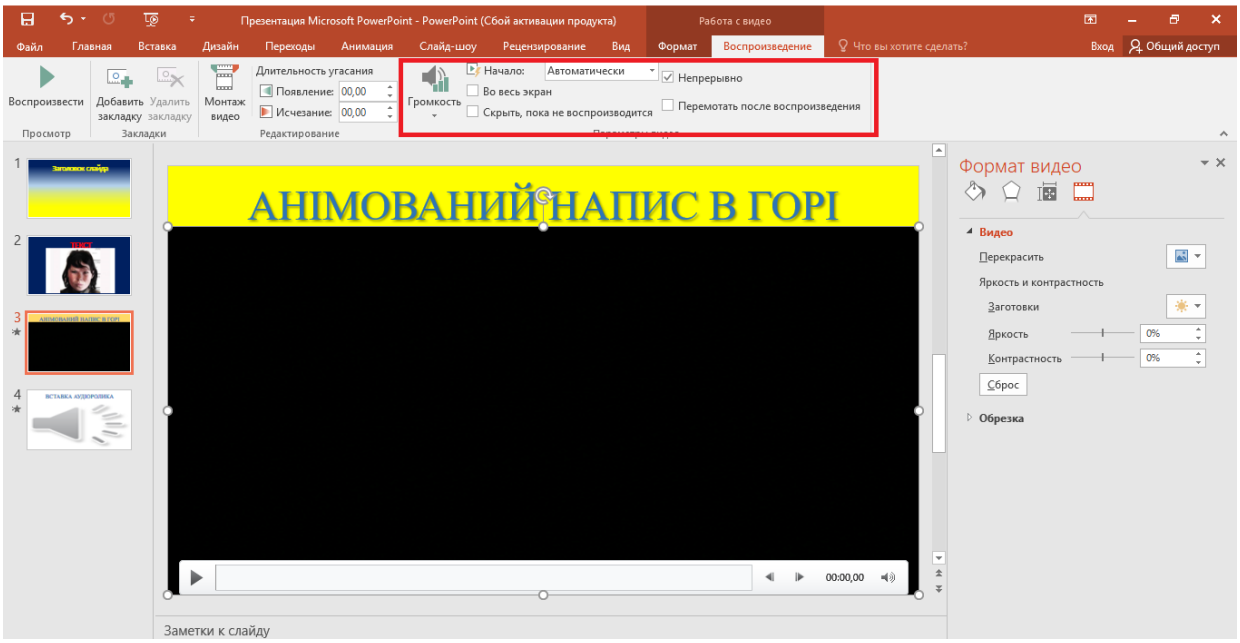


Налаштування запуску анімації.

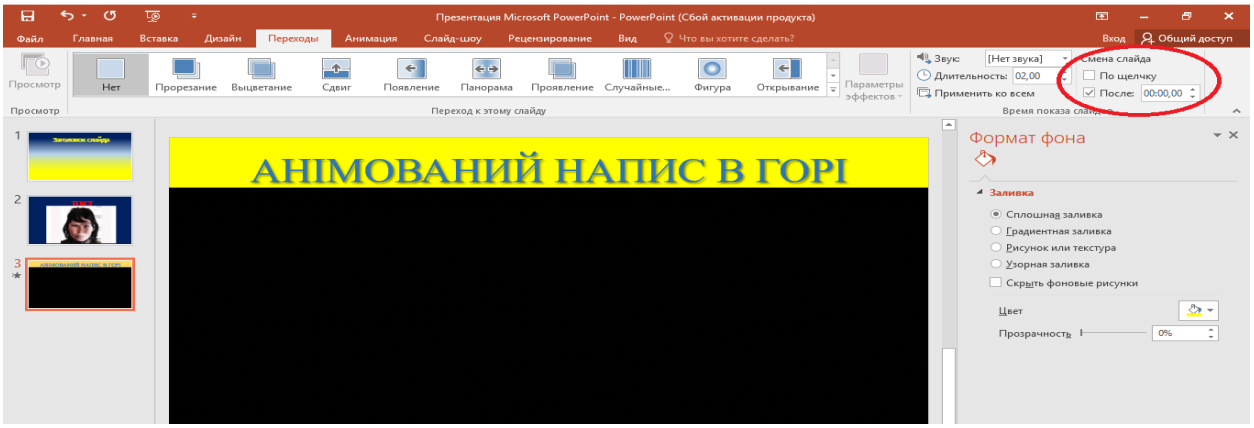


Налаштування запуску відео:

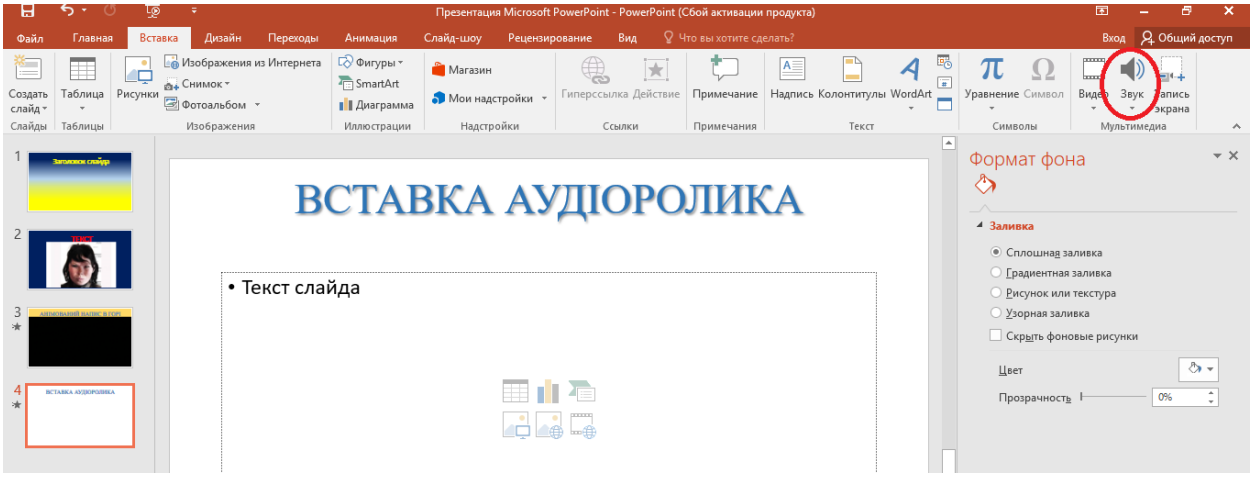


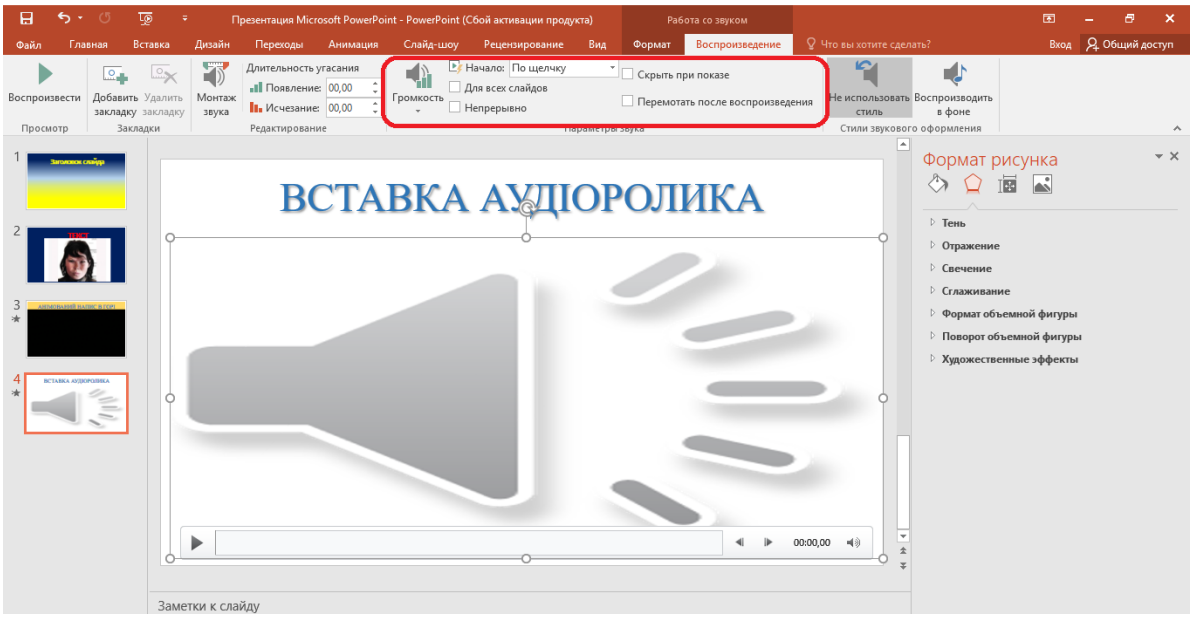


Налаштування зміни слайда (автоматично)

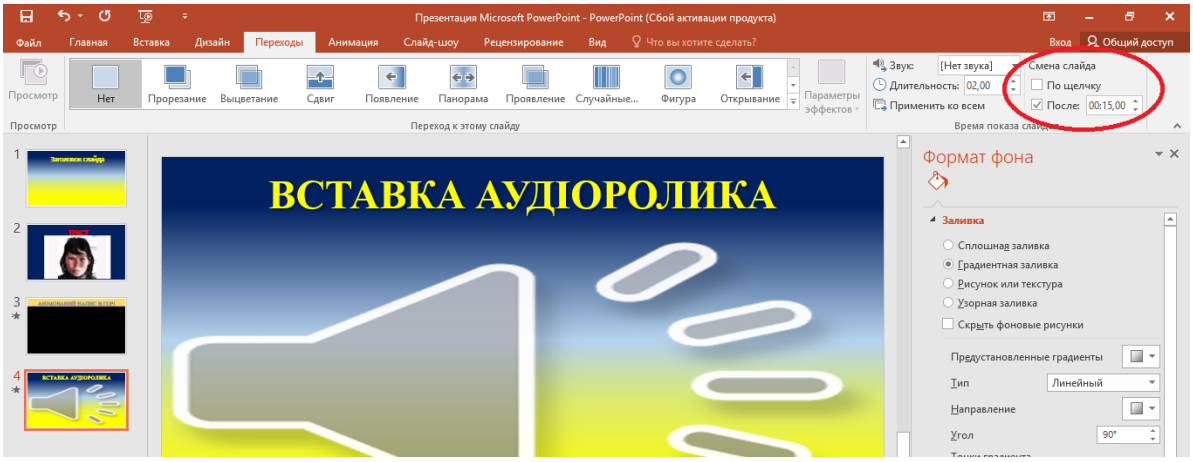


4-й слайд

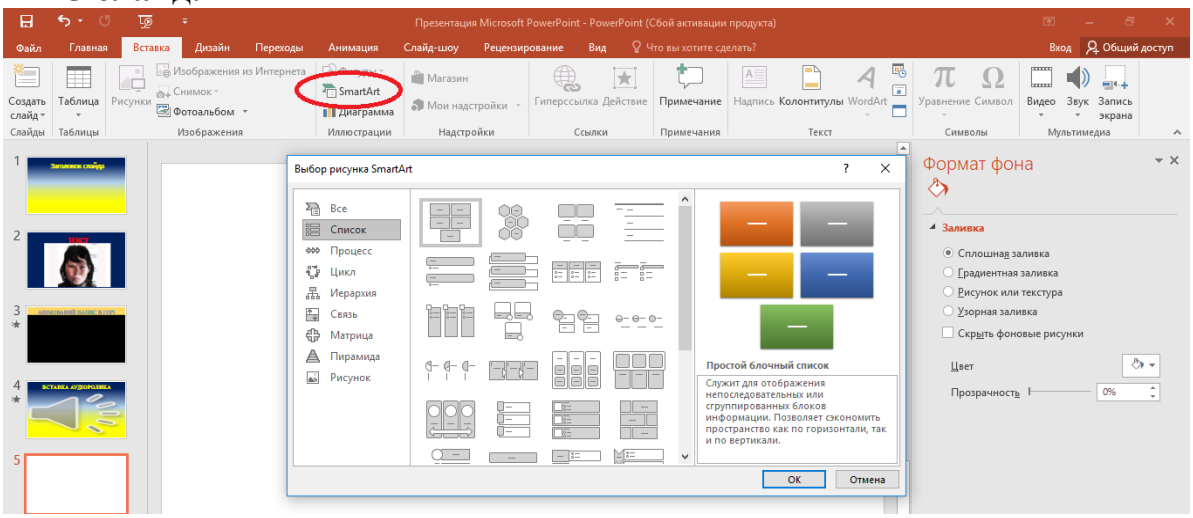




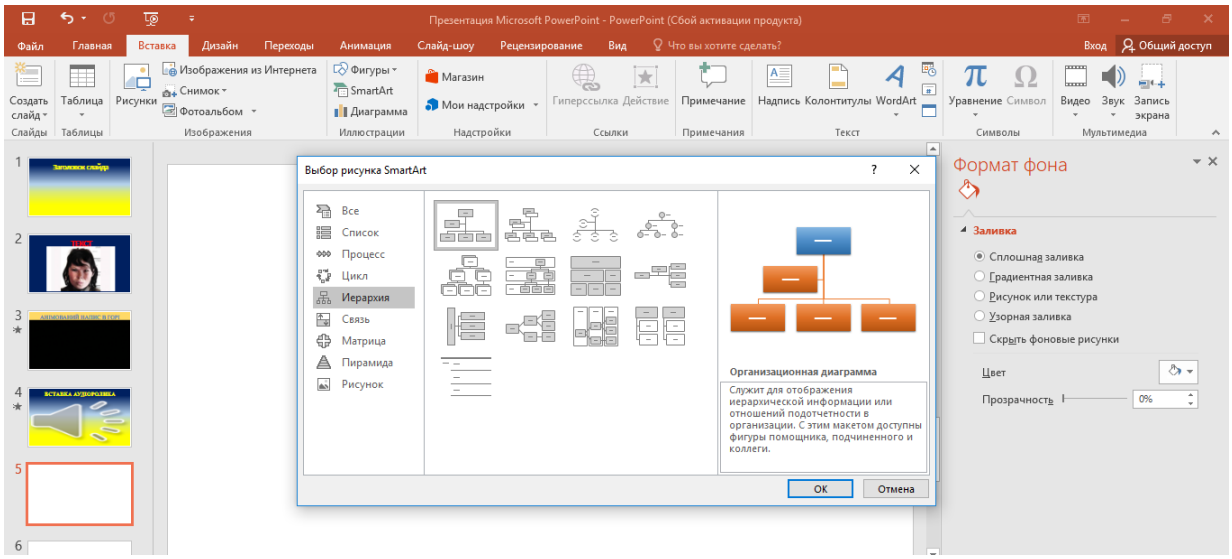
Налаштування зміни слайда

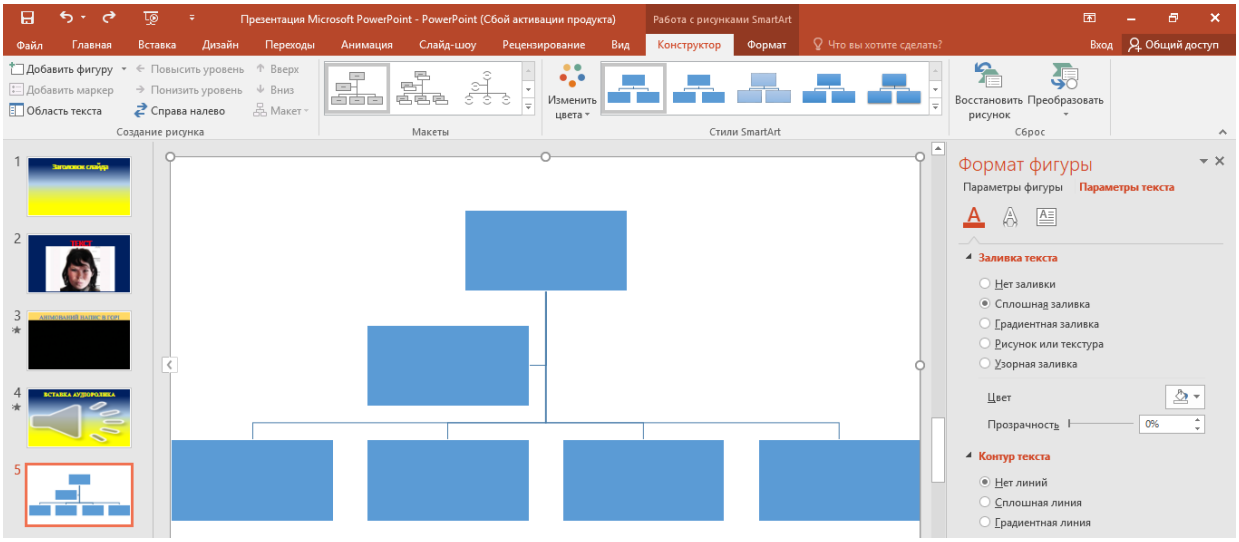


5 слайд. Вставка блок-схем

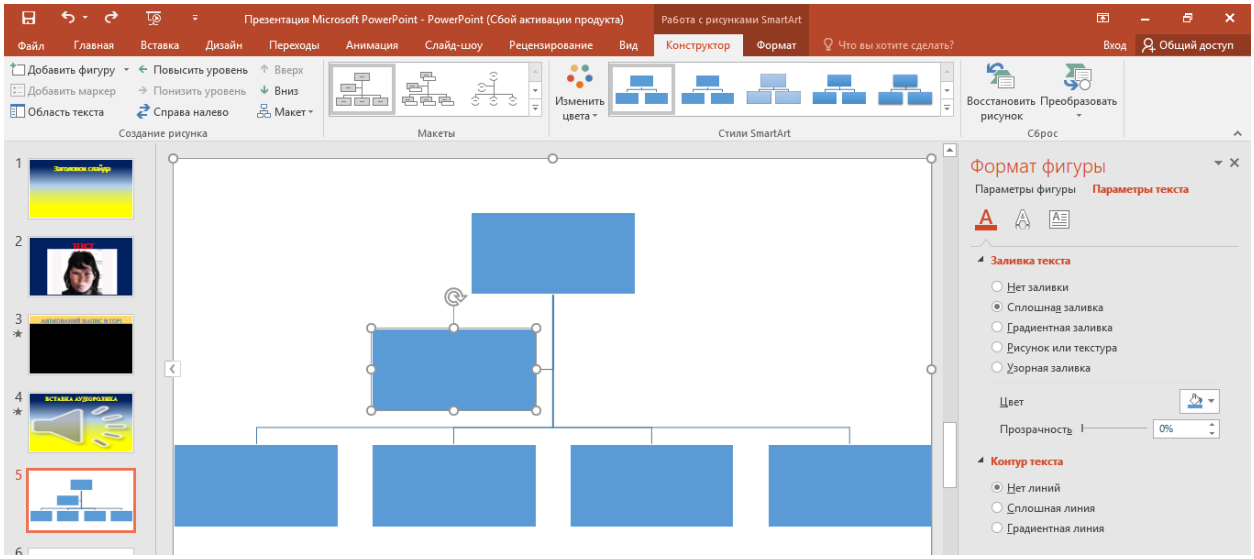


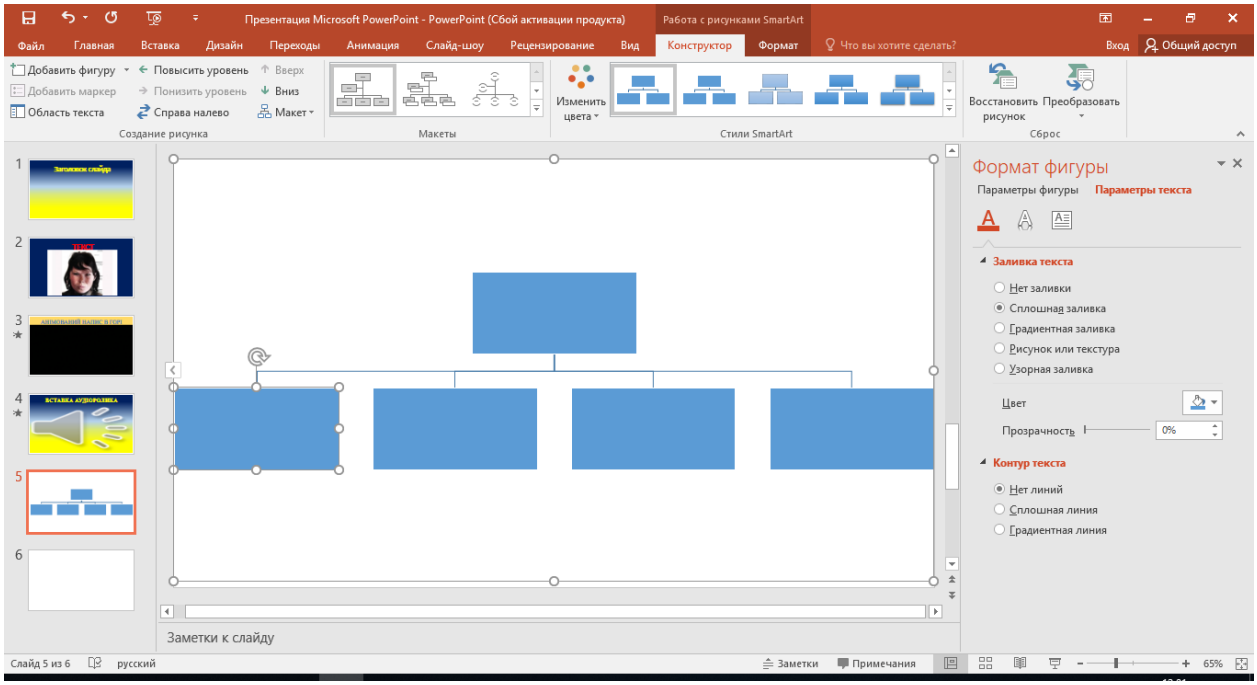
Обираємо потрібну



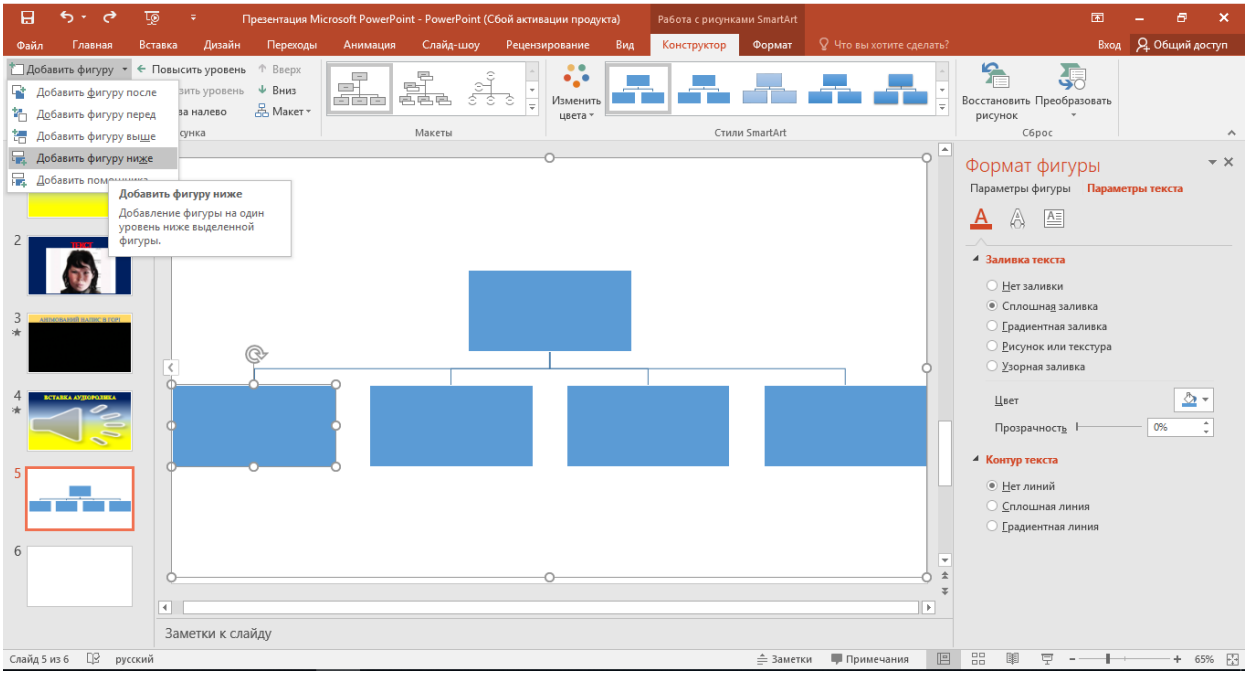


Для видалення непотрібного блоку слід його виділити та натиснути клавішу **Delete**.

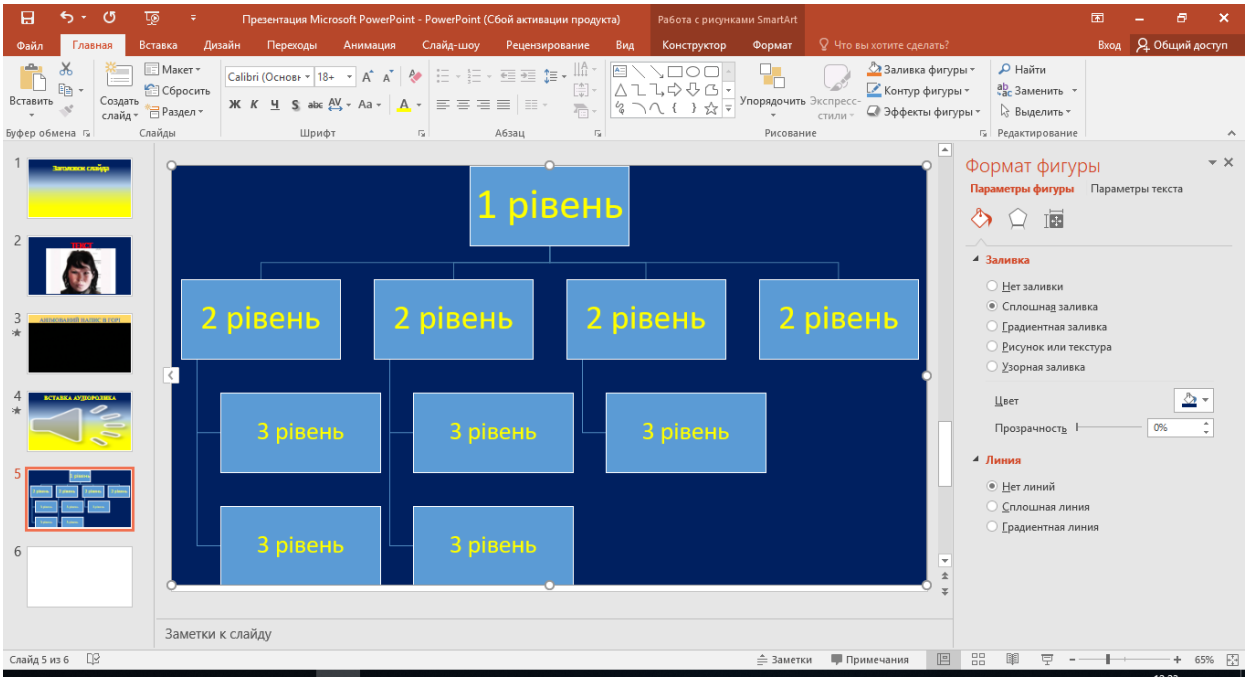




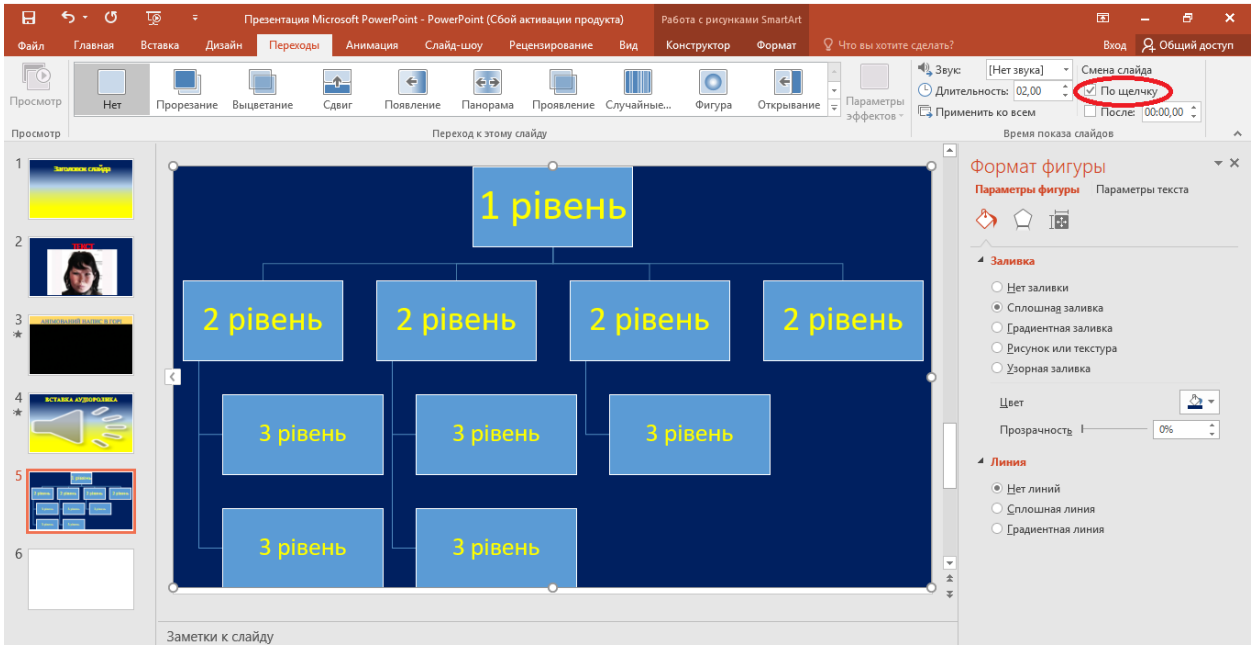
L Для додавання нового блоку потрібно виділити той блок, що буде головним (стартовим) та добавити нову фігуру.



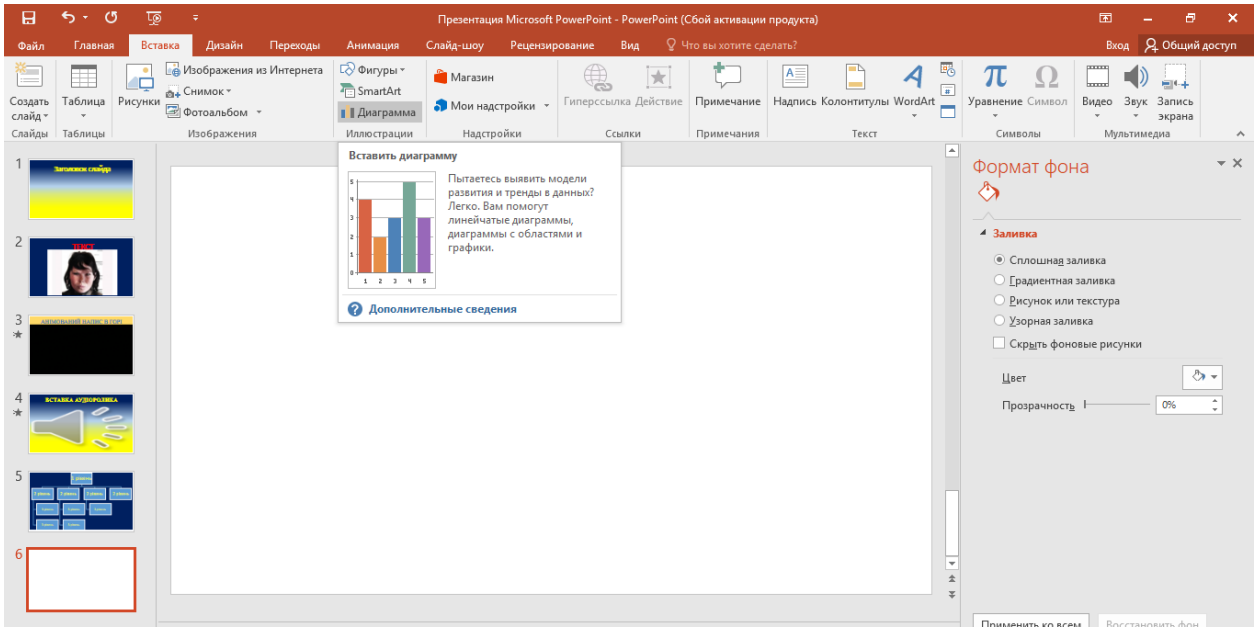
Формуємо необхідну структуру



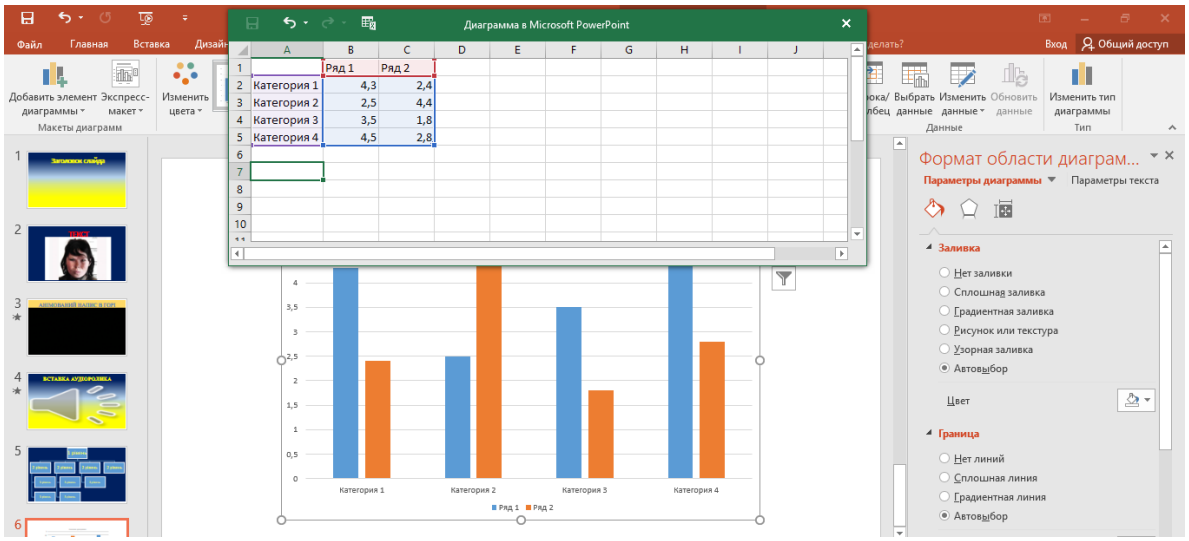
Перехід до наступного слайду налагоджуємо клацанням миші.



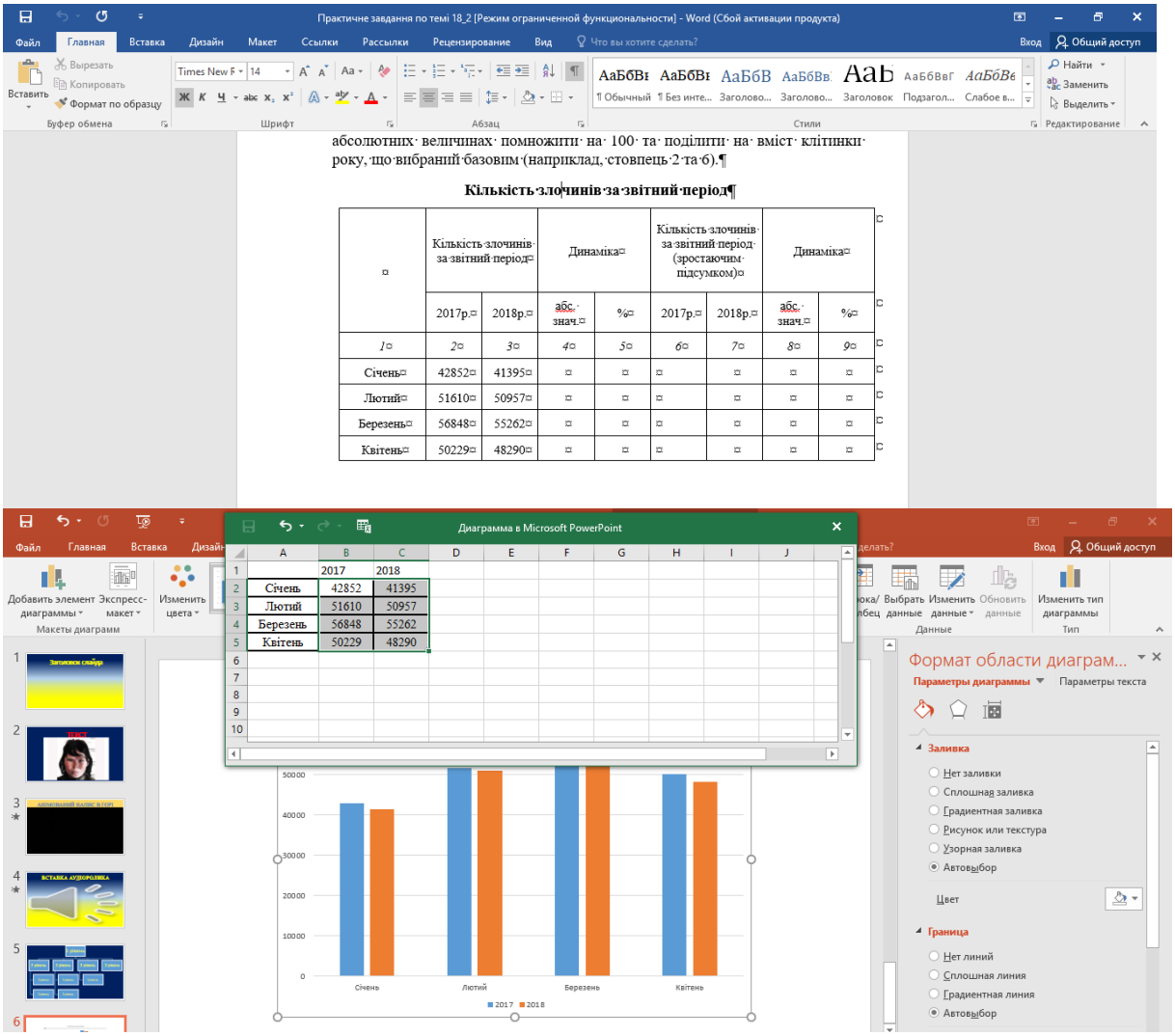
6 слайд. Вставка діаграми



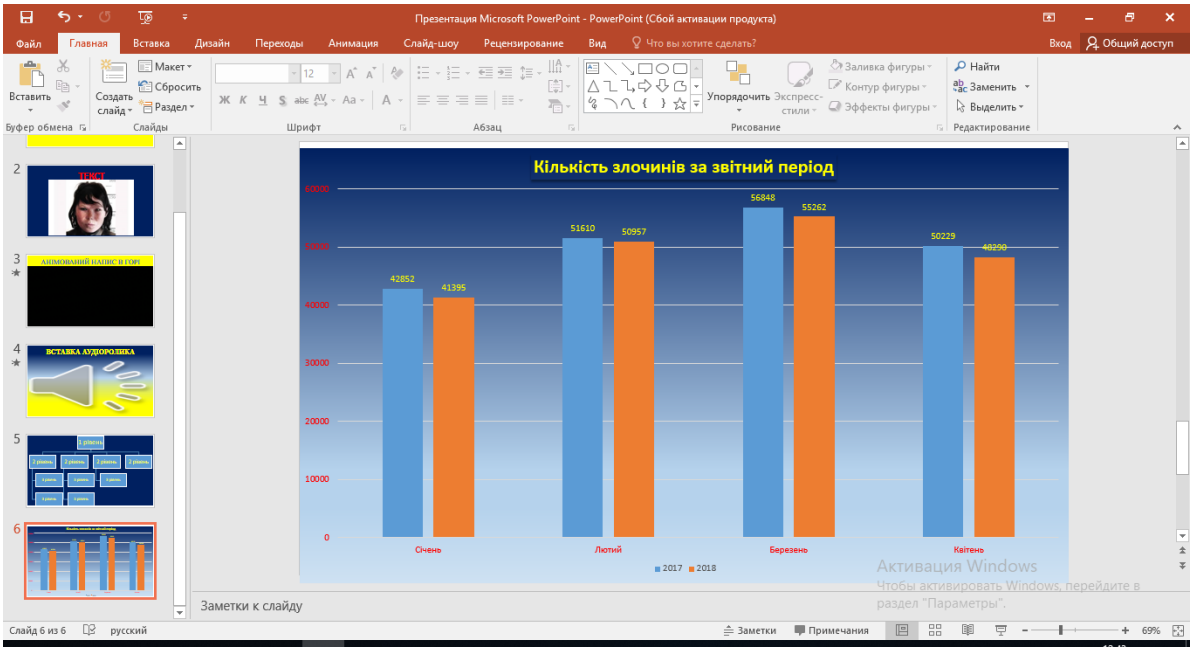
Обираємо потрібний нам формат діаграми



Підставляєте дані з таблиці **кількість злочинів за звітний період**, що була складена в процесі виконання практичного завдання з номером 18_2.



Відформатуйте діаграму належним чином.



Контрольні питання

1. Що таке «презентація»?
2. Які ви знаєте види презентацій? Охарактеризуйте кожен з них.
3. Які є типи презентацій?
4. На які види поділяються навчальні презентації?
5. Що ви розумієте під поняттям «планування презентації»?
6. Як поділяються презентації за структурою?
7. Які існують вимоги щодо структури та змісту навчального матеріалу?
8. Які ви знаєте вимоги щодо сприйняття кольорів і форм у презентації?
9. Назвіть загальні правила використання шрифтів та принципи відбору шрифтів для презентації.
10. Чим слід керуватися під час вибору шрифтів для презентації?
11. Які ви знаєте основні елементи слайдової презентації?
12. Які способи створення слайдів ви знаєте?
13. Що таке «макет» слайду, як його застосувати?
14. Як можна оформити дизайн слайду?
15. Як створити фон слайду власноруч?
16. Як ви знаєте режими відображення слайдів?

17. Що означає слово «анімація»?
18. Як додати переходи між слайдами презентації?
19. Як додати анімацію до об’єктів слайду?
20. Як встановити параметри анімації елементів слайду?
21. Як встановити порядок відображення анімації різних об’єктів слайду?
22. Як автоматизувати показ слайдів?
23. Як встановити параметри зміни слайдів?
24. Як відбувається демонстрація презентації?
25. Як сформувати довільний показ створеної презентації?
26. Які способи керування презентацією ви знаєте?
27. Що означає «застосувати ефект «Прихований слайд» під час показу слайдів?
28. Як відобразити приховані слайди?
29. Як створити рукописні примітки під час демонстрації презентації?
30. Як вилучити рукописні примітки зі слайдів презентації?
31. Що означає «Налаштувати демонстрацію» презентації? Як це зробити?
32. Як відмінити режим показу слайдів?
33. Як задати час демонстрації конкретного слайду презентації?
34. Яку роль відіграють графічні об’єкти на слайдах?
35. Які є способи введення графічних об’єктів у слайд?
36. Які макети графічних об’єктів має PowerPoint?
37. Як помістити на слайд об’єкт WordArt?
38. Як помістити на слайд «фігури»?
39. Як помістити на слайд «надпис»?
40. Як помістити на слайд малюнки?
41. Як помістити на слайд картинки?
42. Як помістити на слайд таблицю ?
43. Як розмістити на слайді заздалегідь створену таблицю Word?
44. Як помістити на слайд діаграму?
45. Як помістити на слайд об’єкт SmartArt?
46. Як згрупувати (розгрупувати) відповідні графічні об’єкти на слайді?
47. Як встановити звукове оформлення слайдів?
48. Як можна додати звук із файлу?
49. Як можна додати звук із організатора кліпів?
50. Як додати універсальні звуки PowerPoint?
51. Як можна самому записати звук?

52. Як можна додати відео програми PowerPoint?
53. Як можна додати відео з веб-сайта?
54. Як додати відео з будь-якого файлу?
55. Як користуватися колекцією кліпів?
56. Що розуміють під поняттям «гіперпосилання»?
57. Як можна організувати гіперпосилання?
58. Як створити гіперпосилання на файл або веб-сторінку?
59. Як створити гіперпосилання на слайд поточної презентації?
60. Як створити гіперпосилання на певний слайд з іншої презентації?
61. Як створити гіперпосилання на електронну адресу?
62. Які ви знаєте формати збереження презентацій?
63. Як відправити презентацію електронною поштою?
64. Як можна зберегти презентацію на веб-сайті?
65. Як можна опублікувати слайди презентації?
66. Як створити відео з презентації?

Джерела до розділу 6

1. Короткий посібник користувача PowerPoint. Сайт Майкрософт. URL : https://support.microsoft.com/uk-ua/office/%D1%81%D1%82%D0%B2%D0%BE%D1%80%D0%B5%D0%BD%D0%BD%D1%8F-%D0%BF%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D1%96%D1%97-%D0%B2-powerpoint-422250f8-5721-4cea-92cc-202fa7b89617.

2. Нелюбов В. О., Куруца О. С. Основи інформатики. Microsoft PowerPoint: Навчальний посібник. Ужгород: ДВНЗ УжНУ, 2018. 96 с.: іл URL : https://www.uzhnu.edu.ua/uk/infocentre/get/15627.

Розділ 7
ОБМІН ІНФОРМАЦІЄЮ У МЕРЕЖІ ІНТЕРНЕТ

7.1. Засоби та технології обміну інформацією у мережі Інтернет

Комп'ютерні мережі. Види, класифікація.

Із розвитком комп'ютерної техніки одночасно розвивалися і засоби обміну інформацією між декількома комп'ютерами. На початку 70-х років був розроблений прообраз сучасної високошвидкісної технології Ethernet. У той же час кілька університетів США стали обмінюватися даними за допомогою модемів, що працюють на невеликій швидкості. Ця технологія поклала початок системі телеконференцій Usenet. Різноманітні підходи та ідеї, які використовуються при побудові мережі, в той час ще не забезпечували сумісності різних систем. Незабаром був розроблена концепція об'єднання мереж різних компаній і організацій за допомогою спеціально розроблених для цих цілей шлюзів (gateways). Шлюзи використовують загальний протокол для обміну даними, який отримав назву Internet Protocol (IP).

Протокол IP став використовуватися в якості стандарту і для локальних мереж. Все більша стандартизація і розширення можливостей, що надаються сприяли тому, що кількість комп'ютерів, що мають доступ до цих послуг, неухильно росло. Згодом користувачі стали сприймати таке вільне об'єднання комп'ютерів як щось єдине – Internet. Далі ми будемо використовувати транскрипцію цього терміну – Інтернет.

Так що ж це таке Інтернет? Це – сукупність державних, регіональних, корпоративних та інших комп'ютерних мереж, а також окремих комп'ютерів, об'єднаних між собою різноманітними каналами передачі даних і уніфікацією застосовуваних технологій. На сьогоднішній день мережа Інтернет охоплює практично всі країни світу, її послугами користується вже більше 50 мільйонів чоловік, і їх кількість продовжує неухильно зростати.

Інтернет часто називають «Мережею мереж». За своєю структурою це повністю децентралізована мережа, що складається з безлічі інших мереж. Інтернет не має жодного єдиного/об'єднуючого

центру управління чи керівництва. Із самого початку в структуру майбутньої мережі Інтернет було закладено такі якості, як надійність передачі інформації і висока відмовостійкість.

Три ключових поняття складають основу Інтернет – вузловий комп'ютер, канал передачі даних і протокол TCP / IP.

Вузловий комп'ютер, званий також хостом, забезпечує передачу інформації в мережу від абонентів, підключених до нього, і прийом інформації для своїх абонентів. Друга, не менш важлива функція хоста – регулювання і, при необхідності, перенаправлення іншим шляхом потоків даних від інших хостів. Зазвичай хост-комп'ютери встановлюються в організаціях, що надають доступ до мережі.

Якщо хост-комп'ютери є як би вузликами мережі, то канали передачі даних – це нитки, що зв'язують воєдино всі такі вузлики. Найбільш часто для цієї мети використовуються звичайні комутовані і виділені телефонні лінії. Дещо рідше використовуються оптоволоконні і супутникові канали передачі даних, їх широке поширення стримується дорожнечею установки і підключення.

І, нарешті, протокол передачі даних TCP / IP (Transmission Control Protocol / Internet Protocol) – стандартний мережевий протокол зв'язку, який використовується для з'єднання комп'ютерних систем через Інтернет, забезпечує надійну пересилання інформації в масштабах всієї мережі. Програмне забезпечення для роботи з протоколом TCP / IP встановлюється на хост-комп'ютерах і машинах абонентів мережі. На відміну від інших протоколів передачі даних TCP / IP був розроблений спеціально для роботи в Інтернет, тому в нього спочатку закладені такі необхідні якості, як гарантована доставка інформації без втрат до місця призначення, зміна шляху проходження інформації при відмові одного з сегментів мережі, гнучкість і розширюваність.

Сучасні електронно-обчислювальні комплекси – це відкриті системи ЕОМ, тобто мають в своїй основі можливість підключення різних систем, – як програмного, так і апаратного характеру.

Комп'ютерні комунікації.

Інтернет (Internet) – глобальна мережа комп'ютерів, пов'язаних між собою за допомогою базового протоколу, наприклад TCP / IP. (Інтранет – внутрішня (закрита) мережа, що використовує технології Інтернет – найефективніша клієнт-серверна технологія) Локальні і глобальні комп'ютерні інформаційні мережі.

Локальна мережа – мережа підприємства, організації і т.д.

Глобальна мережа – Інтернет – мережа в світових або регіональних масштабах.

Глобальні мережі розвиваються у межах відкритих інформаційних систем. (Fido, Goldnet, AT50).

Модеми, канали зв'язку.

Канал зв'язку (КС) – технічний засіб для передачі сигналів між пристроями, що знаходяться на відстані один від одного. Інформація, передана за допомогою одиночних або послідовних сигналів, називається повідомленням. КС складається з трьох основних частин: передавача (модуляція), приймача (демодуляція) і лінії зв'язку (фізичне середовище).

Загасання сигналу – розсіювання частинок сигналу.

Пропускна здатність (швидкодія каналу) – кількість біт переданих в одиницю часу (біт / с, байт). Для чіткого визначення різниці між бітом і байтом, усвідомимо для себе, що інформація в інтернеті передається «біт за бітом», з цього і швидкість передачі вимірюється в бітах в секунду, обсяг збережених файлів визначаємо в байтах, так само і швидкість закачування визначаємо в байтах. Наприклад, якщо ми закачуємо фільм з інтернету, швидкість ми вимірюємо в бітах в секунду, а якщо ми закачуємо інформацію з компакт диска на комп'ютер, швидкість ми вимірюємо в байт в секунду. Канали зв'язку: комутовані (призначаються в момент набору номера) і виділені (закріплені). Модем – засіб міжкомп'ютерного з'єднання за допомогою телефонних каналів зв'язку (комп'ютер може зв'язуватися з допомогою модему з факсом).

Мережеве програмне забезпечення і мережевий протокол.

Функціонування апаратної частини мережі повинно бути підтримано відповідними програмами. Мережеві програми дозволяють визначати адреси комп'ютерів, робити доступними програмні і апаратні ресурси для клієнтів мережі, призначати різні права доступу користувачам, захищати інформацію. Ці програми входять до складу мережевих операційних систем, до яких відносяться Windows 7, Windows 10, NetWare і UNIX, причому всі системи дозволяють організувати багаторангові з'єднання.

Мережеве програмне забезпечення можна розділити на два види: програми-сервери, які розміщуються на сервері мережі, і програми-клієнти, розміщені на комп'ютері користувача і користуються послугами сервера. Мережеві протоколи, про які йтиметься нижче, є частиною мережевого програмного забезпечення.

Якщо ви – користувач локальної мережі, як практично буде організовано ваше перебування в цій мережі? Ці умови визначаються топологією мережі, використовуваною операційною системою і адміністратором вашої мережі. Адміністратор мережі (системний

адміністратор) – працівник, що відповідає за організацію та роботу мережі.

Припустимо, ви зібралися працювати в мережі з виділеним сервером. Адміністратор додасть вас як нового користувача мережі. Це означає наступне:

– вам буде присвоєно логін – унікальне ім’я користувача;

– ви заведете собі пароль – секретну послідовність символів, що підтверджує, що саме ви є власником цього логіна;

– адміністратор визначить ваші права доступу до інформаційних і апаратних ресурсів мережі.

Надалі при вході в систему ви кожен раз будете вводити для авторизації доступу свої логін і пароль. Авторизацією називають процес перевірки наявних у користувача прав і дозволів на доступ до ресурсів в домені (мережі).

Вам може бути виділено місце на диску сервера для зберігання ваших особистих файлів і визначено місце, де зберігаються програми загального користування, які ви зможете запускати зі свого комп’ютера. Вам можуть бути доступні мережевий принтер, мережевий CD-ROM і інші пристрої в мережі.

Дістатися до доступних вам ресурсів допоможе папка Мережеве оточення на робочому столі. У ній ви знайдете імена всіх комп’ютерів мережі. Знаючи заздалегідь, на якому комп’ютері знаходиться необхідне вам забезпечення, ви швидше дістанетеся до потрібного ресурсу. Інакше вам доведеться відшукувати його шляхом перебору самостійно. Адміністратор мережі може автоматично внести посилання на доступні вам ресурси в папку Мій комп’ютер на вашому робочому столі. Це значно полегшить пошуки.

Для вас виділяється також унікальне робочий простір на локальному комп’ютері, з якого ви заходите в мережу. Сюди відносяться налаштовуються і змінювані об’єкти Windows (Головне меню, Робочий стіл, папки Вибране та Мої документи, та ін.). Окрім адміністратора і вас ніхто не може проникнути до цього простору, що забезпечує захист інформації від чужого втручання.

Для передачі по мережі файл розбивається на частини – пакети. Кожен пакет забезпечений службовим повідомленням і передається незалежно від інших пакетів. На кінцевому пункті в комп’ютері всі пакети збираються в один файл. Так як пакети передаються незалежно, то кожен пакет може дійти до кінцевого комп’ютера своїм шляхом.

Кожен комп’ютер в мережі має свою унікальну адресу. Правила адресації в мережі повинні бути однаковими, хоча комп’ютери і

операційні системи, що входять в мережу, можуть бути різнорідними. Пакети даних переміщаються по мережі до комп'ютера з потрібним адресою. Спочатку перевіряється найкоротший шлях, якщо він зайнятий або зруйнований, то перевіряється наступний найкоротший шлях і т.д. На кінцевому комп'ютері перевіряється наявність всіх пакетів, що складають файл. Якщо будь-якого пакета не вистачає, комп'ютер-адресат робить запит комп'ютера-відправника і повідомляє, який пакет відсутній. Потрібний пакет наново посилається адресату. Всі правила кодування і пересилки файлів записуються в мережному протоколі.

Мережевий протокол або протокол обміну – це загальне угоду, яка визначає єдині правила передачі інформації в мережі.

Протокол визначає тип використовуваних даних, стандарти зв'язку, правила обробки помилок. Існує безліч мережевих протоколів. Протокол, що дозволяє ділити файли на пакети і передавати пакети від вузла до вузла, називається IP (Internet Protocol). Для об'єднання мереж, що працюють по протоколу IP і мереж, що працюють за іншими протоколами, було створено спеціальний міжмережевий протокол, і названий він був TCP (Transmission Control Protocol) – протокол управління передачею. Протокол TCP забезпечує стійке з'єднання між комп'ютером-відправником і комп'ютером-адресатом і відповідає за розбиття переданих даних на пакети, за збір окремих пакетів в форму вихідних даних, за досилання втрачених пакетів. Так як протоколи IP і TCP працюють спільно, їх об'єднання називають протоколом TCP / IP.

Протокол – система угод, підтримуваних програмним забезпечення та обладнанням (периферією) ЕОМ.

Протокол TCP / IP (Transmission Control Protocol / Internet Protocol) – мережевий протокол, що дозволяє комп'ютерам здійснювати з'єднання за внутрішніми мережами або через Інтернет. Кожен комп'ютер в Інтернет використовує TCP / IP.

Локальні комп'ютерні мережі.

Принципи функціонування різних електронних мереж приблизно однакові. Усі вони являють собою систему, що складається з комп'ютерів, каналів зв'язку і деякої угоди, що дозволяє комп'ютеру – адресатові перетворювати сигнал, що сприймається.

Кожен комп'ютер в складі ЛВС повинен мати наступні компоненти:

- мережевий адаптер (мережеву карту);
- канал зв'язку (лінія зв'язку);
- мережеву операційну систему (мережеві програми).

Мережевий адаптер – пристрій, що відповідає за сполучення

комп'ютера і каналу зв'язку; він приймає і передає сигнали, поширювані по каналу.

Адаптер вставляють до гнізда материнської плати одного комп'ютера і з'єднують з мережним адаптером іншого комп'ютера. Кожному комп'ютеру призначається свою адресу в мережі, що фіксується на мережевій карті. Відповідно до цієї адреси комп'ютер з усієї інформації, що передається по мережі, вибирає призначену саме для нього.

Мережевий кабель забезпечує канал зв'язку комп'ютера з іншими машинами мережі. Використовують різні види мережевих кабелів. Розглянемо їх властивості.

Кручена пара. Кабель містить дві або більше пари проводів, скручених один із іншим уздовж усього кабелю. Скручування дозволяє підвищити стійкість кабелю і знизити вплив кожної пари на все решта. Розрізняють неекрановані і екрановані кручені пари. Максимальна відстань, на якому можуть бути розташовані комп'ютери, з'єднані неекранованої кручений парою, досягає 300 м. Швидкість передачі інформації – від 10 до 155 Мбіт / с. Екранована кручена пара має кращу в порівнянні з неекранованої помехозащищенностью, і швидкість передачі по цьому кабелю – 16 Мбіт / с на відстані до 90 м.

Коаксіальний кабель. Складається з центрального провідника (суцільного або багатожильного), покритого шаром полімерного ізолятора, поверх якого розташований інший провідник (екран). Екран являє собою оплетку з мідного дроту навколо ізолятора або обгорнуту навколо ізолятора фольгу. У високоякісних кабелях присутні і обплетення і фольга. Коаксіальний кабель забезпечує більш високу стійкість перед перешкодами проти кручений парою, дозволяє передавати інформацію на відстань до 2000 м зі швидкістю до 44 Мбіт / с, але він дорожче, і виникають проблеми з нарощуванням кабелю.

Оптичний кабель. Складається з одного або декількох кварцових волокон (іноді полімерних), покритих захисною оболонкою. Оболонка, як правило, складається з декількох шарів для забезпечення кращого захисту волокон. Дозволяє передавати інформацію на далеку відстань зі швидкістю до 10 Гбіт / с.

Топологія – це конфігурація локальної мережі, яка описує схему фізичного з'єднання комп'ютерів, тип обладнання, методи управління обміном, надійність роботи і можливість розширення мережі.

Виділяють два способи з'єднання – послідовне і з'єднання зіркою. При послідовному з'єднанні комп'ютери можуть бути з'єднані кільцем

або загальної шиною.

З'єднання кільцем. При цьому з'єднанні дані передаються послідовно від комп'ютера до комп'ютера, причому, у двох напрямках, що підвищує стійкість до неполадок мережі. Один розрив не виводить мережу з ладу, але два розриву роблять мережу неробочий. Кільцева мережа досить широко застосовується через високу швидкість передачі даних і надійності. Однак вартість такої мережі досить висока за рахунок витрат на адаптери, кабелі та додаткові пристосування.

З'єднання по загальній шині. При такому з'єднанні обмін може здійснюватися безпосередньо між будь-якими комп'ютерами мережі, незалежно від інших. За пошкодження зв'язку одного комп'ютера із загальною шиною цей комп'ютер відключається від мережі, але вся мережа працює. У цьому сенсі мережа досить стійка, але якщо пошкоджується шина, то вся мережа виходить з ладу.

З'єднання зіркою. У цій топології кожен комп'ютер підключається до спеціального концентратора (комутатора, хабу). Така мережа дуже стійка до пошкоджень. При пошкодженні одного із з'єднань від мережі відключається тільки один комп'ютер. Окрім того, ця схема з'єднання дозволяє створювати складні розгалужені мережі.

Всі зазначені схеми можуть, в свою чергу, бути одноранговими або з виділеним сервером, в залежності від способу організації.

У тимчасової мережі всі комп'ютери рівноправні. З кожного комп'ютера є доступ на всі інші комп'ютери мережі.

Мережа з виділеним сервером має центральний комп'ютер – сервер, який керує роботою мережі. Це найбільш потужний комп'ютер, з великим об'ємом оперативної і дискової пам'яті. Сервер розподіляє доступ користувачів до комп'ютерів мережі і до загальних мережних ресурсів. Спільним є жорсткий диск сервера, на ньому знаходяться програми, які можуть все запускати, і через нього користувачі обмінюються інформацією. Загальні апаратурні ресурси можуть бути розподілені по мережі. Наприклад, один комп'ютер в мережі має CD-ROM, а інший – принтер, а на третьому встановлений модем. Мережа робить доступними всі ці пристрої для спільного використання.

Сервер – це головний комп'ютер мережі, що надає доступ до загальної бази даних, спільне використання пристроїв введення-виведення, забезпечення взаємодії користувачів.

Інші комп'ютери називаються робочими станціями або клієнтами.

Кожному клієнту виділяється реєстраційне ім'я та пароль.

Клієнт – комп'ютер в мережі, який має доступ до інформаційних ресурсів і пристроїв сервера.

Клієнти, в свою чергу, можуть бути серверами для інших комп'ютерів. Наприклад, одна і та ж машина, будучи клієнтом головного сервера мережі, може надавати свої інформаційні ресурси (файли, програми, тексти) іншим комп'ютерам.

Глобальні комп'ютерні мережі

На відміну від локальних мереж в глобальних мережах немає будь-якого єдиного центру управління. Глобальна мережа будується на основі декількох потужних комп'ютерів-серверів, з'єднаних між собою. До цих серверів зазвичай підключені регіональні сервери зі своїми мережами, корпоративні та локальні мережі. А до локальних мереж – користувачі окремих комп'ютерів. Хоча для підключення окремого комп'ютера до глобальної мережі зовсім не обов'язково підключати його до мереж проміжних рівнів.

Підключитися до глобальної мережі можна за допомогою прямого доступу по виділеному каналу. У якості виділених каналів можуть бути коаксіальні і оптоволоконні кабелі, радіорелейні лінії, супутниковий зв'язок. За видами каналів розрізняють і модеми: радіомодеми, телефонні модеми, волоконно-оптичні модеми та ін.

За виділених ліній зв'язку швидкість передачі даних збільшується до декількох десятків тисяч бод. Такі лінії зв'язку постійно підключені і вигідні при передачі великих обсягів інформації або термінової передачі даних. Наприклад, система резервування і продажу авіаквитків діє при виділених лініях зв'язку.

Застосування супутникового зв'язку і високошвидкісних оптоволоконних ліній зв'язку підвищує пропускну здатність каналів до сотень мільйонів кілобод. Завдяки таким каналам, виявляється можливим об'єднання всіх комп'ютерних мереж в глобальні мережі, що зв'язують користувачів незалежно від їх географічного розташування.

Інтернет. Сервіси мережі Інтернет

Електронна пошта, або e-mail, є аналогом звичайної паперової пошти. Електронна адреса дозволяє абсолютно однозначно ідентифікувати користувача цієї послуги серед мільйонів інших користувачів мережі. За допомогою спеціальних програм для пересилки електронної пошти, знаючи адресу іншої людини, можна відправити йому текстове повідомлення, програми, зображення, словом, будь-яку інформацію, здатну зберігатися в електронному вигляді на комп'ютері, і вона буде доставлена через кілька хвилин навіть на інший кінець Землі. Наразі будь-яка інша людина, знаючи вашу електронну адресу, зможе відправити електронне послання вам. Електронна пошта (E-mail) є сервіс, призначений для пересилки повідомлень між користувачами

Інтернету і локальних мереж. Основна ідея полягає в наступному: кожен користувач має унікальний поштову адресу, як правило утворений з його реєстраційного (вхідного) імені та імені сервера, де він зареєстрований. Таким чином, зберігається деяка аналогія з паперової поштою, де адреса складається з двох частин: «Куди» і «Кому». «Куди» – на сервер, «Кому» – користувачеві. Ім'я користувача й ім'я сервера поділяються символом «@» (званим «комерційне ат», а користувачі часто використовують термін «равлик»). Ніякі прогалини в адресі не допускаються.

Для роботи з електронною поштою існує багато різних програм.

Телеконференції, або як їх ще називають, групи новин, схожі на електронну пошту. Різниця полягає в тому, що телеконференції – це як би величезний, безперервно оновлюється електронний журнал, розбитий на безліч розділів по інтересам, на які можна підписатися і отримувати повідомлення тільки з цікавлять вас розділів, а нецікаві просто ігнорувати. Ви можете не тільки читати повідомлення, що надходять в телеконференції, а й посилати туди свої питання, пропозиції і висловлювати думки, які прочитають всі люди, підписані на ці розділи.

Ну і нарешті World-Wide-Web (WWW). WWW – це гіпертекстова середа, що містить величезну кількість різних документів, таких як інформаційно-довідкові бази даних, урядові документи, каталоги бібліотек і багато, багато іншого. Ви можете переглядати такі документи в реальному часі, переходячи від одного документа до іншого простим натисканням на кнопку миші, наведеної на потрібну вам посилання. Основна перевага WWW полягає в тому, що документи можуть мати посилання не тільки в межах однієї бази або комп'ютера, але можуть посилатися і на інші документи, що зберігаються на віддаленому комп'ютері. У результаті ми отримуємо як би єдине гіпертекстове простір, по якому можна переміщатися в будь-якому необхідному напрямку в пошуках потрібної інформації.

Електронна пошта і дошки оголошень – найдешевший вид міжрегіональної зв'язку – це система міжкомп'ютерного зв'язку, при якій один ПК, використовуючи спеціальний протокол, залишає повідомлення на спеціальному комп'ютері (сервері), фізичне місцезнаходження якого не має значення, – якщо дане повідомлення орієнтоване на використання одним користувачем – це електронна пошта; якщо ж повідомлення призначене широкому колу користувачів – це дошка оголошень.

Система телеконференцій і чат-серверів – це система

міжкомп'ютерного зв'язку в реальному часі.

World Wide Web («Всесвітня павутина») – система доступу до даних, що використовується в Інтернет. Користувач отримує доступ до сторінок (pages) інформації, що містить текст, графіку і посилання на інші сторінки інформації. Графічні програми перегляду (graphical browser programs, браузери) дозволяють переходити на іншу сторінку, що містить потрібну вам інформацію, за допомогою клацання миші на засланні.

Система WWW складається з великого числа програм-серверів, що виконуються на машинах мережі Інтернет. Спільно сервери WWW утворюють розподілену базу даних мережевого гіпертексту. Сервер наповнюється інформацією на будь-яку тему, включаючи образи фотографій і картин, музики, шумів і мови. Далі користувач через мережу Інтернет за допомогою однієї з програм перегляду у себе на комп'ютері звертається до цього сервера на його адресу в мережі. Користувач бачить текст, у якому, виділені деякі ділянки тексту – «посилання». Досить клацнути по такому ділянці мишкою і розкриється зміст нового документа. При цьому посилання може практично миттєво (за кілька секунд) привести користувача на сервер WWW, встановлений на іншому кінці світу.

Технологія World Wide Web базується на трьох важливих стандартах. Перший з них - URL (Universal, або Uniform Resource Locator, універсальний адресу ресурсу) – надає стандартний спосіб завдання розташування даних, доступних в глобальній комп'ютерній мережі Інтернет.

Другий – протокол HTTP (Hyper Text Transfer Protocol, протокол передачі гіпертексту) – надає доступ до інформації і дозволяє передавати гіпертекстові документи по мережі.

Нарешті, HTML (Hyper-Text Markup Language, мова розмітки гіпертексту) дозволяє створювати текстові документи, що включають посилання на URL інших даних. Найчастіше ці посилання вказують на інші документи HTML, що наразі є доступними за допомогою HTTP. У результаті перед користувачем розстеляється величезна павутина взаємозалежної інформації.

Слід зазначити, що HTML не дозволяє точно задавати зовнішній вигляд документа. Можна лише пропонувати свій варіант оформлення. Різні програми перегляду можуть інтерпретувати ваші пропозиції по-своєму. Автори, які орієнтуються на можливості тільки однією з програм перегляду, обмежують коло потенційної аудиторії.

URL – спеціальна форма адреси інформації в мережі Інтернет, яка

містить дані про ім’я сервера, на якому зберігається документ, шлях до каталогу файлу та власне ім’я файлу. URL-адреса складається з двох частин. Спочатку вказується спосіб зв’язку, за допомогою якого буде здійснюватися доступ до даних. Від цього залежить, яка додаткова інформація буде потрібно. Потім міститься інформація про те, де ці дані розташовані. Поділяються ці частини двокрапкою, наприклад: http: // ім’я_сервера / шлях / файл.

Розглянемо найбільш поширені способи доступу до даних в мережі Інтернет.

HTTP (протокол передачі гіпертексту) був розроблений спеціально для World Wide Web. При використанні цього протоколу необхідно вказати ім’я машини, а також повідомити додаткову інформацію, яку комп’ютер зможе використовувати для пошуку і створення необхідних даних. Ці додаткові дані зазвичай представляють собою ім’я файлу і інформацію про каталог. Частково через те, що перші розробки були створені на системах Unix, для поділу імен каталогів і файлу в URL використовується пряма похила риска «/». Наприклад, «http://www.ctc.msiu. ua».

FTP (File Transfer Protocol, протокол передачі файлів) – давно використовується метод доступу, розроблений для передачі великих обсягів інформації з Інтернет. Цей метод набув широкого поширення вже досить давно. Щоб отримати доступ до файлу або каталогу FTP, необхідно вказати ім’я машини і ім’я файлу або каталогу цієї машини. Наприклад, «ftp://prep.ai.mit.edu».

Поява в листопаді 1996 року сервісу ICQ (можна прочитати як I Seek You, тобто «Я шукаю тебе», а російськомовні користувачі ласкаво охрестили цю програму «аською»), надало ще одну, справді революційну, можливість спілкування користувачам Інтернет. Назва відображає найважливіша відмінність цієї програми від більшості інших програм спілкування в Інтернеті. ICQ насправді дозволяє «бачити» всіх ваших друзів і знайомих, щойно вони з’являються в мережі Інтернет у режимі он-лайн. ICQ надає можливість, забувши про відстані, миттєво зв’язатися зі своїми знайомими або діловими партнерами в будь-який час. ICQ дозволяє обмінюватися повідомленнями, посилати файли і URL. За допомогою зручної системи налаштувань можна встановити необхідний рівень конфіденційності – від найпростішого до самого «засекреченого», коли ви бачите всіх, а вас не бачить ніхто.

В ОС Linux можливості цього сервісу надають програми licq і kicq. Ці програми виконуються у фоновому режимі, використовуючи мінімум пам’яті і ресурсів мережі. Ви можете займатися чим завгодно, тому що

ICQ попередить, коли надійде нове повідомлення.

Кожен користувач ICQ має свій особистий номер, який можна поміщати на візитних картках і інших ділових паперах – адже прямі контакти набагато ефективніше, ніж тривала переписка (навіть і по електронній пошті). Про популярність ICQ свідчить величезна кількість її користувачів, що стає дедалі більше.

Пошук інформації в Інтернет.

Сучасна Мережа дійсно у змозі запропонувати своєму користувачеві масу інформації самого різного профілю. Тут можна познайомитися з новинами, цікаво провести час, отримати доступ до різноманітної довідкової, енциклопедичної та навчальної інформації. Інтернет можна ефективно використовувати для вирішення найрізноманітніших завдань на роботі і вдома.

Найголовніша проблема, що виникає при роботі з Мережею, – швидко знайти потрібну інформацію і розібратися в ній, оцінити інформаційну цінність того чи іншого ресурсу для своїх цілей. Шлях до величезного інформаційного багажу людства, що зберігається в бібліотеках, фонотеках, фільмотеки, лежить через картки каталогів. В Інтернеті існують аналогічні механізми для знаходження необхідної інформації. Йдеться про пошукових серверах, службовців відправною точкою для користувачів Мережі. Зі змістовної точки зору про них можна говорити як про спеціальну службу Інтернету, хоча вони використовують механізми Всесвітньої Павутини і з технічної точки зору не виходять за її рамки.

Пошукові сервери досить численні і різноманітні. Прийнято розрізняти пошукові індекси і каталоги. Сервера-індекси працюють таким чином: регулярно читають зміст більшості веб-сторінок Мережі («індексують» їх), і поміщають їх повністю або частково в загальну базу даних. Користувачі пошукового сервера мають можливість здійснювати повнотекстовий пошук по цій базі даних, використовуючи ключові слова, які стосуються їх цікавить. Видача результатів пошуку зазвичай складається з витягів рекомендованих увазі користувача сторінок і їх адрес (URL), оформлених у вигляді гіперпосилань. Працювати з пошуковими серверами цього типу зручно, коли добре уявляєш собі, що саме хочеш знайти.

Каталоги виросли зі списків цікавих посилань, закладок (bookmarks). По суті справи вони являють собою багаторівневу смислову класифікацію посилань, побудовану за принципом «від загального до конкретного». Іноді посилання супроводжуються коротким описом ресурсу. Переважно пошук у назвах рубрик

(категоріях) і описах ресурсів можливий за ключовими словами. Каталогами користуються тоді, коли не цілком чітко знають, що саме шукають. Переходячи від найзагальніших категорій до більш приватним, можна визначити, з яким саме ресурсом Мережі слід ознайомитися. Пошукові каталоги доречно порівнювати з тематичними бібліотечними каталогами, словниками-тезаурусами або біологічними класифікаціями тварин і рослин. Ведення пошукових каталогів частково автоматизовано, але до сих пір класифікація ресурсів здійснюється головним чином вручну.

Пошукові каталоги бувають загального призначення і спеціалізовані. Пошукові каталоги загального призначення включають в себе ресурси самого різного профілю. Спеціалізовані каталоги об'єднують тільки ресурси, присвячені певній тематиці. Їм часто вдається досягти кращого охоплення ресурсів зі своєї області і побудувати більш адекватну рубрикацію.

Історія пошукових служб починається в середині 90-х років. У 1994 році два аспіранти Стенфордського Університету, Девід Філо і Джері Янг, почали роботу над створенням каталогу Yahoo (http://www.yahoo.com/; англ. «Yahoo» – «йеху» з «Мандрів Гуллівера» Джонатана Свіфта). Вони переслідували просту мету: організувати власні посилання. Щоб зробити це ефективним чином, їм довелося побудувати спеціальну систему з використанням бази даних. Вона могла одночасно витримувати звернення тисяч користувачів. І ці звернення не забарилися наслідувати. На початку 1995 року Марк Андресс, один з співзасновників корпорації Netscape Communications, запропонував творцям вже завоював величезну популярність Yahoo перенести систему з кампусу Стенфордського Університету на сервера Netscape. Величезне навантаження з університетської мережі була знята, а Yahoo став комерційним проектом. Сьогодні його творці – мультимільйонери; над веденням каталогу трудяться тисячі фахівців в самих різних областях знання.

Один з перших індексуючих пошукових серверів, AltaVista («вид з висоти») корпорації Digital (тепер Compaq), з'явився в 1995 році. Кільком службовцям корпорації-виробника суперкомп'ютерів спало на думку використовувати новітні сервери для зчитування вмісту Всесвітньої Павутини в базу даних і здійснення пошуку по ній. Сервер AltaVista, розташований за адресою http://altavista.digital.com/, – один із найбільших пошукових серверів сьогоднішньої Мережі.

Останнім часом пошукові каталоги загального призначення і індексуючи пошукові сервера інтенсивно інтегруються. Yahoo вже не

тільки каталог, але і пошуковий сервер. AltaVista, як і багато інших пошукові сервера, початково пропонували виключно пошук по базі даних, сьогодні включає в видачу результатів пошукового запиту ще й список рубрик, що відповідають темі запиту. Пошукові технології не стоять на місці. Традиційні індексуючі сервера шукали в базі даних документи, що містять ключові слова з пошукового запиту. За такого підходу дуже складно оцінити значення і якість ресурсу, що видається користувачеві. Альтернативний підхід – шукати такі веб-сторінки, на які посилаються інші ресурси з даної тематики. Чим більше посилань на сторінку існує в Мережі – тим більше шансів, що ви її знайдете. Такий своєрідний мета-пошук здійснює пошуковий сервер Google (http://www.google.com/).

Крім пошукових серверів, приносять в свої бази веб-сторінки по всій Мережі, є пошукові сервера, орієнтовані більш вузько в географічному і мовному відношенні. Так, існує багато російських пошукових серверів. Їх короткий список ви знайдете в наступному розділі.

У світі існує величезна кількість WWW серверів самого різного призначення. Без спеціальних засобів орієнтування в цьому гігантському обсязі інформації просто неможлива. Вирішують цю проблему пошукові сервери, які зберігають мільйони посилань на різні теми і виробляють пошук потрібних документів за запитом користувача.

Для того щоб полегшити пошук документів були створені каталоги WEB-серверів і пошукові машини. У більшості випадків каталог являє собою тематичні добірки посилань на Web-ресурси (медицина, політика, програмування та т. ін.). Пошукові ж машини дозволяють потрапити на сторінку, текст якої містить заданий набір слів. Кожна пошукова машина має свої специфічні можливості, переваги і недоліки. Слід зазначити, що наповнення мережі Інтернет російськомовної інформацією, хоча і відбувається швидкими темпами, все ще значно відстає від рівня англомовної інформацією. Англійська мова продовжує залишатися основною мовою спілкування користувачів Інтернет.

Робота з пошуковими серверами

Робота з пошуковими серверами не становить великих труднощів. Ви заходите на свій улюблений пошуковий сервер, в рядку запиту набираєте потрібною мовою ключові слова або фразу, відповідні ресурсу або ресурсів Мережі, які ви хочете знайти. Потім натискаєте мишею на кнопку з англійським написом «Search» або українським

написом «Пошук», і через кілька секунд в робочому вікні браузера з'являються результати пошуку.

Зазвичай пошуковий сервер видає результати пошуку невеликими порціями, наприклад, по 10 на одну сторінку видачі. Тому часто вони займають більше однієї сторінки. Тоді під списком рекомендованих посилань буде знаходитися посилання, що пропонує перейти до наступної «порції» результатів пошуку.

В ідеальному випадку той ресурс, який ви шукаєте, пошуковий сервер помістить на першу сторінку результатів пошуку, і ви відразу розпізнаєте одне з посилань по короткому описі. Однак часто доводиться переглянути кілька ресурсів, перш ніж виявляється відповідний. Як правило, користувач переглядає їх в нових вікнах браузера, не закриваючи вікно браузера з результатами пошуку. Іноді пошук і перегляд знайдених ресурсів ведеться в одному і тому ж вікні браузера. Якщо ресурс не задовольняє очікувань користувача, то користувач повертається до результатів пошуку, використовуючи кнопку «Назад» («Back») в меню браузера.

Ключові слова, що становлять пошуковий запит, зазвичай просто розділяються пробілами. Різні пошукові сервера по-різному інтерпретують це. Деякі з них відбирають за таким запитом тільки документи, що містять всі ключові слова, тобто сприймають пробіл в запиті як логічний зв'язку «і». Деякі інтерпретують пробіл як логічне «або» і шукають документи, що містять хоча б одне з ключових слів. Під час формування пошукового запиту більшість серверів дозволяють в явному вигляді вказати логічні зв'язки, що об'єднують ключові слова, і задати деякі інші параметри пошуку. Логічні зв'язки зазвичай позначаються за допомогою англійських слів «and», «or», «not». На різних пошукових серверах при формуванні розширеного пошукового запиту використовується різний синтаксис. Зазвичай на титульній сторінці пошукового сервера є посилання з назвою, схожою на «допомогу» (англ. «Help»). Можливо, саме вона вказує на документ, що пояснює правила формування розширеного пошукового запиту. Прочитайте такий документ на пошуковому сервері, яким станете користуватися найчастіше, і освойте все багатство можливостей, що надаються цим сервером. Це дозволить вам складати більш точні запити, а грамотна побудова пошукового запиту грає вирішальну роль в процесі пошуку.

Із першого разу вдало поставити запитання пошукового сервера виходить не завжди. Якщо запит короткий і в ньому присутні не менше часто вживані слова, може бути знайдено дуже багато документів, сотні

тисяч і мільйони. Навпаки, якщо ваш запит виявиться занадто деталізованим або в ньому будуть використані дуже рідкісні слова, ви побачите повідомлення про те, що ресурсів, відповідаючих вашому запиту, в базі сервера не знайдено.

Поступове звуження або розширення фокусу пошуку через збільшення або зменшення переліку ключових слів, заміна невдалих пошукових термінів на більш вдалі допоможуть вам поліпшити результати пошуку.

Ще один дуже важливий момент амце вибір відповідного для ваших завдань пошукового сервера. Як було зазначено, працювати з індексується пошуковими серверами добре, коли зрозуміло, що саме потрібно знайти. Каталогами користуються в тих випадках, коли не цілком чітко знають, що саме шукають. Коли предметна область окреслена, але що саме в ній вас цікавить в даний момент, ви не цілком розумієте, дуже корисним може виявитися використання спеціалізованого пошукового каталогу.

Наведемо список деяких найбільш відомих пошукових серверів загального призначення. Всі ці сервера в даний час пропонують і повнотекстовий пошук, і пошук за категоріями, таким чином, поєднуючи в собі переваги сервера і каталогу, які індексуються.

Спробуйте також попрацювати з пошуковим сервером Google, розташованим за адресою http://www.google.com/. Не пропустіть цю можливість використовувати останні досягнення в області пошукових технологій Інтернету.

Якщо ви шукаєте файл з певним назвою, але не знаєте, на якому FTP- сервері його знайти або з якого FTP-сервера виявиться швидше його завантажити, вам допоможе FTP Search (http://ftpsearch.lycos.com/) – винайдена в Норвегії служба пошуку по ftp-серверів, розташована на WWW. Це ще один яскравий приклад вдалої інтеграції різних служб Мережі на основі Web.

7.2. Нормативно-правова база обробки юридичної інформації в мережі Інтернет

Основні принципи побудови системи інформаційно-аналітичного забезпечення законотворчої та правозастосовної діяльності визначаються великим обсягом опрацьовуваної інформації, складністю алгоритмів перетворення даних, значною кількістю користувачів. Вона належить до відкритих систем, безперервно обслуговує в реальному часі

правотворчий та правозастосовний процеси.

Опрацювання потоків інформації охоплює декілька етапів, кожний з яких має свої специфічні алгоритми й технологічні операції. Отже, робота над законопроектом тільки в підрозділах Верховної Ради України складається з близько ста різних операцій опрацювання даних, кожна з яких є важливою в розробці якісного нормативно-правового акту.

Системна інформатизація законотворчого процесу в українському парламенті дозволила впровадити сучасну організацію та технологію опрацювання даних, що охоплює використання нових методів і засобів, фіксацію та попередню підготовку інформації, зберігання, актуалізацію, запобіжне дублювання інформації на випадок можливих пошкоджень оригіналу й оперативне надання даних користувачам у потрібних їм аспектах. При цьому пропонуються різноманітні форми надання інформації: одержання твердих копій, видача на екран, компакт-диски та інші носії.

Створення та розвиток СІАЗ (служба інформаційно-аналітичного забезпечення) відбуваються із дотриманням низки загальновідомих принципів, які слід розрізняти кожний окремо. Принцип системного підходу базується на системному аналізі об’єкта, потоків інформації, алгоритмів їх перетворення, а також системи в цілому, тобто на виборі цілей, засобів, етапів, критеріїв доцільності інших чинників, що впливають на функціонування системи. Ці чинники можуть мати правовий, політичний, економічний, соціальний, організаційний, технічний характер. Сутність принципу «нових завдань» полягає в перебудові традиційних методів і прийомів керування відповідно до нових можливостей сучасних методів і засобів обробки даних, тобто в докорінній реорганізації всієї системи обробки інформації та керування на нових засадах.

7.3. Імпорт даних з Інтернет до таблиці MS Excel

У програмі Excel можна працювати з численними типами джерел даних, зокрема з внутрішніми та зовнішніми даними.

Визначення зовнішніх даних.

Зовнішні дані – це дані, що зберігаються в іншому розташуванні, наприклад на сервері. Ви можете їх імпортувати або відобразити в книзі, використовуючи для цього один чи кілька зв’язків із зовнішніми даними. До зовнішніх джерел даних відносяться таблиці SQL Server,

куби служб аналізу SQL Server Analysis Services, дані Ринку Microsoft Azure тощо. Зв'язки із зовнішніми даними, що використовуються в книзі, дають змогу надсилати запити й отримувати дані з баз даних, указаних у зв'язках. Завдяки цьому ви можете оновлювати дані й бачити в книзі найсвіжішу інформацію.

Як альтернативу роботі із зовнішніми даними ви можете використовувати внутрішні дані програми Excel. Внутрішні дані зберігаються безпосередньо в книзі й не вимагають підтримки зовнішніх зв'язків даних, навіть якщо зовнішній зв'язок використовувався для імпорту даних у книгу.

Обмін даними та робота в Інтернеті.

Можливість використовувати найсвіжіші дані. За допомогою Microsoft Excel можна одержувати їх у вигляді електронних таблиць прямо з Web-серверів у мережі Internet. Microsoft Excel містить вбудовані функції, що дають змогу легко поміщати на Web-сервер документи, створені в середовищі редактора Micro-soft Excel. До їх числа належать: майстер збереження документа у форматі HTML, засіб перегляду вмісту документів Microsoft Excel для користувачів, що не працюють з цим додатком, і ряд інших.

Можна використовувати вбудований Internet Assistant для перетворення таблиці у формат HTML і публікації на Web-сер-вері. Microsoft Excel дає імпортувати дані з HTML-документів, знайдених на Web-сервері, відновлюючи при цьому формат і оформлення таблиці. Після імпорту дані доступні для виконання будь-яких операцій у редакторі Microsoft Excel.

Web Queries. У Microsoft Excel існує операція створення запиту до даних, що зберігаються на Web-сервері. Можна створити постійне посилання на сторінку в Інтернеті, і дані в таблиці оновлятимуться автоматично.

Практичні завдання

Завдання № 1.

Використовуючи мережу Інтернет, слід знайти відповідні закони та законодавчі документи, що регламентують юридичну та правоохоронну діяльність в Україні з точки зору обробки і захисту інформації, та ввести їх до таблиці 1.

Таблиця 1

№ з/п	Назва закону	Основні поняття, визначення	№ Закону, дата. Чинний чи ні	Вказати зміни, якщо є і які
1	Закон України «Про інформацію». Поняття правової інформації.			
2	Кримінально-процесуальний та Кримінальний кодекси України			
3	Інформаційні системи державно-правового характеру			
4	Закон України «Про електронні документи та електронний документообіг»			
5	Закон України «Про електронний підпис». Технічне та юридичне забезпечення електронного цифрового підпису.			
6	Закон України «Про порядок відправлення та передавання електронних документів, а також їх одержання»			
7	Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»			
8	Законі України «Про телекомунікації»			
9	Закон України «Про Національну систему конфіденційного зв’язку»			
10	АІПС «Нормативні акти України»«			
11	Кримінальний кодекс України «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку»			

№ з/п	Назва закону	Основні поняття, визначення	№ Закону, дата. Чинний чи ні	Вказати зміни, якщо є і які
12	Види загроз для комп'ютерної інформації			
13	Комп'ютерні технології в юридичній діяльності.			
14	Електронне (віртуальне) судочинство			
15	Єдиний державний реєстр виконавчих проваджень			
16	Нотаріальні реєстри			
17	Всесвітня електронна мережа правових документів			
18	Загальноправові бази даних			
19	Комп'ютерна мережа Верховної Ради України			
20	Комп'ютерні злочини			

Основні пошукові портали

Найбільш популярні пошукові системи в Інтернеті: Google, Yahoo, Msn, Aol, Ask, Altavista, Excite, Lycos, All The Web; українські – Uaport, Poshuk, El.visti, Meta, Uaportal, Bigmir, Echo та ін.

У мережі Інтернет багато сайтів правової тематики. Українські юридичні ресурси в Інтернеті можна класифікувати наступним чином:

Бази законодавства:

– LIGAOnline – www.liga.net – база законодавства компанії «ЛігаБізнесІнформ».

– «АТ Информтехнология»–www.nau.kiev.ua – розроблювач популярної програми «Нормативні акти України».

– «Сервер Верховної Ради України» – www.rada.gov.ua – безкоштовна база законодавства, інформація щодо юридичних видань, посилання на зарубіжні законодавства.

– «Сервер законодавчих актів України на Trifle.Net» (відомий також як базазаконодавства на сервері Apex). URL : www.apex.dp.ua.

Каталоги юридичної інформації:

– Розділ «Ukraine/Law» на Yahoo!-(англ.) dir.yahoo.com/Government/Law/. «BRAMA: Ukrainian Law and Legal Matters». URL : www.brama.com (англ.) каталог української юридичної інформації

– «FindLaw:Ukraine-(engl.)» URL : www.findlaw.com, довідник ресурсів Інтернету юридичної тематики.

– «Ukraine at CEE Source: Central and East European Legal, Political, Business and Economics WWW Resources» – (англ.) URL : www.law.gonzaga.edu – розділ про Україну в базі даних по праву, політиці й економіці країн Центральної і Східної Європи.

– Розділ «Правительство» на «Ping:» URL : www.topping.od.ua. Державні органи:

– «Перелік серверів державних органів» на сайті Верховної Ради України URL : portal.rada.gov.ua.

– «Кабінет Міністрів України» – (укр.) інформація про Кабінет Міністрів України. URL : www.kmu.gov.ua/.

– «Головне керування державної служби України». URL : www.guds.gov.ua/.

– «Міністерство закордонних справ України». URL : www.mfa.gov.ua/.

– «Міністерство внутрішніх справ України» – (англ.,укр.). URL : www.mvs.gov.ua/.

– Сайт постійного представництва України в ООН. URL : www.un.org .ua/.

– «Національний банк України». URL : www.bank.gov.ua.

– «Інформаційний центр Міністерства юстиції України». URL : www.informjust.kiev.ua.

Завдання № 2

Ситуація: Вночі у місті Д. було здійснено злочин, що може бути класифіковано як пограбування (заволодіння чужим майном) магазину побутової техніки. У цей час у магазині знаходилися товари різних постачальників з Європи та США. Потрібно скласти перелік товарів (15 позицій), які було викрадено та класти таблицю поточного курсу гривні відносно інших валют

Курс долара США	**Курс євро**	**Курс польського злотого**

Алгоритм виконання

Актуальні курси іноземної валюти можна подивитися за посиланням http://katani.dp.ua/ . Для того, щоб імпортувати дані про

курс зі сторінки до мережі Інтернет потрібно використовувати пункт меню «Дані» в MS Excel, як на рисункунижче (рис. 7.1).

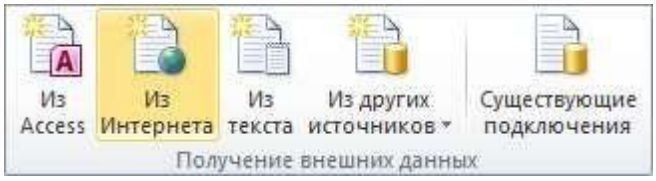


Рис. 7.1. Можливі варіанти отримання даних у редакторі MS Excel

У вікні в рядок Адрес введіть URL сайту, з якого буде братися інформація про курси валют (наприклад http://katani.dp.ua/) і натисніть Enter.

На попередження безпеки (рис. 7.2) на сторінці відповідайте згодою.

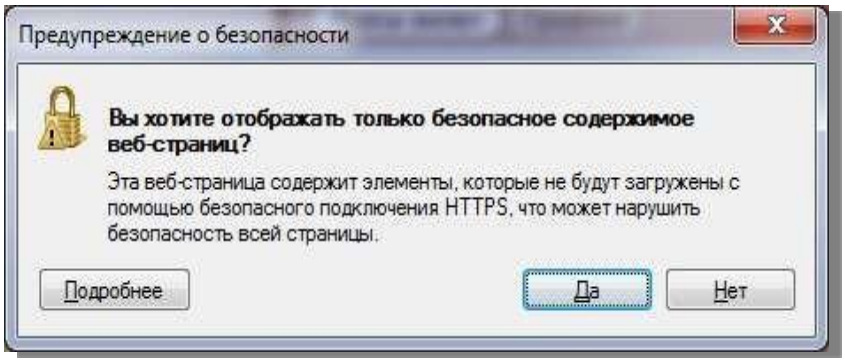


Рис. 7.2. Вікно попередження безпеки

Далі дозволяємо продовжувати виконання сценарію (рис. 7.3):

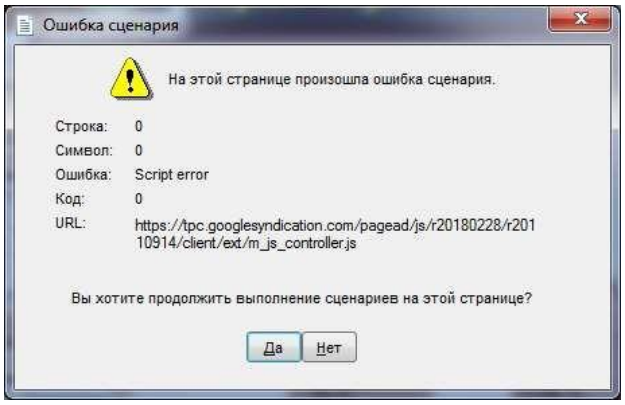


Рис. 7.3. Вікно продовження сценарію

Коли сторінка завантажиться, то на таблицях, що MS Excel може імпортувати, з'являться жовто-зелені стрілки (рис. 7.4). Клацання по такій стрілці позначає таблицю для імпорту.

Рис. 7.4. Загальний вигляд веб-сторінки у редакторі MS Excel

Коли всі необхідні таблиці позначені – натисніть кнопку ***Імпорт (Import)*** внизу вікна. Через деякий час, потрібний для завантаження даних, вміст імпортованих таблиць з'явиться в осередках на аркуші.

Для додаткового налаштування можна клацнути по будь-якій із цих осередків правою кнопкою миші та вибрати в контекстному меню команду ***Властивості діапазону*** (Data range properties). У цьому діалоговому вікні можна, при бажанні, налаштувати періодичність оновлення та інші параметри (рис. 7.5):

Котирування акцій, тому що вони змінюються кожні кілька хвилин, можна оновлювати частіше (прапорець Оновлювати кожні N хв.), а ось курси валют, у більшості випадків, достатньо оновлювати раз на день (прапорець Оновлення під час відкриття файлу).

Зверніть увагу, що весь імпортований діапазон даних сприймається Excel як єдине ціле та отримує власне ім'я (в нашому прикладі це буде http://katani.dp.ua/).

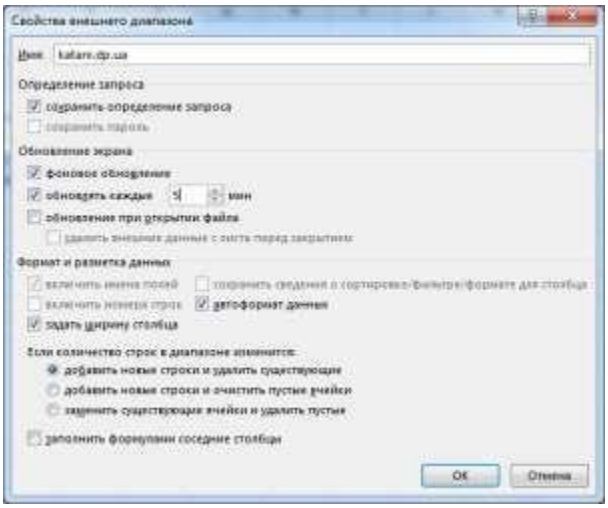


Рис. 7.5. Властивості зовнішнього діапазону

Таблиця 7.1

Перелік викраденого майна в відповідних грошових еквівалентах

	Найменування товарів	**Ціна в доларах США**	**Ціна в грн.**	**Ціна в євро**	**Ціна в Злотих (польських)**
1	Телевізор Samsung UE-43MU6172	242			
2	Телевізор Samsung UE-32M5002	360			
3	Телевызор Samsung UE-50MU6172	528			
4	Samsung UE-22H5600	820			
5	ТелевізорSamsung UE-32J5200	918			
…	…..	….			
15	Телевізор Samsung UE-40NU7122	655			

1. Розрахувати вартість у національній валюті, у доларах США, польських злотих. Встановіть для кожної валюти відповідний грошовий формат.
2. Побудуйте графіки вартості товарів за різними валютами.

Контрольні питання

1. Надайте визначення WWW?
2. Як називається комплекс апаратних та програмних засобів, що дозволяють комп'ютерам обмінюватися даними?
3. Що називають Web-вузлом?
4. Що таке URL?
5. За допомогою яких пристроїв можна підключитися до мережі «Інтернет»?
6. Комп'ютер, що надає послуги іншим комп'ютерам у мережі (клієнтам), називається?
7. Які бувають типи фаєрволів?
8. Сформуйте алгоритм дій щодо пошуку в мережі інтернет.
9. Які основні пошукові портали ви знаєте?
10. Що називають пошуковим порталом?
11. Нормативно-правовий документ це…
12. Сформуйте алгоритм дій щодо пошуку нормативно-правових документів у мережі інтернет.
13. Сформуйте алгоритм дій щодо створення каталогу нормативно-правових документів.
14. Які основні пошукові портали ви знаєте?
15. Набуття практичних навичок із роботою у законодавчих базах юридичних документів
16. Як визначається чинність нормативно-правового документу?
17. Що відноситься до каталогу юридичних документів?
18. Які існують законодавчі бази?
19. Що називають пошуковим порталом?
20. Дати визначення поняття «зовнішні дані».
21. Дати визначення поняття «Веб-запиту» у редакторі MS Excel.
22. Надати алгоритм формування таблиці даних з використання веб-порталу.
23. Надати алгоритм створення каталогу за результатами даних отриманих з веб-запиту.
24. Навести класифікацію можливих способів отримання

зовнішніх даних у редакторі MS Excel.

25. Яким чином змінювати автоматичне оновлення даних із веб-запиту?

26. Чи є можливість формувати запит даних із внутрішнього веб-серверу?

27. Які параметри можна редагувати у вікні властивості зовнішнього діапазону.

28. В яких випадках можна погоджуватися з «попередження небезпеки», що з'являється у вікні «попередження безпеки»?

29. Навести приклади застосування веб-запитів у правоохоронній діяльності?

Джерела до розділу 7

1. Інформаційні системи та технології: підручник / кол. авт.; ред. В. Б. Вишня. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2021. 296 с.

2. Міністерство внутрішніх справ України. Розшук. Інформаційний ресурс. URL : https://wanted.mvs.gov.ua/.

3. Національні інформаційні системи. Інформаційний ресурс. URL : https://nais.gov.ua/.

4. Єдиний державний реєстр судових рішень. Інформаційний ресурс. URL : https://reyestr.court.gov.ua/.

5. Офіційний сайт Верховної Ради України URL : http://www.rada.gov.ua.

6. Науково-дослідний центр правової інформатики. URL : http://ippi.org.ua.

7. Інноваційні сили України. URL : http://it-force.com.ua.

8. Український IT-портал. URL : http://www.ua-admin.com.

9. Ліга Закон. URL : http://www.ligazakon.ua/.

10. Юридична бібліотека (Україна). URL : http://law.biz.ua.

Розділ 8
ЗАХИСТ ІНФОРМАЦІЇ НА РІВНІ КОРИСТУВАЧА ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА

8.1. Безпека в комп'ютерних мережах

Комп'ютерна мережа (Мереживна взаэмодія)

Інформаційно-комунікаційні технології, що з'явилися у другій половині ХХ ст., суттєво змінили життя людства. Саме вони створили передумови формування інформаційного суспільства, в якому визначальну роль відіграють інформація та нові знання. Саме в такому суспільстві ми з вами сьогодні живемо.

Перші ЕОМ були призначені лише для швидкої обробки числових даних. Згодом обчислювальна техніка стала широко використовуватися в наукових дослідженнях, виробництві, освіті, побуті тощо. У користувачіввіддалених один від одного комп'ютерів виникла потреба у швидкому обміні даними. Для цього було запропоновано об'єднати комп'ютери в єдину систему і в такий спосіб передавати дані від одного комп'ютера до іншого. Так були створені комп'ютерні мережі.

Комп'ютерна мережа – це сукупність комп'ютерів та інших пристроїв,зв'язаних каналами передавання даних.

Комп'ютерні мережі забезпечують спільний доступ до даних. У мережі виділяють комп'ютери, на яких розміщують великі масиви даних, а користувачі інших комп'ютерів мережі одержують доступ до них. Це дає можливість, наприклад, людям, які працюють над одним проєктом, використовувати дані, створені іншими, тобто працювати над проєктом одночасно.

За допомогою комп'ютерної мережі є можливим спільне користування периферійними пристроями: принтерами, сканерами, модемами тощо. Невигідно мати їх біля кожного персонального комп'ютера, наприклад, у комп'ютерному класі або в банку.

Комп'ютерні мережі також дозволяють у короткі терміни розв'язувати складні інженерні задачі. У 2006 р. у Києві відкрито Центр суперкомп'ютерних обчислень. Найпотужніший суперкомп'ютер в Україні дозволяє вітчизняним ученим здійснювати обробку великих масивів даних, що зберігаються в різних організаціях, швидше

виконувати складні обчислення. Створення комп'ютерних мереж відкрило нові можливості для електронного зв'язку. Сьогодні люди, що мають комп'ютери, можуть спілкуватися між собою, незважаючи на віддаль і час. Із появою комп'ютерних мереж комп'ютер став своєрідним вікном у величезний світ інформації.

Основне призначення всіх комп'ютерних мереж – це спільний доступ до мережевих ресурсів (апаратного забезпечення комп'ютерів, периферійних пристроїв), спільне використання даних та швидкий обмін ними, спільне використання програмного забезпечення. Короткі відомості про комп'ютерні мережі.

Мережева взаємодія. Мережева взаємодія передбачає віддалений доступ до мережевих ресурсів та відбувається за технологією. Залежно від повноважень комп'ютери в мережі розподіляються на сервери та клієнтів. Клієнт – це комп'ютер користувача, який здійснює запит, сервер – комп'ютер, що обробляє цей запит і відповідає на нього. Звертаємо вашу увагу: сервером та клієнтом називаються як комп'ютери в мережі, так і програмне забезпечення, що працює на цих комп'ютерах.

Централізовані мережі. У централізованих мережах виділяється один потужний комп'ютер – виділений сервер, що виконує основні функції з організації роботи мережі. Такі мережі ще називають «клієнт-виділений сервер». Усі клієнти отримують доступ до ресурсів мережі через сервер.

На сервері встановлюється спеціальна операційна система (наприклад, 52 р). Операційна система дозволяє організувати і контролювати роботу комп'ютерів і користувачів у мережі, надавати кожному користувачеві певні права доступу до ресурсів і даних цієї мережі. Для цього кожен користувач отримує ім'я користувача (логін) та пароль для входу до мережі. Прикладами такої мережі можуть бути комп'ютерні мережі банків, корпорацій, вищих навчальних закладів, деяких шкіл м. Києва та інші. Перевагами централізованих комп'ютерних мереж є висока швидкість обміну даними і можливість розподіляти права доступу користувачів у них. Але суттєвим недоліком є те, у разі виходу з ладу сервера вся мережа перестає працювати.

Децентралізовані мережі. У децентралізованих мережах немає виділеного сервера: будь-який комп'ютер може бути як сервером, так і клієнтом. Такі мережі ще називають щоранговими. Як клієнт, комп'ютер в одноранговій мережі може здійснювати запит щодо доступу до ресурсів інших комп'ютерів мережі. Як сервер, комп'ютер повинен обробляти запити від інших комп'ютерів мережі та надавати

потрібні дані.

В одноранговій мережі всі комп'ютери мають однакові права (ранги) щодо доступу до ресурсів кожного й до периферійних пристроїв. Кожен користувач мережі може на своєму жорсткому диску визначити папки і файли, які він надає для загального користування.

У таких мережах на всі комп'ютери встановлюється операційна система, яка забезпечує їм рівні можливості.

Перевагою однорангових мереж є працездатність мережі у разі виходу з ладу будь-якого з комп'ютерів, а недоліком – неможливість розподіляти права клієнтів щодо роботи в мережі. Прикладом такої мережі може бути мережа комп'ютерного класу у більшості шкіл.

Типи комп'ютерних мереж. Об'єднані в мережу комп'ютери можуть бути розташовані в одній кімнаті, одному будинку, районі, місті, країні чи навіть у різних країнах. У багатьох школах України комп'ютери, встановлені в комп'ютерному класі, у кабінетах адміністрації, бібліотеці, кінолекційній залі та інших кабінетах, об'єднані в мережу.

У такій мережі є сервер, на якому можуть зберігатися:

– дані про всіх учнів та вчителів школи; розклад уроків, гуртків, факультативів;

– електронні журнали успішності учнів;

– практичні завдання до уроків; мультимедійне навчання; архіви учнівських робіт.

Працюючи в мережі, учні й учителі мають доступ до цих даних для підготовки до уроків, написання рефератів, створення презентацій, колективної роботи над проєктами тощо.

Прикладом мережі, що розташована в кількох спорудах, може бути мережа торговельного підприємства (центральний офіс, магазин, склад). У ній централізовано можна зберігати відомості про товари та їхню вартість, обробляти дані щодо продаж, що надходять із комп'ютерів, встановлених у різних відділах підприємства, вести облік товарів. Спеціальні мережеві програми дозволяють автоматизовано планувати роботу підприємства. Директор може перевірити, які товари ще є на складі або в торговому залі, а які відсутні, чи виконані доручення, розіслані ним мережею тощо.

І шкільна мережа, й мережа торговельного підприємства об'єднують комп'ютери, що розміщені на невеликих відстанях у межах одного приміщення або сусідніх приміщень. Такі мережі називаються локальними. Локальна мережа він комп'ютерна мережа, що об'єднує комп'ютери, які знаходяться в одному приміщенні або кількох

приміщеннях, розташованихна невеликій відстані одне від одного.

Але локальні мережі не дозволяють забезпечити спільний доступ до даних тим користувачам, що знаходяться, наприклад, у різних частинах міста. На допомогу приходять регіональні мережі, що об'єднують комп'ютери в межах одного регіону (району, міста, країни). Прикладами такої мережі є комп'ютерна мережа, що об'єднує комп'ютери, що знаходяться в будинках одного або кількох кварталів, комп'ютери директорів шкіл району, комп'ютерна мережа «Воля» у Києві та інші. Ще одним прикладом регіональної комп'ютерної мережі є Українська науково-освітня телекомунікаційна мережа «УРАН».

Мережа «УРАН» забезпечує школи, університети та інші заклади освіти, науки й культури України інформаційними послугами, такими як:

– оперативний доступ та обмін даними;
– накопичення даних для виконання наукових досліджень;
– дистанційне навчання;
– функціонування електронних бібліотек та віртуальних лабораторій;
– проведення телеконференцій.

Сьогодні мережа «УРАН» об'єднує понад 60 науково-дослідницьких таосвітніх закладів України.

Регіональна мережа – комп'ютерна мережа, що об'єднує комп'ютери, розміщені в межах одного регіону.

Глобальна комп'ютерна мережа – це комп'ютерна мережа, що об'єднує комп'ютери і мережі, розташовані в усіх частинах земної кулі. У наш час найбільш відома глобальна комп'ютерна мережа – Інтернет, але існують й інші глобальні мережі.

Історія створення комп'ютерних мереж. Уперше здійснити віддалений зв'язок між комп'ютерами вдалося у 60-х роках XX ст. Саме в цей час почали створювати і запроваджувати найпростіші локальні комп'ютерні мережі. А в 1969 р. у США була створена комп'ютерна мережа ARPANET, розроблена на замовлення Міністерства оборони США. Вона проєктувалася як стійка до пошкоджень мережа для швидкої передачі оперативних даних. Наприклад, у разі ядерного нападу мережа ARPANET здатна продовжувати нормальну роботу під час виходу з ладу будь-якої її частини: потоки даних почнуть обходити пошкоджену ділянку. Об'єднавши комп'ютери кількох великих університетів і дослідних компаній країни, ARPANET мала й наукове призначення.

Невдовзі успішні творці ARPANET приступили до розробки

програми Internetting Project (Проєкт об'єднання мереж). Були випробувані різні варіанти взаємодії мережі ARPANET із іншими мережами США. Успіх цього проєкту сприяв створенню у США у 80-х роках XX ст. досить потужної мережі «Інтернет».

Це створило передумови для успішної інтеграції багатьох мереж США та інших країн світу в єдину світову мережу. Таку «мережу мереж» тепер скрізь називають Інтернет.

Спочатку ця мережа використовувалася переважно в наукових проєктах. Однак з часом Інтернет став невід'ємною частиною життя багатьох людей. Сьогодні до Інтернету підключені мережі, що охоплюють усі континенти, навіть Антарктиду, і з'єднують кожний куточок на планеті. Кількість користувачів Всесвітньої мережі різко збільшується і вже досягла близько 1,5 млрд. Понад 1000 нових комп'ютерів підключаються до Інтернету щодня, понад 20 млн електронних повідомлень подорожує Інтернетом щотижня.

Використання міжмережевних екранів

Міжмережевий екран, Мережевий екран, Фаєрвол, Файрвол (англ. *Firewall*, буквально «вогняна стіна») – пристрій або набір пристроїв, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік згідно з набором правил та інших критеріїв.

Фаєрвол може мати вигляд окремого приладу (так званий маршрутизатор або роутер) або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі-сервер. Простий і дешевий фаєрвол може не мати такої гнучкої системи налаштувань правил фільтрації пакетів і трансляції адрес вхідного та вихідного трафіку (функція редиректу).

Залежно від активних з'єднань, що відслідковуються, фаєрволи поділяють на:

– stateless (проста фільтрація), які не відслідковують поточні з'єднання (наприклад TCP), а фільтрують потік даних виключно на основі статичних правил;

– stateful (фільтрація з урахуванням контексту) – із відслідковуванням поточних з'єднань та пропуском тільки таких пакетів, що задовольняють логіці й алгоритмам роботи відповідних протоколів та програм. Такі типи фаєрволів дозволяють ефективніше боротися з різноманітними DDoS- атаками та вразливістю деяких протоколів мереж.

Функції екранів:

– *Фільтрація пакетів.* Це одна з трьох загальновідомих функцій

мережевого екрана. У цьому разі виконуються зовсім прості функції (фактично як у спеціалізованого маршрутизатора), які полягають у перегляді заголовка кожного пакета та перевірки IP адреси та порта на правильність.

– *Проксі сервер.* Це друга загальновідома функція. Різниця між проксі сервером та фільтрацією пакетів полягає в тому, що проксісервер вимагає, щоб всі сеанси зв'язку встановлювались через нього, а не напряму.

– *Проксі сервер програм*. Це третя функція. Цей різновид проксі сервера відрізняється «розумінням» протоколів програм, що здійснюють передачу даних. Хороший приклад такого сервера – поштовий сервер.

– *Кешування даних.* Це не є традиційною функцією мережевих екранів, але на цей час є надзвичайно популярною властивістю. Ідея полягає у тому, що, оскільки всі дані проходять через мережевий екран, він може зберігати найбільш популярну інформацію і при наступному звертанні за нею видати її зі свого кешу.

– *Статистика та повідомлення*. Важливою властивістю мережевого екрану є ведення історії всіх мережевих з'єднань, а також вивід повідомлень про атаки на мережу чи комп'ютер. Історія з'єднань допомагає правильно настроїти мережевий екран, щоб комп'ютер був одночасно захищений від нападів і відкритий для доступу авторизованим користувачам.

– *Управління.* Для персональних мережевих екранів основна характеристика – зручність їхнього налаштування. Управління міжмережевими екранами здебільшого відбувається дистанційно (використовуючи HTML інтерфейс чи інший), що потребує впевненості в надійності авторизації та каналу зв'язку.

Принципи роботи брандмауера. Різновиди брандмауерів. Брандмауер, або міжмережевий екран – це «напівпроникна мембрана», що розташовується між внутрішнім сегментом мережі і зовнішньою мережею або іншими сегментами мережі «Інтернет», і контролює всі інформаційні потоки у внутрішній сегмент та з нього. Контроль трафіку полягає в його фільтрації, тобто у вибірковому пропущенні через екран, а іноді із виконанням спеціальних перетворень і формуванням сповіщень для відправника, якщо його даним у пропуску відмовлено. Фільтрація здійснюється на підставі набору умов, попередньо завантажених в брандмауер, і відображає концепцію інформаційної безпеки корпорації. Брандмауери можуть бути виконані у вигляді як апаратного, так і програмного комплексу, записаного в комутуючий

пристрій або сервер доступу (сервер-шлюз, просто сервер, хост-комп'ютер і т.д.), вбудованогов операційну систему.

Робота брандмауера полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і залежно від результатів аналізу пропускає пакети інформації у внутрішню мережу (сегмент мережі) або їх відфільтровує.

Ефективність роботи міжмережевого екрана, що працює під управлінням Windows, зумовлена тим, що він повністю заміщає реалізованийстек протоколів TCP \ IP, і тому порушувати його роботу з допомогою спотворення протоколів зовнішньої мережі (що часто роблять хакери) неможливо.

Міжмережеві екрани зазвичай виконують такі функції:

– фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі (внутрішньої підмережі) від зовнішніх каналів зв'язку;

– багатоетапну ідентифікацію запитів, що надходять до мережі (ідентифікація серверів, вузлів зв'язку про інших компонентів зовнішньої мережі);

– перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;

– реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;

– контроль цілісності програмного забезпечення і даних;

– економію адресного простору мережі (у внутрішній підмережі може використовуватися локальна система адресації серверів);

– приховування IP адрес внутрішніх серверів з метою захисту від хакерів.

Брандмауери можуть працювати на різних рівнях протоколів.

На мережевому рівні виконується фільтрація вступників пакетів, заснована на IP адресі. На транспортному рівні фільтрація припустима ще й за номерами портів TCP і прапорів. На прикладному рівні може виконуватисяаналіз прикладних протоколів (FTP, HTTP, SMTP і т.д.) і контроль за змістомпотоків даних.Можна в брандмауері створювати ту експертну систему, яка, аналізуючи трафік, діагностує події, що можуть становити загрозу безпеки внутрішньої мережі, та інформує про це адміністратора. Експертна система здатна також у разі небезпеки (спам, наприклад) автоматично посилюватиумови фільтрації і так далі.

Політика безпеки під час роботи в мережі

Під час роботи в мережевому середовищі необхідно бути упевненим у тому, що секретні дані такими і залишаться, оскільки лише користувачі, що мають відповідні повноваження, зможуть одержати до

них доступ. Однак важливо забезпечити захист не тільки конфіденційної інформації, але і функціонування мережі в цілому. Кожна мережа має потребу в захисті від навмисного чи випадкового ушкодження. Однак у користувачів не повинно бути труднощів під час виконання роботи.

Найбільшу *загрозу для безпеки* мережі мають:

– несанкціонований доступ;
– електронне підслуховування;
– навмисне чи ненавмисне ушкодження.

Несанкціонований доступ – це навмисне звертання користувача до даних, доступ до яких йому не дозволений, з метою їхнього читання, відновлення чи руйнування.

Рівень захисту мережі залежить від її призначення. Наприклад, мережа, що зберігає дані великого банку, вимагає більш могутнього захисту, ніж локальна мережа, що з'єднує комп'ютери невеликої громадської організації.

Політика безпеки. Для захисту мережі необхідно проводити певну політику, тобто дотримуватися набору правил і розпоряджень. Вироблення політики безпеки (*security policy*) – перший крок, який повинна зробити будь-яка організація, забезпечуючи захист своїх даних. Політика встановлює «генеральну лінію», спираючись на яку і адміністратор, і користувачі будуть вносити зміни, знаходити вихід з позаштатних ситуацій при розширенні мережі.

Адміністратор повинен навчити користувачів мережі всім особливостям роботи і методам безпеки. Для цього він може скласти посібник, а в разі потреби – організувати навчання, особливо нових користувачів.

Керування доступом у Windows. Права користувача призначаються шляхом додавання його в одну з вбудованих груп, що містять набір уже призначених прав користувача. Однак у разі потреби можна створити нову групу і призначити їй певні права. Призначення прав групам здійснюється за допомогою групової політики. Користувачам, доданим у групу, автоматично надаються усі права, призначені групі. У Windows існують такі *групи*:

- *Адміністратори* – мають усі права та можливості в системі.
- *Оператори архіву* – можуть архівувати та відновлювати файли на комп'ютері незалежно від усіх дозволів, установлених для цих файлів.
- *Досвідчені користувачі* – можуть створювати локальні групи та облікові записи користувачів, а також видаляти користувачів із

локальних груп, створених ними, змінювати та видаляти створені ними облікові записи.

Вони можуть керувати додаванням та видаленням користувачів із груп *Досвідчені користувачі*, *Користувачі*, *Гості*. Вони не мають прав на архівування та поновлення каталогів, завантаження та вивантаження драйверів, керування журналами безпеки та аудиту.

- *Користувачі* – можуть виконувати найбільш поширені завдання: запуск програм, друк документів, копіювання файлів і так далі. Користувачі мають право створювати локальні групи та змінювати групи, створені ними. Вони не можуть організовувати загальний доступ до ресурсів комп'ютера.
- *Гості* – призначена для запуску комп'ютера разовими користувачами. Члену цієї групи надаються обмежені можливості.
- *Реплікатор* – створена для підтримки функції реплікації (створення копії) каталогу.

Обліковий запис – запис користувача, що містить усі відомості, що визначають користувача в операційній системі Windows. Це ім'я користувача і пароль, необхідні для входу користувача в систему, імена груп, членом яких користувач є, а також права і дозвіл, що він має під час роботи в системі і доступі до її ресурсів.

У Windows є *два вбудовані облікові записи* користувачів – *Адміністратор* і *Гість*, що створюються автоматично під час встановлення системи. Користувач з ім'ям Адміністратор є членом групи адміністраторів і може виконувати всі необхідні дії в мережі. Обліковий запис Гість призначений для тих, хто не має реального облікового запису. Цей обліковий запис не вимагає пароля. Він входить у вбудовану групу Гостей і має всі права, що привласнені цій групі.

Із користувачем пов'язаний профіль користувача. *Профіль користувача* – набір параметрів середовища Windows, що завантажується під час входу користувача в систему. Він містить усі параметри настроювання середовища Windows, доступні для користувача, у тому числі групи програм, колір екрана, мережеві підключення дисків і принтерів, властивості миші, розміри і положення вікон.

Немаловажне значення *має контроль подій*, що відбуваються в мережі, оскільки в цих умовах зловмисник не настільки помітний і має досить часу і ресурсів для виконання своїх завдань. Цей процес відслідковує дії користувачів у мережі. Він є частиною захисту мережі, оскільки в *журналі безпеки* відбиті імена всіх користувачів, що працювали з конкретними ресурсами або намагалися одержати до них доступ.

8.2. Програмні засоби, що містять небезпеку

Перехоплювачі паролів першого роду.

Перехоплювачі паролів першого роду діють по наступному алгоритму. Зловмисник запускає програму, яка імітує запрошення користувачеві для входу в систему, і чекає введення. Коли користувач вводить ім'я і пароль, закладка зберігає їх в доступному для зловмисника місці, після чого закінчує роботу і здійснює вихід з системи користувача-зловмисника (у більшості операційних систем вихід користувача з системи можна здійснити програмно). Після закінчення роботи закладки на екрані з'являється справжнє запрошення для входу користувача в систему.

Користувач, що став жертвою закладки, бачить, що він не увійшов до системи, і що йому знову пропонується ввести ім'я і пароль. Користувач припускає, що під час введення пароля відбулася помилка, і вводить ім'я і пароль повторно. Після цього користувач входить в систему, і подальша його робота протікає нормально. Деякі закладки, що функціонують за цією схемою, перед закінченням роботи видають на екран правдоподібне повідомлення про помилку, наприклад: «Пароль введений неправильно. Спробуйте ще раз».

Основною перевагою цього класу перехоплювачів паролів є те, що написання подібної програмної закладки не вимагає від зловмисника жодної спеціальної кваліфікації. Будь-який користувач, що вміє програмувати хоча б мовою BASIC, може написати таку програму за лічені години. Єдина проблема, яка може тут виникнути, полягає в програмній реалізації виходу користувача з системи. Проте відповідний системний виклик документований для всіх операційних систем, відомих авторові. Якщо зловмисник не полінується уважно вивчити документацію щодо операційної системи, то він вирішить цю проблему дуже швидко.

Перехоплювачі паролів першого роду є найбільш небезпечні для тих операційних систем, у яких запрошення користувачеві на вхід має дуже простий вигляд. Наприклад, у більшості версій ОС UNIX це запрошення виглядає так: login: user; password:

Захист від перехоплювачів паролів першого роду.

Ускладнення зовнішнього вигляду запрошення на вхід в систему дещо утрудняє вирішення завдання перехоплення паролів, проте не створює для зловмисника жодних принципових труднощів. Для того,

щоб істотно утруднити впровадження в систему перехоплювачів паролів першого роду, необхідні складніші заходи захисту. Прикладом операційної системи, де такі заходи реалізовані, є Windows NT.

У Windows NT звичайна робота користувача і автентифікація користувача при вході в систему здійснюються на різних робочих полях (desktops). Робочим полем Windows NT є сукупність вікон, одночасно видимих на екрані. Тільки процеси, вікна яких розташовані на одному робочому полі, можуть взаємодіяти між собою, використовуючи засоби Windows GUI. Поняття робочого поля Windows NT близьке до поняття терміналу UNIX.

Процес Winlogon, що одержує від користувача ім'я і пароль, виконується на окремому робочому полі (робочому полі автентифікації). Жодний інший процес, у тому числі і перехоплювач паролів, не має доступу до цього робочого поля. Тому запрошення користувачеві на вхід до системи, що виводиться перехоплювачем паролів першого роду, може розташовуватися тільки на робочому полі прикладних програм, де виконуються всі програми, запущені користувачем.

Перемикання екрана комп'ютера з одного робочого поля на інше здійснюється при натисненні комбінації клавіш Ctrl+Alt+Del. Win32 – підсистема Windows NT – обробляє цю комбінацію по-особливому: повідомлення про натиснення Ctrl+Alt+Del посилається тільки процесу Winlogon. Для всіх інших процесів, зокрема для всіх прикладних програм, запущених користувачем, натиснення цієї комбінації клавіш непомітно.

При старті системи на екран комп'ютера спочатку відображається робоче поле автентифікації. Проте користувач вводить ім'я і пароль не відразу, а тільки після натиснення Ctrl+Alt+Del. Коли користувач закінчує сеанс роботи з системою, на екран також виводиться робоче поле автентифікації, і, так само як і у попередньому випадку, новий користувач може ввести пароль для входу до системи лише після натиснення Ctrl+Alt+Del.

Якщо до системи упроваджений перехоплювач паролів першого роду, то для того, щоб він зміг перехопити пароль користувача, він повинен принаймні обробити натиснення користувачем Ctrl-Alt-Del. Інакше під час натиснення користувачем цієї комбінації клавіш відбудеться перемикання на робоче поле автентифікації, робоче поле прикладних програм стане неактивним, і перехоплювач паролів просто не зможе нічого перехопити – повідомлення про натиснення користувачем клавіш надходитимуть на інше робоче поле. Проте для

всіх прикладних програм факт натиснення користувачем Ctrl+Alt+Del завжди залишається непоміченим. Тому пароль буде сприйнятий не програмною закладкою, а процесом Winlogon.

Звичайно, перехоплювач паролів може імітувати не перше запрошення операційної системи, де користувачу пропонується натиснути Ctrl+Alt+Del, а те запрошення, яке висвічується після натиснення користувачем цієї комбінації. Проте в звичайних умовах (за відсутності програмної закладки) це друге запрошення автоматично відміняється за достатньо короткий час (від 30 с до 1 хв, залежить від версії Windows NT). Якщо друге запрошення є на екрані комп'ютера тривалий час, цей факт повинен насторожити користувача. Окрім того, як показує досвід, користувачі, що тривалий час працюють з Windows NT, звичкають починати роботу з системою з натиснення Ctrl+Alt+Del незалежно від того, що відображається на екрані.

Захист Windows NT від перехоплювачів паролів першого роду досить надійний. Мабуть, під час розробки заходів захисту операційної системи від перехоплювачів паролів першого роду слід орієнтуватися на механізм, подібний вищеописаному. Слід звернути особливу увагу на такі дві умови, виконання яких обов'язкове для забезпечення надійного захисту від перехоплювачів паролів першого роду:

1. Програма, одержуючи від користувача ім'я і пароль під час входу до системи, виконується на ізольованому терміналі (терміналі автентифікації), недоступному прикладним програмам.

2. Факт перемикання призначеної для користувача консолі на термінал автентифікації непомітний прикладним програмам. Прикладні програми не можуть заборонити перемикання консолі на термінал автентифікації.

Якщо операційна система не підтримує ці можливості (а жодна операційна система, відома авторові, крім Windows NT, ці можливості не підтримує), захищеність системи від перехоплювачів паролів першого роду можна підвищити адміністративними заходами. Кожен користувач системи повинен бути проінструктований, що якщо він кілька разів поспіль не може увійти до системи з першого разу, він повинен звернутися до адміністратора.

Перехоплювачі паролів другого роду.

Перехоплювачі паролів другого роду перехоплюють всі дані, що вводяться користувачем з клавіатури. Прості програмні закладки такого типу просто скидають всі ці дані на жорсткий диск комп'ютера або в будь-яке інше місце, доступне зловмисникові. Досконаліші закладки аналізують перехоплені дані і відсівають інформацію, що свідомо не

має відношення до паролів. Декілька подібних закладок було в різний час написано для операційної системи MS-DOS, деякі з них використовувалися на практиці, причому дуже ефективно.

Цими закладками є резидентні програми, які перехоплюють одне або декілька переривань процесора, що мають відношення до роботи з клавіатурою. Інформація про натиснуту клавішу і введений символ використовується закладками для своїх цілей.

Наприкінці 1997 р. на хакерських серверах в Інтернеті з'явилися перехоплювачі паролів другого роду для Windows3.x і Windows95. Приклади їх використання зловмисниками для здійснення несанкціонованого доступу поки не зустрічалися на практиці. У телеконференціях в Інтернеті (newsgroups) кілька разів зустрічалися повідомлення про атаки Windows95 перехоплювачами паролів другого роду. Проте ця інформація жодного разу не підтверджувалася.

Створення подібних програмних закладок не потребує великих зусиль. Програмні інтерфейси Win16 і Win32 підтримують спеціальний механізм фільтрів (hooks), який може бути використаний для перехоплення паролів користувачів. За допомогою цього механізму прикладні програми і сама операційна система вирішують цілу низку завдань, у тому числі і завдання підтримки національних розкладок клавіатури. Будь-який русифікатор клавіатури, що працює в середовищі Windows, перехоплює всю інформацію, що вводиться користувачем з клавіатури, у тому числі й паролі. Нескладно написати русифікатора так, щоб він, крім основних функцій, виконував би і функції перехоплювача паролів. Написання програми локалізації клавіатури є достатньо простим завданням. У багатьох довідниках і підручниках з програмування це завдання описано детально, в деяких виданнях наведені початкові тексти простого русифікатора клавіатури. До того ж, Windows підтримує ланцюжки фільтрів, за допомогою яких декілька програм можуть одночасно діставати доступ до інформації, що вводиться з клавіатури, і обробляти її так, як вважають за потрібне, у разі потреби передаючи оброблену інформацію далі по ланцюжку. Можна вбудувати перехоплювач паролів в ланцюжок фільтрів перед русифікатором або після нього так, що вся інформація, що вводиться користувачем з клавіатури, проходить і через русифікатор, і через перехоплювач паролів. В цьому разі завдання написання програмної закладки, що перехоплює паролі користувачів Windows, стає настільки простим, що практично не вимагає від автора закладки спеціальної кваліфікації.

Здебільшого правильне таке твердження: «Якщо операційна

система допускає перемикання розкладки клавіатури при введенні пароля, то для цієї операційної системи можна написати перехоплювач паролів другого роду». Дійсно, якщо для операційної системи існує програма локалізації розкладки клавіатури, і якщо ця програма використовується при введенні пароля, після незначної зміни початкового тексту ця програма перетворюється на перехоплювач паролів другого роду. Якщо ця програма написана на мові програмування С, то достатньо додати в програму чотирьох операторів приблизно такого вигляду:

StoreFile = fopen (FileName, «a+b»); fseek (StoreFile, 0, SEEK_END); fputc (NewSymbol, StoreFile); fclose (StoreFile).

Для деяких операційних систем можна обійтися трьома операторами.

Захист від перехоплювачів паролів другого роду

Для організації захисту від перехоплювачів паролів другого роду необхідно добитися виконання в операційній системі таких трьох умов:

1. Перемикання розкладки клавіатури під час введення пароля неможливе. Інакше завдання створення перехоплювача паролів другого роду істотно спрощується.
2. Конфігурація ланцюжка програмних модулів, що беруть участь в отриманні операційною системою пароля користувача, доступна тільки адміністраторам системи.
3. Доступ на запис до файлів цих програмних модулів надається тільки адміністраторам системи.

Для підвищення стійкості системи захисту до помилок адміністраторів можна сформулювати останню умову так: доступ на запис до файлів програмних модулів, що беруть участь в отриманні пароля користувача, не надається нікому. Доступ на запис до атрибутів захисту цих файлів надається тільки адміністраторам. Будь-які звернення з метою запису до цих файлів, а також до їх атрибутів захисту, реєструються в системному журналі аудиту.

Якщо в системі виконується третя умова в другому формулюванні, адміністрування операційної системи в частині обслуговування клавіатури (зокрема, установка і зміна розкладок клавіатури), дещо ускладняються.

Для того щоб вказані умови виконувалися, необхідно, щоб підсистема захисту операційної системи підтримувала розмежування доступу і аудит.

Для більшості сучасних операційних систем всі умови, крім першої, можуть бути забезпечені організаційними заходами. Перша

умова в неросійськомовних версіях операційних систем зазвичай виконується автоматично. Для більшості російськомовних версій операційних систем (зокрема, для російської версії Windows NT 4.0) добитися виконання цієї умови неможливо – можливість створювати користувачів із російськими іменами закладена в програмне забезпечення операційних систем. У всіх англомовних версіях Windows NT і у всіх відомих авторові версіях UNIX можливе створення і підтримка політики безпеки, за якої виконуються всі три вказані умови.

Якщо забезпечити виконання першої умови в цій операційній системі неможливо, потрібно добитися виконання другої і третьої умов. Виконання цих умов значно підвищує захищеність системи від перехоплювачів паролів другого роду.

Перехоплювачі паролів третього роду.

До перехоплювачів паролів третього роду належать програмні закладки, що повністю або частково підміняють собою підсистему автентифікації операційної системи. Оскільки завдання створення такої програмної закладки набагато складніше, ніж завдання створення перехоплювача паролів першого або другого роду, цей клас програмних закладок з'явився зовсім недавно. Існують дві демонстраційні версії перехоплювачів паролів третього роду (обидві для Windows NT). Випадки застосування зловмисниками перехоплювачів паролів третього роду поки не траплялися.

Перехоплювач паролів третього роду може бути написаний для будь-якої операційної системи. Складність створення такого перехоплювача паролів залежить від складності алгоритмів, що реалізовуються підсистемою автентифікації, складності інтерфейсу між її окремими модулями, а також від ступеня документованості підсистеми автентифікації операційної системи. Загалом завдання створення перехоплювача паролів третього роду набагато складніше, ніж завдання створення перехоплювача паролів першого або другого роду. Мабуть, цим і пояснюється невелика кількість програмних закладок цього класу. Проте через широке розповсюдження операційної системи Microsoft Windows NT, що містить достатньо могутні вбудовані засоби захисту від перехоплювачів паролів першого і другого роду, використання перехоплювачів паролів третього роду з метою здійснення несанкціонованого доступу можливе найближчим часом.

Захист від перехоплювачів паролів третього роду

Оскільки перехоплювачі паролів третього роду частково беруть на себе функції підсистеми захисту операційної системи, перехоплювач паролів третього роду під час впровадження в систему повинен виконати принаймні одну з таких дій:

– підмінити собою один або декілька системних файлів;

– упровадитися в один або декілька системних файлів по одному з «вірусних» алгоритмів;

– використовувати підтримувані операційною системою інтерфейсні зв'язки між програмними модулями підсистеми захисту для вбудовування себе в ланцюжок програмних модулів.

– використовувати для тієї ж мети низькорівневі інтерфейсні зв'язки операційної системи, використовувані підсистемою захисту для вирішення своїх завдань.

Кожна з цих дій залишає в операційній системі сліди, які можуть бути виявлені за допомогою таких заходів захисту:

1. Дотримання адекватної політики безпеки. Підсистема автентифікації повинна бути найзахищенішим місцем операційної системи. Заходи, необхідні для підтримки адекватної політики безпеки, дуже розрізняються для різних операційних систем.

У разі дотримання адекватної політики безпеки впровадження в систему перехоплювача паролів третього роду, як і будь-якої іншої програмної закладки, неможливе. Проте, оскільки адміністратори, як і всі люди, схильні допускати помилки у своїй роботі, підтримка адекватної політики безпеки протягом тривалого часу є практично нездійсненним завданням. Окрім того, дотримання адекватної політики безпеки захищає тільки від проникнення програмної закладки в систему. Як тільки перехоплювач паролів упроваджений в систему, заходи щодо підтримки політики безпеки стають безглуздими – за наявності в системі програмної закладки політика безпеки не може бути адекватною. Тому необхідні додаткові заходи захисту.

2. Контроль цілісності виконуваних файлів операційної системи. Необхідно контролювати не лише файли, що входять до складу підсистеми захисту, але і бібліотеки, що містять низькорівневі функції операційної системи.

3. Контроль цілісності інтерфейсних зв'язків усередині підсистеми захисту, а також інтерфейсних зв'язків, використовуваних підсистемою захисту для вирішення низькорівневих завдань.

Створення абсолютно надійного захисту проти перехоплювачів паролів третього роду є неможливою, оскільки машинний код перехоплювачів паролів третього роду виконується не в контексті користувача, а в контексті операційної системи, перехоплювач паролів третього роду може вживати заходи, що утрудняють його виявлення адміністраторами системи, зокрема:

– перехоплення системних викликів, які можуть

використовуватися адміністраторами для виявлення програмної закладки для підміни інформації;

– фільтрація реєстрованих повідомлень аудиту.

Мабуть, відбувається «боротьба щита і меча», коли для будь-якої відомої атаки може бути створений надійний захист від неї, і для будь-якого відомого захисту може бути реалізована атака, що дозволяє його ефективно долати.

Принципи роботи троянських програм.

Троянські коні (логічні бомби). До троянських коней належать програми, що завдають будь-яких руйнівних дій, тобто залежно від будь-яких умов або під час кожного запуску, що знищує інформацію на дисках, виводить систему з ладу тощо.

Більшість відомих троянських коней є програмами, які «підробляються» під будь-які корисні програми, нові версії популярних утиліт або доповнення до них. Дуже часто вони розсилаються по BBS-станціях або електронних конференціях. Порівняно з вірусами «троянські коні» не дуже поширені з достатньо простих причин: вони або знищують себе разом з рештою даних на диску, або демаскують свою присутність і знищуються постраждалим користувачем.

До «троянських коней» також можна віднести «дропери» вірусів – заражені файли, код яких підправлений так, що відомі версії антивірусів не визначають вірусу у файлі. Наприклад, файл шифрується будь-яким спеціальним способом або упаковується унікальним архіватором, що не дозволяє антивірусу «побачити» зараження.

Слід зазначити також «злі жарти» (hoax). До них належать програми, які не завдають комп'ютеру будь-якої прямої шкоди, але виводять повідомлення про те, що така шкода вже завдана, або буде завдана за будь-яких умов, або попереджають користувача про неіснуючу небезпеку. До «злих жартів» належать, наприклад, програми, що «лякають» користувача повідомленнями про форматування диска (хоча жодного форматування насправді не відбувається), детектують віруси в незаражених файлах (як це робить широко відома програма ANTITIME), виводять дивні вірусоподібні повідомлення (драйвер диска CMD640X від якогось комерційного пакету) і так далі – залежно від почуття гумору автора такої програми. Мабуть, до «злих жартів» належить також рядок «CHOLEEPA» в другому секторі вінчестерів фірми Seagate.

До такої ж категорії «злих жартів» можна віднести також свідомо помилкові повідомлення про нові супервіруси. Такі повідомлення періодично з'являються в електронних конференціях і зазвичай викликають паніку серед користувачів.

Принципи роботи утиліт скритого адміністрування.

Троянські коні цього класу за своєю суттю є достатньо могутніми утилітами віддаленого адміністрування комп'ютерів у мережі. За своїми функціями вони багато в чому нагадують різні системи адміністрування, що розробляються і поширюються різними фірмами-виробниками програмних продуктів.

Єдина особливість цих програм примушує класифікувати їх як шкідливі троянські програми – це відсутність попередження про інсталяцію і запуск. При запуску Троя встановлює себе в системі і потім стежить за нею, водночас користувачеві не видається жодних повідомлень про дії Трої в системі. До того ж, посилання на Трої може бути відсутнім в списку активних застосувань. Як наслідок, «користувач» цієї троянської програми може і не знати про її наявність в системі, тоді як його комп'ютер відкритий для дистанційного управління.

Будучи встановленими на комп'ютер, утиліти прихованого управління дозволяють робити з комп'ютером все з будь-якими можливостями, що запрограмував автор: приймати/відсилати файли, запускати і знищувати їх, виводити повідомлення, стирати інформацію, перезавантажувати комп'ютер і так далі. І як наслідок, ця Троя може бути використана для виявлення і передачі конфіденційної інформації, для запуску вірусів, для знищення даних і тому подібне – уражені комп'ютери виявляються відкритими для зловмисних дій хакерів.

Intended-віруси. До таких вірусів належать програми, які на перший погляд є стовідсотковими вірусами, але не здатні розмножуватися внаслідок помилок. Наприклад, вірус, який при зараженні «забуває» помістити в початок файлів команду передачі управління на код вірусу, або записує в неї неправильну адресу свого коду, або неправильно встановлює адресу перехоплюваного переривання (що здебільшого «завішує» комп'ютер) і так далі.

До категорії «intended» також належать віруси, які з наведених вище причин розмножуються тільки один раз – з «авторської» копії. Заразивши який-небудь файл, вони втрачають здібність до подальшого розмноження.

З'являються intended-віруси найчастіше при невмілій перекомпіляції якого-небудь вже існуючого вірусу або внаслідок недостатнього знання мови програмування, або внаслідок незнання технічних тонкощів операційної системи.

Конструктори вірусів. Конструктор вірусів – це утиліта, призначена для виготовлення нових комп'ютерних вірусів. Відомі

конструктори вірусів для DOS, Windows і макровірусів. Вони дозволяють генерувати початкові тексти вірусів (ASM-файли), об'єктні модулі або безпосередньо заражені файли.

Деякі конструктори (VLC, NRLG) забезпечені стандартним віконним інтерфейсом, де за допомогою системи меню можна вибрати тип вірусу, об'єкти (COM або EXE), що вражаються, наявність або відсутність самошифровки, протидію розшифрувальнику, внутрішні текстові рядки, вибрати ефекти, що супроводжують роботу вірусу і тому подібне. Інші конструктори (PS-MPC, G2) не мають інтерфейсу і зчитують інформацію про тип вірусу з конфігураційного файлу.

Поліморфні генератори. Поліморні-генератори, як і конструктори вірусів, не є вірусами у прямому значенні цього слова, оскільки в їх алгоритмі не передбачено функції розмноження, тобто відкриття, закриття і запис у файли, читання і запис секторів і так далі. Головною функцією подібних програм є шифрування тіла вірусу і генерація того, що розшифровує відповідно.

Зазвичай поліморфні генератори розповсюджуються їх авторами без обмежень у вигляді файлу-архіву. Основним файлом в архіві будь-якого генератора є об'єктний модуль, що містить цей генератор. У всіх генераторах, що зустрічалися, цей модуль має зовнішню (external) функцію – виклик програми генератора.

Отже, авторові вірусу, якщо він бажає створити справжній поліморний-вірус, не доводиться довго працювати над кодами власного шифрувальника. На бажання він може підключити до свого вірусу будь-який відомий поліморний-генератор і викликати його з коду вірусу. Фізично це досягається так: об'єктний файл вірусу з'єднується з об'єктним файлом генератора, а в початковий текст вірусу перед командами його запису у файл вставляється виклик поліморного-генератора, який створює коди того, що розшифровує і шифрує тіло вірусу.

Комп'ютерні віруси і механізми боротьби з ними

Шкідливі програми і, перш за все, віруси є дуже небезпечними для інформації в комп'ютерних системах (КС). Недооцінювання цієї небезпеки може мати серйозні наслідки для інформації користувачів. Шкодить використанню всіх можливостей КС і надмірне перебільшення небезпеки вірусів. Знання механізмів дії вірусів, методів і засобів боротьби з ними дозволяє ефективно організувати протидію вірусам, звести до мінімуму вірогідність зараження і втрат від їх дії.

Термін «комп'ютерний вірус» був введений порівняно недавно – у середині 80-х років. Малі розміри, здатність швидко поширюватися,

розмножуючись і упроваджуючись в об'єкти (заражаючи їх), негативна дія на систему – всі ці ознаки біологічних вірусів властиві і шкідливим програмам, що отримали з цієї причини назву «Комп'ютерні віруси». Водночас із терміном «вірус» під час роботи з комп'ютерними вірусами використовуються й інші медичні терміни: «зараження», «місце існування», «профілактика» й інші.

«Комп'ютерні віруси» – це невеликі виконувані або такі, програми що мають властивість до самовідтворення (реплікації) в КС. Віруси можуть виконувати зміну або знищення програмного забезпечення або даних, що зберігаються в КС. Під час розповсюдження віруси можуть себе модифікувати.

Класифікація комп'ютерних вірусів.

На сьогодні у світі налічується більше 50 тисяч тільки зареєстрованих комп'ютерних вірусів. Оскільки переважна більшість сучасних шкідливих програм мають здібність до саморозмноження, то часто їх зараховують до комп'ютерних вірусів. Усі комп'ютерні віруси можуть бути класифіковані за такими ознаками [4, 20]:

– за місцем існування;
– за способом зараження;
– за ступенем небезпеки деструктивних (шкідницьких) дій;
– за алгоритмом функціонування.

За місцем існування в КС, комп'ютерні віруси поділяють на:

– мережеві;
– файлові;
– завантажувальні;
– комбіновані.

Місцем існування мережевих вірусів є елементи комп'ютерних мереж. Файлові віруси розміщуються у виконуваних файлах. Завантажувальні віруси знаходяться в завантажувальних секторах (областях) зовнішніх пристроїв, що записуються у (boot-секторах). Іноді завантажувальні віруси називають бутовими. Комбіновані віруси розміщуються в декількох місцях існування. Прикладом таких вірусів є завантажувальні файлові віруси. Ці віруси можуть розміщуватися як в завантажувальних секторах накопичувачів на магнітних дисках, так і в тілі завантажувальних файлів.

За способом зараження місця існування комп'ютерні віруси поділяють на:

– резидентні;
– нерезидентні.

Резидентні віруси після їх активізації повністю або частково

переміщаються з місця існування (мережа, завантажувальний сектор, файл) в оперативну пам'ять ЕОМ. Ці віруси, використовуючи, як правило, привілейовані режими роботи, дозволені тільки операційній системі, заражають місце існування і при виконанні певних умов реалізують деструктивну функцію. На відміну від резидентних нерезидентні віруси потрапляють в оперативну пам'ять ЕОМ тільки на час їх активності, протягом якого виконують деструктивну функцію і функцію зараження. Пізніше віруси повністю покидають оперативну пам'ять, залишаючись у місці існування. Якщо вірус поміщає в оперативну пам'ять програму, яка не заражає місце існування, то такий вірус вважається нерезидентним.

Арсенал деструктивних або шкідливих можливостей комп'ютерних вірусів дуже великий. Деструктивні можливості вірусів залежать від цілей і кваліфікації їх створювача, а також від особливостей комп'ютерних систем.

За ступенем небезпеки для інформаційних ресурсів користувача комп'ютерні віруси можна поділити на:

– нешкідливі віруси;
– небезпечні віруси;
– дуже небезпечні віруси.

Нешкідливі комп'ютерні віруси створюють автори, у яких не має мети завдати будь-якого збитку ресурсам КС. Ними, як правило, керує бажання показати свої можливості програміста. Іншими словами, створення комп'ютерних вірусів для таких людей – своєрідна спроба самоствердження. Деструктивна дія таких вірусів зводиться до виводу на екран монітора безневинних текстів і картинок, виконання музичних фрагментів і тому подібне.

Проте при всій нешкідливості таких вірусів, як здається, вони завдають певного збитку КС. По-перше, такі віруси витрачають ресурси КС, тією чи іншою мірою знижуючи її ефективність функціонування. По-друге, комп'ютерні віруси можуть містити помилки, що викликають небезпечні наслідки для інформаційних ресурсів КС. Крім того, під час модернізації операційної системи або апаратних засобів КС віруси, створені раніше, можуть призводити до порушень штатного алгоритму роботи системи.

До небезпечних належать віруси, що істотно знижують ефективність КС, але не призводять до порушення цілісності і конфіденційності інформації, яка зберігається в пристроях, що запам'ятовують. Наслідки цих вірусів можуть бути ліквідовані без особливих витрат матеріальних і тимчасових ресурсів. Прикладами

таких вірусів є віруси, що займають пам'ять ЕОМ і канали зв'язку, але не блокують роботу мережі; віруси, що призводять до повторного виконання програм, перезавантаження операційної системи або повторної передачі даних по каналах зв'язку і тому подібне.

Дуже небезпечними слід вважати віруси, що порушують конфіденційність, знищують, необоротно модифікують (у тому числі і шифрування) інформацію, а також віруси, які блокують доступ до інформації, призводять до відмови апаратних засобів і шкодять здоров'ю користувачів. Такі віруси стирають окремі файли, системні області пам'яті, форматують диски, дістають несанкціонований доступ до інформації, шифрують дані і тому подібне.

Відомі публікації, в яких згадуються віруси, що викликають несправності апаратних засобів. Передбачається, що на резонансній частоті рухомі частини електромеханічних пристроїв, наприклад в системі позиціонування накопичувача на магнітних дисках, можуть бути зруйновані. Саме такий режим і може бути створений за допомогою програми-вірусу. Інші автори стверджують, що можливе завдання режимів інтенсивного використання окремих електронних схем (наприклад, великих інтегральних схем), за яких настає їх перегрів і вихід з ладу.

Використання в сучасних ЕОМ постійної пам'яті з можливістю перезапису сприяло появі вірусів, які змінюють програми BIOS, що призводить до необхідності заміни постійних пристроїв, які запам'ятовують.

Можливі також дії на психіку людини – оператора ЕОМ за допомогою підбору відеозображення, що видається на екран монітора з певною частотою (кожен двадцять п'ятий кадр). Вбудовані кадри цієї відеоінформації сприймаються людиною на підсвідомому рівні. Як наслідок, можливе нанесення серйозного збитку психіці людини. У 1997 році 700 японців потрапили до лікарні з ознаками епілепсії після перегляду комп'ютерного мультфільму по телебаченню. Припускають, що саме таким способом була випробувана можливість дії на людину за допомогою вбудовування 25-го кадру .

Відповідно до особливостей алгоритму функціонування віруси можна поділити на два класи:

– віруси, що не змінюють місце існування (файли і сектори) під час поширення;

– віруси, що змінюють місце існування під час поширення.

У свою чергу, віруси, що не змінюють місце існування, можуть бути поділені на дві групи:

– віруси-«супутники» (companion);
– віруси-«черви» (worm).

Віруси-«супутники» не змінюють файли. Механізм їх дії полягає у створенні копій виконуваних файлів. Наприклад, в MS DOS такі віруси створюють копії для файлів, що мають розширення *.EXE. Копії привласнюється те ж ім'я, що і виконуваному файлу, але розширення змінюється на *.COM. При запуску файлу із загальним ім'ям операційна система першим завантажує на виконання файл з розширенням *.COM, який є програмою-вірусом. Файл-вірус запускає потім і файл з розширенням *.EXE.

Віруси-«черви» потрапляють в робочу станцію з мережі, обчислюють адреси розсилки вірусу по інших абонентах мережі і здійснюють передачу вірусу. Вірус не змінює файлів і не записується в завантажувальні сектори дисків. Деякі віруси-«черви» створюють робочі копії вірусу на диску, інші – розміщуються тільки в оперативній пам'яті ЕОМ.

За складністю, ступенем досконалості і особливостями маскування алгоритмів віруси, що змінюють місце існування, поділяють на:

– студентські;
– «стелс»-віруси (віруси-невидимки);
– поліморфні.

До студентських належать віруси, створювачі яких мають низьку кваліфікацію. Такі віруси, як правило, є нерезидентними, часто містять помилки, досить просто виявляються і віддаляються. «Стелс»-віруси і поліморфні віруси створюються кваліфікованими фахівцями, обізнаними з принципом роботи апаратних засобів і операційної системи, а також мають навички роботи з машинно-орієнтованими системами програмування.

«Стелс»-віруси маскують свою присутність в місці існування шляхом перехоплення звернень операційної системи (ОС) до уражених файлів, секторам і переадресують ОС до незаражених ділянок інформації. Вірус є резидентним, маскується під програми ОС, може переміщатися в пам'яті. Такі віруси активізуються при виникненні переривань, виконують певні дії, у тому числі і по маскуванню, і тільки тоді управління передається на програми ОС, оброблювальні ці переривання. «Стелс»-віруси мають здатність протидіяти резидентним антивірусним засобам.

Поліморфні віруси не мають постійних пізнавальних груп – сигнатур. Звичайні віруси для розпізнавання факту зараження місця існування розміщують у зараженому об'єкті спеціальну пізнавальну

двійкову послідовність або послідовність символів (сигнатуру), яка однозначно ідентифікує зараженість файлу або сектора. Сигнатури використовуються на етапі поширення вірусів для того, щоб уникнути багатократного зараження одних і тих же об'єктів, оскільки при багатократному зараженні об'єкта значно зростає вірогідність виявлення вірусу. Для усунення демаскуючих ознак поліморфні віруси використовують шифрування тіла вірусу і модифікацію програми шифрування. За рахунок такого перетворення поліморфні віруси не мають збігів коду.

Будь-який вірус, незалежно від приналежності до певних класів, повинен мати три функціональні блоки: блок зараження (поширення), блок маскування і блок виконання деструктивних дій. Поділ на функціональні блоки означає, що до певного блока належать команди програми вірусу, що виконують одну з трьох функцій, незалежно від місця знаходження команд в тілі вірусу.

Після передачі управління вірусу, як правило, виконуються певні функції блока маскування. Наприклад, здійснюється розшифрування тіла вірусу. Потім вірус здійснює функцію впровадження в незаражене місце існування. Якщо вірусом повинні виконуватися деструктивні дії, то вони виконуються або безумовно, або при виконанні певних умов.

Закінчує роботу вірусу завжди блок маскування. При цьому виконуються, наприклад, такі дії: шифрування вірусу (якщо функція шифрування реалізована), відновлення старої дати зміни файлу, відновлення атрибутів файлу, коректування таблиць ОС і інше.

Останньою командою вірусу виконується команда переходу на виконання заражених файлів або на виконання програм ОС.

Для зручності роботи з відомими вірусами використовуються каталоги вірусів. До каталогу поміщаються такі відомості про стандартні властивості вірусу: ім'я, довжина, файли, що заражаються, місце впровадження у файл, метод зараження, спосіб впровадження в ОП для резидентних вірусів, ефекти, що виникають, наявність (відсутність) деструктивної функції і помилки. Наявність каталогів дозволяє під час опису вірусів указувати тільки особливі властивості, опускаючи стандартні властивості і дії.

Файлові віруси та їх структура. Файлові віруси можуть упроваджуватися тільки у виконувані файли: командні файли (файли, що складаються з команд операційної системи), призначені для користувача і системні програми в машинних кодах, а також в документи (таблиці), що мають макрокоманди. Макрокомандами або макросами є виконувані програми для автоматизації роботи з

документами (таблицями). Тому такі документи (таблиці) можна розглядати як виконуваний файл.

Для International Business Machines (IBM) – сумісних комп'ютерів вірус може упроваджуватися у файли таких типів: командні файли (BAT), завантажувальні драйвери (SYS), програми в машинних (двійкових) кодах (EXE, COM), документи Word (DOC) з версії 6.0 і вище, таблиці EXCEL (XLS). Макровіруси можуть упровадитися і в інші файли, що містять макрокоманди.

Файлові віруси можуть розміщуватися на початку, в середині і в кінці файлу, що заражається.

Незалежно від місця розташування вірусу в тілі зараженого файлу після передачі управління файлу першими виконуються команди вірусу.

У початок файлу вірус упроваджується одним з трьох способів. Перший з них полягає в переписуванні початку файлу в його кінець, а на місце, що звільнилося, записується вірус. Другий спосіб припускає зчитування вірусу і зараженого файлу в оперативну пам'ять, об'єднання їх в один файл і запис його на місце файлу. При третьому способі зараження вірус записується в початок файлу без збереження вмісту. У цьому разі заражений файл стає непрацездатним.

У середину файлу вірус може бути записаний також різними способами. Файл може «розсуватися», а в місце, що звільнилося, може бути:

Файл Вірус Файл

Файл Вірус

Вірус може упроваджуватися в середину файлу без збереження ділянки файлу, на місце якого поміщається вірус. Є і більш екзотичні способи впровадження вірусу в середину файлу. Наприклад, вірус Mutant застосовує метод стиснення окремих ділянок файлу, при цьому довжина файлу після впровадження вірусу може не змінитися.

Найчастіше вірус упроваджується в кінець файлу. За такої умови, як і у випадку з впровадженням вірусу в середину файлу, перші команди файлу замінюються командами переходу на тіло вірусу.

Алгоритм роботи файлового вірусу. Незважаючи на різноманіття файлових вірусів, можна виділити дії і порядок їх виконання, що є під час реалізації більшості вірусів цього класу. Цей узагальнений алгоритм може бути поданий у вигляді такої послідовності кроків:

Крок 1. Резидентний вірус перевіряє, чи заражена оперативна пам'ять, і у разі потреби заражає її. Нерезидентний вірус шукає незаражені файли і заражає їх.

Крок 2. Виконуються дії із збереження працездатності програми, у

файл якої упроваджується вірус (відновлення перших байт програми, настройка адрес програм і так далі).

Крок 3. Здійснюється деструктивна функція вірусу, якщо виконуються відповідні умови.

Крок 4. Передається управління програмі, у файлі якої знаходиться вірус.

У разі реалізації конкретних вірусів склад дій і їх послідовність можуть відрізнятися від наведених в алгоритмі.

Особливості макровірусів. Особливе місце серед файлових вірусів мають макровіруси. Макровірусами є шкідливі програми, написані на макромовах, вбудованих в текстові редактори, електронні таблиці й інше.

Для існування вірусів у конкретній системі (редакторові) необхідно, щоб вбудована в неї макромова мала такі можливості:

– прив’язку програми на макромові до конкретного файлу;

– копіювання макропрограм з одного файлу в інший;

– отримання управління макропрограмою без втручання користувача.

Таким умовам відповідають редактори MS Word, MS Office, Ami Pro, табличний процесор MS Excel. У цих системах використовуються макромови Word Basic і Visual Basic.

При виконанні певних дій над файлами, що містять макропрограми (відкриття, збереження, закриття тощо), автоматично виконуються макропрограми файлів. Водночас управління отримують макровіруси, які зберігають активність доти, доки активний відповідний редактор. Тому під час роботи з іншим файлом в «зараженому редакторові» він також заражається. Тут простежується аналогія з резидентними вірусами по механізму зараження. Для отримання управління макровіруси, що заражають файли MS Office, як правило, використовують один з прийомів:

– у вірусі є в макросі (виконується автоматично, під час відкриття документа, таблиці);

– у вірусі перевизначений один із стандартних макросів, який виконується під час вибору певного пункту меню;

– макрос вірусу автоматично викликається на виконання під час натиснення певної клавіші або комбінацій клавіш.

Перший макровірус WinWord.Concept, що вражає документи Word, з’явився літом 1995 року. Шкідлива функція цього вірусу полягає в зміні формату документів текстового редактора Word у формат файлів-стилів. Інший макровірус WinWord.Nuclear вже не такий

нешкідливий. Він дописує фразу з вимогою заборони ядерних випробувань, що проводяться Францією в Тихому океані. Крім того, цей вірус щорічно 5 квітня намагається знищити важливі системні файли.

Завантажувальні віруси. Заражають завантажувальні Boot-сектори гнучких дисків і Boot-сектори або Master Boot Record (MBR) жорстких дисків.

Завантажувальні віруси є резидентними. Зараження відбувається під час завантаження операційної системи з дисків.

Після включення ЕОМ здійснюється контроль її працездатності за допомогою програми, записаної в постійному пристрої, що запам'ятовує. Якщо перевірка закінчилася успішно, то здійснюється зчитування першого сектора з гнучкого або жорсткого диска. Порядок використання дисководів для завантаження задається користувачем за допомогою програми Setup. Якщо диск, із якого виконується завантаження ОС, заражений завантажувальним вірусом, то зазвичай виконуються такі кроки:

Крок 1. Із першого сектора диска завантажувальний вірус (частина вірусу) отримує управління, зменшує об'єм вільної пам'яті і зчитує з диска тіло вірусу.

Крок 2. Вірус переписує сам себе в іншу ділянку ОП, найчастіше – в старші адреси пам'яті.

Крок 3. Встановлюються необхідні вектори переривань (вірус резидентний).

Крок 4. Під час виконання певних умов виконуються деструктивні дії.

Крок 5. Копіюється Boot-сектор в ОП і передається йому управління.

Якщо вірус було активізовано з гнучкого диска, то він записується в завантажувальний сектор жорсткого диска. Активний вірус, постійно знаходячись в ОП, заражає завантажувальні сектори всіх гнучких дисків, а не тільки системні диски.

Зараження робочих гнучких дисків завантажувальними вірусами виконується з розрахунку на помилкові дії користувача ЕОМ у момент завантаження ОС. Якщо встановлений порядок завантаження ОС спочатку з гнучкого диска, а потім – з жорсткого, то за наявності гнучкого диска в накопичувачі буде перший сектор з гнучкого диска. Якщо диск був заражений, то цього достатньо для зараження ЕОМ. Така ситуація найчастіше виникає під час перезавантаження ОС після «зависань» або відмов ЕОМ.

Віруси та операційні системи

Програми-віруси створюються для ЕОМ певного типу, що працюють з конкретними ОС. Для одних ОС створені тисячі вірусів. Як приклад можна навести ОС MS DOS, що встановлюється на сумісні персональні комп'ютери.

Для ОС Unix, OS/2, Windows і деяких інших ОС відома невелика кількість вірусів. Привабливість ОС для створювачів вірусів визначається такими чинниками:

– поширеність ОС;
– відсутність вбудованих антивірусних механізмів;
– відносна простота;
– тривалість експлуатації.

Усі наведені чинники характерні для MS DOS. Наявність антивірусних механізмів, складність систем і відносно малі терміни експлуатації роблять завдання створення вірусів важко вирішуваним. Тому автори вірусів для Windows, OS/2 часто вдаються до використання з цих операційних систем MS DOS для впровадження вірусів.

Основним недоліком MS DOS є можливість повного і безконтрольного доступу будь-якої активної програми до всіх системних ресурсів ЕОМ, включаючи і модулі самої ОС.

Операційна система Microsoft Windows 3.1 і її модифікація Microsoft Windows for Workgroups 3.11 не є самостійними ОС, а більше схожі на дуже великі програми MS DOS. У цих ОС введені обмеження на доступ до ОП. Кожна програма дістає доступ тільки до свого віртуального простору ОП. Доступ же до дисків, файлів і портів зовнішніх пристроїв не обмежений. Зберігають працездатність і завантажувальні віруси, розроблені для MS DOS, оскільки вони отримують управління ще до завантаження Microsoft Windows 3.1, в цей період часу їх дії нічим не обмежені.

Слабкість захисних функцій ОС Microsoft Windows 95/98 також пояснюється сумісністю з MS DOS. Ця ОС має таку ж стійкість до дії вірусів, як і Microsoft Windows 3.1. До того ж, у цій ОС набули поширення і макровіруси.

Значно краще захищена від вірусів операційна система OS/2. Ця система повністю незалежна від MS DOS. Усі програми, що виконуються в OS/2, працюють в окремих адресних просторах, що повністю виключає можливість взаємного впливу програм. Існує можливість заборонити робочим програмам (несистемним) мати доступ до портів периферійних пристроїв. Якщо ЕОМ із Microsoft OS/2 використовується як файл-сервера ШМ LAN Server, то за допомогою

драйвера 386 HPFS можна вказувати права доступу до каталогів і файлів. Можна також захистити каталоги від запису до файлів, що містяться в них. У цій системі є можливість виконання програм MS DOS. Але в OS/2 для вірусів, створених для MS DOS, значно менше можливостей.

Методи і засоби боротьби з вірусами

Через масове поширення вірусів, серйозність наслідків їх дії на ресурси КС виникла потреба розробки і використання спеціальних антивірусних засобів і методів їх застосування. Антивірусні засоби застосовуються для вирішення таких завдань:

– виявлення вірусів в КС;
– блокування роботи програм-вірусів;
– усунення наслідків дії вірусів.

Виявлення вірусів бажано здійснювати на стадії їх впровадження або, принаймні, до початку здійснення деструктивних функцій вірусів. Необхідно зазначити, що не існує антивірусних засобів, що гарантують виявлення всіх можливих вірусів.

У разі виявлення вірусу необхідно відразу ж припинити роботу програми-вірусу, щоб мінімізувати збиток від його дії на систему.

Усунення наслідків дії вірусів здійснюється у двох напрямках:

– видалення вірусів;
– відновлення (якщо треба) файлів, областей пам’яті.

Відновлення системи залежить від типу вірусу, а також від часу виявлення вірусу щодо початку деструктивних дій. Відновлення інформації без використання дублюючої інформації може бути нездійсненним, якщо віруси при впровадженні не зберігають інформацію, на місце якої вони поміщаються в пам’ять, а також якщо деструктивні дії вже почалися, і вони передбачають зміни інформації.

Для боротьби з вірусами використовуються програмні і апаратно-програмні засоби, що застосовуються в певній послідовності і комбінації, утворюючи методи боротьби з вірусами. Можна виділити методи виявлення вірусів і методи видалення вірусів.

Відомі такі методи виявлення вірусів:

– сканування;
– виявлення змін;
– евристичний аналіз;
– використання резидентних сторожів;
– вакцинація програм;
– апаратно-програмний захист від вірусів.

Сканування – один з найпростіших методів виявлення вірусів.

Сканування здійснюється програмою-сканером, що проглядає файли у пошуках пізнавальної частини вірусу – сигнатури. Програма фіксує наявність вже відомих вірусів, за винятком поліморфних вірусів, що застосовують шифрування тіла вірусу, змінюючи при цьому кожного разу і сигнатуру. Програми-сканери можуть зберігати не сигнатури відомих вірусів, а їх контрольні суми. Програми-сканери часто можуть видаляти виявлені віруси. Такі програми називають поліфагами.

Метод сканування застосовний для виявлення вірусів, сигнатури яких уже виділені і є постійними. Для ефективного використання методу необхідне регулярне оновлення відомостей про нові віруси.

Метод виявлення змін ґрунтується на використанні програм-ревізорів. Ці програми визначають і запам’ятовують характеристики всіх областей на дисках, в яких зазвичай розміщуються віруси. Під час періодичного виконання програм ревізорів порівнюють характеристики, що зберігаються, і характеристики, що отримуються при контролі областей дисків. За наслідками ревізії програма видає зведення про згадану наявність вірусів.

Зазвичай програми-ревізори запам’ятовують у спеціальних файлах образи головного завантажувального запису, завантажувальних секторів логічних дисків, характеристики всіх контрольованих файлів, каталогів і номери дефектних кластерів. Можуть контролюватися також об’єм встановленої оперативної пам’яті, кількість підключених до комп’ютера дисків і їх параметри.

Головною перевагою методу є можливість виявлення вірусів усіх типів, а також нових невідомих вірусів. Досконалі програми-ревізори виявляють навіть «стелс»-віруси. Наприклад, програма-ревізор Adinf, розроблена Д. Мостовим, працює з диском безпосередньо по секторах через BIOS. Це не дозволяє використовувати «стелс»-вірусам можливість перехоплення переривань і «підставки» для контролю області пам’яті, потрібної вірусу.

Є у цього методу і недоліки. За допомогою програм-ревізорів неможливо визначити вірус у файлах, які надходять у систему вже зараженими. Віруси будуть виявлені тільки після поширення в системі.

Програми-ревізори непридатні для виявлення зараження макровірусами, оскільки документи і таблиці дуже часто змінюються.

Евристичний аналіз порівняно недавно почав використовуватися для виявлення вірусів. Як і метод виявлення змін, цей метод дозволяє визначати невідомі віруси, але не вимагає попереднього збору, обробки і зберігання інформації про файлову систему.

Суть евристичного аналізу полягає в перевірці можливих місць

існування вірусів і виявлення в них команд (груп команд), характерних для вірусів. Такими командами можуть бути команди створення резидентних модулів в оперативній пам'яті, команди прямого звернення до дисків, минаючи ОС. Евристичні аналізатори у разі виявлення «підозрілих» команд у файлах або завантажувальних секторах видають повідомлення про можливе зараження. Після отримання таких повідомлень потрібно ретельно перевірити ймовірно заражені файли і завантажувальні сектори всіма наявними антивірусними засобами. Евристичний аналізатор є, наприклад, в антивірусній програмі Doctor Web.

Метод використання резидентних сторожів заснований на застосуванні програм, які постійно знаходяться в оперативній пам'яті ЕОМ і відстежують всі дії решти програм.

У разі виконання будь-якою програмою підозрілих дій (звернення для запису в завантажувальні сектори, приміщення в ОП резидентних модулів, спроби перехоплення переривань і тому подібне) резидентний сторож надсилає повідомлення користувачу. Програма-сторож може завантажувати на виконання інші антивірусні програми для перевірки «підозрілих» програм, а також для контролю всіх файлів, що надходять ззовні (із змінних дисків, по мережі).

Істотним недоліком цього методу є значний відсоток помилкових тривог, що заважає роботі користувача, викликає роздратування і бажання відмовитися від використання резидентних сторожів. Прикладом резидентного сторожа є програма Vsafe, що входить до складу MS DOS.

Під вакцинацією програм розуміється створення спеціального модуля для контролю її цілісності. Як характеристика цілісності файлу зазвичай використовується контрольна сума. У разі зараження вакцинованого файлу, модуль контролю виявляє зміну контрольної суми і повідомляє про це користувача. Метод дозволяє виявляти всі віруси, у тому числі і незнайомі, за винятком «стелс»-вірусів.

Найнадійнішим методом захисту від вірусів є використання апаратно-програмних антивірусних засобів. Наразі для захисту ЕОМ використовуються спеціальні контролери і їх програмне забезпечення. Контролер встановлюється в роз'єм розширення і має доступ до загальної шини. Це дозволяє йому контролювати всі звернення до дискової системи. У програмному забезпеченні контролера запам'ятовуються області на дисках, зміна яких в звичайних режимах роботи не допускається. Отже, можна встановити захист на зміну головного завантажувального запису, завантажувальних секторів,

файлів конфігурації, виконуваних файлів й інше.

Під час виконання заборонених дій будь-якою програмою контролер надсилає відповідне повідомлення користувачу і блокує роботу комп'ютера.

Апаратно-програмні антивірусні засоби мають низку переваг перед програмними:

– працюють постійно;
– виявляють всі віруси, незалежно від механізму їх дії;
– блокують недозволені дії, роботи вірусу або некваліфікованого користувача.

Недолік у цих засобах один – залежність від апаратних засобів. Зміна останніх призводить до необхідності заміни контролера.

Прикладом апаратно-програмного захисту від вірусів є комплекс Sheriff.

Методи видалення наслідків зараження вірусами.

Під час видалення наслідків зараження вірусами здійснюється видалення вірусів, а також відновлення файлів і областей пам'яті, в яких знаходився вірус. Існує два методи видалення наслідків дії вірусів антивірусними програмами.

Перший метод припускає відновлення системи після дії відомих вірусів. Розробник програми-фага, що видаляє вірус, повинен знати структуру вірусу і його характеристики розміщення в місці існування.

Другий метод дозволяє відновлювати файли і завантажувальні сектори, заражені невідомими вірусами. Для відновлення файлів програма відновлення повинна завчасно створити і зберігати інформацію про файли, отриману в умовах відсутності вірусів. Маючи інформацію про незаражений файл і використовуючи зведення про загальні принципи роботи вірусів, здійснюється відновлення файлів. Якщо вірус піддав файл незворотнім змінам, то відновлення можливе тільки з використанням резервної копії або з дистрибутива. У разі їх відсутності існує тільки один вихід – знищити файл і відновити його вручну.

Якщо антивірусна програма не може відновити головний завантажувальний запис або завантажувальні сектори, то можна спробувати це зробити вручну. У разі невдачі слід відформатувати диск і встановити ОС.

Існують віруси, які, потрапляючи в ЕОМ, стають частиною його ОС. Якщо просто видалити такий вірус, то система буде непрацездатною.

Одним із таких вірусів є вірус One Half. Під час завантаження ЕОМ вірус поступово зашифровує жорсткий диск. При зверненні до вже

зашифрованих секторів резидентний вірус One Half перехоплює звернення і розшифровує інформацію. Видалення вірусу призведе до неможливості використовувати зашифровану частину диска. Під час видалення такого вірусу потрібно спочатку розшифрувати інформацію на диску. Для цього необхідно знати механізм дії вірусу.

Профілактика зараження вірусами комп'ютерних систем. Щоб забезпечити ЕОМ від дії вірусів, користувач, перш за все, повинен мати уявлення про механізм дії вірусів, щоб адекватно оцінювати можливість і наслідки зараження КС. Головною ж умовою безпечної роботи в КС є дотримання низки правил, що апробовані на практиці і показали свою високу ефективність.

Правило перше. Використання програмних продуктів, що отримані законним шляхом. Вірогідність наявності вірусу в піратській копії набагато більша, ніж в офіційно отриманому програмному забезпеченні.

Правило друге. Дублювання інформації. Перш за все, слід зберігати дистрибутивні носії програмного забезпечення. До того ж, запис на носії, що допускає виконання цієї операції, має бути, якщо є можливість, заблокований. Слід особливо поклопотатися про збереження робочої інформації. Переважно регулярно створювати копії робочих файлів на знімних машинних носіях інформації із захистом від запису. Якщо створюється копія на незнімному носієві, то бажано її створювати на інших ВЗУ або ЕОМ. Копіюється або весь файл, або зміни, що тільки вносяться. Останній варіант застосовний, наприклад, під час роботи з базами даних.

Правило третє. Регулярно використовувати антивірусні засоби. Перед початком роботи доцільно виконувати програми-сканери і програми- ревізори. Антивірусні засоби повинні регулярно оновлюватися.

Правило четверте. Особливо обережними слід бути у разі використання нових знімних носіїв інформації і нових файлів. Нові дискети обов'язково повинні бути перевірені на відсутність завантажувальних і файлових вірусів, а отримані файли – на наявність файлових вірусів. Перевірка здійснюється програмами-сканерами і програмами, що здійснюють евристичний аналіз. Під час першого виконання виконуваного файлу використовуються резидентні сторожі. У процесі роботи з отриманими документами і таблицями доцільно заборонити виконання макрокоманд засобами, вбудованими в текстові і табличні редактори (MS Word, MS Excel), до завершення повної перевірки цих файлів.

Правило п'яте. Під час роботи в розподілених системах або в

системах колективного користування доцільно нові змінні носії інформації і файли, що вводяться в систему, перевіряти на спеціально виділених для цієї мети ЕОМ. Доцільно для цього використовувати автоматизоване робоче місце адміністратора системи або особи, що відповідає за безпеку інформації. Тільки після всесторонньої антивірусної перевірки дисків і файлів вони можуть передаватися користувачам системи.

Правило шосте. Якщо не передбачається здійснювати запис інформації носія, то слід заблокувати виконання цієї операції. На магнітних дискетах 3,5 дюйма для цього досить відкрити квадратний отвір.

Постійне дотримання всіх наведених рекомендацій значно зменшить вірогідність зараження програмними вірусами і захистить користувача від безповоротних втрат інформації.

У особливо відповідальних системах для боротьби з вірусами необхідно використовувати апаратно-програмні засоби (наприклад, Sheriff).

Порядок дій користувача у разі виявлення зараження ЕОМ вірусами.

Навіть у разі скрупульозного виконання всіх правил профілактики можливість зараження ЕОМ комп'ютерними вірусами повністю виключити не можна. І якщо вірус все ж таки потрапив в КС, то наслідки його перебування можна звести до мінімуму, дотримуючись певної послідовності дій.

Щодо наявності вірусу в КС можуть свідчити такі події:

– поява повідомлень антивірусних засобів про зараження або про передбачуване зараження;

– об'єктивні ознаки наявності вірусу, такі як повідомлення, що видаються на монітор або принтер, звукові ефекти, знищення файлів й інші аналогічні дії, які однозначно вказують на наявність вірусу в КС;

– неявні ознаки зараження, що можуть бути викликані й іншими причинами, наприклад, відмовами апаратних і програмних засобів КС. До неявних проявів наявності вірусів в КС можна віднести «зависання» системи, уповільнення виконання певних дій, порушення адресації, відмови пристроїв і тому подібне.

Отримавши інформацію про передбачуване зараження, користувач повинен переконатися в цьому. Вирішити таку задачу можна за допомогою всього комплексу антивірусних засобів. Переконавшись в тому, що зараження відбулося, користувачеві слід виконати таку послідовність кроків:

Крок 1. Вимкнути ЕОМ для знищення резидентних вірусів.

Крок 2. Здійснити завантаження еталонної операційної системи із змінного носія інформації, в якій відсутні віруси.

Крок 3. Зберегти на змінних носіях інформації важливі для вас файли, які не мають резервних копій.

Крок 4. Використовувати антивірусні засоби для видалення вірусів і відновлення файлів, областей пам'яті. Якщо працездатність ЕОМ відновлена, то здійснюється перехід до кроку 8, інакше – до кроку 5.

Крок 5. Здійснити повне стирання і розмітку (форматування) незнімних зовнішніх пристроїв, що запам'ятовують. У ЕОМ для цього можуть бути використані програми MS-DOS FDISK і FORMAT. Програма форматування FORMAT не видаляє головний завантажувальний запис на жорсткому диску, в якому може знаходитися завантажувальний вірус. Тому необхідно виконати програму FDISK з недокументованим параметром MBR, створити за допомогою цієї ж програми розділи і логічні диски на жорсткому диску. Потім виконується програма FORMAT для всіх логічних дисків.

Крок 6. Відновити ОС, інші програмні системи і файли з дистрибутивів і резервних копій, створених до зараження.

Крок 7. Ретельно перевірити файли, збережені після виявлення зараження, і, у разі потреби, видалити віруси і відновити файли.

Крок 8. Завершити відновлення інформації всесторонньою перевіркою ЕОМ за допомогою всіх антивірусних засобів, що є у розпорядженні користувача.

За умови виконання рекомендацій щодо профілактики зараження комп'ютерними вірусами, а також за умови вмілих і своєчасних дій у разі зараження вірусами збиток інформаційним ресурсам КС може бути мінімальним.

Пакетні фільтри

Останнім часом найбільш популярними серед засобів захисту інформаційних ресурсів в Інтернеті є міжмережеві екрани (Firewall або брандмауери). Міжмережевий екран розміщується на шлюзі між локальною мережею і мережею «Інтернет». Окрім інших функцій, брандмауер може проглядати IP-пакети і залежно від адреси відправника і одержувача пропускати або не пропускати пакети, що намагаються проникнути в систему.

Міжмережевий екран (МЕ) розташовується на межі мережі і регулює доступ до корпоративних ресурсів. Цей пристрій аналізує і збирає інформацію про зовнішні пакети і сеанси в мережі (залежно від типу брандмауера), згідно прийнятих правил: пропустити або не

пропустити конкретний пакет і дозволити або не дозволити організувати конкретний сеанс.

МЕ поділяють на три основні класи:

– фільтри пакетів;

– шлюзи сеансового рівня;

– шлюзи рівня застосувань.

Системи фільтрації пакетів просівають кожен IP-пакет через сито визначених користувачем правил і визначають права пакету на прохід у внутрішню частину мережі. Шлюзи рівня застосувань у відповідь на кожен запит, що надходить, про надання сервісу організовують зовнішній мережевий сеанс; вони ж відкривають відповідний внутрішній сеанс для санкціонованого доступу і передають пакети між зовнішніми і внутрішніми з'єднаннями. Загалом, шлюзи застосувань, порівняно з фільтрами пакетів, забезпечують ретельніший контроль за сеансом, але, як наслідок, вони вимагають застосування і могутніших обчислювальних потужностей. Системи обох типів призначені для того, щоб захистити мережу від небезпек, що знаходяться зовні.

На думку експертів, брандмауери повинні мати три важливі особливості, а саме:

– весь трафік повинен проходити через одну крапку;

– брандмауер зобов'язаний контролювати і реєструвати весь трафік, що проходить;

– платформа МЕ повинна бути неприступна для атак.

Фільтри пакетів виконують оцінку даних на основі IP-інформації, що наявна в заголовку пакета, а точніше в адресі відправника і одержувача пакета. Фільтр не тільки зчитує IP-заголовок, але і зіставляє отриману інформацію зі списком правил фільтрації для дозволу або заборони передачі пакета. У правилах фільтрації наявні поля IP-адрес, типи протоколів, номери портів відправника і одержувача. Перш ніж дозволити пакету продовження передбачуваного для нього маршруту, фільтри пакетів порівнюють вказані в ньому дані із зумовленими значеннями. Загалом фільтри пакетів є найкращим вирішенням МЕ, але, завдяки своєму умінню перевіряти пакети різних протоколів, є і найгнучкішими інструментами вирішення поставленого завдання. Крім того, фільтри працюють швидко, оскільки для ухвалення рішення вони просто проглядають інформацію про пакет. Проте фільтри пакетів мають декілька істотних недоліків: вони не в змозі відстежувати конкретний мережевий сеанс і не в змозі запобігти атаці з імітацією IP-адреси.

Імітація IP-адреси буває, коли хакер привласнює IP-адресу

законного користувача – часто ним є внутрішня адреса того, хто має доступ до ресурсів. Оскільки фільтри пакетів «проглядають» інформацію про IP-адресу, то вони допускають пакет з дозволеною адресою в мережу незалежно від того, звідки ініційований сеанс і хто ховається за адресою. Проте вдосконалена версія цього механізму, відома як динамічна фільтрація пакетів, дозволяє аналізувати адресу, з якої хтось намагається здійснити доступ, і здійснює «пінгування» (ping) для перевірки цієї адреси. Очевидно, якщо зловмисник використовує внутрішню IP-адресу компанії ззовні, то ping не досягне відправника пакета і сеанс не отримає продовження. Динамічну фільтрацію пакетів підтримують продукти типу WatchGuard Security System компанії Seattle Software Labs і BorderWare Firewall Server, компанії Secure Computing (цей продукт був придбаний Secure разом з компанією Border Network Technologies з Торонто).

Компанії Seattle Software Labs, Cisco і Checkpoint Software Technologies також підтримують технологію перетворення мережевої адреси, яка забезпечує звичайну фільтрацію пакетів із спотворенням. Під час проходження пакета через брандмауер його IP-адреса замінюється якоюсь іншою, вибраною з відрізку адрес. Така заміна дозволяє приховати внутрішні адреси від зловмисника за межами мережі. Інші типи брандмауерів, наприклад шлюзи рівня застосування і шлюзи рівня каналу, мають цю ж властивість за замовчанням.

Контрольні питання

1. Дайте визначення WWW?
2. Комплекс апаратних та програмних засобів, що дозволяють комп’ютерам обмінюватися даними, – це?
3. Що називають Web-вузлом?
4. Що таке URL?
5. За допомогою яких пристроїв можна підключитися до мережі «Інтернет»?
6. Комп’ютер, що надає послуги іншим комп’ютерам у мережі (клієнтам), називається?
7. Які бувають типи фаєрволів?
8. Що називається комп’ютерною мережею? Яка існує класифікація комп’ютерних мереж? Дайте обґрунтовану відповідь
9. Використання міжмережевних екранів. Функції екранів.
10. Політика безпеки під час роботи в мережі.

11. За яким алгоритмом діють перехоплювачі паролів другого роду?
12. За яким алгоритмом діють перехоплювачі паролів першого роду?
13. За яким алгоритмом діють перехоплювачі паролів третього роду?
14. Що не належить до «шкідливих програм»?
15. Сигнатура вірусу – це?
16. Комп'ютерні віруси не класифікують за?
17. Назвіть складові частини сучасного антивірусу.
18. Віруси, що весь час знаходяться в оперативній пам'яті, називаються?
19. До явних проявів роботи вірусу належать?
20. Головною характеристикою троянської програми є?

Джерела до розділу 8

1. Інформаційні системи та технології: підручник / кол. авт.; ред. В. Б. Вишня. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2021. 296 с.
2. Заплотинський Б. А. Інформаційні технології в юридичній діяльності. посіб. КІІВтаП НУ ОЮА, 2018, 108 с.
3. Український ІТ-портал. URL : http://www.ua-admin.com.
4. Ліга: Закон. URL : http://www.ligazakon.ua/.
5. Юридична бібліотека (Україна) URL : //law.biz.ua
6. Наказ НПУ від 22.05.2018 № 509 «Про організацію інформаційного обліку комп'ютерної техніки та комп'ютерних програм, що використовуються в органах та підрозділах поліції».
7. СТ НПУ від 28.12.2019 № 15392/20/27-2019 «Про надання доступу до інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції» .

Розділ 9
КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

9.1. Види організації радіозв'язку. Проблемні питання використання засобів радіозв'язку підрозділами Національної поліції

Одним із факторів, що впливають на ефективність діяльності поліції є її оснащення комунікаційними технологіями за допомогою яких здійснюється управління нарядами, підрозділами, службами. І, безумовно, система радіозв'язку займає важливе місце серед комунікаційних засобів, необхідних для виконання службових завдань, що постають перед підрозділами Національної поліції. Однак значна частина радіостанцій, що використовуються на сучасному етапі в МВС, є аналоговими, і це значно знижує функціональність роботи їх підрозділів. Вже давно назрів перехід на цифрові системи радіозв'язку.

Проблема заміни застарілого аналогового обладнання радіозв'язку на сучасні цифрові системи постає не тільки в органах системи МВС, як Національна поліція, Державна прикордонна служба, Національна гвардія, Державна служба з надзвичайних ситуацій, але і у підрозділах інших міністерств: Збройних сил України, Мінцифри, Адміністрації Держспецзв'язку, Національної комісії, що здійснює державне регулювання у сфері зв`язку та інформатизації (НКРЗІ). Вважаючи, що це загальнодержавна проблема, Кабінет Міністрів України видав Розпорядження від 23 грудня 2020 р. № 1618-р «Про затвердження плану заходів щодо впровадження єдиної багатозонової системи цифрового радіозв'язку». У даному розпорядженні Кабінет міністрів доручив переліченим вище міністерствам:

– утворити робочу групу для визначення можливості впровадження єдиної багатозонової системи цифрового радіозв'язку;

– підготувати та схвалити технічне завдання з виконання науково-дослідної роботи з питань дослідження стану розподілу радіочастотного ресурсу України, визначення технології та розроблення пропозицій щодо впровадження єдиної багатозонової системи цифрового радіозв'язку у певних частотних діапазонах (далі - науково-дослідна робота), визначити замовника науково-дослідної роботи;

– підготувати та подати в установленому порядку Кабінетові Міністрів України проект постанови Кабінету Міністрів України «Про внесення змін до Національної таблиці розподілу смуг радіочастот України та Плану використання радіочастотного ресурсу України»;

– за результатами роботи робочої групи та на підставі звіту про проведену науково-дослідну роботу розробити фінансово-економічне обґрунтування та подати Кабінетові Міністрів України пропозиції щодо фінансування заходів із побудови єдиної багатозонової системи цифрового радіозв'язку [1].

Радіозв'язок, як і інші види зв'язку, призначений для передачі інформації на відстані. Принципова відмінність радіосистем передачі інформації виявляється в тому, що умови розповсюдження радіохвиль у радіолінії нестаціонарні, тобто можуть змінюватися залежно від часу та частоти. Однак передача за допомогою радіозв'язку в деяких випадках є єдиним методом зв'язку (наприклад зв'язок з рухомими об'єктами).

Розглянемо різновиди організації систем радіозв'язку. Їх поділяють на конвенціональні та транкінгові. У конвенціональних мережах радіозв'язку за групою абонентів закріплюється певний частотний канал. Такий спосіб радіозв'язку є виправданим, коли кількість абонентів мережі невелика, а зона покриття мала. Перевагою конвенціональної системи радіозв'язку є простота й невисока вартість. Але використання частотного спектра є неефективним.

Конвенціональний радіозв'язок організовується шляхом симплексних та дуплексних радіомереж. Симплексні мережі організовуються коли група користувачів працюють на одній частоті (симплексному каналі). Усі користувачі чують один одного й викликають необхідного абонента голосом. У радіомережі можуть використовуватися портативні, автомобільні й стаціонарні радіостанції. Усі вони рівнозначні. Зрозуміло, дальність зв'язку між автомобільними (стаціонарними) станціями вище. У дуплексних радіомережах радіозв'язок організовується одночасно на двох частотах. На першій частоті здійснюється прийом, на другій – передача. Таким побудовані телефонні системи. Для організації професійного рухомого радіозв'язку дуплексний радіозв'язок практично не використовується.

Розглянемо напівдуплекс (двохчастотний симплекс). Радіозв'язок організовується з використанням двох частот: прийомної та передавальної, але, в порівнянні з дуплексом, не одночасно, а почерзі. Одночасно користувач може знаходитися або в режимі «передача» чи на «прийомі». Двохчастотний симплекс використовується за допомогою ретрансляторів.

Ретранслятор це такий засіб зв'язку, що приймає радіосигнал, а потім передає його в ефір. Для покращення дальності зв'язку потрібно побороти кривизну Землі, а це можливо шляхом підіймання приймача та передавача. У разі, коли в системі є рухомі користувачі (автотранспорт), то це може бути реалізовано шляхом встановлення спеціального пристрою на великій висоті, що буде приймати й передавати радіосигнали. Практично всі сучасні системи зв'язку мають в своєму складі ретранслятори [2, 152].

До транкінгових систем можна віднести такі системи, де пошук вільного каналу здійснюється за допомогою абонентських радіостанцій, що весь час сканують частотні канали транкінгової системи в пошуках сигналу від стаціонарної станції чи вільного каналу, на якому можна було б викликати іншого користувача.

У підрозділах Національної поліції України переважно використовуються радіомережі конвенціонального зв'язку. Основу складають аналогові засоби радіозв'язку, що вже давно не задовольняють потреб організації сучасного зв'язку. Однак перехід на цифрові технології, скажімо, на той же стандарт TETRA чи інші стандарти цифрових засобів зв'язку потребує багато коштів, і, на жаль, не увесь можливий функціонал цих систем можна використовувати.

Досвід бойових дій під час проведення ООС показав ряд проблемних питань з організації зв'язку в тактичній (оперативній) ланці управління. На теперішній час основний спосіб організації радіозв'язку в тактичній ланці управління є транкінговий зв'язок. Із метою підвищення зони покриття, стійкого зв'язку у радіомережах з командирами підпорядкованих військових частин та підрозділів (до батальйону включно) передбачено роботу літаків-ретрансляторів [3].

Необхідність переходу до цифрового зв'язку пояснюється рядом переваг цифрового транкинга перед аналоговими системами, такими як велика спектральна ефективність за рахунок використання певних видів модуляції сигналу і складних алгоритмів перетворення мовного сигналу, підвищена ємність систем зв'язку, покращення якості мовного обміну по всій території обслуговування радіостанції шляхом використання цифрових сигналів та стійким до перешкод кодуванням.

Цифрові транкінгові системи в порівнянні з аналоговими мають ряд переваг за рахунок реалізації вимог по підвищеній оперативності та безпеці зв'язку, надання широких можливостей по передачі даних, більш широкого спектру послуг зв'язку (включаючи специфічні послуги зв'язку для реалізації спеціальних вимог служб громадської безпеки),

можливостей організації взаємодії абонентів різних мереж.

Розглянемо переваги цифрових транкінгових систем радіозв'язку.

1. Покращена оперативність зв'язку.
2. Можливість передачі даних.
3. Підвищена безпека зв'язку.
4. Розширені послуги зв'язку (автоматична реєстрація абонентів, роумінг, управління потоком даних, переадресація виклику).
5. Можливість взаємодії абонентів різних мережах радіозв'язку.

В наступних розділах розглянемо можливості цифрових систем радіозв'язку конвенціональних та трангінгових мереж.

9.2. Можливості конвенціональної цифрової системи DMR1

Основними споживачами систем на базі технології DMR1, як і систем конвенційного радіозв'язку, є підрозділи нижнього і середнього рангу МВС, де потреба в засобах професійного радіозв'язку очевидна і не потребує обґрунтувань.

Технологія DMR1 в секторі професійних засобів зв'язку дозволяє задовольнити зростаючі вимоги споживачів до засобів зв'язку вже не обмежуючись лише їх надійністю, а пояснюючи необхідність:

– забезпечення захисту радіоефіру від прослуховування;
– організації передачі текстових повідомлень разом з голосом;
– збільшення розбірливості мови при сильних оточуючих акустичних перешкодах;
– збільшення терміну безперервної роботи акумуляторних батарей і т. і.

Всім цим вимогам відповідає новий стандарт конвенційного професійного радіозв'язку – DMR1 (Digital Mobile Radio), в основу якого закладений двохінтервальний протокол TDMA. DMR1 розроблений Європейським інститутом телекомунікаційних стандартів (ETSI), як єдиний загальноєвропейський стандарт цифрового радіозв'язку. На основі протоколу TDMA вже створено ряд стандартів зв'язку, широко і успішно використовуються у всьому світі, наприклад, GSM і TETRA, і можна з великою часткою впевненості заявити, що цей же протокол буде застосовуватися для вирішення завдань подальшого підвищення ефективності використання частотного ресурсу. Протокол TDMA має ряд переваг, актуальних для систем зв'язку як нинішнього, так і майбутніх поколінь. Це універсальність функціональних можливостей, невисока вартість обладнання, більш довгий термін

роботи акумуляторів, відкритість для реалізації нових функцій і перевірена на практиці здатність підвищувати ефективність використання частотного ресурсу без ризику перевантаження каналів зв'язку або створення перешкод. Стандарт DMR1 позиціонується як відкритий стандарт, тобто передбачається, що обладнання різних виробників буде сумісне [4].

Відкритий стандарт для цифрових мобільних рацій (DMR1) з'явився в 2005 році. Його вимоги складаються з трьох частин, послідовно з'являлися протягом наступних років, тому виробництво радіостанцій, які повністю відповідають стандарту почалося в 2007 році. Радіостанції DMR1 працюють, головним чином, в типових частотних діапазонах VHF / UHF, а саме 136-174 / 403-470 МГц. DMR1 – загальний стандарт, тому йому відповідають радіостанції багатьох брендів. Найбільш відомі – це Motorola, Hytera, Vertex Standard.

Поява стандарту DMR1 обумовлено декількома простими факторами:

– цифрова якість зв'язку в порівнянні з аналоговими радіостанціями;

– функціонал, який надає застосування цифрових технологій, наприклад, можливість передачі текстових повідомлень;

– висока частотна ефективність - завдяки цифровим технологіям, а саме, кодування сигналів, можна ущільнювати канали та передавати значно більше інформації без втрати якості;

– сумісність з аналоговими радіостанціями;

– відносно проста апаратна частина і низькі вимоги до інфраструктури;

– захищеність переданої інформації від прослуховування.

– Таким чином привабливість радіостанцій стандарту DMR1 для користувача важливі такі можливості:

– забезпечення захищеності радіоефіру від несанкціонованого прослуховування;

– можливість поряд з голосовим зв'язком надсилання текстових повідомлень розміром як у випадку зі стільниковим зв'язком;

– висока якість розбірливості переданої мови в умовах підвищеного рівня різнорідних оточуючих шумів;

– тривалість автономної роботи радіостанцій від акумуляторів;

– нечутливих до умов експлуатації, наприклад, до мінусових температур.

В основі технології DMR1 лежать механізми TDMA (Time Division Multiple Access – багатостанційний доступ з тимчасовим поділом

каналів), що дозволяє розмістити два тимчасові інтервали на одній несучій частоті з сіткою частот 12,5 кГц.

Стандарт DMR1 заснований на застосуванні технології поділу сигналів за часом TDMA, що дозволяє на одній частоті створювати два канали передачі інформації за допомогою коротких пакетів даних. Зокрема, технологія може застосовуватися не тільки в стандартних частотних діапазонах 134-176 / 403-470 МГц, а й у всьому частотному спектрі 50-999 МГц. Одним із основних внутрішніх параметрів збудованої подібним чином системи є двобічний рознос, який може змінюватися в залежності від частотного діапазону. Для кодування дуплексного розносу відводиться 15 біт інформації, завдяки якій сигнал потім відновлюється в послідовний мовний потік.

Технічно стандарт DMR1 є структурою таймслотов з тривалістю 30 мілісекунд. У цьому проміжку часу 27.5 мс призначаються безпосередньо для корисної інформації, кодуємої 216-ю бітами, а решту часу – 48 бітів супроводу. У DMR1 можливі два режими – симплексного зв'язку і двочастотний симплекс з дуплексним розносом (при наявності ретранслятора). Власне, в першому режимі виграшу по щільності передачі інформації не вийде, оскільки система залишиться одноканальною подібно аналоговій. У другому випадку реалізується два незалежних голосових з'єднання в одному частотному каналі.

Для багатьох абонентів систем радіозв'язку найважливішою перевагою цифрових стандартів є те, що вони можуть більш ефективно використовувати ресурс частотних каналів. Цієї ефективності дозволяє домогтись метод TDMA, коли 1 частотний канал шириною 12,5 КГц, розділяється на два тимчасових слоти. Тобто ці два інтервали в одному каналі можна застосовувати для організації передавання двох окремих викликів. Існує можливість виділення одного з інтервалів для обслуговування викликів, а в другому одночасно робити передачу інформації. Технічні прилади DMR1 налаштовані на ту ж частотну смугу, що і ліцензовані аналогові мережі PMR. Абонентам не потрібно переходити на інші частотні діапазони чи докупати ліцензії.

Стандарт DMR1 надає можливість використання технологій управління живленням радіоприладів і так званим режимом очікування, які сприяють заощадженню заряду акумулятора. Абонентам мереж радіозв'язку слід мати розбірливий та перешкодостійкий голосовий зв'язок. Якщо виклик пропущений, або виникла помилка оператора, непередане повідомлення або непрацюючий акумулятор, приводять до негативних подій. До недоліків аналогових систем радіозв'язку можна віднести обмежену дальність їх дії і розбірливість передавання мовного

сигналу. Аналогові сигнали мають низьку перешкодостійкість, що негативно впливає на якість переговорів. Доволі часто погіршується мовний сигнал за рахунок підвищення рівня шумів і недоліків передачі. Особливо це трапляється на гранічних можливостях під час передавання чи приймання сигналу. У мережах стандарту DMR1 застосовуються спеціальні алгоритми виправлення помилок, що покращують мовний сигнал до початкового стану. У системах DMR1 вбудований декодер, який придушує вуличний шум, що практично не передається, і тому абонент, що примає сигнал, його не чує.

Стандарт DMR1 постійно вдосконалюється, реалізуючи функціональний набір який раніше був не характерний для сектора засобів конвенційного радіозв'язку. До основних функціональних можливостях цифрового стандарту DMR1 слід віднести:

– цифрову обробку сигналу;
– управління акумуляторною батареєю;
– пріоритетний аварійний виклик;
– покращений режим «вільні руки»;
– вбудований приймач GPS сигналів для реалізації програм із контролю місця розташування;
– віддалений контроль;
– опціональне шифрування;
– двобічний виклик;
– одночасну передачу голосу і даних (в тому числі пакетних);
– роботу в аналоговому режимі, що особливо актуально під час поступової міграції аналогових конвенціональних систем.

Типи викликів, реалізованих у межах стандарту DMR1:

– індивідуальний виклик «радіостанція – радіостанція»;
– груповий виклик «радіостанції – група радіостанцій»;
– груповий виклик «радіостанція – усі радіостанції»;
– передача пакетних даних з канальної швидкістю 2 кбіт / с.

Стандарт DMR1 відрізняє швидке встановлення виклику (до 200 мс).

Закладений в рамках стандарту DMR1 функціонал дозволяє реалізувати широкий набір рішень, зокрема:

– передачу пакетних даних (пропускна здатність каналу до 2 кбіт/с);
– передачу телеметрії;
– передачу текстових повідомлень;
– додатки з контролю місця розташування.

Наступність і сумісність з існуючими аналоговими системами зв'язку дозволяє зберегти зроблені раніше інвестиції і замінити парк

застарілих аналогових абонентських терміналів в міру необхідності.

Основна проблема застосування засобів зв'язку стандарту DMR1 (Digital Mobile Radio – цифровий рухомий радіозв'язок) фірми Motorola – робота на фіксованих частотах, у достатньо вузькому діапазоні частот (136 – 174 МГц) що призводить до низької стійкості при впливі засобів РЕБ (радіоелектронна боротьба). Крім цього, наявність лише 2 голосових каналів для одного ретранслятора, а також низька швидкість передачі даних, призводить до низької продуктивності мережі та, відповідно, до низької вірогідності обслуговування мобільних абонентів [3].

9.3. Порівняльний аналіз основних транкінгових цифрових систем радіозв'язку

До найбільш поширених стандартів цифрового транкінгового радіозв'язку, на основі яких у багатьох країнах організовані системи зв'язку, відносяться:

– EDACS, розроблений фірмою Ericsson;

– TETRA, розроблений Європейським інститутом стандартів зв'язку;

– APCO 25, розроблений Асоціацією офіційних представників служб зв'язку органів громадської безпеки;

– Tetrapol, розроблений фірмою Matra Communication (Франція);

– iDEN, розроблений фірмою Motorola (США).

Усі ці стандарти відповідають сучасним вимогам до систем транкінгового радіозв'язку. За допомою них можна створювати різні конфігурації мереж зв'язку: від простих однозонових систем до складних багатозонових систем національного рівня. Мережі на основі даних стандартів організовують різні режими передавання мовного сигналу (індивідуальний та груповий зв'язок), обміну будь-якими даними (спеціальні пакети, короткі комутовані повідомлення), можливість організації зв'язку з телефонною мережею загального користування та стільникового зв'язку. У мережах радіозв'язку цих стандартів використовуються сучасні способи перетворення мовних сигналів, що забезпечені ефективними методами завадо стійкого кодування будь-якої інформації. Виробники радіоприладів забезпечують відповідність їх стандартам MIL STD 810 по різних кліматичних і механічних впливах.

Розглянемо систему EDACS. Одним із перших стандартів

цифрового транкінгового радіозв'язку був стандарт EDACS (Enhanced Digital Access Communication System), розроблений фірмою Ericsson (Швеція). Спочатку він передбачав тільки аналогову передачу мови, проте пізніше була розроблена спеціальна цифрова модифікація системи EDACS Aegis [5].

Система EDACS працює за допомогою закритого фірмового протоколу, що відповідає вимогам із безпеки користування системами транкінгового радіозв'язку, які були спільно розроблені рядом фірм-виробників обладнання рухомого зв'язку разом з правоохоронними органами (Документ APS 16).

Цифрові системи EDACS випускалися на діапазони частот 138-174 МГц, 403-423, 450-470 МГц і 806-870 МГц з розносом частот 30; 25; і 12,5 кГц.

У системах EDACS використовується частотне розділення каналів зв'язку з використанням високо швидкісного (9600 біт / с) виділеного каналу управління, що розроблений для обміну цифровою інформацією між радіостанціями і пристроями керування роботою мережі. Це підтримує високу оперативність зв'язку в радіомережі (встановлення зв'язку не перевищує 0,25 с). Швидкість передачі інформації в частотному каналі дорівнює 9600 біт / с.

Кодування мовного сигналув системі проводиться за допомогою компресії імпульсно-кодової послідовності зі швидкістю 64 Кбіт / с. Основними функціями стандарту EDACS є спеціальні режими виклику (груповий, індивідуальний, екстрений, статусний), а також динамічне управління пріоритетністю, дистанційне виключення радіостанцій (за втрати чи краліжки радіостанцій).

Системи стандарту EDACS можуть працювати як у цифровому, так і в аналоговому режимі, що дозволяє абонентам застосовувати застарілі технічні засоби радіозв'язку.

Системи зв'язку відрізняється високою надійностю і відмовостійкістю мереж. Висока відмовостійкість забезпечується за допомогою в апаратурі системи EDACS спеціальної архітектури і принципом поділеної обробки даних. Базова станція системи зв'язку працює навіть у разі відмови всіх ретрансляторів, окрім одного. Останній працездатний ретранслятор працює як ретранслятор каналу управління, призначаючи свій власний частотний канал, після чого переходить в режим ретранслятора робочого каналу.

У системі EDACS використовується наскрізне шифрування інформації, однак у зв'язку з закритим протоколом застосовується або стандартний алгоритм захисту, пропонований фірмою Ericsson, або за

згодою, використання власних програмно-апаратних модулів, що реалізують оригінальні алгоритми, які повинні бути сумісні з системним протоколом EDACS.

У світі розгорнуто велику кількість мереж стандарту EDACS. Але, в даний час фірма Ericsson припинила поставки обладнання для розгортання нових мереж даного стандарту і тільки підтримує функціонування діючих мереж.

Розглянемо систему TETRA. TETRA є стандарт цифрового транкінгового радіозв'язку, що складається з специфікацій, розроблених Європейським інститутом телекомунікаційних стандартів ETSI (European Telecommunications Standards Institute). Стандарт TETRA створювався як єдиний загальноєвропейський цифровий стандарт. До квітня 1997 р абревіатура TETRA означала трансєвропейських транкінгового радіо (Trans-European Trunked RAdio). Однак у зв'язку з великим інтересом, виявленим до стандарту в інших регіонах, територія його дії не обмежується тільки Європою. На сьогодні TETRA розшифровується як Наземне транкінгового радіо (TErrestrial Trunked RAdio).

TETRA – відкритий стандарт і обладнання різних виробників буде сумісне. Доступ до специфікацій TETRA вільний для всіх, хто вступив у асоціацію «Меморандум про взаєморозуміння та сприяння стандарту TETRA» (MoU TETRA). Асоціація, до якої в кінці 2018 р входило понад 100 учасників, об'єднує розробників, виробників, випробувальні лабораторії та користувачів різних країн.

Стандарт TETRA11 складається з двох частин: TETRA V + D (TETRA Voice + Data) – стандарту на інтегровану систему передачі мовного сигналу і даних, і TETRA PDO (TETRA Packet Data Optimized) – стандарту, що призначений тільки на передачу даних.

У стандарт TETRA входять специфікації бездротового інтерфейсу, інтерфейсів між мережею TETRA і цифровою мережею з інтеграцією послуг (ISDN), телефонною мережею загального користування, мережею передачі даних, АТС і т. п. У стандарті є опис всіх послуг, що надаються мережами TETRA [6].

Інтерфейс стандарту TETRA1 призначений для роботи в стандартній сітці частот з кроком 25 кГц. Необхідний мінімальний дуплексний рознос радіоканалів – 10 МГц. Для мереж стандарту TETRA використовуються деякі піддіапазони частот. У країнах Європи за службами безпеки закріплені діапазони 380-385 / 390-395 МГц, а для комерційних організацій передбачені діапазони 410-430 / 450-470 МГц. В Азії для систем TETRA використовується діапазон 806-870 МГц.

У мережах стандарту TETRA V + D застосовується метод багатостанційного доступу з тимчасовим поділом каналів зв'язку. На одній фізичній частоті організовано до 4 незалежних інформаційних каналів.

Інформаційні повідомлення передаються за допомогою мультикадра тривалістю 1,02 с. Мультикадр містить 18 кадрів, один з яких є контрольним. Кадр має тривалість 56,67 мс і містить 4 тимчасові інтервали (time slots). У кожному з часових інтервалів передається інформація свого тимчасового каналу. Часовий інтервал має довжину 510 біт, з яких 432 є інформаційними (2 блоки по 216 біт).

У системах стандарту TETRA використовується відносна фазова модуляція типу p / 4-DQPSK (Differrential Quadrum Phase Shift Keying). Швидкість модуляції – 36 Кбіт / с.

Для перетворення мови в стандарті використовується кодек із алгоритмом перетворення типу CELP (Code Excited Linear Prediction). Швидкість цифрового потоку на виході кодека становить 4,8 Кбіт / с. Цифрові дані з виходу мовного кодека піддаються блоковому і згортаючому кодуванню, шифруванню, після чого формуються інформаційні канали. Пропускна здатність одного інформаційного каналу становить 7,2 Кбіт / с, а швидкість цифрового інформаційного потоку даних – 28,8 Кбіт / с. (при цьому загальна швидкість передачі символів в радіоканалі завдяки додаткової службової інформації та контрольного кадру в мультикадрі відповідає швидкості модуляції і дорівнює 36 Кбіт / с.).

У мережах стандарту TETRA мобільні станції можуть працювати в режимі «подвійного спостереження» («Dual Watch»). Він забезпечує прийом повідомлень від користувачів, які працюють як у режимі транкінгового, так і конвенціонального зв'язку.

Для збільшення зон обслуговування в мережах TETRA передбачається можливість використання абонентських радіостанцій в якості ретрансляторів.

TETRA надає користувачам ряд послуг, шо включені до стандарту за заявкою Асоціації європейської поліції (Schengen Group), що співпрацює з технічним комітетом ETSI:

- виклик, дозволений диспетчером;
- пріоритетний доступ та виклик (якщо перевантажена система);
- переривання обслуговування непріоритетних викликів;
- виборче прослуховування абонентів;
- дистанційне прослуховування обстановки у абонента;
- динамічне перегрупування (динамічне створення, модифікація і

видалення груп користувачів);

– ідентифікація сторони, що викликає.

Стандарт TETRA може забезпечувати два рівня безпеки переданої інформації:

– стандартний рівень, який застосовує шифрування інтерфейсу (як у мережі стільникового зв'язку GSM);

– високий рівень, при якому використовується наскрізне шифрування.

Засоби захисту радіоінтерфейсу стандарту TETRA – це способи аутентифікації абонента і структури, забезпечення конфіденційності трафіку шляхом потоку несправжніх імен і спеціального шифрування повідомлень.

Найбільш високий рівень захисту повідомлень є вимогою спеціальних груп абонентів. Наскрізне шифрування допомагає захистити мовну інформацію і повідомлення на лінії зв'язку між базовими і мобільними користувачами.

Мережі TETRA використовуються в Європі, Південно-Східної Азії, Африці, Північній і Південній Америці, Китаї, Австралії,.

Розглянемо систему APCO 251. Стандарт APCO 251 розроблений Асоціацією офіційних представників служб зв'язку органів громадської безпеки (Association of Public safety Communications Officials-international), що об'єднує користувачів систем зв'язку, що працюють в службах громадської безпеки.

Зараз стандарт включає всі основні документи, що регламентують принципи побудови інтерфейсу, протоколи шифрування, методи кодування мовного сигналу.

При створенні специфікацій стандарту, вони були поділені на два етапи реалізації – бФаза I і Фаза II. У 2000 р були сформовані спеціальні вимоги до кожної з фаз стандарту.

Основними принципами розроблення стандарту APCO 251, озвучені його розробниками, були вимоги:

– плавного переходу до засобів цифрового радіозв'язку;

– по відкритій системній архітектурі для підтримки конкуренції серед виробників засобів зв'язку;

– про створення можливостей взаємодії різних спецслужб безпеки під час проведення операцій.

Системна архітектура даного стандарту зв'язку працює в якості транкінгових та конвенціональних систем радіозв'язку. В цих мережах користувачі взаємодіють між собою або в режимі безпосереднього зв'язку, або через ретранслятор. Основним функціональним блоком

системи стандарту APCO 251 є спеціальні радіо підсистеми на основі однієї або декількох стаціонарних радіостанцій.

Стандарт APCO 251 надає можливість використання у стандартних діапазонах частот, що використовуються системами радіозв'язку:
138-174, 406-512 або 746-869 МГц. Основний метод доступу до каналів зв'язку – частотний, але можливе застосування в мережах стандарту APCO 251 множинного доступу з тимчасовим поділом каналів.

У Фазі I стандартний період сітки частот становить 12,5 кГц, в Фазі II – 6,25 кГц. Так при смузі 12,5 кГц використовується чотирьохпозиційна частотна модуляція за методом C4FM зі швидкістю 4800 символів в секунду, а при смузі 6,25 кГц – чотирьохпозиційна фазова модуляція зі згладжуванням фази по методу CQPSK. Такі методи модуляції допомогають працювати на однакових приймачах, що доповнюються різними підсилювачами потужності, так для Фази I – прості підсилювачі з високим ККД, а для Фази II – підсилювачі з високою лінійністю і обмеженою шириною випромінюваного спектру.

Інформація у вигляді мовного сигналу в радіоканалі передається кадрами по 180 мс, згрупованими по 2 кадри. Для кодування мовного сигналу в системі використовується кодек IMBE (Improved MultiBand Excitation). Він також працює в системі супутникового зв'язку Inmarsat. Швидкість кодування – 4400 біт / с. Після завадостійкого кодування мовної інформації швидкість інформаційного потоку збільшується до 7200 біт / с.

У мережі APCO 251 вбудована система ідентифікації абонентів, що може створювати в одній мережі до 2 мільйонів радіостанцій і до 65 тисяч груп. Затримка при з'єднанні в підсистемі відповідно до вимог до стандарту APCO 251 не повинна перевищувати в режимі конвенціонального зв'язку – 250 мс, при зв'язку через ретранслятор – 350 мс).

Мережі APCO 251 забезпечують 4 рівня криптографічного захисту. Застосовується потоковий метод шифрування інформації на основі нелінійних алгоритмів формування шифрувальної послідовності. Під час використання спеціального режиму OTAR (Over-the-air-re-keying) ключі шифрування передаються по радіоканалу.

APCO є міжнародною організацією. Система працює в США, Канаді, Австралії, Карибському регіоні. До Асоціації входять ФБР, Міністерство оборони США, Федеральний комітет зв'язку, поліції ряду штатів США, Секретна служба і багато інших державних організації. До виробників обладнання стандарту APCO 251 належать Motorola, Stanlite

Electronics, E.F.Johnson, Transcrypt і ін. Фірма Motorola розробила свою першу радіомережу, побудовану на системі APCO 251, що називається ASTRO.

Розглянемо систему Tetrapol. Стандарт цифрового транкінгового радіозв'язку Tetrapol був створений в 1987 р, фірмою Matra Communications. Вона уклала контракт із французькою жандармерією на розробку і введення до експлуатації системи цифрового радіозв'язку Rubis. Наразі радіомережа французької жандармерії охоплює більше половини території Франції і обслуговує понад 20 тис. Абонентів. У 1994 році фірма Matra створила свій форум Tetrapol, було розроблено специфікації Tetrapol PAS (Publicly Available Specifications), які ідентифікують цей стандарт цифрового транкінгового радіозв'язку.

Стандарт Tetrapol описує цифрову транкінгову систему радіозв'язку з виділеним каналом керування і частотним методом поділу каналів зв'язку. Стандарт працює як в однозоновій, так і в багатозоновій мережі зв'язку, він підтримує прямий зв'язок між користувачами без використання засобів мережі і ретрансляції сигналів на частотних каналах.

Мережі зв'язку стандарту Tetrapol працюють в діапазоні частот від 70 до 520 МГц, який включає два піддіапазона: нижче 150 МГц (VHF) і вище 150 МГц (UHF). Більшість радіоінтерфейсів для мереж цих піддіапазонів є спільною, але вони відрізняються в використанні різних методів завадостійкого кодування і кодового перемежування. У піддіапазоні UHF працює двобічний рознос каналів прийому і передачі у частотній смузі 10 МГц.

Розмежування частоти між каналами зв'язку становить 12,5 або 10 кГц. Мається можливість до розносу між каналами в 6,25 кГц. У мережах стандарту Tetrapol використовується ширина смуги до 5 МГц, що дозволяє організовувати 400-500 радіоканалів. Однак в одній зоні можна розмістити від 1 до 24 каналів.

Стандарт дозволяє отримати швидкість передачі інформації в каналі зв'язку до 8000 біт / с. Передача повідомлень відбувається по кадрам довжиною 160 біт і тривалістю 20 мс. Усі так звані кадри об'єднуються в Суперкадр тривалістю 4 с (200 кадрів). Уся інформація обробляється згортуючим кодуванням, перемежовується, скремблюється, піддається диференціальному кодуванню і остаточне форматується кадр.

У мережах стандарту Tetrapol застосовується GMSK модуляція з BT = 0,25.

З метою перетворення мовної інформації, в системах

використовується кодек з алгоритмом мовоперетворювача, який базується на методі аналізу шляхом синтезу типу RPCELP (Regular Pulse Code Excited Linear Prediction). Швидкість такого перетворення дорівнює 6000 біт / с.

У системах вибудовуються три основні режими радіозв'язку: транкінгового, режиму конвенціонального зв'язку і режиму ретрансляції.

У режимі режимі транкінгового зв'язку користувачі поєднуються за допомогою базових станцій (БС), які роздають канали зв'язку між абонентами. У такому випадку сигнали управління передаються на, спеціальному виділеному для кожної БС частотному каналі. У режимі конвенціонального зв'язку обмін повідомленнями між користувачами організовується без участі базової станції. У режимі ретрансляції зв'язок між користувачами вибудовується за допомогою ретранслятора, який має зафіксовані канали передачі і прийому повідомлень.

У мережах стандарту Tetrapol можна організовувати два види інформаційного обміну – передача мовної інформації і передача даних.

При передачі даних можна обмінюватись повідомленнями відповідно до протоколу X.400, організовувати доступ до централізованих баз даних та працювати з інтернет-мережами відповідно до протоколу TCP / IP, отримувати від приймачів GPS дані про місцезнаходження об'єкта, передавати відеосигнали.

Стандарт Tetrapol дозволяє виконувати наступні дії: аутентифікацію абонента, динамічне перегрупування, пріоритетний виклик, роумінг, управління передавачем абонента.

Взагалі стандарт Tetrapol був розроблений на замовлення правоохоронних органів, тому він містить різні складові забезпечення безпеки зв'язку, спрямовані на запобігання прослуховування переговорів, несанкціонованого доступу до мережі, створення навмисних перешкод, аналіз трафіку конкретних абонентів. Це досягається шляхом управління доступом до системи, наскрізним шифруванням інформації, автоматичної переконфігурації мережі, можливість передачі диспетчером радіомережі секретних ключів користувачам по радіоканалу, аутентифікація абонентів.

Мережі стандарту Tetrapol поширені у Франції. Це мережі зв'язку Rubis національної жандармерії Франції, також система Acropole французької поліції, система Iris служби залізниць. Також вони використовуються поліцією Каталонії та Мадрида, спецпідрозділами Чеської Республіки, служби транспорту Німеччини.

Розглянемо систему iDEN [7]. Технологія iDEN (integrated Digital

Enhanced Network) була розроблена компанією Motorola на початку 90-х років. Взагалі стандарт iDEN розроблявся якк корпоративний стандарт з відкритою архітектурою. Зокрема, компанія Motorola, зберігаючи за собою всі права з модифікації системного протоколу, надає можливість ліцензійно виробляти засоби радіомереж іншим виробникам.

Цей стандарт дозволяє створювати такі мережі, що підтримують усі види пересувного радіозв'язку: диспетчерського зв'язку, мобільного телефонного зв'язку, передачі текстової інформації і будь-яких даних. Технологія iDEN призначена для великих корпоративних мереж.

Користувачі мереж iDEN можуть передавати й отримувати на свої радіостанції текстову інформацію, а також передавати дані в комутаційному режимі зі швидкістю 9,6 Кбіт / с, а в пакетному – до 32 Кбіт/с. Абоненти зв'язку можуть заходити до мережі Інтернет, користуватись електронною поштою та факсимільним зв'язком.

Мережі iDEN базуються на технології МДТП (метод доступу з тимчасовим поділом). Так у кожному частотному каналі шириною 25 кГц створюється 6 мовних каналів. Це можливо завдяки розбиття кадру тривалістю 90 мс на тимчасові інтервали по 15 мс, в кожному з них передається інформація на окремому каналі.

Кодування мовного сигналу здійснюється за допомогою спеціального кодеку типу VSELP. Швидкість передачі інформації в одному каналі складає 7,2 Кбіт / с, а сумарна швидкість цифрового потоку в радіоканалі дорівнює 64 Кбіт / с. Це можливо за умови використання 16-позиційної квадратурной модуляції M16-QAM.

Системи зв'язку побудовані на використанні стандартних для Америки і Азії частотних діапазонів 805-821 / 855-866 МГц. IDEN має найкращу спектральну ефективність серед розглянутих мереж цифрового транкінгового зв'язку, він може вбудувати в 1 МГц до 240 інформаційних каналів. Але зони покриття базових станцій в системах iDEN менше, ніж у системах інших мереж, що витікає з малою потужністю абонентських радіостанцій (0,6 Вт – для портативних станцій і 3 Вт – для мобільних).

Система iDEN більше схожа на стільникові системи, що дозволяє обслуговування великої кількості абонентів і інтенсивний трафік завдяки побудові широкосмугових мереж. У мережі створюється до 10000 віртуальних мереж, у кожній із яких може бути до 65500 абонентів, об'єднаних при необхідності в 255 груп. Також кожна група користувачів може використовувати всю зону зв'язку, що підтримується цією системою.

Мережі iDEN побудовані в США, Канаді, Мексиці, Колумбії,

Бразилії, Аргентині, Китаї, Ізраїлі, Японії, Сингапурі та інших країнах. Взагалі кількість абонентів iDEN в світі більше 3 млн.

Розглянемо технічні характеристики і функціональні можливості представлених мереж транкінгового зв'язку. Усі стандарти мають достатньо високі технічні характеристики. Вони забезпечують можливість побудови різноманітних конфігурацій мереж зв'язку, можуть підтримувати різноманітні режими передачі мовної інформації та повідомлень, дозволяють зв'язок із фіксованими мережами. У пристроях зв'язку даних систем застосовуються сучасні методи перетворення мовного сигналу і завадостійкого кодування інформації. Всі стандарти забезпечують високу оперативність зв'язку.

Але у стандарті EDACS організовується передача оцифрованої мовної інформації по аналоговому каналу зв'язку. За функціональними особливостями стандарт EDACS поступається іншим стандартам, бо його розробили набагато раніше. Стандарти TETRA, APCO 25, Tetrapol і iDEN специфікують більш широкий спектр надаваних стандартних послуг зв'язку, за рівнем можна порівняти між собою.

Ми розглядаємо стандарти для потреб Міністерства внутрішніх справ, і всі вони забезпечують виконання більшості вимог, що пред'являються до спеціальних систем радіозв'язку. Розглянуті цифрові стандарти підтримують високу оперативність зв'язку (час доступу абонентів для всіх систем – не більше 0,5 с). Вони забезпечують високі показники відмовостійкості мереж радіозв'язку за рахунок гнучкої архітектури. Усі стандарти можуть забезчити захист інформації: для систем TETRA і Tetrapol стандарти передбачають можливість побудови як стандартного алгоритму шифрування, так і будь-яких інших алгоритмів шляхом наскрізного шифрування; у мережах EDACS ввбудований стандартний фірмовий алгоритм або існує можливість за узгодженням з фірмою використовувати власні алгоритми захисту.

Розглянемо перелік послуг, який надається кожним стандартом. Можна відзначити, що стандарти TETRA, APCO 25, Tetrapol забезпечують високий рівень спеціальних вимог, а EDACS – менший. Стандарт iDEN взагалі не передбачає виконання спеціальних послуг.

Ресурси радіочастотного спектру цифрових транкінгових систем радіозв'язку є найважливішим критерієм вибору тієї чи іншої системи. У такому випадку найбільш перспективні стандарти, які підтримують можливість побудови мереж зв'язку в найбільш широкому діапазоні частот.

Системи EDACS працюють в діапазонах 138-174, 403-423, 450-470

і 806-870 МГц. Системи TETRA дозволяють застосування таких діапазонів: 380-385 / 390-395, 410-430 / 450-470 МГц і 806-870 МГц. Системи APCO 25 відповідно до функціональних і технічних вимог забезпечують можливість роботи в будь-якому з діапазонів, відведених для мобільного радіозв'язку. Стандарт Tetrapol обмежує верхню частоту своїх систем на рівні 520 МГц. Системи стандарту iDEN працюють тільки в діапазоні 800 МГц, що обмежує їх використання для побудови певного кола систем.

Надважливо під час аналізу стандартів радіозв'язку потрібно вивчити відомості про те, чи є він відкритим або корпоративним (закритим).

Корпоративні стандарти (EDACS і Tetrapol) є власністю їх розробників. Придбання обладнання можливо тільки у обмеженого кола виробників. Відкриті стандарти, до яких належать TETRA і APCO 25, підтримують виробників базового обладнання, абонентських радіостанцій, тестової апаратури для випуску сумісних радіо засобів. Доступ до технічних вимог мереж забезпечується фірмам, які заключили договір та є членами асоціації. Абоненти, які користуються можливостями відкритих стандартів радіозв'язку, можуть вибирати більшу кількість виробників обладнання. Відкриті стандарти більш широко підтримуються державними та правоохоронними органами країн.

Це дослідження даних систем цифрового транкінгового радіозв'язку за основними критеріями дозволяє отримати певні висновки про перспективність їх впровадження як у світі, так і в Україні.

Стандарт EDACS є найменш перспективним у розвитку. Він використовує малу спектральну ефективність і недостатні функціональні особливості. Компанія Ericsson відмовилась від розвитку стандарту і тільки підтримує вже встановлене обладнання.

Стандарт iDEN має недостатньо спеціальних вимог, необхідних правоохоронним структурам, а також, побудований на використанні частотного діапазону 800 МГц. Вважаючи на надвисоку шарокосмуговість стандарту, що є його ключовою перевагою, перспективи розвитку є тільки у США та Канаді.

Стандарт Tetrapol має достатньо високі технічні показники та функціональні можливості, але, основним недоліком є його статус, як корпоративного, тобто закритого стандарту. Цей факт суттєво впливає на перспективах його поширення.

Найбільш конкурентоспроможними є стандарти TETRA і APCO 25,

адже вони мають високі технічні характеристики і дозволяють використовувати широкий спектр функціональних можливостей, включно з підтримкою спеціальних вимог правоохоронних структур, мають достатню частотно-спектральну ефективність. Ще однією вагомою перевагою стандартів TETRA і APCO 25 є наявність статусу відкритих мереж.

Але автори дослідження віддають перевагу європейському стандарту TETRA. Даний стандарт підтримує більшість великих світових виробників обладнання цифрового радіозв'язку та воно впроваджене у багатьох країнах світу.

9.4. Досвід організації використання систем цифрового радіозв'язку патрульними поліцейськими Управління патрульної поліції в Дніпропетровській області ДПП

Патрульна поліція Дніпропетровської області почала переоснащення засобів зв'язку на цифрові. Вважаючи на можливості, переваги та недоліки засобів зв'язку вибір був зроблений на користь цифрового радіозв'язку стандарту DMR. У першу чергу у такого стандарту багато переваг. Стандарт DMR має такі переваги:

– висока якість мовного сигналу, тобто цифрові радіостанції забезпечують дуже високу якість прийому та передачі мовних сигналів за допомогою цифрової обробки сигналів;

– низький рівень споживання енергії, адже цифрові радіостанції DRM споживають практично на 40 % менше енергії, ніж аналогові, це пояснюється тим, що радіостанція DMR-стандарту передають несучу частоту дискретно за допомогою таймслотів;

– можливість передавати будь-яку інформацію (мовну інформацію, текстові повідомлення, дані, географічні координати);

– можливість роботи як у цифровому так і в аналоговому режимі, це дозволяє здійснити перехід на цифрові види зв'язку поступово, не змінюючи всі абонентські радіостанції і базове устаткування одночасно;

– робота одночасно двом групам абонентів на одному частотному каналі (економія частотних ресурсів);

– багатофункціональна система диспетчерського зв'язку, адже за допомогою спеціалізованого програмного забезпечення на базову станцію можна впровадити багато можливостей цифрового радіозв'язку, а саме, це і моніторинг із передаванням GPS координат транспорту з мобільною станцією та переміщення портативних радіостанцій, це і вихід у міську телефонну мережу з будь-якої

абонентської радіостанції, це і з'єднання декількох ретрансляторів або радіостанцій в будь-якій точці земної кулі через IP-протокол, тобто вихід у мережу Інтернет, також можливий запис переговорів диспетчера і абонентських радіостанцій, і багато іншого;

– протокол DMR відкритий і багато розробників програмної підтримки постійно покращують і розширюють перелік можливостей, що надаються цифровим стандартом радіозв'язку DMR, особливо це стосується алгоритмів шифрування інформації.

Багато виробників розробили радіостанції цифрового стандарту DMR. Найбільш популярними є Hytera, Motorola, Kenwood, Entel та інші. Але діяльність поліцейських пов'язана з надважкими для техніки умовами. Тому вони повинні відповідати умовам водозахищеності, ударостійкості, надійності і простоті використання. Вироби, що відповідають таким умовам називаються радіостанціями мілітарістандарту. Найбільш наближена до військових стандартів радіостанції Motorola. Відносно недорогими, але надійними є моделі портативних радіостанцій Motorola DP1400 та мобільних Motorola DM1400.

Портативна (носима) радіостанція Motorola DP1400 має такий вигляд (рис. 9.1).

Рис. 9.1. Радіостанція Motorola DP1400

Наведемо характеристики радіостанції Motorola DP1400 [8]:

– частотний діапазон UHF: 400-470 МГц, VHF: 136-174 МГц;
– кількість каналів – 16;
– частотна відстань між каналами – 25/20 / 12.5 кГц;
– робоча напруга – 7,5 В;

термін служби батареї без підзарядки (цикл 5/5/90):

– NiMH 1400 мА × ч – аналоговий режим: близько 9 години / цифровий режим: близько 11,5 годин;
– Slim Li-Ion 1600 мА × ч – аналоговий режим: близько 10,5 годин / цифровий режим: близько 13,5 годин;
– Li-Ion 2200 мА × ч – аналоговий режим: близько 14,5 годин / цифровий режим: близько 18,5 годин;
– стабільність частоти ± 0.5 ppm;
– опір антени – 50 Ω;

вага з батареєю:

– NiMH 1400 мА × ч – 406 грам;
– Slim Li-Ion 1600 мА × ч – 341 грам;
– Li-Ion 2200 мА × ч – 346 грам;
– вихідна потужність передавача VHF High power: 5 Вт, VHF Low power: 1 Вт, UHF High power: 4 Вт, UHF Low power: 1 Вт;
– аналогова FM модуляція 11K0F3E @ 12.5KHz;
– 14K0F3E @ 20KHz;
– 16K0F3E @ 25KHz;
– 4FSK цифрова модуляція 12.5kHz дані: 7K60F1D and 7K60FXD;
– 12.5kHz голос: 7K60F1E and 7K60FXE;
– 12.5kHz дані і голос: 7K60F1W;
– кондуктивно паразитне випромінювання -36 dBm <1 GHz / -30 dBm> 1 GHz;
– межі модуляції ± 2.5KHz @ 12.5KHz;
– ± 4.0KHz @ 20KHz;
– ± 5.0KHz @ 25KHz;
– FM шум 40dB @ 12.5KHz;
– 45dB @ 20KHz;
– 45dB @ 25KHz;
– потужність суміжного каналу 60dB @ 12.5KHz;
– 70dB @ 20 / 25KHz;
– чутливість звукового каналу TIA603D;
– звукові спотворення ≤ 3 %;

– тип цифрового вокодера AMBE + 2 ™;
– цифровий протокол ETSI-TS102 361-1,2,3;

чутливість приймача :

– аналоговий режим 0.3μV (12dB SINAD);
– 0.22μV (Typical) (12dB SINAD);
– цифровий режим (BER5%) 0.25μV (12dB SINAD);
– 0.19μV (Typical) (12dB SINAD);
– селективність TIA-603 – 45 dB @ 12.5 kHz / 70 dB @ 20/25 kHz;
– блокування радіоперешкод TIA-603 – 70 dB;
– інтермодуляція TIA-603 – 70 dB;
– відношення сигнал / шум -40 dB @ 12.5 kHz / -45 dB @ 20/25 kHz;
– потужність звукового динаміка – 0,5 Вт;
– звукові спотворення ≤ 5 % (3 % typical);
– чутливість звукового каналу TIA603D;
– кондуктивно паразитне випромінювання < -57 dBm;
– діапазон робочих температур -30 ... + 60 °C;
– температура зберігання -40 ... + 85 °C;
– захищеність від пилу і вологи – IP54 стандарт;
– вологість MIL-STD-810 C / D / E / F / G стандарт;
– стандарт з удароміцності та вібрації – військовий стандарт MIL-STD-810 C / D / E / F / G.

Відсутність екрану на цих моделях радіостанцій є також перевагою їх ударостійкості та водозахищеності. Радіостанції Motorola DP1400 складають основу переносних радіостанцій патрульних поліцейських Управління патрульної поліції у Дніпропетровській області ДПП.

Для автомобілів були придбані цифрові радіостанції Motorola DM1400 (рис. 9.2):

Рис. 9.2. Цифрова радіостанція Motorola DM1400

Ця радіостанція має такі технічні характеристики [9]:

– частотний діапазон UHF: 400-470 МГц, VHF: 136-174 МГц;
– кількість каналів – 16;
– частотна відстань між каналами – 25/20 / 12.5 кГц;
– робоча напруга – 10.8-15.6 В;

струм живлення:

– режим очікування – 0.81 A max;
– режим прийому – 2 A max;
– режим передачі на малій потужності (до 25 Вт) – 11.0 A max;
– режим передачі на великої потужності (45 Вт VHF, 40 Вт UHF) – 14.5 A max;
– стабільність частоти ± 0,5 ppm;
– опір антени – 50 Ω;
– вага – 1,3 кг;
– вихідна потужність передавача VHF High power: 25-45 Вт, VHF Low power: 1-25 Вт, UHF High power: 25-40 Вт, UHF Low power: 1-25 Вт;
– аналогова FM модуляція 11K0F3E @ 12,5KHz;
– 14K0F3E @ 20 KHz;
– 16K0F3E @ 25 KHz;
– 4FSK цифрова модуляція 12,5kHz дані: 7K60F1D and 7K60FXD;
– 12,5 kHz голос: 7K60F1E and 7K60FXE;
– 12,5 kHz дані і голос: 7K60F1W;
– кондуктивно паразитне випромінювання -36 dBm <1 GHz / -30 dBm > 1 GHz;
– межі модуляції ± 2,5 KHz @ 12,5KHz;
– ± 4,0KHz @ 20KHz;
– ± 5,0KHz @ 25KHz;
– FM шум 40 dB @ 12,5KHz;
– 45dB @ 20KHz;
– 45dB @ 25KHz;
– потужність суміжного каналу 60 dB @ 12,5KHz;
– 70dB @ 20 / 25KHz;
– звукові спотворення ≤3%
– тип цифрового вокодера AMBE + 2 ™
– цифровий протокол ETSI-TS102 361-1,2,3;

чутливість приймача :

– аналоговий режим 0,3μV (12dB SINAD);
– 0,22μV (Typical) (12dB SINAD);

– цифровий режим (BER5%) 0.25μV (12dB SINAD);
– 0,19μV (Typical) (12dB SINAD);
– селективність TIA-603 – 60 dB @ 12,5 kHz / 70 dB @ 20/25 kHz;
– блокування радіоперешкод TIA-603 – 70 dB;
– інтермодуляція TIA-603 – 65dB;
– відношення сигнал / шум -40 dB @ 12.5 kHz / -45 dB @ 20/25 kHz;
– потужність звукового динаміка – 4 Вт;
– звукові спотворення ≤5% (3 % typical);
– кондуктивно паразитне випромінювання < -57dBm;
– діапазон робочих температур -30 ... + 60 ℃;
– температура зберігання -40 ... + 85 ℃;
– захищеність від пилу і вологи – IP54 стандарт;
– вологість MIL-STD-810 C / D / E / F / G стандарт;
– стандарт по ударомiцності і вібрації – військовий стандарт MIL-STD-810 C / D / E / F / G.

У якості базових ретрансляторів цифрового радіозв'язку використовуються моделі Motorola SLR5500.

Використання описаних вище засобів цифрового радіозв'язку, що працюють на стандарті DMR, дозволяє забезпечувати надійний зв'язок практично з усіма підрозділами Управління патрульної поліції в Дніпропетровській області.

Таким чином, ми розглянули вузькосмугові стандарти систем цифрового радіозв'язку як приклад використання комунікаційних технологій у діяльності підрозділів Національної поліції. Частотний діапазон, на якому вони працюють, обмежений. Однак для організації радіомереж можна застосовувати стандарт LTE, що використовується у стільникових мережах зв'язку.

Для переоснащення мереж радіозв'язку Національної поліції доцільніше використовувати стандарти DMR та TETRA. Дотепер впровадження певних систем цифрового зв'язку замість аналогових вирішується, переважно, на рівні Головних управлінь та Управлінь обласних підрозділів Національної поліції. Хоча вибирати та впроваджувати певний стандарт цифрового зв'язку необхідно на рівні, щонайменше, Міністерства внутрішніх справ.

Вважаючи, що від**повідно розпорядження Кабінет Міністрів України видав** від 23 грудня 2020 р. № 1618-р «Про затвердження плану заходів щодо впровадження єдиної багатозонової системи цифрового радіозв'язку» найближчим часом державні фахівці зроблять загальнодержавний вибір конкретного стандарту цифрового зв'язку.

Впровадження систем цифрового радіозв'язку, в першу чергу, для

потреб правоохоронних служб та збройних сил України є пріоритетною задачею в умовах воєнного протистояння з російським ворогом.

Контрольні питання

1. Охарактеризуйте радіозв'язок як різновид комунікаційної технології.
2. Які існують види організації радіозв'язку?
3. Вкажіть проблемні питання використання засобів радіозв'язку підрозділами Національної поліції на сучасному етапі.
4. Якими є можливості конвенціональної аналогово-цифрової системи DMR?
5. Перелічте основні транкінгові цифрові системи радіозв'язку.
6. Наведіть практичні приклади використання комунікаційних технологій поліцейськими. У чому полягають переваги цифрового радіозв'язку стандарту DMR?

Джерела до розділу 9

1. Про затвердження плану заходів щодо впровадження єдиної багатозонової системи цифрового радіозв'язку. Розпорядження Кабінету Міністрів України від 23 грудня 2020 р. № 1618-р.
2. Системи радіозв'язку та їх застосування оперативно-рятувальною службою / І. В. Бурляй, Б. Б. Орел, О. М. Джулай: Посібник. Чернігів: РВК «Деснянська правда», 2007. 288 с.
3. Аналіз напрямків розвитку систем радіозв'язку НАТО/ В. Думітраш, О. Бондаренко, О. Думітраш, А. Гетьман. Збірник наукових праць ВІТІ № 1 – 2020. URL : https://www.ukrmilitary.com/ 2020/08/signal.html.
4. Обладнання стандарту DMR. URL : https://ntech.com.ua/?page_id=739&lang=uk.
5. Системи професійного мобільного радіозв'язку / Д.І. Мусієнко. Сучасна спеціальна техніка. 2018 №1 (52). URL : http://elar.naiau.kiev.ua/bitstream/123456789/13663/1/№1 2018_p146-155.pdf.
6. Цифровой стандарт радиосвязи TETRA. URL : https://mkt.com.ua/tekhnologii/sistemy-radiosvyazi/tetra.
7. Транкінговий зв'язок: функціональні можливості. Транкінгові системи зв'язку. А. О. Денисов. URL : http://stunaudio.ru/uk/trankingovaya-svyaz-funkcionalnye-vozmozhnosti-trankingovye-sistemy/.
8. Motorola DP1400. Технические характеристики. URL : https://viva-telecom.org/11185/motorola/dp1400/ttx/.

9. Технические данные производителя Motorola DM1400 URL : https://viva-telecom.org/11189/motorola/dm1400/ttx/.

10. Захист інформаційних ресурсів підрозділів Національної поліції місцевого рівня: методичні рекомендації / [О. С. Гавриш, О. В. Махницький, С. О. Прокопов, Е. В. Рижков]. Дніпропетровськ: Дніпропетровський державний університет внутрішніх справ, 2018. 34 с.

11. Впровадження сучасних систем цифрового радіозв'язку у підрозділах Національної поліції: науково-практичні рекомендації / [В. О. Мирошиченко, С. О. Прокопов, Е. В. Рижков]. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2021. 29 с.

12. Рижков Е. В. Джерела формування актуальних компетенцій з питань спеціальної техніки у майбутніх працівників кримінальної поліції / Е. В. Рижков // Правові та організаційно-тактичні засади оперативно-розшукової діяльності Національної поліції України: матеріали III Всеукраїнської науково-практичної інтернет-конференції (м. Одеса, 07 жовтня 2022 р.). Одеса: ОДУВС, 2022. С. 186-188.

13. Спеціальна техніка в правоохоронній діяльності: навч. посібник / Ю. П. Синиціна, С. О. Прокопов Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2022. 244 с.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ДО ВСІХ ТЕМ

Основні нормативні акти:

– Конституція України від 28.06.1996 за №254к/96-ВР;

– закони:

1. Закон України «Про Національну поліцію» (ВВР), 2015, № 40-41, Ст. 379.
2. Закон України «Про інформацію» від 02.10.1992 за № 2657-XII.
3. Закон України «Про доступ до публічної інформації» від 13.01.2011 за № 2939-VI.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 за № 2594-IV.
5. Закон України «Про захист персональних даних» від 01.06.2010 за № 2297-VI.
6. Закон України «Про засади запобігання і протидії корупції» від 07.04.2011 за № 3206-VI.
7. Закон України «Про захист інформації в автоматизованих системах» від 5.07.1994 за № 80/94-ВР.

– *підзаконні акти:*

1. Постанова Кабінету Міністрів України «Про затвердження Положення про єдину інформаційну систему МВС та переліку її пріоритетних інформаційних ресурсів» від 14.11.2018 за № 1024.
2. Наказ МВС України «Про затвердження положення про ІТС Інформаційний портал Національної поліції України» від 03.08.2017 за № 595.
3. Наказ МВС від 14.06.2019 № 508 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».
4. Наказ НПУ від 12.02.19 №141 « Про організацію використання систем відеоспостереження органами (підрозділами) поліції» є Доручення НПУ від 29.07.2017 № 7407/07/20-2017 «Про затвердження Методичних рекомендацій щодо порядку формування інформаційної підсистеми «Масові заходи» ІПНП України».
5. Наказ НПУ від 28.12.2018 № 1227 «Про деякі питання щодо введення окремих обліків в ІТС «Інформаційний портал НПУ».
6. Наказ НПУ від 22.05.2018 № 509 «Про організацію інформаційного обліку комп’ютерної техніки та комп’ютерних

програм, що використовуються в органах та підрозділах поліції».

7. СТ НПУ від 28.12.2019 № 15392/20/27-2019 «Про надання доступу до інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції» .

Підручники:

1. Інформаційні системи та технології : підруч. / В. Б. Вишня, Є. В. Рижков, В. О. Мирошниченко, Ю. П. Синиціна, О. Д. Станіна. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 280 с.
2. Інформаційне забезпечення юридичної діяльності: підруч. /кол. авт. ; за заг. ред. д.т.н., проф. В. Б. Вишні. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 228 с.

Навчальні посібники, інші дидактичні та методичні матеріали:

1. Вишня В. Б. Основи інформаційної безпеки : навч. посіб. / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : ДДУВС, 2020. 128 с.
2. Спеціальна техніка в правоохоронній діяльності : навч. посібник / Ю. П. Синиціна, С. О. Прокопов, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 244 с.; іл. ISBN 978-617-8032-47-0
3. Косиченко О. О. Правові інформаційні ресурси Інтернет: довідник. Дніпро: ДДУВС, 2017. 64 с., іл.
4. Косиченко О. О., Махницький О. В. Інформаційне забезпечення юридичної діяльності: навчальний посібник. Дніпро: Дніпропетровський державний внутрішніх справ, 2018. 245 с.

Монографії та інші наукові видання:

1. Впровадження сучасних систем цифрового радіозв’язку у підрозділах Національної поліції : наук.-практ. рекоменд. / В. О. Мирошниченко, С. О. Прокопов, Е. В. Рижков, Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 29 с.
2. Захист інформаційних ресурсів підрозділів Національної поліції місцевого рівня: методичні рекомендації / О. С. Гавриш, О. В. Махницький, С. О. Прокопов, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2018. 34 с.
3. Синиціна Ю. П., Станіна О. Д. Обґрунтування актуальності цифрової комунікація закладів вищої освіти (Rationale for the relevance of digital communication in higher education institutions) Міжн. колект.моногр. / Selected aspects of digital society development «Digital Economyand Digital Society» III Міжнародна конференція (28-29 травня

2021 p.). Katowice, University of Technology, Poland, 2021.mon # 45 – 148-156 c ISBN 978 – 83 – 960717 – 1 – 2.

4. Синиціна Ю. П., Рижков Е. В., Станіна О. Д. Штучний інтелект: що змінилося за 50 років. Theoretical foundations of engineering. Tasks and problems: collective monograph / Boiko T., Boiko P., – etc. – International Science Group. Boston : Primedia eLaunch, 2021. 485 p. Available at : DOI- 10.46299/ISG.2021.MONO.44TECH.III URL : https://isg-konf.com/ru/theoretical-foundations-of-engineering-tasks-and-problems-ru/.

5. Синиціна Ю. П., Бекишев А. Методологічні аспекти цифрової комунікації закладів вищої освіти. *Науковий вісник*, м. Дніпро, 2021, № 3, С. 340-348; ISSN – 2078-3566; «Index Copernicus International» «CrossRef», DOI: 10.31733/2078-3566-2021-3-340-348. URL : https://visnik.dduvs.in.ua/wp-content/uploads/2021/12/21_3_ua/PDF/NV-3-2021-340-348.pdf.

Інші джерела:

1. Синиціна Ю. П., Причина В. Р. Оцінка системи управління інформаційної безпеки методом таксономії Nauka i edukacja w warunkach zmian cywilizacyjnych: Mater. II Międz. Konf. Nauk.-Prakt. / Pod red. Stanisława Kowalczyka Łódź : Nowa nauka, 2020, p. 76 – 78 ISBN 978-83-7364-968-2.

2. Синиціна Ю. П. APT-атак – пріоритетний напрямок розвитку кібербезпеки Інформаційні технології в освіті та практиці : матеріали Всеукр. наук.-практ. конф. 19.12.2020 р., м. Львів : ЛьвДУВС, 2020. С. 66-68.

3. Синиціна Ю. П. Сучасні підходи до безпеки операційних систем Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11.2020 р., м. Дніпро:ДДУВС, 2020. С. 66-68.

4. Синиціна Ю. П., Дудуник В. В. Актуальні питання взаємозв'язку інформаційної та національної безпеки України Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро:ДДУВС, 2020. С. 164-167.

5. Синиціна Ю. П., Кліменко А. О. Актуальні питання інформаційної безпеки в діяльності Національної поліції України Сучасні інформаційні технології в діяльності національної поліції України: Всеукр. наук.-практ.семін. 26.11. 2020 р., м. Дніпро:ДДУВС, 2020. С. 174-176

6. Синиціна Ю. П. Автоматизовані інформаційні системи в правоохоронній діяльності Економічна та інформаційна безпека: актуальні питання та інновації: Всеукр. наук.-практ. конф. (м. Дніпро, 04 листопада 2021 р.,). Дніпро: ДДУВС, 2021. С. 220-222.

7. Синиціна Ю. П. Державного управління забезпечення національної безпеки: інформаційна безпека Міжнародна та національна безпека: теоретичні і прикладні аспекти: VI Міжн. наук.-практ. конф. м. Дніпро, (11 березня 2022р.,). Дніпро: ДДУВС, 2022. С. 263-266

8. Синиціна Ю. П. Інформаційна безпека у системі права національної безпеки України Управління проєктами. Перспективи розвитку проєктного та нейроменеджменту, інформаційних технологій управління, технологій створення та використання об'єктів права інтелектуальної власності: зб. наук.праць за матеріал. IV Міжн. наук.-практ. інтер.-конф. (24-25 березня 2022 р.). УДУНТ, УКРНЕТ, НДІІВ НАПрН України, Дніпро: Юрсервіс, 2022. С. 165 – 168.

Інтернет-ресурси:

1. Вся Україна – жителі http://www.nomer.org/allukraina.

2. База даних Ошибка! Недопустимый объект гиперссылки.Законодавство України» http://zakon.rada.gov.ua.

3. Портал МВС. URL : https://mvs.gov.ua/.

4. Реєстр організаторів державної експертизи у сфері технічного захисту інформації. URL : http://dstszi.kmu.gov.ua/dstszi/control /uk/publish/article...

5. Перелік сертифікованих засобів криптографічного захисту інформації. URL : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/ article…

6. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації. URL : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/ article…

7. Перелік суб'єктів господарювання, які мають ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), торгівлі криптосистемами і засобами криптографічного захисту інформації. URL : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article…

8. Перелік суб'єктів господарювання, які мають ліцензії на провадження господарської діяльності з надання послуг в галузі технічного захисту інформації. URL : http://dstszi.kmu.gov.ua/dstszi/ control/uk/ publish/article.

Д О Д А Т К И

Додаток А

П Р О Т О К О Л
огляду

Київ **13.10.2022**

Огляд розпочато о 15:15
Огляд закінчено о 18:22

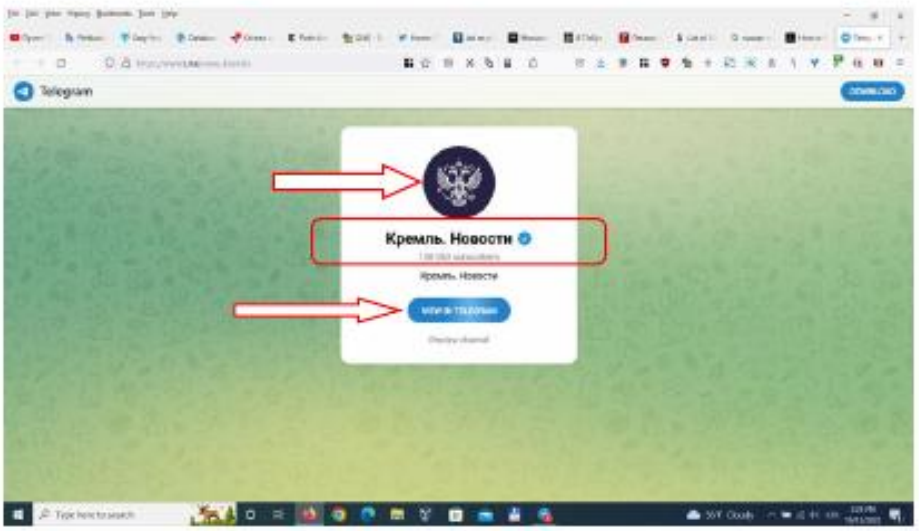
Старший слідчий І відділу Департаменту спеціальних розслідування військових злочинів Державного Бюро Розслідувань П.І.Б. слідчого, здійснюючи досудове розслідування кримінального провадження, зареєстрованого у ЄРДР за номером 31909000001456789 від 24.02.2022 за ч. 2 ст. 437, ч. 2 ст. 437, 440 КК України, в службовому кабінеті № 2102 приміщення Державного Бюро Розслідувань (01032, 15 Симона Петлюри, буд. 15), при змішаному освітленні, дотримуючись вимог ст.ст. 104-106, 237 КПК України, провів огляд віртуального простору без спеціальних умов (наприклад, без необхідності надавати дані доступу до закритого облікового запису) використовуючи операційні можливості додатку «Телеграм», а саме спеціального відкритого публічного профайлу, зареєстрованого за користувачем: **"KREML.NOVOSTI", ID: t.me/news_kremlin, located URL: https://www. t.me/news_kremlin**

Огляд проведено на персональному службовому компютері:
Device name: DESKTOP-7ABMTT1, Processor: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz, Installed RAM: 16.0 GB (15.9 GB usable), Device ID: 5D646F90-EF6C-4345-83D5-1394429B74C7, Product ID: 00329-10330-00000-AA552, System type: 64-bit operating system, x64-based processor
Windows specifications: Edition: Windows 10 Enterprise, Version: 20H2, OS build: 19042.2130

За результатами огляду встановлено:

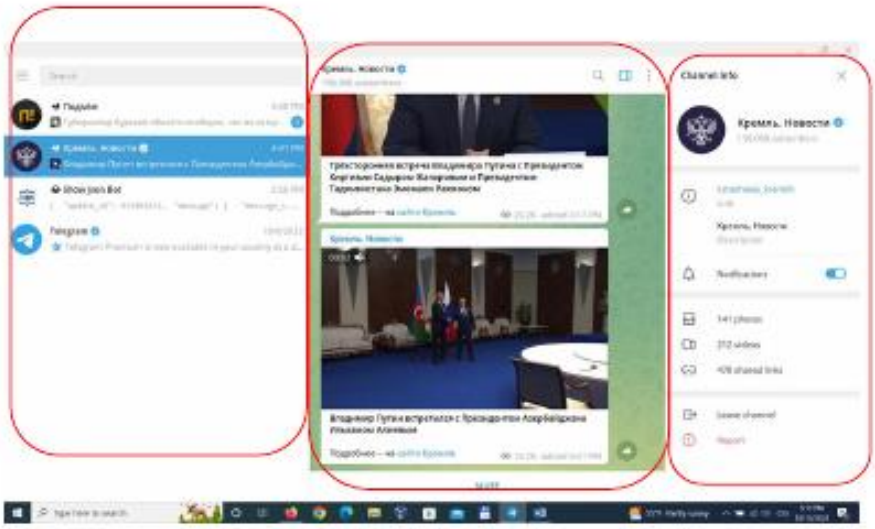
Після того як ми відкриваємо посилання за адресою URL: https://www.t.me/news_kremlin, ви маєте можливість отримати інформацію про телеграм-канал. Посередині екрана ви знайдете біле поле з назвою каналу KREML.NOVOSTI і відображення голограми синього кольору за якою можна встановити верифікувати телеграм канал. На цьому ж каналі також можна подивитися кількість підписників [158063] на дату проведення огляду. В подальшому натискаємо на ідентифікатор синьої кнопки на позначку – «Переглянути у Телеграм». Натискаємо на ліку кнопку мишкою що надасть можливість переглянути повну інформацію за профілем «Телеграм Робочий додаток».

Знімок № 1 – Опис сторінки Головного каналу користувача за профілем "Kreml. Novosti"



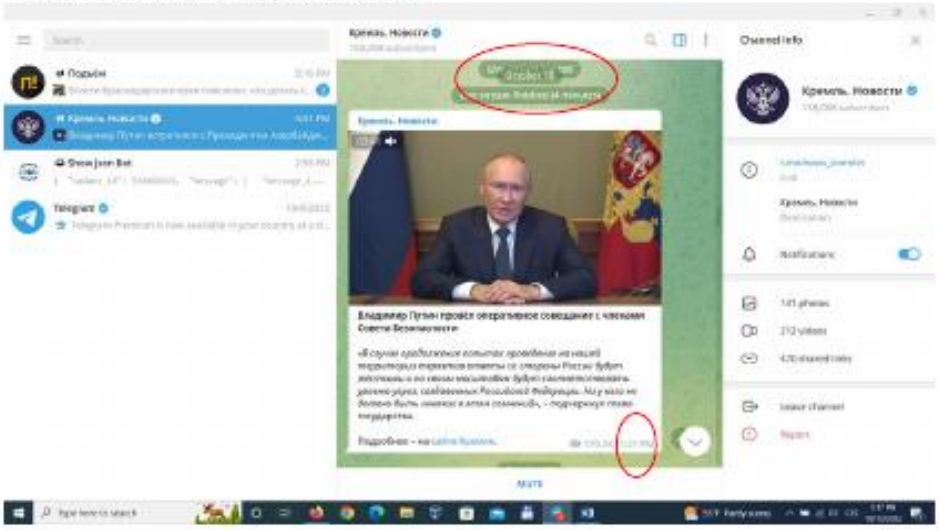
Шляхом натискання лівою кнопкою на «Перегля Телеграму» маємо повну інформацію що дозволить ідентифікувати канал. На наступному зображенні ми можемо переглянути відомості каналу «Телеграм» розділені на три секції. В лівій секції Ви маєте можливість отримати інформацію про поточні оперативні контакти цього профіля, в середньому – це стіна зі всіма повідомленнями абонента (заяви, відео, фото). Відкриваючи канал в додатку надасть Вам можливість переглянути інформацію щодо останніх повідомлень абонента. В правій частині екрану – Ви можете ознайомитись з відомостями щодо каналу, а саме: Фото профілю, URL адреси, кількість фото, відео матеріалів, поширень). В ході проведення огляду останнє повідомлення, відображено на каналі – Зустріч Президента РФ з Президентом Республіки Азербайджан від 13 жовтня, 16:41.

Знімок № 2 – Опис сторінки Головного каналу користувача за профілем "Kreml. Novosti"



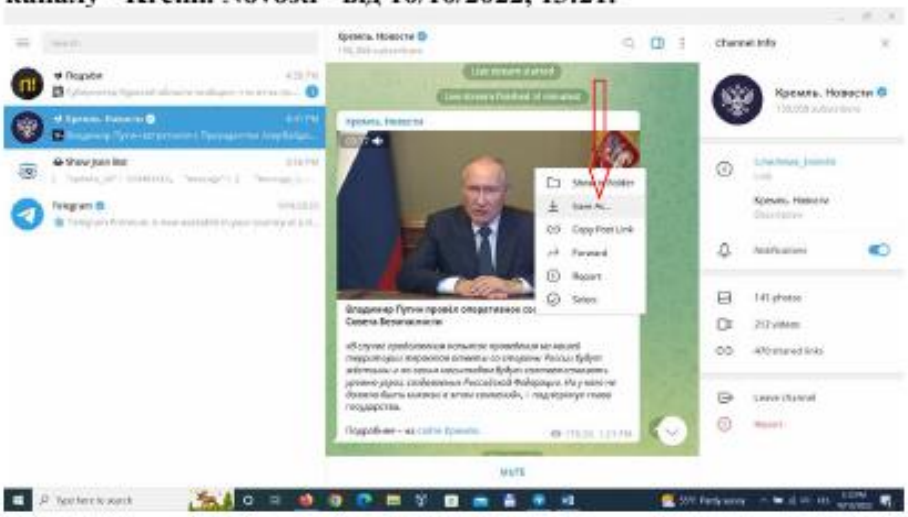
Перемотуючи стіну каналу ми можемо знайти відомості щодо попередніх даних, відображених на даному каналі. Для, прикладу ми знайшли повідомлення про живу трансляцію промови путіна щодо оголошення масових атака України як поста за атаку на Кримський міст.

Знімок № 3 – Опис сторінки Головного каналу користувача за профілем "Kreml. Novosti" від 10/10/2022

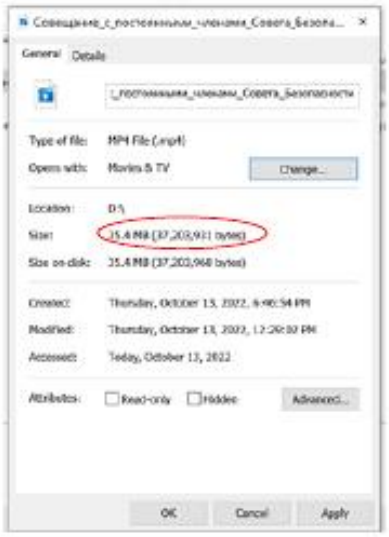


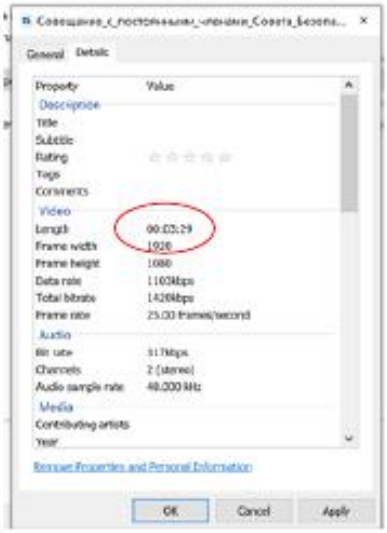
Натискаючи правою кнопкою мишки на відео ми маємо можливість загрузити відео.

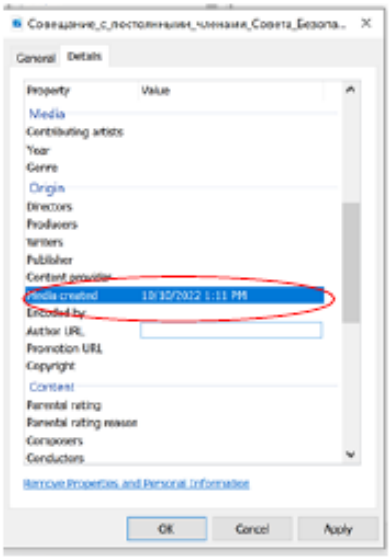
Знімок № 4. – Демонструє можливості зашруження змісту Телеграм каналу "Kreml. Novosti" від 10/10/2022, 13:21.

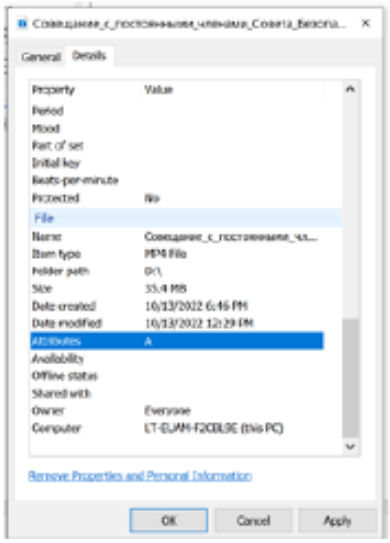


Шляхом натискання лівої кнопки мишки ми здійснюємо збереження файлу за назвою: "Совещание_с_постоянными_членами_Совета_Безопасности.mp4". Розміри відео 36.362 Kb – Деталі наведенні в подальшому:


General
Details
Type of file:
Opens with:
Change...
Location:
Size:
Size on disk:
Created:
Modified:
Accessed:
Attributes:
Read-only
Hidden
Advanced...
OK
Cancel
Apply


General
Details
Property
Value
Description
Title
Subtitle
Rating
Tags
Comments
Video
Length
00:03:29
Frame width
1920
Frame height
1080
Data rate
1103kbps
Total bitrate
1420kbps
Frame rate
25.00 frames/second
Audio
Bit rate
317kbps
Channels
2 (stereo)
Audio sample rate
48,000 Hz
Media
Contributing artists
Year
Remove Properties and Personal Information
OK
Cancel
Apply


General
Details
Property
Value
Media
Origin
Content
Remove Properties and Personal Information
OK
Cancel
Apply


General
Details
Property
Value
File
Remove Properties and Personal Information
OK
Cancel
Apply

Довжина відео 03:29 хвилини. Виходячи з даних вказаних вище створено 10.10.2022 о 13:11.

Загружено відео так само як і знімки екранів ідентифікується за адресою:
Совещание_с_постоянными_членами_Совета_Безоп асности.md5 file with the result "cfe62187d3f333a85afd6329d4bd7d19 *Совещание_с_постоянными_членами_Совета_Безопасности.mp4", the Telegram screenshots.md5 file with the result "4584c4cab8a7c96a9ebb21c2f4a67513 *Telegram screenshots.docx" and video properties.md5 file with the result "acfa27a5290a2f3f47cfd1eb4bc0ef5b *video properties.docx"

Для перевірки автентичності використано можливості Total Commander x64 10.51.

Будь-які зміни, внесені до змісту цих файлів будуть змінювати типовий ідентифікаційний номер первинного, вказаного вище файлу.

Зібрані відеоматеріали від копійовано на носії інформації, опечатано та приєднано до матеріалів кримінального провадження.

Старший слідчий І відділу
Департаменту спеціальних розслідування
військових злочинів
Державного Бюро Розслідувань **І. Прізвище**

Додаток Б

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Поняття системи «Google».
2. Найбільш популярні сервіси Google.
3. Адреса українського серверу Google.
4. Поняття акаунта Google.
5. Збереження документа на Google Disk.
6. Надання спільного доступу до документу.
7. Настроювання стилів в Google Документах.
8. Історія змін в Google Docs.
9. Створення найпростішого документа в он-лайн сервісі Google Docs.
10. Найпростіші прийоми форматування символів і фрагментів тексту у Google Docs.
11. Основні прийоми роботи з копіюванням і вставкою текстових об’єктів, одночасна обробка декількох документів у Google Docs.
12. Настроювання параметрів документа у Google Docs.
13. Введення спеціальних символів у Google Docs.
14. Книга Google sheets, аркуші книги, клітинки та їх адресація.
15. Введення даних у Google sheets.
16. Прості обчислення у Google sheets.
17. Поняття комп’ютерної мережі.
18. Класифікація комп’ютерних мереж.
19. Локальні комп’ютерні мережі.
20. Глобальні комп’ютерні мережі.
21. Глобальна комп’ютерна мережа Internet.
22. Структура Internet.
23. Основні принципи побудови і роботи Internet.
24. Поняття про основні протоколи Internet.
25. Протоколи TCP/IP.
26. Адресація комп’ютерів у Internet.
27. Здійснення доступу до глобальної мережі Internet.
28. Основні служби Internet.
29. Електронна пошта в Internet. Види електронної пошти в Internet.
30. Перевага і недоліки використання електронної пошти.
31. Налаштування особистої поштової скриньки.
32. Служба WWW. Протоколи цієї служби.
33. Поняття мови гіпертекстової розмітки.
34. Поняття Web-сторінки.
35. Поняття гіперпосилання.

36. Створення гіперпосилання.
37. Об’єкти, що можуть знаходитися на Web-сторінці.
38. Пошук інформації в Інтернеті.
39. Основні види інформаційних ресурсів у Internet.
40. Пошукові системи в Internet. Основні типи пошукових систем.
41. Принципи складання запитів у пошукових системах.
42. Структура юридичних ресурсів у Internet-просторі України.
43. Поняття бази даних. База даних як основна складова інформаційної системи. Поняття предметної області.
44. Використання списку MS Excel як бази даних. Створення списку.
45. Основні операції зі списком MS Excel. Пошук. Сортування. Фільтри.
46. Поняття інформаційної системи.
47. Використання інформаційних систем в юридичної діяльності.
48. Робота з таблицями. Сортування.
49. Робота з таблицями. Пошук.
50. Робота з таблицями. Фільтрація.
51. Редагування таблиць. Основні операції.
52. Адресація клітинок у формулах (відносна, абсолютна, змішана) та її зміна.
53. Копіювання таблиць. Уведення даних у таблиці.
54. Порядок обчислення функції ЯКЩО.
55. Обробка списків за допомогою форми.
56. Поняття шаблону MS Word.
57. Створення шаблонів із полями форм для юридичних документів у MS Word.
58. Поняття макросу.
59. Створення макросів у MS Word.
60. Поняття розширеного фільтру.
61. Логічні операції за умови використання розширеного фільтру.
62. Послідовність створення розширеного фільтру (список, діапазон розташування критеріїв відбору та інше).
63. Поняття проміжних підсумків різних видів.
64. Створювання та використання форми для корекції інформації у списку.
65. Створювання автоматичних фільтрів за різними умовами відбору.
66. Сортування списків за одним полем, за двома чи трьома полями в одному напрямку.
67. Сортування списків за одним полем, за двома чи трьома полями у різних напрямках.
68. Створення конкретного юридичного документа на основі захищеного шаблона з полями.
69. Створення макросу за допомогою засобу запису.

70. Збереження макросів.
71. Видалення макросів.
72. Змінювання макросів.
73. Створення кнопок у меню для виконання макросів.
74. Робота зі списками.
75. Нумеровані списки.
76. Маркіровані списки.
77. Багаторівневі списки.
78. Робота з колонками тексту.
79. Настроювання параметрів абзацу.
80. Відступи та інтервали.
81. Статистика.
82. Перевірка правопису.
83. Автозаміна.
84. Номер сторінки, колонтитули, виноски, зміст.

Додаток В

РЕКОМЕНДАЦІЇ
щодо протидії кіберзагрозам на робочих місцях

І. Правила створення та використання надійних паролів

У процесі створення облікового запису в соціальних мережах, реєстрації в інтернет-магазинах або додатках у смартфонах, необхідно вказувати пароль – так працює будь-яка система авторизації. Конфіденційність приватних даних захищена ненадійно, якщо пароль є нестійким до зламу. Безліч людей нехтують власною безпекою та встановлюють прості паролі, які хакери без зусиль можуть зламати менше ніж за секунду. Для прикладу, у рейтинг найуживаніших паролів, який щорічно складає компанія Nord Security, постійно потрапляють такі комбінації як 123456, qwerty, password, фрази на кшталт iloveyou або власні імена (перевірити, чи немає у переліку вашого пароля, можна тут: https://nordpass.com/most-common-passwords-list/).

Надійний пароль – один з основних способів захисту для будь-якого облікового запису. Тому найважливіше правило, якого слід дотримуватися: що він складніший, то краще.

Під надійними паролями слід розуміти такі, що:

– складаються з не менше 8 символів;

– включають літери (у верхньому і нижньому регістрі), цифри та спеціальні символи;

– не містять персональної інформації (наприклад: дати народження своєї та своїх близьких, номерів телефонів, номерів та серій документів, що посвідчують особу, номерів власного автотранспорту, банківської картки, адреси реєстрації), а також фраз зі щоденного вжитку (назв книг, відомих цитат, текстів пісень);

– не використовуються в будь-яких інших облікових записах та потребують негайної зміни у разі підозри щодо їх компрометації.

Для захисту облікових записів ефективно використовувати парольні фрази. (набір слів, зашифрованих користувачем). Наприклад, оберіть будь-яку фразу – рядок із вірша, пісні, книжки тощо. Видаліть пробіли та замініть деякі літери цифрами, спецсимволами, переведіть певні букви у верхній регістр.

Для створення складних паролів також можна використовувати сервіси генерації паролів, наприклад:

– https://www.cyberpolice.gov.ua/generate-password/,
– https://www.eset.com/ua/home/generator-paroley/,
– https://www.avast.ua/random-password-generator#pc,
– https://identitysafe.norton.com/password-generator

– програма Password Tech Portable (колишня назва PWGen) або інші програми і способи.

Зауважимо, що створені за допомогою генераторів паролі важко запам'ятати, тож для їх зберігання радимо користуватися менеджерами паролів.

Перевірити паролі та поштові адреси на предмет витоку можна на сайті https://haveibeenpwned.com.

Перевірити наскільки надійний пароль ви використовуєте допоможуть:

– https://zillya.ua/check-password;
– https://howsecureismypassword.net;
– інструмент Password Checkup на сторінці https://passwords.google.com/ може перевірити надійність паролів, які були збережені в обліковому записі Google, а також вкаже, чи не були вони зламані, чи не використовуєте ви однакових паролів на різних сервісах. Підкреслимо, що безпечніше – не зберігати паролів у браузері взагалі.

Не використовуйте для перевірки сервісів, які мають походження з іноземної держави, до якої застосовано санкції згідно із Законом України» Про санкції», чи розроблені / виготовлені юридичною особою – резидентом такої іноземної держави або юридичною особою, частка статутного капіталу якої перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави.

Не варто зберігати пароль у відкритому вигляді біля комп'ютера та надсилати його у месенджерах. На випадок якщо пароль хтось вгадає або викраде, додатковий рівень безпеки для ваших облікових записів – це двофакторна автентифікація.

ІІ. Двофакторна автентифікація – один із найдієвіших способів захисту облікових записів: електронної пошти, месенджерів, облікових записів у соціальних мережах та інших.

Під час входу до своїх облікових записів більшість людей використовують лише один спосіб підтвердження особи. Зазвичай це – введення логіна і пароля. Проте це недостатньо надійно, особливо якщо як пароль ви використовуєте просте слово чи комбінацію, що легко зламати хакерам. Двофакторна автентифікація – це використання одразу двох різних способів підтвердження. Вона дає можливість значно підсилити рівень вашого захисту та убезпечити персональні дані від кіберзловмисників. Якщо хтось намагатиметься увійти до вашого облікового запису з незнайомого пристрою – наштовхнеться на додаткову перепону, а ви отримаєте сповіщення про таку спробу входу.

Додатковим фактором для перевірки може бути підтвердження:

– через код, надісланий у смс;
– через дзвінок на мобільний;
– через лист на e-mail;

– через надсилання сповіщення – така можливість, наприклад, є для облікових записів Google;

– через код, згенерований за допомогою спеціальних мобільних додатків (наприклад, Google Authenticator, Microsoft Authentificator чи інші) тощо.

Як встановити двофакторну автентифікацію:

1. Увійдіть у потрібний обліковий запис (наприклад, Facebook, Telegram, Google чи інший).
2. Зайдіть у розділ меню Налаштування, а потім Безпека.
3. Оберіть пункт із налаштуваннями двофакторної автентифікації, якщо така функція є (зверніть увагу, може називатися також – двоетапна перевірка).
4. Виконайте всі необхідні дії за запропонованою інструкцією.

Використовуйте двофакторну автентифікацію всюди, де це можливо.

III. Щодо користування електронною поштою (службовою і приватною):

1. Не використовуйте приватну електронну пошту для цілей службової діяльності та службову електронну пошту в приватних цілях.
2. Не використовуйте в браузерах можливість запам’ятовувати паролі.
3. Не використовуйте паролі, що були встановлені «за замовчуванням».
4. Використовуйте виключно надійні (стійкі) паролі.
5. Перевіряйте всі файли, отримані електронною поштою, на предмет відсутності вірусів та шкідливого програмного забезпечення.
6. Не відкривайте вкладень у підозрілих повідомленнях, листах від адресатів, щодо авторства яких виникають сумніви (наприклад: автор із невідомих причин змінив мову спілкування; тема листа є нетиповою для автора; спосіб, у який автор звертається до адресата, є нетиповим) у повідомленнях із нестандартним текстом, що спонукають до переходу на підозрілі посилання або до відкриття підозрілих файлів – архівів, виконуваних файлів і вкладень із виконуваними файлами, що мають, зокрема, розширення «.exe», «.bat», «.cmd», «.vbs», «.docm», «.xlsm».
7. Не використовуйте точки публічного доступу до Інтернету для входу до службової електронної пошти.
8. Створюйте повністю окремі облікові записи електронної пошти для різних цілей: один обліковий запис електронної пошти для підписки на інформаційні бюлетені та покупки, ще один для онлайн-облікових записів, як-от Facebook, Uber, і т.п.

IV. Щодо користування особистими пристроями (знімними/зовнішніми носіями інформації, комп’ютерами, планшетами, ноутбуками, смартфонами):

1. Установіть для розблокування пристроїв біометричний захист (відбиток пальця, сканування обличчя) або паролі, якщо немає біометричного

захисту, на всі пристрої, що перебувають в особистому користуванні (PIN-коди, паролі на вхід до всіх облікових записів) та блокуйте пристрої щоразу після закінчення роботи з ними. Ніколи не залишайте свій ноутбук / смартфон / планшет розблокованими, поки вас немає поруч.

2. Налаштуйте на усіх Wi-Fi-пристроях використання технології WPA3 (Щоб мережа Wi-Fi була захищена протоколом WPA3, він повинен підтримуватися як клієнтом, так і роутером. У іншому випадку рекомендуємо вибрати в налаштуваннях роутера режим безпеки WPA2-PSK) та періодично змінюйте паролі доступу.

Намагайтесь уникати відкритих Wi-Fi-мереж, а якщо використовуєте, вмикайте безпечний VPN. Рекомендовані: ExpressVPN, Surfshark, PrivateInternetAccess, CyberGhostVPN, NordVPN, ProtonVPN, ClearVPN.

3. Із метою унеможливлення завантаження на особистий пристрій програм-шпигунів та іншого шкідливого програмного забезпечення слід дотримуватися таких правил:

1) установлювати додатки лише з офіційних та перевірених сервісів (Chrome Store, Add-ons та Play Market для Android, App Store для IOS) або сайтів розробників. Їх працівники перевіряють на надійність усі програми перед їх розміщенням. Однак, зловмисники кожного дня намагаються розмістити програми, що зовні можуть виглядати цілком безпечними та корисними, приховуючи свою основну мету (на кшталт отримання доступу до персональних даних або інфікування пристрою). Якщо ви вважаєте, що у додатка немає необхідності, наприклад, у доступі до мікрофону або GPS даних – не надавайте згоду на такі дії.

2) перевіряти, які доступи отримують застосунки.

Усі додатки, завантажені на смартфон, під час їх налаштування запитують у користувача згоду на використання даних пристрою. Процедура надання дозволу на використання даних користувача мобільного додатку є обов’язковою для більшості програм. Водночас, надаючи подібний дозвіл користувач не завжди знає до яких саме особистих даних він надав доступ представникам цього додатку, оскільки зазвичай інформація подається іноземною мовою та має великий обсяг інформації. Часто, користувачі перегортають до кінця ліцензійну угоду та погоджуються з умовами не вчитуючись в текст, тим самим ігноруючи зміст.

Зокрема, у ліцензійній угоді зазначаються умови щодо використання розробниками або третіми особами будь-яких користувацьких даних. У таких випадках, вже не маючи необхідності запитувати дозвіл, треті особи отримують доступ до даних, дозвіл на використання яких користувач надав самостійно (це можуть бути контакти, фотографії, інформація розміщена в соціальних мережах, вподобання, геолокація тощо).

Останнім часом набувають популярності додатки, що наразі збирають інформацію про інші встановлені сервіси. Також збираються дані про сам пристрій та сайти, які відвідав користувач (хоча ці дії та інформація не є

необхідними для їх функціоналу). У подальшому ця інформація може бути використана сторонніми особами на власний розсуд і навіть передаватися третім особам.

Перед встановленням додатків звертайте увагу на дозволи доступу, які будуть надаватися розробникам або власникам цього додатку.

Що менше доступів мають застосунки, то безпечніше. Проте це впливає на зручність користування. Оберіть оптимальний для себе рівень безпеки.

Android: Налаштування смартфону → Програма, яку перевіряєте → Дозволи застосунку. У цьому ж розділі можна налаштувати функцію автоматичного відкликання дозволів, якщо застосунок не використовується протягом тривалого часу.

iOS: Налаштування → Параметри → Приватність. Варіанти налаштувань:

– завжди дозволяти (застосунок має доступ до даних, навіть якщо ви його не використовуєте);

– дозволяти, лише коли застосунок використовується;

– запитувати щоразу (застосунок питатиме про доступ до налаштувань щоразу, коли ви його відкриваєте);

– не дозволяти.

3) не використовувати зламаних версій платних застосунків. Через них часто поширюється шкідливе програмне забезпечення;

4) налаштувати пристрої таким чином, щоб унеможливити автоматичне встановлення (оновлення) додатків із невідомих джерел;

5) періодично видаляти з особистих пристроїв додатки (програми), які не використовуються;

6) видаліть та не використовуйте програм та сервісів, які мають походження з іноземної держави, до якої застосовано санкції згідно із Законом України «Про санкції», чи розроблені / виготовлені юридичною особою – резидентом такої іноземної держави чи юридичною особою, частка статутного капіталу якої перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави.

7) видаляти старі плагіни та розширення веб-браузера та переконатися, що ті, які використовуються, оновлені;

8) не підключати технічних засобів із модулями передачі даних – Bluetooth, GSM тощо.

9) встановити налаштування для месенджерів.

Telegram:

Налаштування → Приватність і безпека:

Номер телефону – Ніхто

Хто може знайти за номером – Мої контакти

Відвідини та стан у мережі – Ніхто

Фото та відео профілю – Мої контакти

Пересилання повідомлень – Мої контакти

Хто може мені телефонувати – Мої контакти або Ніхто

Виклики → Peer-to-peer – Мої контакти

Групи й канали – Мої контакти

Двоетапна перевірка – Встановити пароль

WhatsApp:

Налаштування → Обліковий запис → Конфіденційність:

Востаннє в мережі – Ніхто

Фото профілю – Мої контакти

Групи – Мої контакти

Налаштування – Обліковий запис – Двоетапна перевірка – Увімкнути

Viber:

Оберіть меню «Додатково» і налаштуйте там такі пункти:

Параметри – Виклики і повідомлення – встановіть тумблер навпроти «Блокування невідомих абонентів».

Параметри – Загальні – Використовувати проксі-сервер.

Вкладку «Конфіденційність» налаштуйте таким чином:

– встановіть тумблер навпроти «Автоматична перевірка на спам»;
– зніміть тумблер навпроти «Одноранговий зв’язок»;
– встановіть тумблер навпроти «Запити».

Контролюйте, хто може додавати вас у групи – перейдіть в «Настройка додавання в групи» і поставте галочку навпроти «Мої контакти».

– зніміть тумблер навпроти «Пропонувати друзів»;
– Особисті дані – зніміть тумблери навпроти «Збирати аналітику», «Дозволити персоналізацію контенту» та «Дозволити служби точної геолокації».

Зверніть увагу на функції «Запит ваших даних» і «Видалити ваші дані» та перегляньте, які саме дані про вас зберігаються на серверах Viber.

Signal:

У меню «Налаштування» відредагуйте такі пункти:

Приватність – Зникаючі повідомлення – виберіть безпечний для вас період, упродовж якого в чаті зберігатимуться відправлені повідомлення (пропонуються опції від 30 секунд до 4 тижнів, також можна встановити власний таймер).

Приватність – Безпека програми – встановіть тумблер навпроти «Блокування екрану».

Приватність – Безпека програми – встановіть тумблер навпроти «Клавіатура в режимі інкогніто».

4. Постійно здійснюйте оновлення операційних систем та іншого програмного забезпечення. Установлюйте оновлення для операційної системи смартфону або застосунків одразу після отримання повідомлення

про їх випуск. Це забезпечує підвищення рівня безпеки та усуває виявлені недоліки системи. Рекомендації щодо оновлень регулярно публікує Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA https://www.facebook.com/UACERT.

Припинення підтримки програмного забезпечення означає, що виробник програмного забезпечення більше не створюватиме та впроваджуватиме оновлення безпеки, продуктивності чи функцій для цієї програми. Як наслідок, ті, хто продовжує використовувати непідтримуване програмне забезпечення, піддають свою систему величезній кількості вразливостей. Із огляду на те, що виробник програмного забезпечення більше не надає оновлення системи безпеки, ці вразливості залишаться невиправленими, і кіберзлочинці зможуть використовувати їх скільки завгодно. Тому ніколи не використовуйте непідтримуване програмне забезпечення та стежте за тим, щоб всі програми були в актуальному стані.

5. Використовуйте антивірусне програмне забезпечення, регулярно перевіряйте пристрій на наявність загроз.

Рекомендовані антивіруси: Avast, ESET, McAfee, Zillya.

Уважно віднесіться до попереджень антивірусного програмного забезпечення. У разі отримання тривоги від системи захисту комп'ютера (антивіруса, фаєрволу тощо) не перешкоджайте діям за замовчуванням антивірусу (блокування, видалення, карантин, тощо). Чітко усвідомте, що спростувати небезпечність про яку повідомив антивірус, може лише кваліфікований спеціаліст з інформаційної безпеки.

Систематично оновлюйте антивірусні бази. У них міститься інформація щодо нових загроз, небезпечних файлів і шкідливих кодів. Це правило особливо важливе для безкоштовних версій антивірусів.

Завантажуйте антивірус винятково з офіційних сайтів або магазинів застосунків (AppStore, Google Play). Програмне забезпечення з невідомих джерел, швидше за все, містить шкідливий програмний код. У жодному разі не використовуйте антивірусів, які мають походження з іноземної держави, до якої застосовано санкції згідно із Законом України «Про санкції», чи розроблені / виготовлені юридичною особою – резидентом такої іноземної держави або юридичною особою, частка статутного капіталу якої перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави.

6. Регулярно створюйте резервні копії важливої інформації. Для збереження резервних копій використовуйте зовнішні носії інформації. Перш ніж створювати резервні копії своїх файлів на зовнішньому диску, шифруйте їх, щоб ніхто не міг отримати доступ до них у разів втрати чи викрадення зовнішнього диску.

7. Скануйте перед підключенням USB-накопичувачі та інші зовнішні пристрої на наявність шкідливих додатків і вірусів. Ніколи не використовуйте USB-накопичувачі, джерело якого не знаєте, оскільки воно

може бути заражене зловмисним програмним забезпеченням.

8. Не використовуйте особисті пристрої (знімні / зовнішні носії інформації, комп'ютери, планшети, ноутбуки, смартфони) для обробки, зберігання та обміну інформацією, яка обробляється під час виконання службових обов'язків.

9. Не працюйте під обліковим записом адміністратора системи.

10. Відмовтеся від програмного забезпечення або його оновлення, якщо воно потребує додавання у «список виключення» систем захисту комп'ютера.

11. Відключіть автоматичні оновлення та в ручному режимі оновлюйте програмне забезпечення, у ході чого додатково його перевіряйте на авторитетних ресурсах, призначених для аналізу підозрілих файлів, наприклад:

– https://www.virustotal.com/,
– https://malwr.com/,
– https://www.reverse.it/.

12. Не завантажуйте файлів із невідомих джерел або від невідомих чи малознайомих відправників. Шкідливий код можуть містити навіть файли, які мають вигляд безпечних – наприклад, файли форматів *.docx, *.xlsx тощо. Якщо потрібно завантажити такий файл – перед відкриттям перевірте його антивірусом із попередньо оновленою версією вірусної бази.

Про кіберінциденти можна повідомляти Кіберполіцію callcenter@cyberpolice.gov.ua та CERT-UA cert@cert.gov.ua.

Шкідливе програмне забезпечення або код може бути новим, тому файл не може не визначатися антивірусом як шкідливий, тому не варто втрачати пильності. Будь-який пристрій може бути уражений шкідливим програмним забезпеченням. Це не завжди може бути очевидним для користувача. Нетипова поведінка пристрою має вас насторожити. Уваги потребують, зокрема, такі ознаки:

– батарея дуже швидко розряджається за невисокої інтенсивності використання (у налаштуваннях пристрою можна перевіряти, які саме програми найбільше використовують заряд батареї);
– значне уповільнення роботи пристрою;
– раптове зменшення обсягу вільної пам'яті;
– часті збої в роботі комп'ютера чи смартфона. Наприклад, часті перезавантаження, раптові вимкнення;
– поява спливаючих вікон, реклами;
– неможливість доступу до операційної системи;
– сильний шум або нагрівання пристрою при роботі;
– поява програм чи додатків, яких ви особисто не встановлювали;
– самовільна зміна пристроєм налаштувань;
– передання великих обсягів трафіку навіть тими програмами, які рідко використовуються;

– самовільне включення Wi-Fi, геолокації навіть при відключенні опцій вручну;

– отримання незрозумілих системних повідомлень;

– самовільна робота курсора чи клавіатури.

Якщо комп'ютер був заражений, необхідно виконати наступні дії:

1) зафіксувати підозрілі факти роботи комп'ютеру (фото, відео);

2) вимкнути Інтернет, але не вимикати комп'ютер без дозволу фахівців;

3) звернутися до експертів за допомогою.

Якщо володієте базовими знаннями та розумієте як діяти без фахівця:

4) завантажити ПК у безпечному режимі;

5) перевірити систему антивірусними сканерами;

6) оновити операційну систему.

V. Щодо користування соціальними мережами (обов'язково для службових профілів, рекомендовано для особистих профілів)

Заборонено використовувати мобільні додатки та соціальні мережі, які мають походження з іноземної держави, до якої застосовано санкції згідно із Законом України «Про санкції», чи розроблені / виготовлені юридичною особою – резидентом такої іноземної держави або юридичною особою, чия частка статутного капіталу перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави, зокрема, соціальні мережі «ВКонтакте» та «Одноклассники», сервіси «Mail.ru».

1. Установіть надійні паролі для входу до облікових записів. Не використовуйте один пароль для різних облікових записів. Ніколи не використовуйте паролі повторно.

2. Використовуйте функцію двофакторної авторизації, де тільки можливо (щоб увійти до профілю з незнайомого пристрою, сервіс вимагатиме пройти додаткову ідентифікацію як власника облікового запису, зокрема, на вказаний номер телефону чи на поштову скриньку буде надіслано повідомлення з кодом підтвердження, або необхідно буде ввести один із паролів, що попередньо були збережені через інший обраний спосіб підтвердження).

3. Здійсніть додаткові налаштування профілю в соціальних мережах з метою отримання інформації щодо несанкціонованих входів до ресурсів із невідомого пристрою або інтернет-браузера.

4. Використовуйте як «логін» поштову адресу українських поштових сервісів.

5. Не здійснюйте авторизацію профілів із незнайомих чи незахищених пристроїв (існує ймовірність, що після завершення роботи не буде здійснено вихід із свого облікового запису чи пристрій запам'ятає вказаний при вході логін та пароль, а також ймовірність ураження такого пристрою шкідливим програмним забезпеченням, що може здійснювати збір і передачу відомостей

щодо паролів і логінів зацікавленим особам) або використовувати режим приватного користування, при якому інформація щодо відвідування ресурсу не зберігається.

Не здійснюйте авторизацію профілів через загальнодоступний Wi-Fi. Якщо таки доведеться – обов'язково використовуйте VPN.

Дотримуйтесь своїх власних пристроїв, наскільки це можливо (чужий комп'ютер може бути заражений шкідливим програмним забезпеченням або має клавіатурний шпигун, який відстежує та зберігає все, що вводиться з клавіатури).

6. З метою недопущення отримання зацікавленими особами додаткової (приватної) інформації щодо особи, членів її сім'ї, колег, необхідно:

– не публікувати в соціальних мережах інформацію, що може поставити під загрозу особисте життя особи, життя членів її сім'ї та інших осіб;

– не публікувати фото- та відеоматеріали, за допомогою яких можна визначити місцезнаходження військових частин (підрозділів);

– обмежити доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі (вибрати налаштування, які найбільше захищають додаткові відомості про власника облікового запису);

– не зазначати геолокацію (місце розташування) та доступність пошуку облікового запису в соціальній мережі за номером мобільного телефону та адресою поштової скриньки;

– переглянути список друзів у соціальній мережі, якщо серед них є незнайомі чи підозрілі люди (облікові записи), необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу. У подальшому необхідно бути уважними під час додавання до списку «друзів» нових користувачів.

Слід пам'ятати, що представники соціальної мережі ніколи не писатимуть в особисті повідомлення, а лише на пошту, зазначену під час реєстрації.

Складіть список облікових записів по пріоритету для найбільш чутливих облікових записів:

– електронна пошта;
– інтернет-банкінг / Paypal;
– сайти електронної комерції;
– будь-який обліковий запис, де вказані дані вашої картки;
– будь-який обліковий запис, який містить конфіденційну інформацію (адресу, номер телефону тощо).

Видаліть облікові записи, що не використовувались вами протягом останніх 6 місяців.

Якщо у вас є обліковий запис Google, ви можете перевірити журнал останніх дій для свого облікового запису. Він покаже вам, із яких браузерів і пристроїв ви отримували до нього доступ, коли та з якої

IP-адреси. Якщо там є щось, що ви не впізнаєте, або старий сеанс із комп'ютера товариша, ви зможете завершити його. Така ж опція доступна для багатьох інших онлайн-облікових записів.

Перш ніж остаточно повернути смартфон, ноутбук чи комп'ютер, переконайтеся, що ви не забули скинути його до заводських налаштувань. Це зітре всі дані, які зберігалися на ньому, включаючи доступ до ваших особистих облікових записів, дані та налаштування системи та програм, фотографії, відео чи будь-які інші дані.

VI. Щодо підключення до мережі Інтернет

Не використовуйте застарілі версії ОС Windows, які не підтримуються Microsoft, зокрема, Windows 7 та старіші версії.

Захист пристроїв із Windows 10 та 11 (найпоширеніші версії) здійснюється за допомогою служби «Безпека у Windows». Шукаємо її таким шляхом: Налаштування – Оновлення та захист – Безпека у Windows (або відразу через Пошук).

Зокрема, тут можна налаштувати та перевірити:

– Захист від вірусів і загроз. Серед функцій – швидка перевірка поточних загроз, налаштування захисту в реальному часі, перевірка наявності оновлень тощо. Тут налаштуйте OneDrive для відновлення файлів на випадок їх втрати. Тримайте антивірус активним, оновлюйте сигнатури.

– Захист облікових записів. Таким чином можна налаштувати спосіб захисту при вході в систему. Наприклад, використання паролю, фізичного ключа безпеки чи інших. Установіть один із варіантів. Налаштуйте динамічне блокування екрану.

– Брандмауер і захист мережі. Брандмауер має бути увімкнений, щоб працював захист від несанкціонованого доступу.

– Керування програмами та браузерами. Наразі можна встановити налаштування, що захистять ваш пристрій від шкідливих і потенційно небажаних програм, файлів, сайтів.

– Продуктивність та справність пристрою. Зокрема можна побачити інформацію щодо обсягу пам'яті, роботи акумулятора, програм тощо.

– Параметри сім'ї. У разі потреби налаштуйте функцію «Батьківський контроль», що допоможе підвищити рівень безпеки дитини під час користування комп'ютером.

Система сама підкаже, де у налаштуваннях захисту є прогалини та які дії потрібно виконати, щоб покращити безпеку. Звертайте увагу на ті позиції, біля яких з'являється знак оклику ⚠. Щоб поліпшити захист, потрібно просто дотримуватися вказаних інструкцій.

Одним із найпоширеніших способів входу до мережі Інтернет у публічних місцях є підключення до відкритих точок Wi-Fi. Зазвичай вони є безплатними та вхід до них здійснюється без введення паролів. Саме відсутність паролю робить їх вразливішими для злому з боку зацікавлених осіб, які мають на меті отримати доступ до персональних даних та

відомостей, що зберігаються на телефоні, планшеті, комп'ютері.

Під час здійснення входу до мережі використовуйте лише ті точки доступу до Wi-Fi, що мають протоколи безпеки для захисту бездротового з'єднання WPA3 чи WPA2.

У публічних місцях найкраще користуватися особистим Wi-Fi модемом або здійснювати вхід до мережі Інтернет із мобільного пристрою за передплаченим пакетом послуг мобільного оператора та / або використовувати шифроване VPN-з'єднання до корпоративного чи особистого проксі-серверу.

Підключайтеся до публічних Wi-Fi-мереж тільки в разі крайньої потреби. Завжди використовуйте перевірений VPN для таких сесій. Рекомендуємо: ExpressVPN, Surfshark, PrivateInternetAccess, CyberGhostVPN, NordVPN, ProtonVPN, ClearVPN.

Деякі браузери – наприклад, Opera – мають вбудовану функцію VPN (Opera: Налаштування → Основні → VPN → увімкнути VPN).

Встановіть режим конфіденційності та безпеки для вебсайтів: у налаштуваннях браузера встановіть функцію «Безпечний перегляд» і вимкніть автоматичне завантаження файлів.

Chrome:

Налаштування → Конфіденційність та безпека → Безпека → Безпечний перегляд → Покращений захист;

Налаштування → Конфіденційність та безпека → Безпека → Додатково → Завжди використовувати безпечне з'єднання;

Налаштування → Завантажені файли → Завжди вказувати місце для завантаження.

Firefox:

Налаштування → Файли і програми → Завжди запитувати, де зберегти файли;

Налаштування → Приватність браузера → Безпека → Блокувати небезпечний і шахрайський вміст;

Налаштування → Приватність браузера → Безпека → Увімкнути HTTPS-режим у всіх вікнах.

Opera:

Відкрити всі налаштування браузера → Конфіденційність і безпека → Безпека → Увімкнути захист від шкідливих сайтів і завжди використовувати безпечні з'єднання;

Відкрити всі налаштування браузера → Завантаження → Запитувати папку збереження перед завантаженням.

Tor:

Налаштування → Конфіденційність і захист → Захист → Рівень безпеки → Високий;

Налаштування → Конфіденційність і захист → Захист → Підроблений

вміст та захист від шкідливих програм → Блокувати небезпечний та обманний вміст;

Налаштування → Конфіденційність і захист → Захист → Сертифікати → Запитувати у OCSP-серверів підтвердження поточного статусу сертифікатів;

Налаштування → Конфіденційність і захист → Захист → Режим «Тільки HTTPS»;

Налаштування → Основні → Файли та Програми → Завжди видавати запит на збереження файлів.

Обов'язково встановіть складний пароль для Wi-Fi-мережі. Якщо ваш роутер має відповідну можливість, створіть гостьову мережу для тимчасових користувачів, а для власної мережі встановіть «білий» перелік пристроїв, що можуть під'єднуватись.

На персональних комп'ютерах, мобільних пристроях та планшетах вимкніть функцію «Автоматичне підключення до Wi-Fi».

Відключайте Bluetooth, Wi-Fi та геопозиціонування відразу після використання. Обов'язково встановлюйте пароль для своєї Wi-Fi-мережі. Регулярно виконуйте бекапування даних і контактів. Не переходьте за посиланнями від незнайомців у месенджерах, пошті тощо.

Посадовим особам, які виконують завдання в зоні проведення операції Об'єднаних сил, не слід використовувати особисті модеми чи Wi-Fi-роутери для входу до мережі Інтернет (передачу сигналу можна зафіксувати спеціальною технікою та визначити місцезнаходження).

VII. Щодо убезпечення від фішингових атак

Фішинговий сайт – це шахрайський веб-ресурс, який розташовано за максимально схожою з офіційним сайтом доменною адресою (наприклад, statevvebsite.org.ua замість statewebsite.gov.ua) і який копіює його зовнішній вигляд (дизайн). Метою такого ресурсу є отримання персональних даних громадян, у тому числі їх паспортних даних або реквізитів платіжних карток, для подальшого використання в злочинних цілях.

Наприклад, у мережі Інтернет було розміщено фішинговий ресурс Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування. Закликаємо громадян бути пильними та нагадуємо, що єдиною офіційною адресою Реєстру в мережі Інтернет є portal.nazk.gov.ua.

Справжня: portal.nazk.gov.ua

Фішингова: portal.nazk.org.ua

Кіберзлочинці, використовуючи засоби соціальної інженерії, надсилають на електронні адреси громадян листи від імені державних установ та пропонують їм перейти за зазначеним посиланням для отримання «важливої» інформації або її «уточнення». Перейшовши за таким посиланням, громадянин потрапляє на копію реальної сторінки держустанови, де йому пропонують «зареєструватись» або будь-яким іншим

чином внести необхідні шахраям дані.

1. Ставтесь із підозрою до листів із вкладеннями й посиланнями. Краще уточніть у відправника за телефоном, зазначеним на офіційному сайті державної установи, чи був надісланий Вам такий лист. Можливо, що адресу електронної пошти відправника могли підмінити або зламати.

2. Якщо Ви все ж таки вирішили перейти за будь-яким посиланням, що надійшло Вам на адресу електронної пошти, переконайтеся в правильності написання URL-адреси, за якою Вам пропонують перейти, у відсутності незначних помилок (відмінностей) у доменному імені державної установи.

Усі державні установи в Україні мають єдине ім'я – gov.ua та вигляд statewebsite.gov.ua. Усі інші доменні розширення є ознакою фішингового ресурсу.

Перевірте, чи безпечне посилання, перш ніж натискати його. Перевірку можна здійснити на сайтах:

https://global.sitesafety.trendmicro.com,

https://www.virustotal.com,

https://zulu.zscaler.com.

Якщо ви використовуєте надійне антивірусне рішення, це також може допомогти вам визначити, чи є веб-сайт небезпечним для вашої безпеки та / або конфіденційності. Для цього може відображатися зелений значок поруч із результатами пошуку Google або блокуватися сторінка, якщо вона небезпечна. Потенційно шкідливі посилання можуть надходити до вас через електронну пошту, посилання на Facebook, Twitter та інші соціальні мережі, програми обміну миттєвими повідомленнями.

3. Якщо обраний Вами сайт не підтримує безпечне https-з'єднання, не вводьте свої персональні дані, реквізити кредитних карток, логіни та паролі електронної пошти або облікових записів у соціальних мережах.

4. Не ігноруйте попередження браузера про перехід на підозрілий сайт.

5. Якщо є потреба відвідати ресурс, краще ввести його адресу вручну, щоб запобігти переспрямуванню на шкідливий сайт.

6. На облікових записах, де є можливість, налаштуйте двофакторну автентифікацію.

Додаток Г

Методичні рекомендації щодо написання наукової статті, тез

Науковий текст характеризується смисловою завершеністю, цілісністю та логічною послідовністю. Найважливішим засобом вираження зв'язків є специфічна фразеологія, що вказує на послідовність розвитку думки (спочатку, насамперед, потім, по-перше, по-друге, отже і т. ін.), заперечення (проте, тимчасом, але у той час як, тим не менше, аж ніяк), причинно-наслідкові відношення (таким чином, тому, завдяки цьому, відповідно до цього, внаслідок цього, окрім того, до того ж), перехід від однієї думки до іншої (відтак раніше ніж перейти до, звернімося до, розглянемо, зупинимось на, розглянувши, перейдемо до, необхідно зупинитися на, необхідно розглянути), результат, висновок, підсумовуючи, слід сказати).

Засобами логічного зв'язку можуть виступати також займенники, прикметники, дієприкметники (цей, той, такий, зазначений, названий, вказаний тощо).

Не завжди ці та подібні їм слова прикрашають наукову працю, але вони є своєрідними дороговказами, що попереджають про повороти думки автора, інформують про особливості його творчого шляху. Слова «дійсно», «зрозуміло», «насправді» тощо вказують, що наступний текст повинен бути доведенням, «з іншого боку», «навпаки», «але» тощо готують читача до сприйняття протиставлення, «бо», «оскільки», «адже», «зокрема» – пояснення.

До обов'язкових вимог об'єктивності викладу матеріалу належить посилання на джерело повідомлення, автора висловленої думки. У тексті цю умову можна реалізувати за допомогою спеціальних вставних слів і словосполучень (на думку, за даними, за словами, як слушно зазначає).

Інколи зазначені словосполучення не лише допомагають окреслити хід думки дослідника, а й сприяють удосконаленню композиції роботи.

Фразеологія наукової прози є вельми специфічна. Вона покликана, з одного боку, визначати логічні зв'язки між частинами висловлювань («як показав аналіз», «на підставі отриманих даних», «підсумовуюче сказане», «звідси випливає, що» тощо), з іншого боку, позначити певні поняття, будучи, по суті, термінами.

Обов'язковий елемент наукової праці – звертання до цитат. Звертатись до них доцільно тільки у тих випадках, коли цитата дійсно містить потрібну аргументацію. Слід пам'ятати, що цитування – це не засіб для захисту авторитетною думкою власного тексту або аргументованого переконання опонентів.

Найчастіше застосовують два види посилань на літературні джерела:

– зроблені усередині тексту (безпосередньо у рядку після тексту, до

якого має відношення посилання);

– підрядкові, розташовані унизу сторінки під рядками основного тексту.

Іноді окремі види посилань комбінують між собою.

Посилання, зроблені усередині тексту, беруть у дужки. Підрядкові посилання пов'язують з місцем тексту, до якого вони мають відношення, арабськими цифрами (за порядковими номерами посилань) у вигляді: текст1 ® 1 Посилання. Замість числових позначень іноді застосовують значок у вигляді зірочки (текст* ® *Посилання).

Місце позначення, яке пояснює зв'язок тексту з посиланням може бути різним:

– після цитати, якщо пояснюючий текст знаходиться перед нею або вміщений у її середину (Савченко В. І. зазначав: «Текст цитати» 1; Текст цитати, – зазначав В. І. Савченко, – текст цитати»1);

– після пояснюючого тексту, якщо його розміщено після цитати («Текст цитати, – писав С. В. Мироненко 1, доповнюючи надалі новими даними 2);

– після слів, до яких відноситься бібліографічне посилання (якщо це не цитата) або в кінці речення, якщо посилання важко віднести до конкретних слів.

Числа та знаки у тексті. Однозначні числа не біля одиниць фізичних величин, якщо вони зустрічаються у тексті у непрямих відмінках, краще писати у буквеній, а не цифровій формі (наприклад, одного, трьох, семи). Якщо однозначні цілі числа навіть у непрямих відмінках стоять поруч з двох- і багатозначними, то їх наводять у цифровій формі.

Багатозначні числа у цифровій формі, починаючи з 4-значних, діляться пропусками на групи справа наліво (по три цифри, наприклад, 2 700, 4 660 000 500). Крапки у пропусках не ставлять. Не розбиваються на групи цифри у числах, що позначають номери (після знака номера), у марках машин і механізмів, у позначеннях нормативних документів (стандарти, технічні умови, постанови, накази тощо).

Великі круглі числа (тисячі, мільйони, мільярди) зручніше писати у вигляді поєднання цифр із скороченням тис., млн, млрд, наприклад, 6 тис., 12 млн, 14 млрд.

У числах з десятковими дробами ціле число відокремлюють від дробу комою, а не крапкою. Прості дроби у тексті пишуть через похилу риску, наприклад: 1/7, 2/5.

Знак №, §, %, 0, 0С у тексті може стояти тільки біля цифри. Якщо такий знак застосований без поєднання з числом у цифровій формі, то його замінюють словом. Математичні позначення =, @, №, ^, //, <, >, та деякі інші у тексті передають тільки словами дорівнює, приблизно дорівнює, не дорівнює, перпендикулярно, паралельно, менше, більше.

Скорочення у тексті. Довільні скорочення слів застосовувати неприпустимо.

Щоб правильно користуватись скороченнями, слід звертатись до словників прийнятих скорочень, що можна знайти у довідкових виданнях.

Дозволяється скорочувати слова перед цифрами, що позначають посилання у тексті на певний елемент чогось (табл. 7.1):

Таблиця 7.1

Правила скорочення слів

Том	т.
Випуск	вип.
Частина	ч.
Рисунок	рис.
Видання	вид.
Таблиця	табл.
Розділ	розд.
Номер	№
Додаток	дод.
Пункт	п.
і таке інше	і т. ін.
дивись	див.
та інші	та ін.

Наукова стаття – один із основних видів публікацій. Вона містить виклад проміжних або кінцевих результатів наукового дослідження, висвітлює конкретне окреме питання з теми дисертації, фіксує науковий пріоритет автора, робить матеріал надбанням фахівців.

Наукові статті до дисертацій мають обов’язково бути опубліковані у виданнях, перелік яких затверджений ВАК України.

Наукова стаття направляється до редакції в завершеному вигляді відповідно до вимог, які публікуються в окремих номерах журналів або збірниках у вигляді пам’ятки авторам.

Оптимальний обсяг наукової статті – 0,5 авторського аркуша (до 12 сторінок друкованого на комп’ютері тексту через 1,5 інтервали, шрифт 14).

Рукопис статті, окрім основного тексту, має містити повну назву роботи, прізвище та ініціали автора (-ів), анотацію (на окремій сторінці), список використаної літератури.

Стаття повинна мати такі структурні елементи:

1. Вступ – постановка наукової проблеми, її актуальність, зв’язок із найважливішими завданнями науки й народного господарства України, значення для розвитку певної галузі науки або практичної діяльності (перший абзац або 5–10 рядків). Метою вступу є доведення до читача основних завдань, які ставив перед собою автор статті.

Зазвичай вступ має включати у себе:

– визначення наукової гіпотези;

– докладно пояснювати причини, за якими було почато дослідження;

– розкривати рівень актуальності даної теми.

2. Аналіз останніх досліджень і публікацій, у яких започатковано розв'язання даної проблеми та на яке спирається автор; існуючі погляди на проблему; труднощі при розробці даного питання, виділення невирішених питань у межах загальної проблеми, котрим присвячена стаття (0,5 – 2 сторінки друкованого тексту через півтора інтервали).

3. Формулювання мети статті (постановка завдання) передбачає виголошення головної ідеї даної публікації, яка суттєво відрізняється від існуючих, доповнює або поглиблює вже відомі підходи; уведення до наукового обігу нових фактів, висновків, рекомендацій, закономірностей або уточнення відомих раніше, але недостатньо вивчених.

4. Виклад змісту власного дослідження – основна частина статті. У ній висвітлюються основні положення й результати наукового дослідження, особисті ідеї, думки, отримані наукові факти, виявлені закономірності, зв'язки, тенденції, програма експерименту, методика отримання та аналіз фактичного матеріалу, особистий внесок автора в досягнення й реалізацію основних висновків тощо (п'ять – вісім сторінок).

5. Висновок, у якому формулюється основний умовивід автора, зміст висновків і рекомендацій, їхнє значення для теорії й практики, суспільна значущість, коротко накреслюються перспективи подальших досліджень з теми (третина сторінки). Тут необхідно зробити короткий висновок чи підтвердилась гіпотеза, що була висловлена у передмові, чи ні. У цьому ж розділі робляться альтернативні висновки, у випадку, коли результати дослідження дозволяють розуміти його подвійно.

6. Бібліографічний список цитованої літератури, у якому вміщені бібліографічні описи тих джерел і літератури, на які є посилання у тексті статті.

7. Анотації, додаються до статей українською, російською та англійською мовами.

Жанр наукової статті потребує дотримання певних правил:

– у правому верхньому куті розміщуються прізвище та ініціали автора (ініціали ставлять перед прізвищем); за необхідності вказуються відомості, що доповнюють дані про автора;

– назва статті стисло відбиває її головну ідею, думку (п'ять – сім слів);

– слід уникати стилю наукового звіту чи науково-популярної статті;

– недоцільно ставити риторичні запитання; мають переважати розповідні речення;

– не слід постійно виділяти текст цифрами 1, 2 і т.д., ті чи інші думки, положення; слід починати перелік елементів, позицій з нового рядка,

відокремлюючи їх один від одного крапкою з комою;

– у тексті прийнятним є використання різних видів переліку: спочатку, на початку, спершу, потім, далі, нарешті; по-перше, по-друге, по-третє; на першому етапі, на другому етапі тощо;

– цитати у статті мають містити точні бібліографічні посилання;

– усі посилання на авторитети подаються на початку статті, основний же її обсяг присвячують викладу власних думок; не слід наводити для підтвердження достовірності своїх висновків і рекомендацій висловлювання інших учених, оскільки це свідчить, що ідея дослідника не нова, була відома раніше і не підлягає сумніву;

– стаття має завершуватися конкретними висновками і рекомендаціями.

Тези доповіді – це опубліковані до початку наукової конференції (з'їзду, конференції, симпозіуму) матеріали попереднього характеру, де викладено основні аспекти наукової доповіді. Вони фіксують науковий пріоритет автора та містять матеріали, відсутні в інших публікаціях. Можливий виклад однієї тези. Рекомендований обсяг тез наукової доповіді становить дві-три сторінки машинописного тексту через 1 чи 1,5 інтервали. Схематично структура тез наукової доповіді виглядає таким чином: теза – обґрунтування – доказ – аргумент – результат – перспективи.

При підготовці тез наукової доповіді слід дотримуватися таких правил:

– у правому верхньому куті розміщують прізвище автора та його ініціали; за необхідності вказують інші дані, які доповнюють відомості про автора (студент, аспірант, викладач, місце роботи або навчання).

– назва тез доповіді стисло відбиває головну ідею, думку, положення (п'ять – сім слів).

Виклад суті доповіді доцільно здійснювати у такій послідовності: актуальність проблеми; стан розробки проблеми (перелічуються вчені, які зверталися до розробки цієї проблеми); наявність проблемної ситуації між необхідністю її вивчення, удосконалення та сучасним станом її розробки та втілення; основна ідея, положення, висновки дослідження, якими методами це досягнуто; основні результати дослідження, їхнє значення для розвитку теорії або практики.

Посилання на джерела, цитати в тезах доповіді використовуються рідко. Дозволяється включати цифровий, фактичний матеріал.

Формулювання кожної тези починається з нового рядка. Кожна теза містить самостійну думку, що висловлюється в одному або кількох реченнях. Виклад суті ідеї чи положення здійснюється без наведення конкретних прикладів.

Виступаючи на науковій конференції (з'їзді, симпозіумі), можна послатися на опубліковані тези доповіді і зупинитися на одній з основних (дискусійних) тез. Тези засвідчують апробацію результатів наукового дослідження.

Доповідь – документ, у якому викладаються певні питання, подаються висновки, пропозиції. Вона призначена для усного (публічного) читання та обговорення.

Наукова доповідь – це публічне повідомлення, розгорнутий виклад певної наукової проблеми (теми, питання).

Структура тексту доповіді практично аналогічна плану статті та може складатися із вступу, основної й підсумкової частини.

Методика підготовки доповіді на науково-практичній конференції дещо інша, ніж статті.

Існують два методи написання доповіді. Перший полягає в тому, що дослідник спочатку готує тези свого виступу, на основі тез пише доповідь на семінар або конференцію, редагує її й готує до опублікування в науковому збірнику у вигляді доповіді чи статті. Другий, навпаки, передбачає спочатку повне написання доповіді, а потім у скороченому вигляді ознайомлення з нею аудиторії. Обрання способу підготовки доповіді залежить від змісту матеріалу й індивідуальних особливостей науковця.

Специфіка усного виступу накладає суттєвий відбиток на зміст і форму доповіді. Під час доповіді слід зважати, що суттєва частина матеріалу опублікована в її тезах. Окрім того, частина матеріалу подається на плакатах (слайдах, моніторі комп'ютера, схемах, діаграмах, таблицях та ін.). Тому доповідь повинна містити коментарі до ілюстративного матеріалу, а не його повторення. Можна зупинитися лише на одній (найсуттєвішій, дискусійній) тезі доповіді, зробивши посилання на інші, вже опубліковані. Це дозволить на 20–40 % скоротити доповідь. Доповідач має реагувати на попередні виступи з теми своєї доповіді. Доцільним є полемічний її характер: це викликає інтерес слухачів.

Під час написання доповіді слід зважати на те, що за 10 хвилин людина може прочитати матеріал, що надруковано на чотирьох сторінках машинописного тексту (через два інтервали). Обсяг доповіді становить 8 – 12 сторінок (до 30 хвилин). Доповідь на чотирьох-шести сторінок називається повідомленням.

Доповідь – це одна з багатьох форм оприлюднення результатів наукової роботи, можливість за короткий термін «увійти» в наукове товариство за умови яскравого виступу. Якщо доповідь зроблено за змістом дисертації, дисертант забезпечує апробацію своєї роботи.

Додаток Д

Напрями застосування цифрових сервісів для наукової діяльності

Напрями застосування	**Найменування чи клас цифрових сервісів**
Визначення актуальних напрямів для проведення наукових досліджень. Пошук, критичний добір наукових даних і наукової літератури, оприлюднення й розповсюдження освітніх та наукових матеріалів. Аналіз наукових публікацій, які є найбільш цитованими. Аналіз зарубіжного і вітчизняного досвіду з досліджуваної проблеми.	1. Електронні бібліотеки та репозитарії (Zenodo, EBSCO, DBLP, Електронна бібліотека НАПН України, Електронна бібліотека ЗВО, Національна бібліотека України імені В. І. Вернадського, Educational resources information center); 2. Електронні наукові видання; 3. Наукометричні бази даних (Google Scholar, Scopus, Web of Science, Open Ukrainian Citation Index (OUCI); 4. Національний репозитарій академічних текстів; 5. Пошукові системи мережі Інтернет (Google, Yahoo!)
Наукова комунікація з колегами, науковим керівником чи консультантом, з професорсько-викладацьким складом та адміністрацією ЗВО/наукової установи. Пошук партнерів для спільних наукових проектів та співпраці.	1. Соціальні та професійні електронні мережі (Facebook, LinkedIn, Publons, ResearchGate); 2. Месенджери (Telegram, Viber, WhatsApp) 3. Системи для відеоконференцзв’язку (Zoom, Microsoft Teams, Skype) 4. Цифровий ідентифікатор ORCID.
Для опрацювання кількісних даних та визначення статистичної рівнозначності між групами досліджуваних об’єктів.	Google таблиці, Microsoft Excel, Statistica, StatGraphics, orange.biolab.si.
Для складання бібліографічних описів у пристатейних списках наукових джерел.	EndNote, Mendeley, Biblioexpress, Zotero.
Для розробки і складання тестів, анкет, опитувальників.	Google Форми, MyTest, Knowing, Quizlet, Proprofs, Kahoot!, ClassMarker, PLICKERS, Easy Test Maker
Для організації та участі у масових	Системи для відеоконференцзв’язку

заходах (конференції, вебінари та ін.). Для організації і проведення навчальних занять, вебінарів, майстер-класів, презентацій та ін.	(Zoom, Microsoft Teams, Skype, Google Meet, Google Класс, OpenMeetings, BigBlueButton та ін.).
Для підготовки цифрових презентацій (візуалізація отриманих наукових результатів), для виступів на наукових заходах (апробації наукових результатів) і захисту дисертаційної роботи.	Програмні засоби для створення презентацій та відеоматеріалів: Microsoft PowerPoint, Canva, Prezi, Google презентації, uvScreenCamera, VideoCap, CamStudi, Windows Movie Maker, Apple Keynote, LibreOffice / OpenOffice / NeoOffice Impress, ProShow Producer, Corel Presentations, Lotus Freelance Graphics, Lotus Symphony Presentations, SoftMaker, Ability Presentations, GoBe Productive, Thinkfree Show, KPresenter.
Для віддаленого контролю цифрових пристроїв, обміну файлами між керуючою та керованою машинами, для спільної (одночасної) роботи: з текстом рукопису дисертації спільно з науковим керівником чи підготовкою наукової публікації та ін.	1. Програми віддаленого управління (TeamViewer, Any Desk, Ammy Admin та ін.) 2. Google Документи, Office 365, Google Диск та ін.
Для безпечного використання цифрових технологій та захисту даних.	1. Антивірусні програми (Avast AntiVirus, AVG AntiVirus, Avira AntiVirus). 2. Хмарні сховища (Dropbox, Google Диск). 3. Архіватори (WinRAR).
Планування науково-дослідницької діяльності та управління науковими проектами.	Google Календар, Trello, MeisterTask, Asana, Any.DO, Todoist, TickTick та ін.
Для організації та автоматизації процесу управління науковим масовим заходом (конференція, семінари). З метою забезпечення рецензування та збереження матеріалів наукового заходу.	Morressier, EasyChair, COMS - Conference Management Software, notso.easyscience.education
Для перевірки унікальності наукових текстів (запобігання академічного плагіату).	Unicheck, Content-watch, Advego, Plagiarisma та ін.
Організація і проведення опитувань,	Facebook, Telegram, Viber, YouTube,

презентацій результатів наукових досліджень, організація тематичних груп та ін.	сайти ЗВО/наукових установ, блоги та спеціалізовані сайти з проблематики дослідження
Для проведення аналітики, моніторингу, отримання наукометричних і вебометричних даних про оприлюднені результати дослідження. Для визначення рейтингів вчених, наукових колективів та ЗВО/наукових установ.	Scopus, Web of Science, Google Scholar, Open Ukrainian Citation Index (OUCI), статистичні сервіси Електронних бібліотек, ResearchGate, Бібліометрика української науки, Портал «Наука України: доступ до знань», Webometrics та ін.
Для верифікації фото та відео матеріалів.	1. Верифікація фото (Google Chrome, Tineye, Baidu, Google Maps, Google Street View та ін.) 2. Верифікація відео (YouTube DataViewer, Wolfram Alpha, InVID та ін.)
Для розбудови іміджу вченого потрібно мати особисті профілі у різних наукометричних системах. Варто презентувати свої досягнення і підтримувати наукову комунікацію з колегами через соціальні та професійні мережі.	1. ORCID, Scopus, Web of Science, Google Scholar. 2. ResearchGate, Facebook та ін.

Навчальне видання

Гребенюк Андрій Миколайович
Рижков Едуард Володимирович
Синиціна Юлія Петрівна
Прокопов Сергій Олександрович

ІНФОРМАЦІЙНІ ТА КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

Навчальний посібник

Редактор, оригінал-макет – *А. В. Самотуга*
Верстка – *С. В. Лобань*
Коректор *М. С. Касян*

Підп. до друку 21.12.2023. Формат 60х84/16. Друк – цифровий. Гарнітура – Times.
Ум.-друк. арк. 19,59. Обл.-вид. арк. 21.06. Зам. № 23/23-нп

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Гагаріна, 26, rvv_vonr@dduvs.in.ua
Свідоцтво про внесення до державного реєстру ДК № 6054 від 28.02.2018