Національна академія педагогічних наук України

Інститут педагогічної освіти і освіти дорослих імені Івана Зязюна

Методичні вказівки

для підготовки до практичних занять з дисципліни
ІКТ В ОСВІТНЬО-НАУКОВІЙ ДІЯЛЬНОСТІ
для здобувачів ступеня доктора філософії на третьому (освітньо-науковому) рівні вищої освіти у галузі 01 «Освіта, педагогіка»
за спеціальністю 011 «Освітні, педагогічні науки»

ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАТИЗАЦІЯ ОСВІТИ

ПРАКТИЧНЕ ЗАНЯТТЯ 1.

Тема: Хмарні технології для інформатизації освіти. Сервіси Google Drive.

Практичні завдання

1.Створення/реєстрація/вхід в акаунт gmail. Створення папки на диску Google.
2.Створення текстового документа. Спільна робота з документами Google
3.Створення Google форми

Методичні вказівки.

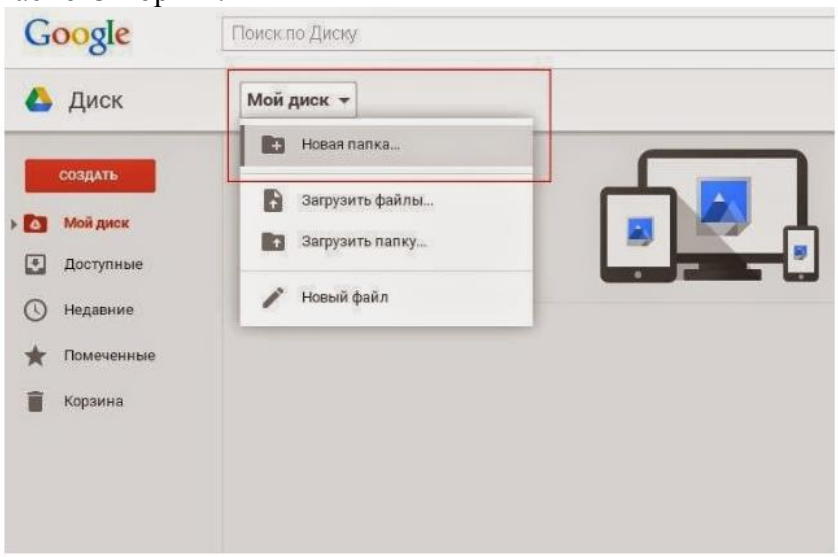
Завдання 1. Створення/реєстрація/вхід в акаунт gmail. Створення папки на диску Google.

Інструкція для виконання

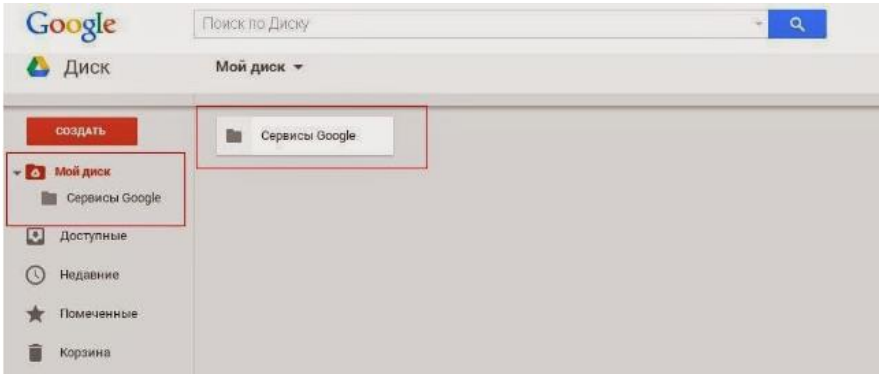
Для того, щоб створити нову папку на диску Google, Вам потрібно зайти в інтерфейс Диска Google. Це можна зробити, наприклад, зайшовши в свій аккаунт електронної пошти Gmail і перейшовши в панель Сервіси в правому верхньому куті екрану.

Крім того, ви можете перейти в диск за прямим посиланням drive.google.com

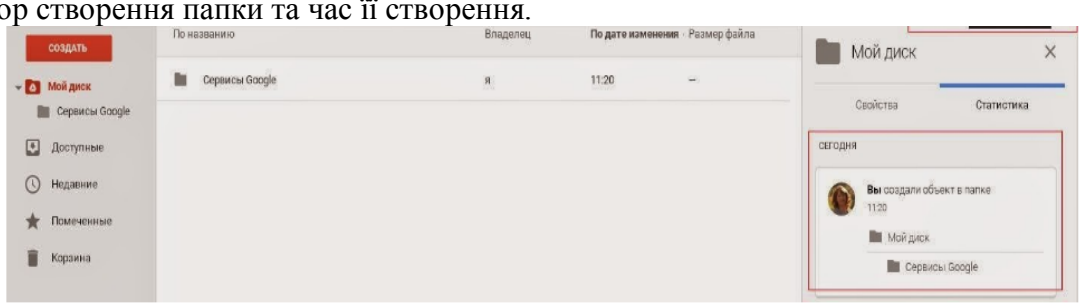
В інтерфейсі диска знаходимо кнопку "Нова папка з плюсом", натискаємо на нього. У нас з'являється вікно, в якому прописуємо ім'я нашої папки "Сервіси Google", натискаємо Створити.



Після цього ваша папка "Сервіси Google" відобразиться в кореневому каталозі Мій диск.



Якщо Ви натиснете на кнопку "Показати властивості", з правого боку буде вказано, хто автор створення папки та час її створення.



Завдання №2. Створення текстового документа. Спільна робота з документами Google

Google Документи – це текстовий редактор. З його допомогою можна прямо в Інтернеті створювати і форматувати документи, а також редагувати їх разом з іншими користувачами в режимі реального часу. Що можна зробити в Google Документах:

– Завантажити документ Word і перетворити його в документ Google.

– Змінити поля, відступи, шрифти, кольори і безліч інших параметрів форматування.

– Надати іншим користувачам право на редагування, додавання коментарів або перегляд того чи іншого документа.

– Спільно редагувати файл в режимі реального часу і спілкуватися з іншими користувачами у вбудованому чаті.

– Переглянути історію змін документа і відновити будь-яку версію.

– Завантажити документ Google на свій комп'ютер у вигляді файлу Word, OpenOffice, RTF, PDF, HTML або ZIP.

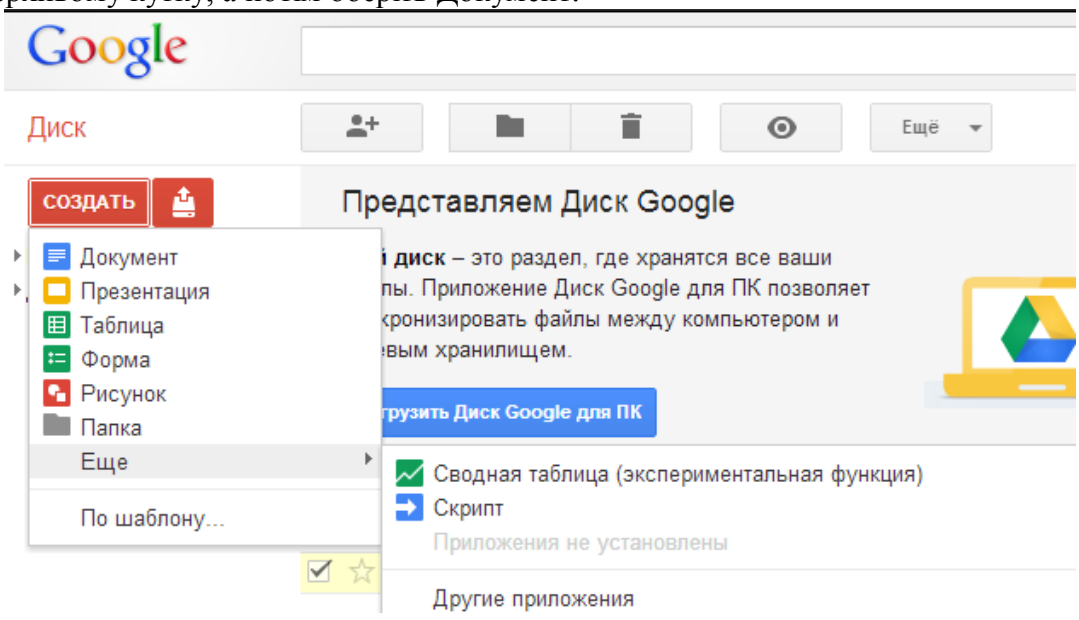
– Перекласти документ на іншу мову.

– Прикріпити документ до повідомлення електронної пошти.

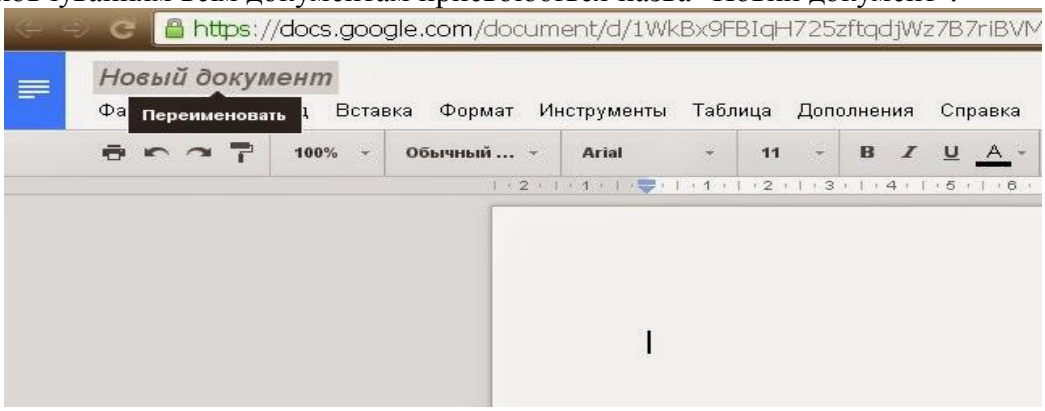
Більш детальну інформацію ви знайдете в короткому посібнику користувача з Google Документами: https://support.google.com/docs/ answer/7068618?visit_id=1-636590120622 834277-1643882542&rd=1.

Інструкція для виконання

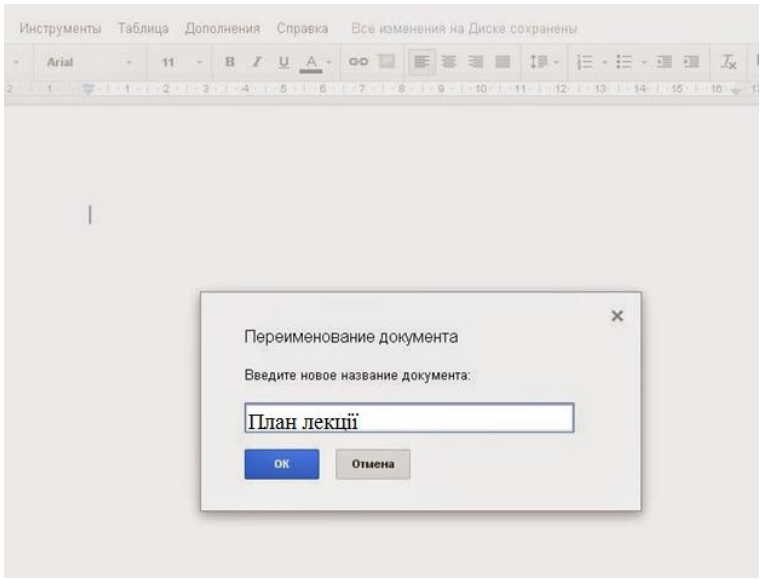
Для того, щоб створити в своєму диску текстовий документ, перейдіть в свій Диск Google, як описано в завданні Створення папки на Диску Google. Перейдіть в папку, в якій ви хочете створити документ і натисніть червону кнопку Створити, яка знаходиться в лівому верхньому кутку, а потім оберіть Документ.



На Диску Google буде автоматично створений новий документ. Зверніть увагу, що за замовчуванням всім документам присвоюється назва "Новий документ".



Щоб привласнити йому потрібну Вам назву, клацніть по заголовку Новий документ і введіть Вашу назву.



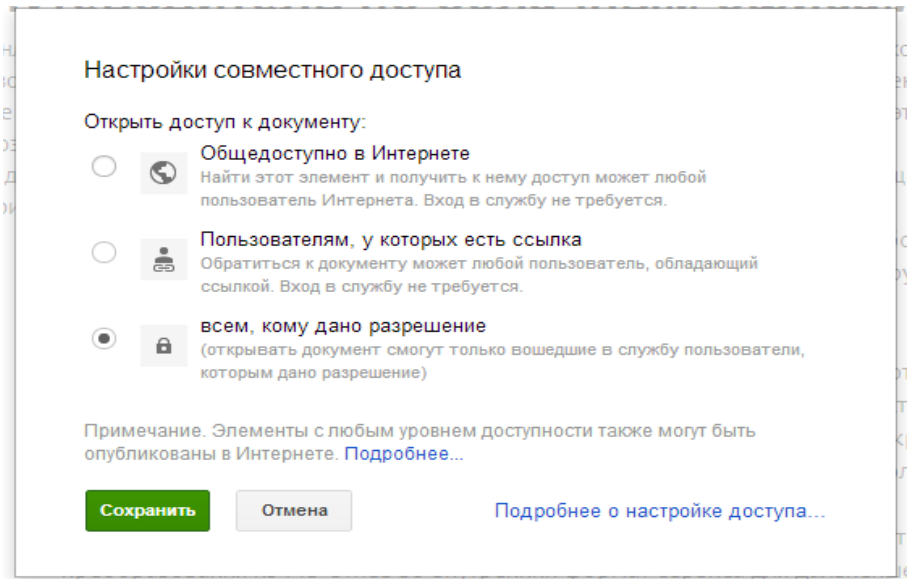
Як і в інших текстових редакторах, Ви починаєте з порожнього листа.

Вправи:

1. Створіть власний документ "План лекції".
2. Почніть складати план лекції. Запишіть тему лекції. Запишіть мету. Тривалість. Основні етапи заняття.
3. Використовуйте панелі форматування, щоб змінити шрифт, його розмір, колір і т. ін.
4. Використовуйте гіперпосилання, таблиці, зображення, символи.
5. Перегляньте шаблони документів для учнів і викладачів в галереї шаблонів. Коли знайдете той, який хотіли б використовувати, клацніть Використовувати цей шаблон.

Спільна робота з документами Google

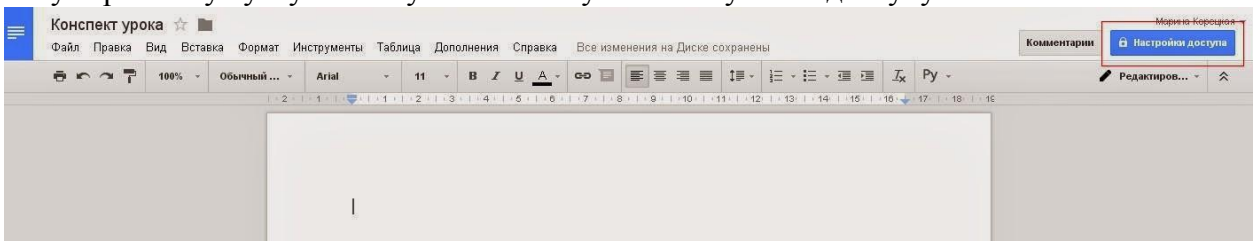
Одна з головних хмарних переваг Документів Google – зручність спільної роботи з документами і розподілу ролей: всі зміни в процесі роботи з документом відображаються в реальному часі в вигляді курсорів різних кольорів в тих позиціях, де відбувається редагування; права доступу досить прості в управлінні. Можна відкрити загальний доступ до документа, а також додати користувача і вказати його рівень доступу (редактор, власник, коментування, читання).



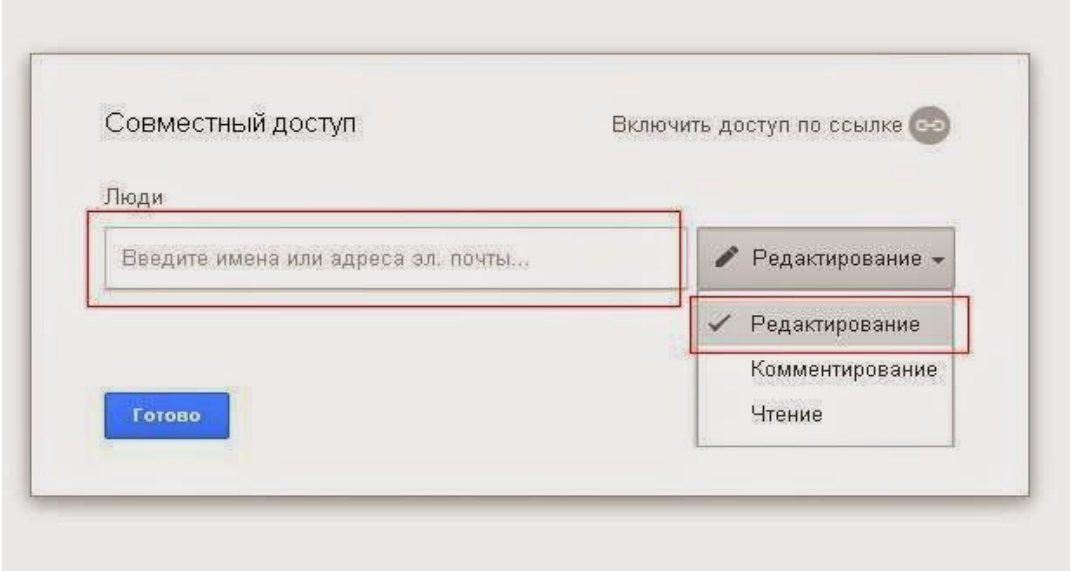
Контакти нескладно об'єднати в групи, що робить розподіл прав більш оперативним, особливо при роботі в команді.

Інструкція для виконання

Для того, щоб надати права на редагування документа іншому користувачу, потрібно в правому верхньому кутку натиснути на кнопку "Налаштування доступу".



У з’явившомуся діалоговому вікні з знаходимо поле "Спільний доступ", де вказуємо адресу особи, якій хочете надати доступ.



В даному полі підтримується функція живого пошуку (якщо ми будемо вводити ім'я адресата або електронну адресу, то система буде пропонувати контакти, що відповідають умовам пошуку).

Потім міняємо "Рівень доступу" (вибираємо зі списку) Редагування.

Таким чином, редактори зможуть: редагувати цей документ, запрошувати і видаляти інших співавторів, створювати копії документів.

Як тільки ми закінчили вносити зміни, натискаємо кнопку Готово.

Вправи:

1. Надайте Спільний доступ до вашого документа "План лекції" викладачеві. Для цього в поле Люди введіть електронну адресу katehod89@gmail.com. Натисніть на спадне меню праворуч від текстового поля і виберіть тип доступу Редагування.

2. Відкрийте Спільний доступ до свого документа іншим учасникам заняття. Натисніть на спадне меню праворуч від текстового поля і виберіть тип доступу Коментування (Користувач зможе переглядати і коментувати файл, але не може вносити зміни).

3. Подивіться документи інших учасників заняття, залиште коментарі.

Завдання №3. Створення Google форми

Форма Google – це інструмент, що забезпечує зворотний зв'язок.

Форма Google – відмінний помічник. За допомогою форми можна проводити різні опитування, вікторини, створювати анкети, тести.

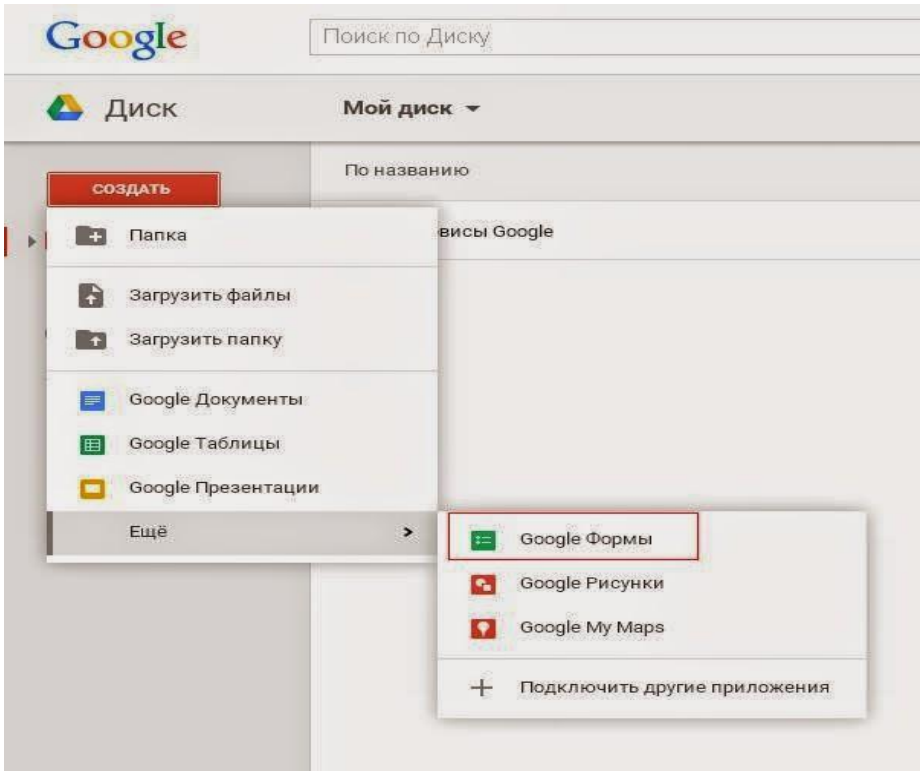
При створенні форми автоматично створюється таблиця Google в якій автоматично накопичуються результати заповнення форми. Таблиця надає зручні можливості зберігання і обробки зібраних даних.

Інструкція для виконання

Створення форми в Google диску.

Для того, щоб створити свою форму Google, перейдіть на Диск Google.

Натисніть червону кнопку Створити, наведіть курсор на пункт Ще й виберіть Google Форми.

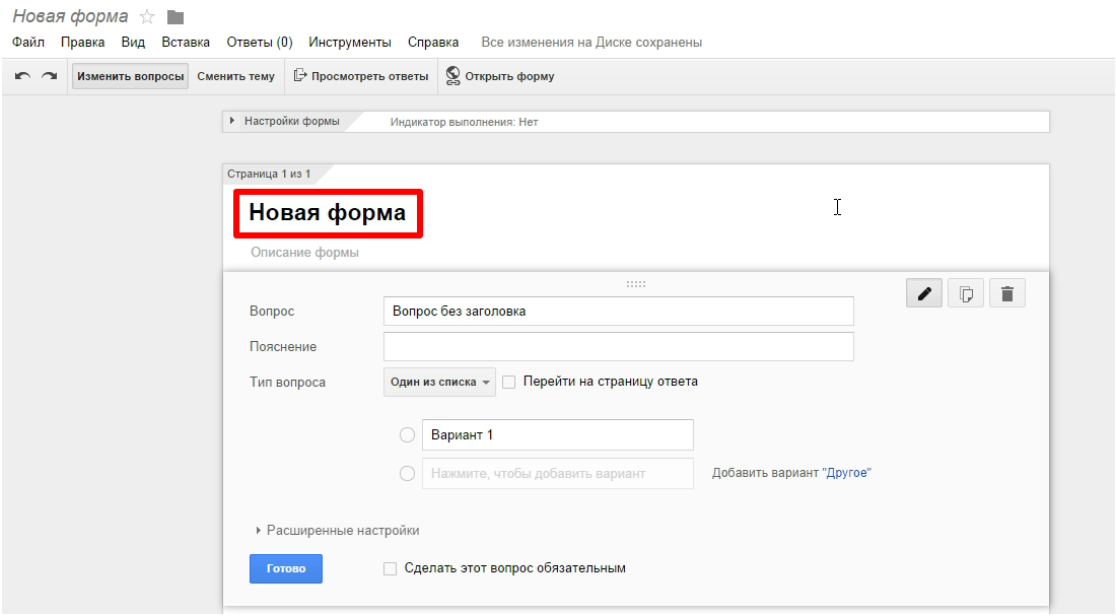


Додайте питання у новостворений шаблон. Ви також можете структурувати форму, розділивши її на кілька сторінок і додавши до них заголовки.

Відкриється інтерфейс редактора форми.

Додавання та редагування питань

Дайте формі власну назву, натиснувши на назві Нова форма. Після цього переходите до редагування форми.



Введіть текст питання в поле Питання.
Додайте пояснення (за бажанням).
Виберіть у спадному меню Тип питання один із запропонованих:

Текст. Респонденту пропонується вписати короткий відповідь.

Текст (абзац). Респондент вписує розгорнуту відповідь.

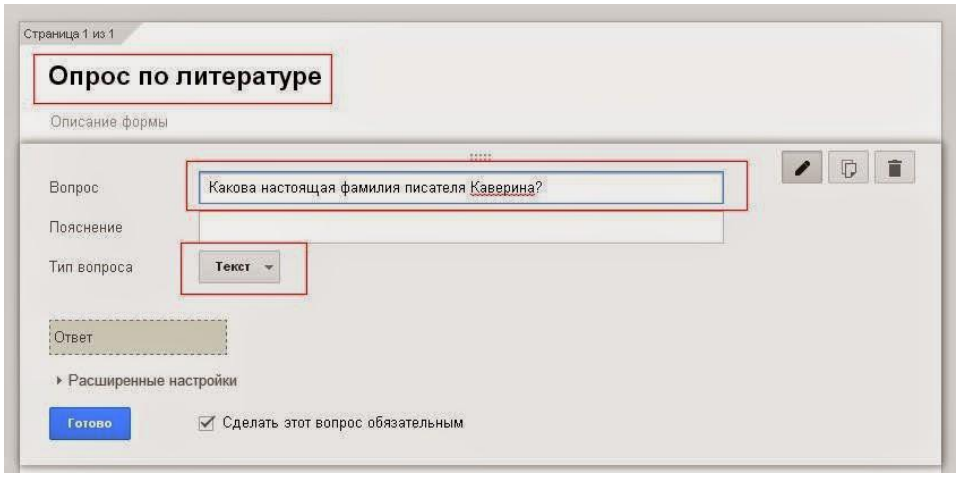
Один зі списку. Респондент повинен вибрати один варіант відповіді з декількох.

Кілька зі списку. Респондент може вибрати кілька варіантів відповіді.

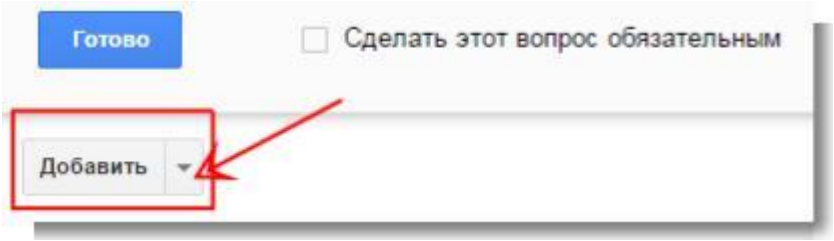
Випадаючий список. Респондент вибирає один варіант зі спадного меню.

Шкала. Респондент повинен поставити оцінку, використовуючи цифрову шкалу (наприклад, від 1 до 5).

Сітка. Респондент вибирає певні точки в сітці, що складається з стовпців і рядків.



При необхідності встановіть прапорець Зробити питання обов'язковим.
Клацніть Готово.
Щоб додати питання:
Клацніть Додати елемент.



Виберіть Тип питання.

Щоб додати зображення:

Перейдіть в меню Вставка або розкрийте список Зображення.

Виберіть Зображення.

Після завантаження зображення ви можете дати йому ім'я і вказати, який текст буде відображатися при наведенні на нього курсора миші.

Зображення в формах не прив'язані до запитань. Ви можете змінити положення зображення, потягнувши його вниз у формі.

Відправлення форми:

По електронній пошті: одержувачі зможуть відповісти на форму безпосередньо в повідомленні:

Клацніть Файл → Надіслати → Надіслати форму ел. поштою.

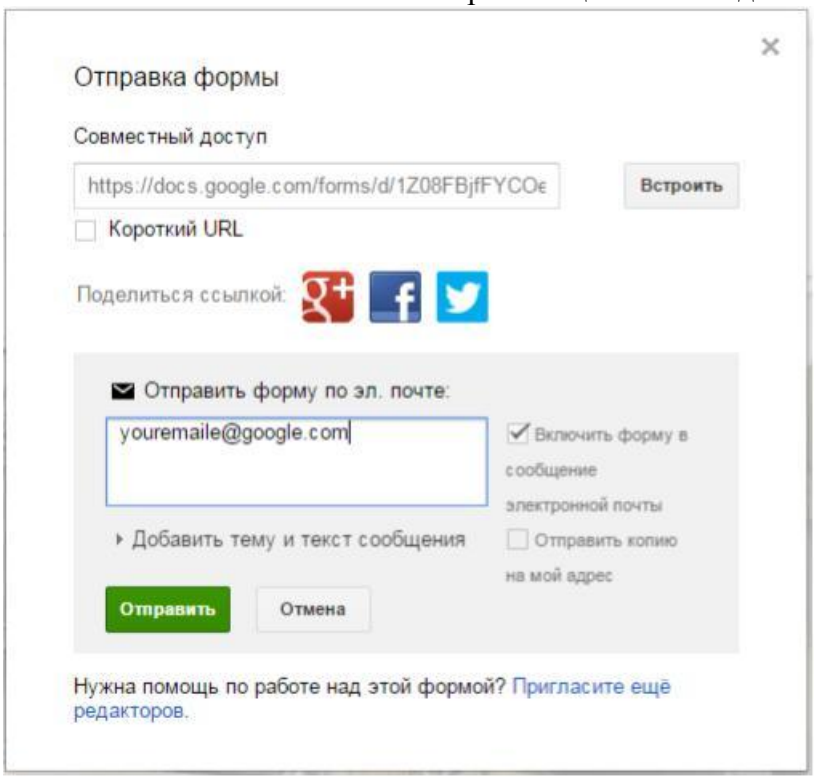
Введіть адреси електронної пошти.

Клацніть Готово.

Публікація веб-адреси форми для всіх:

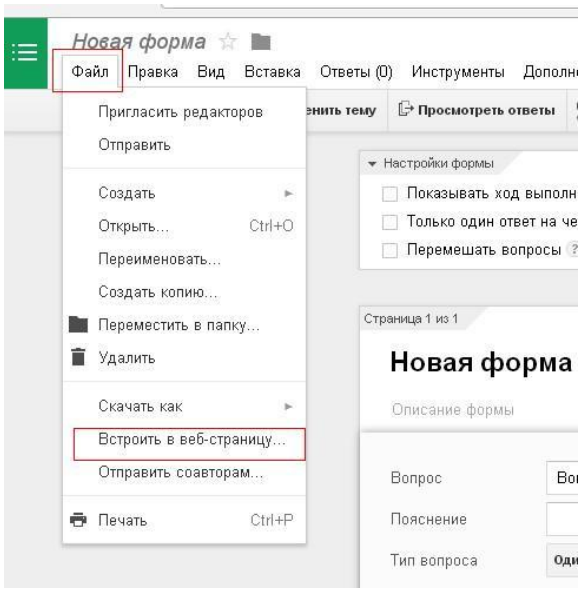
У редакторі форми клацніть Відкрити форму.

Скопіюйте URL і вставте його в презентацію або повідомлення електронної пошти.

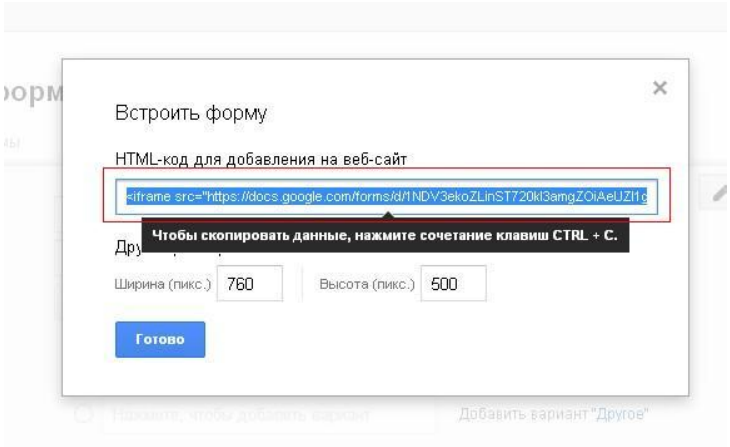


Розміщення Форми на веб-сайті:

У редакторі форми в меню Файл виберіть Вбудувати в веб-сторінку.



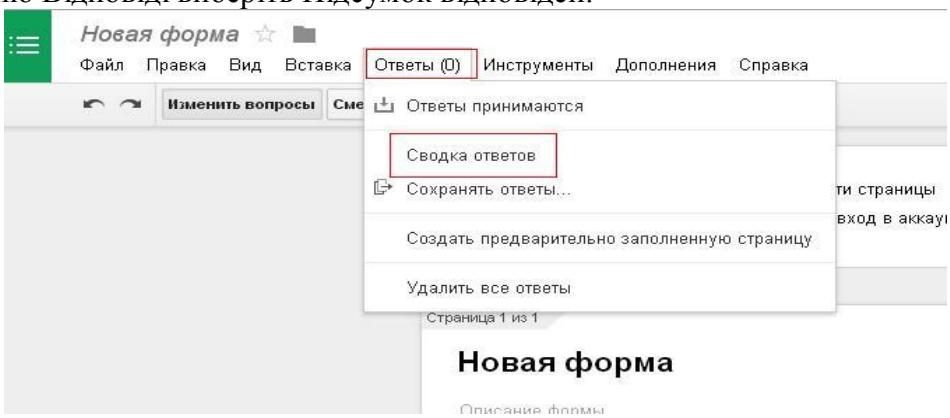
Скопіюйте код



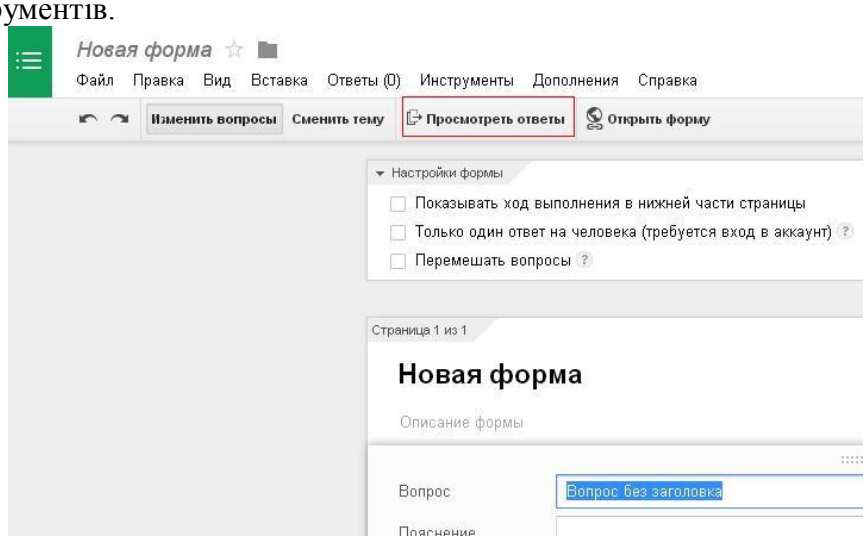
Вставте цей код в свій сайт або блог, включивши при цьому кнопку HTML. Висоту і ширину вбудованої форми можна змінити змінивши числа в коді.

Перегляд результатів опитування

Щоб переглянути, скільки респондентів заповнили Форму і дізнатися їхні відповіді: В меню Відповіді виберіть Підсумок відповідей.



Щоб побачити повністю всі відповіді, клацніть Переглянути відповіді на панелі інструментів.



Вправи:

1. Створіть Google форму з питаннями:

Як тебе звати? [Текст]
Скільки хвилин ти читав на цьому тижні? [Час]
Оціни останню прочитану тобою книгу. [Шкала]

2. Додайте викладача в якості співавтора. Додайте хоча б одне зображення. І нарешті, відправте форму співучасникам заняття.
3. Перегляньте результати опитування

Література

1. Балик, Н., Шмигер, Г. (2011). *Технології Веб 2.0 в освіті.* Тернопіль: Навчальна книга – Богдан.
2. Букач, А. (2013). *Практичні аспекти використання сервісів Веб 2.0 педагогічними і методичними працівниками в умовах функціонування міського інформаційно-освітнього простору.* Біла церква.
3. Вакалюк, Т. (2016). *Хмарні технології в освіті. Навчально-методичний посібник для студентів фізико-математичного факультету.* Житомир: ЖДУ.
4. Кадемія, М. Кобися, В., Коваль, М. (2010). *Соціальні сервіси Веб 2.0 і Веб 3.0 у навчальній діяльності*. Вінниця: ТОВ «Планер».
5. Калініна Л., Носкова М. (2013). Google-сервіси для вчителя. Перші кроки новачка. Львів: ЗУКЦ.
6. Морзе, Н., & Кузьмінська, О. (2012). Хмарні обчислення в освіті: досвід та перспективи впровадження. *Інформатика*, 1, 1–109.
7. Про сервіси Google – https://sites.google.com/site/edugservis/home
8. Хрипун, В. О. (2019). *Хмарні сервіси Google в роботі керівника закладу дошкільної освіти*. Полтава: ПУЕТ.

ПРАКТИЧНЕ ЗАНЯТТЯ 2.

Тема: Наукові електронні бібліотеки та наукометрія.

Практичні завдання

Завдання 1. Створення профілю в Google Scholar. Дослідження наукометричних та бібліометричних методів оцінки публікаційної діяльності вчених.

Завдання 2. Робота з проектом «Бібліометрика української науки».

Завдання 3. Створення веб-портрета вченого.

Методичні вказівки.

Завдання 1. Створення профілю в Google Scholar. Дослідження наукометричних та бібліометричних методів оцінки публікаційної діяльності вчених.

Зареєструватись або увійти до облікового запису Google, перейти до стартової сторінки Google Scholar. Створити авторський профіль Google Scholar. Серед запропонованих документів, які були індексовані Google Академією, знайти власні та додати їх до профілю. Обрати спосіб оновлення профілю: автоматично чи після підтвердження автором – система надсилає лист для перегляду й підтвердження оновлень.

Користуючись ресурсами платформи «Google Академія» встановити наявність наукометричних профілів науковців, що працюють в ІПООД імені Івана Зязюна. На основі аналізу наукометричних профілів науковців скласти рейтинг за такими параметрами: загальна кількість цитувань наукових робіт вчених, h-індекс, i10-індекс, кількість робіт у профілі, що були процитовані. Простежити взаємозв'язок між отриманими даними. На основі аналізу наукометричних профілів науковців скласти рейтинг 10 найчастіше цитованих джерел. Зробити висновок відносно отриманих результатів.

Завдання 2. Робота з проектом «Бібліометрика української науки».

Ознайомитись з функціоналом проекту. Здійснити пошук інформації про себе, про установу, аспірантом якою ви є, про наукові колективи цієї установи. Встановити рейтингові показники. У розділі «Аналітика» простежити рейтинги вчених, наукових колективів та установ відповідної галузі. Здійснити аналіз профілів науковців, що працюють за тематикою, спорідненою темою вашого дисертаційного дослідження. Доповнити список джерел для власного дослідження.

Завдання 3. Створення веб-портрета вченого.

З’ясувати можливості розбудови веб-портрету науковця засобами вебпорталів: Google Scholar, «Український індекс наукового цитування», «Науковці України», ORCID, ResearcherID, Impactstory, соціальні мережі: ResearchGate, Academia.edu, Sciencecommunity.org. E-LIS repository. Підготувати звіт.

Література.

1. Бібліометрика української науки: інформаційно-аналітична система. (2014). *Бібліотечний вісник*, 4, 8–12.
2. Іванова, С. М., Яцишин, А. В., & Кільченко, А. В. (Упор.). (2018). *Електронні науково-освітні системи у науковій та науковопедагогічній діяльності: глосарій*. Київ: ІІТЗН НАПН України.
3. Мар’їна, О. Ю. (2017). *Бібліотека в цифровому просторі: монографія*. Харків: ХДАК.
4. Назаровець, С. (2019). *Унікальні ідентифікатори авторів-науковців: пропозиції, реєстрація, використання.* URL : https://doi.org/10.6084/m9.figshare.923504.
5. Назаровець, С. (2012). *Алтметрікс: новий підхід до оцінки якості наукових досліджень*. URL: http://eprints.rclis.org/18908/1/nazarovets_kyiv2012.pdf.
6. Симоненко, Т. (2015). Бібліометричні системи Scopus і Google Scholar: сфери використання. *Бібліотечний вісник,* 2(226), 10–16.
7. Тихонова, І. (2016). *Ефективне використання комплексу ресурсів Web of Science у науковій діяльності.* URL: http://www.lp.edu.ua/sites/default/files/news/2016/3153/attachments/tykhonkova_nulp_15_09_16cmp.pdf.

ПРАКТИЧНЕ ЗАНЯТТЯ 3.

Тема: Соціальні мережеві сервіси. Блоги. Етика дотримання авторських прав в Інтернеті.

Практичне завдання

Завдання 1. Створення та координація віртуальних предметних спільнот.

Завдання 2. «Використання соціальних мереж для науковців.

Методичні вказівки.

Завдання 1. Створення та координація віртуальних предметних спільнот.

Здійснити пошук веб-платформ, що дозволяють створювати віртуальні спільноти для науковців. Скласти докладний перелік із зазначенням переваг та недоліків. Створити облікові записи та розпочати наукову дискусію. Підготувати звіт щодо ефективності віртуальних предметних спільнот.

Завдання 2. «Використання соціальних мереж для науковців.

Зареєструватись у соціальних мережах для науковців (на власний вибір): Academia.edu, Social Science Research Network, Myexperiment.org, Ukrainian Scientists Worldwide, Science-community.org. Ознайомитись з функціоналом мереж, здійснити порівняльний аналіз. Обґрунтувати яке значення для наукової практики мають професійні та мультидисциплінарні соціальні мережі для вчених. Визначити переваги та недоліки взаємодії науковців засобами соціальних мереж, блог-платформ, тематичних форумів тощо.

Література.

1. Бібліометрика української науки: інформаційно-аналітична система. (2014). *Бібліотечний вісник*, 4, 8–12.
2. Годлевська, К.В. (2019) Соціальні медіа як інструмент освіти для миру. *Освіта для миру = Edukacja dla pokoju*, 2, 260–271.
3. Іванова, С. М., Яцишин, А. В., & Кільченко, А. В. (Упор.). (2018). *Електронні науково-освітні системи у науковій та науковопедагогічній діяльності: глосарій*. Київ: ІІТЗН НАПН України.
4. Мар'їна, О. Ю. (2017). *Бібліотека в цифровому просторі: монографія*. Харків: ХДАК.
5. Назаровець, С. (2019). *Унікальні ідентифікатори авторів-науковців: пропозиції, реєстрація, використання.* URL : https://doi.org/10.6084/m9.figshare.923504.
6. Назаровець, С. (2012). *Алтметрікс: новий підхід до оцінки якості наукових досліджень*. URL: http://eprints.rclis.org/18908/1/nazarovets_kyiv2012.pdf.
7. Симоненко, Т. (2015). Бібліометричні системи Scopus і Google Scholar: сфери використання. *Бібліотечний вісник,* 2(226), 10–16.
8. Тихонова, І. (2016). *Ефективне використання комплексу ресурсів Web of Science у науковій діяльності.* URL: http://www.lp.edu.ua/sites/default/files/news/2016/3153/attachments/tykhonkova_nulp_15_09_16cmp.pdf.

ПРАКТИЧНЕ ЗАНЯТТЯ 4.

Тема: Основні положення теорії інформаційної та кібернетичної безпеки

Практичні завдання

1.Розглянути та проаналізувати наведені нижче інциденти інформаційної безпеки, з ціллю виявлення загроз ІБ та подальшого їх аналізу:

1) За повідомленнями світових інформаційних агентств, невідомі хакери зламали сервер Hotmail.com, після чого в будь-яку з 40 млн. віртуальних поштових скриньок, розташованих на цьому сервері, можна було проникнути без пароля – просто ввівши ім'я користувача. Протягом якого часу поштові адреси користувачів Hotmail.com були доступні будь-якому охочому, залишилося невідомим.

У понеділок вранці, компанія Microsoft (власниця Hotmail) на дві години відключила сервер і, за її заявою, повністю відновила систему безпеки Hotmail.

Незабаром після цього шведські ЗМІ повідомили, що відповідальність за здійснення атаки (а саме упровадження шкідливого коду) на сервер Hotmail, взяла на себе група хакерів під назвою Hackers Unite, до якої входить один швед і сім американців.

«Ми зробили це не для того, щоб щось зруйнувати, – заявив 21-річний шведський представник Hackers Unite. – Ми хотіли показати світові, наскільки погана система безпеки Microsoft».

2) В помсту за дуже маленьку премію 63-річний Рожер Дурон (колишній системний адміністратор компанії UBS Paine Webber) встановив на серверах компанії «логічну бомбу», яка знищила всі дані і паралізувала роботу компанії на тривалий час.

Впровадження «логічної бомби» Дурон здійснив з домашнього комп'ютера за кілька місяців до того, як отримав дуже маленьку, на його погляд, премію. «Логічна бомба» була встановлена приблизно на 1500 комп'ютерів в мережі філій по всій країні і налаштована на певний час – 9.30, якраз на початок банківського дня.

Звільнився Дурон з UBS Paine Webber 22 лютого 2002 року, а четвертого березня 2002 «логічна бомба» послідовно видалила всі файли на головному сервері центральної бази даних і 2000 серверів в 400 філіях банку, при цьому відключивши систему резервного копіювання.

3) Поверхом вище серверної прорвало трубу з гарячою водою, і системні блоки серверів виявилися заповненими окропом.

4) Співробітники компанії «Вимпелком» (колишні і діючі) організували в Інтернеті сайт www.sherlok.ru, про який в компанії «Вимпелком» дізналися в червні 2004 р. Організаторами даного сайту пропонувалася послуга – пошук людей за прізвищем, за номером телефону та іншими даними. У липні організатори сайту запропонували нову послугу – деталізацію телефонних переговорів стільникових операторів. В даному випадку під деталізацією розмов малося на увазі роздруківка номерів всіх вхідних і вихідних дзвінків з вказівкою тривалості розмов і їх вартості, яка використовується операторами, наприклад для виставлення рахунків абонентів. За цими даними можна зробити висновок про поточну діяльність абонента, його сферу інтересів і коло знайомств.

Співробітники компанії «Вимпелком», виявивши даний сайт, самостійно зібрали докази злочинної діяльності сайту і передали справу в МВС. Співробітники МВС порушили кримінальну справу і спільно з компанією «Вимпелком» встановили особи організаторів даного злочинного бізнесу. А 18 жовтня 2004 році було затримано на місці злочину головний підозрюваний.

Крім того, 26 листопада 2004 р були затримані інші шестеро підозрюваних, в числі яких були троє співробітників абонентської служби самої компанії «Вимпелком». В ході слідства з'ясувалося, що сайт був створений колишнім студентом Московського державного університету, який не працював в даній компанії.

5) Наприкінці 1999 року були виведені з ладу веб-сервери таких корпорацій, як Amazon, Yahoo, CNN, eBay, E-Trade і ряду інших, трохи менш відомих. Через рік, у грудні 2000-го «різдвяний сюрприз» повторився: сервери найбільших корпорацій були атаковані за технологією DDoS при повному безсиллі мережевих адміністраторів. З тих пір повідомлення про DDoS-атаки вже не є сенсацією. Головною небезпекою тут є простота організації і те, що ресурси хакерів є практично необмеженими, так як атака є розподіленою.

6) Японська фірма Dai Nippon Printing, що спеціалізується на випуску поліграфічної продукції, допустила найбільший витік інформації в історії своєї країни. Хирофумі Йокояма, колишній співробітник одного з підрядників компанії, скопіював на мобільний вінчестер і вкрав персональні дані клієнтів фірми. В цілому під загрозу потрапили 8,64 млн. чоловік, так як викрадена інформація містила імена, адреси, телефони і номери кредитних карт. У викраденій інформації містилися відомості про клієнтів 43

різних компаній, наприклад про 1 504 857 клієнтів компанії American Home Assurance, 581 293 клієнтів компанії Aeon Co та 439 222 клієнтів NTT Finance.

7) Звільнившись, колишній системний адміністратор вирішив повернути у колишнього керівництва інтерес до своєї персони з використанням недосконалості системи

«Банк-Клієнт», яка застосовується практично у всіх банках України. План системного адміністратора полягав у тому, що він вирішив розробити свою програму захисту і запропонувати її банку, повернувшись на своє колишнє місце роботи. Реалізація плану полягала в проникненні в систему «Банк-Клієнт» і внесенні в неї мінімальних змін. Весь розрахунок був зроблений на те, що в банку повинні були виявити злом системи.

Для проникнення в зазначену систему колишній системний адміністратор скористався паролями і кодами, які дізнався ще в процесі роботи з даною системою. Вся інша інформація, необхідна для злому, була отримана з різних хакерських сайтів, де в подробицях були розписані різні випадки зломів комп'ютерних мереж, методики злому і там же розміщувалося все необхідне для злому програмне забезпечення.

Створивши в системі лазівку, колишній системний адміністратор періодично проникав в комп'ютерну систему банку і залишав в ній різні знаки, намагаючись привернути увагу до фактів злому. Фахівці банку повинні були виявити злом і забити тривогу, але, на його подив, проникнення в систему ніхто навіть не помічав.

Тоді системний адміністратор вирішив змінити свій план, внісши в нього корективи, які б не змогли залишитися непоміченими. Він вирішив підробити платіжне доручення і перевести по ньому через комп'ютерну систему банку велику суму. За допомогою ноутбука і мобільного телефону з вбудованим модемом системний адміністратор близько 30 разів проникав в комп'ютерну систему банку: переглядав документи, рахунки клієнтів, рух грошових коштів – в пошуках відповідних клієнтів. В якості таких клієнтів ним були обрані регіональна митниця і дніпропетровська фірма-банкрут.

Отримавши в черговий раз доступ до системи банку, він створив платіжне доручення, в якому з особового рахунку регіональної митниці зняв і перерахував через банк на рахунок фірми-банкрута 5 млн. гривень. Крім того, ним цілеспрямовано було зроблено кілька помилок в «платіжці», що в свою чергу повинно було ще більше сприяти приверненню уваги з боку фахівців банку. Однак навіть такі факти не були помічені фахівцями банку, які обслуговували систему «Банк-Клієнт», і вони спокійно перерахували 5 млн гривень на рахунок вже не існуючої фірми.

Насправді системний адміністратор розраховував на те, що грошові кошти не будуть переказані, що факт злому буде виявлений до переказу коштів, але на практиці все виявилося по-іншому і він став злочинцем і його липовий переказ переріс в крадіжку.

2. На основі проведеного аналізу заповнити таблицю (зразок таблиці подано нижче) аналізу інцидентів ІБ та виявлених загроз (для кожного з розглянутих інцидентів ІБ).

№	Інцидент ІБ	Тип виявленої (реалізованої) загрози	Джерело загрози та тип порушника	Спосіб реалізації загрози	Використані уразливості	Вид активів, які підлягають захисту	Наслідки (порушення)		
							К	Ц	Д
1.	злам сервера Hotmail.com	упровадження програмних закладок або комп'ютерних вірусів.	антропогенне джерело – група хакерів «Hackers Unite»; зовнішній порушник з високим потенціалом.	одержання зловмисником інформації про програмно-апаратне середовище, тип та параметри засобів обчислювальної техніки, тип та версії операційної системи, склад прикладного програмного забезпечення та інше.	- уразливості системного ПЗ; - уразливості прикладного ПЗ; - уразливості в апаратних засобах.	конфіденційні дані користувачів Hotmail – почтові скриньки.	+		+
2.									
3.									

Методичні вказівки.

Для аналізу випадків та заповнення таблиці Вам необхідно врахувати наведену нижче інформацію.

В якості джерел загроз інформаційної безпеки можуть виступати суб'єкти (фізичні особи, організації, держави), об'єкти (технічні засоби, програмне забезпечення) або явища (техногенні аварії, стихійні лиха, інші природні явища).

Таким чином, джерела загроз ІБ можна розділити на три основних групи:

- антропогенні джерела (антропогенні загрози – загрози обумовлені діями суб'єкта);
- техногенні джерела (техногенні загрози – загрози обумовлені технічними засобами);
- стихійні джерела (загрози викликані стихійними лихами або іншими природними явищами).

В якості антропогенних джерел (порушників) загроз інформаційної безпеки можуть виступати:

- спеціальні служби іноземних держав (блоків держав);
- політичні супротивники (політичні партії);
- терористичні, екстремістські угрупування;
- злочинні групи (кримінальні структури);
- зовнішні суб'єкти (окремі фізичні особи);
- суб'єкти підприємницької діяльності та конкуруючі організації;
- розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів;
- особи, які залучаються для установки, налагодження, монтажу, пусконалагоджувальних та інших видів робіт;
- технічний персонал – особи, які забезпечують функціонування інформаційних систем;
- допоміжний персонал (адміністрація, охорона, прибиральники і т. д.);
- користувачі інформаційної системи;
- адміністратори інформаційної системи і адміністратори безпеки;
- колишні працівники (користувачі).

В свою чергу до антропогенних джерел тобто порушників інформаційної безпеки можна віднести:

- осіб, які здійснюють навмисні дії з метою доступу до інформації (впливу на інформацію), що міститься в інформаційній системі, або порушення функціонування самої інформаційної системи чи її інфраструктури (навмисні загрози ІБ);
- осіб, які мають доступ до інформаційної системи, ненавмисні дії яких можуть призвести до порушення інформаційної безпеки (ненавмисні загрози ІБ). А в залежності від наявних прав доступу і можливостей щодо доступу до інформації та (або) до компонентів інформаційної системи, джерела загроз ІБ

(порушників) також можна поділити на два типи:

1) зовнішні джерела – особи, які не мають права доступу до інформаційної системи, її окремих компонентів і реалізують загрози безпеки інформації з-поза меж інформаційної системи;

2) внутрішні джерела – особи, які мають право постійного або разового доступу до інформаційної системи, її окремих компонентів.

Розглядаючи техногенні джерела загроз інформаційної безпеки, необхідно відзначити, що вони пов'язані безпосередньо з відмовами або збоями в роботі технічних засобів або програмного забезпечення і підлягають обов'язковому аналізу для

інформаційних систем, в яких метою захисту є забезпечення цілісності та доступності оброблюваної інформації. Такі загрози можуть бути обумовлені:

- низькою якістю (надійністю) технічних, програмних або програмно- технічних засобів;
- низькою якістю (надійністю) мереж зв'язку і (або) послуг зв'язку;
- відсутністю або низькою ефективністю систем резервування або дублювання програмно-апаратних і технічних засобів;
- низькою якістю (надійністю) інженерних систем (кондиціонування, електропостачання, охоронних систем і т. п.);
- низькою якістю обслуговування з боку обслуговуючих організацій і осіб.

Таким чином, проаналізувавши можливі джерела загроз переходимо безпосередньо до класифікацій загроз інформаційної безпеки.

Сама ж класифікація загроз може бути проведена за безліччю критеріями, однак нижче буде наведено найпоширеніші з них.

1. За природою виникнення: природні (об'єктивні) і штучні (суб'єктивні).

Природними загрозами називають загрози, що виникли в результаті впливу на ІТС або її окремі елементи об'єктивних фізичних процесів чи стихійних природних явищ, незалежних від людини. Прикладами природних загроз можуть служити пожежі, повені, цунамі, землетруси і т. д., а особливістю таких загроз є надзвичайна складність або навіть неможливість їх прогнозування.

Щодо штучних загроз, то вони викликані діяльністю людини. Серед них, у свою чергу, виходячи з мотивації дій, можна виділити ненавмисні (випадкові) загрози, викликані помилками в проектуванні ІТС та її елементів, помилками в програмному забезпеченні, помилками в діях персоналу або їхньою халатністю та іншими причинами, і навмисні (умисні) загрози, пов'язані з цілеспрямованими діями зловмисників.

2. За розташуванням джерела загрози виділяють:

- загрози, джерело яких розташоване поза межами контрольованої зони. Прикладом можуть слугувати: перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв та ліній зв'язку, а також наведень активних випромінювань на допоміжні технічні засоби, що безпосередньо не приймають участі в обробленні інформації (телефонні лінії, мережі живлення, опалення та ін.); перехоплення даних, що передаються каналами зв'язку, їх аналіз з метою вияснення протоколів обміну, правил входження у зв'язок та авторизацію користувача і наступних спроб їх імітації для проникнення в систему; дистанційна фото- і відеозйомка; перехоплення акустичної інформації з використанням спрямованих мікрофонів.
- загрози, джерело яких знаходиться в межах контрольованої зони (наприклад, інсайдери), території (приміщення), на якій знаходиться ІТС. Як приклад можна навести застосування підслуховуючих пристроїв; розкрадання носіїв, які містять конфіденційну інформацію; від'єднання або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку та ін.);

3. За ступенем впливу на ІТС виділяють пасивні і активні загрози.

Реалізація пасивних загроз не здійснює жодних шкідливих чи негативних змін у складі та структурі ІТС. Прикладом такої загрози є – несанкціоноване копіювання файлів з даними. При реалізації ж активних загроз, навпаки, порушується структура ІТС, к приклад можна навести: упровадження апаратних закладок, програмних закладок та комп'ютерних вірусів, які дозволяють подолати систему захисту, при цьому мають можливість прихованого та незаконного здійснення доступ до системних ресурсів з метою реєстрації та передавання критичної інформації або дезорганізації функціонування системи; дії для дезорганізації функціонування системи (змінювання режимів роботи пристроїв або програм, страйк або саботаж персоналу, постановка потужних активних радіозавад на частотах роботи пристроїв системи і т. п.); загроза навмисної модифікації інформації.

4. Класифікація за видом використовуваної уразливості включає:

- загрози, які реалізуються з використанням уразливості системного ПЗ;
- загрози, які реалізуються з використанням уразливості прикладного ПЗ;
- загрози, що виникають в результаті використання уразливості в апаратних засобах;
- загрози, які реалізуються з використанням вразливостей протоколів мережевої взаємодії і каналів передачі даних;
- загрози, які реалізуються з використанням вразливостей, що обумовлюють наявність технічних каналів витоку інформації.

Можна й надалі продовжувати класифікувати загрози за різними критеріями, однак на практиці найчастіше використовується наступна основна класифікація загроз, яка базується на порушенні трьох раніше введених базових властивостей інформації, а саме: загрози порушення конфіденційності, цілісності та доступності інформації. Додатково можна виділити загрозу автентичності.

Однак, необхідно відзначити, що реальні загрози інформаційній безпеці далеко не завжди можна чітко віднести до якоїсь конкретної категорій. Так, наприклад, загроза розкрадання носіїв інформації може бути при певних умовах віднесена до всіх перерахованих категорій.

Для кращого розуміння, далі розглянемо перелік конкретних загроз:

I. Основні ненавмисні штучні загрози ІТС (без злого умислу):

1) ненавмисні дії, результатом яких є часткова або повна відмова системи в тому числі руйнування апаратних, програмних або інформаційних ресурсів ІТС (тобто ненавмисне пошкодження обладнання, видалення, спотворення файлів з важливою інформацією або прикладних чи системних програм тощо);

2) ненавмисне пошкодження носіїв інформації, апаратного устаткування або каналів зв’язку;

3) некомпетентне використання програмного забезпечення, що призводить до втрати працездатності системи (зависання або зациклення) або незворотних змін в системі (це і форматування носіїв інформації, і видалення даних, і спотворення системних файлів тощо);

4) неправомірне вимкнення обладнання або зміна режимів роботи пристроїв та ПЗ;

5) нелегальне встановлення і подальше використання неврахованого ПЗ (ігрове, навчальне, технологічне та ін., використання якого не являється необхідними для виконання порушником своїх службових обов’язків) з необґрунтованим витрачанням ресурсів (тобто завантаження процесора, використання оперативної пам’яті і пам’яті на твердих носіях);

6) некомпетентне використання, настроювання або взагалі відключення засобів захисту ІТС;

7) зараження всієї ІТС або окремих її компонентів шкідливим ПЗ;

8) втрата, передача або навіть ненавмисне розголошення атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, перепусток тощо);

9) повне або часткове нехтування організаційними обмеженнями (встановленими правилами) при роботі в системі;

10) вхід в систему в обхід засобів захисту (наприклад завантаження сторонньої операційної системи з зовнішніх носіїв).

II. Основні навмисні штучні загрози ІТС (дезорганізація роботи системи):

1) навмисне фізичне руйнування ІТС (в результаті вибуху, підпалу тощо) або виведення з ладу всіх або окремих критичних компонентів ІТС;

2) відключення або виведення з ладу систем безперебійного живлення, охолодження або вентиляції, які забезпечують безперервне функціонування обчислювальних систем;

3) проникнення ворожих агентів у число персоналу ІТС, а також вербування (шляхом підкупу, шантажу тощо) персоналу або окремих користувачів, які мають певні повноваження;

4) використання підслуховуючих пристроїв, дистанційної фото- і відеозйомки тощо;

5) крадіжка або несанкціоноване копіювання носіїв інформації;

6) перегляд та аналіз виробничих відходів (документів, списаних носіїв інформації тощо);

7) зчитування залишкової інформації з оперативної пам'яті і зовнішніх носіїв інформації;

8) використання різноманітних уразливостей операційних систем або іншого ПЗ яке встановлено на компонентах ІТС;

9) злом шифрів криптозахисту інформації;

10) перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і ліній зв'язку, а також наведень активних випромінювань на допоміжні технічні засоби, які безпосередньо не беруть участі в обробці інформації (телефонні лінії, мережі живлення, опалення тощо);

11) перехоплення даних, які передаються каналами зв'язку, і їх подальший аналіз з метою з'ясування протоколів обміну, правил входження в зв'язок і авторизації користувача;

12) «крадіжка особистості» – несанкціоноване заволодіння персональними даними особи або одержання паролів чи інших атрибутів розмежування доступу, з подальшим маскуванням під зареєстрованого користувача («маскарад»);

13) «фішинг» – спонукання користувача ввести свої ідентифікаційні та аутентифікаційні дані (логін, пароль) або іншу персональну інформацію шляхом запевнення користувачів щодо достовірності та справжності фальшивих (спеціально створених для цього) мережевих ресурсів, таких як пошта, веб-сайти, сторінки авторизації у соціальних мережах тощо;

14) «вішинг» – отримання у користувача під час телефонної розмови необхідної зловмиснику інформації, шляхом використання різних методів переконання;

15) розсилання спаму;

16) бот-мережі – сукупність комп'ютерів, уражених шкідливим ПЗ, ресурси яких через спеціальні командно-контрольні сервери (C&C) несанкціоновано використовуються зловмисниками;

17) DDoS-атака – розподілена мережева атака, яка за допомогою численної кількості джерел має на меті порушити доступність сервісу (автоматизованої системи) шляхом вичерпання його обчислювальних ресурсів;

18) несанкціонований доступ (НСД) до інформаційних ресурсів та інформаційно-телекомунікаційних систем з подальшим несанкціонованим використання терміналів користувачів (які мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізична адреса, апаратний блок кодування тощо);

19) впровадження апаратних або програмних «закладок», шкідливого ПЗ (комп'ютерних вірусів, троянських коней і т. п.), з метою таємного, незаконного доступу до системних ресурсів, реєстрації та передачі критичної інформації або дезорганізації функціонування системи;

20) незаконне підключення до ліній зв'язку з метою роботи «між рядків», з використанням пауз в діях законного користувача від його імені з подальшим введенням неправдивих повідомлень або модифікацією переданих повідомлень;

21) незаконне підключення до ліній зв'язку з метою підміни законного користувача шляхом його фізичного відключення після входу в систему і успішної аутентифікації з подальшим введенням дезінформації і нав'язування помилкових повідомлень.

Зауважимо, що для досягнення поставленої мети зловмисник буде використовувати не одну загрозу, а деяку їх сукупність, при цьому застосовуючи різноманітні напрями, методи та способи реалізації даних загроз.

До основних напрямків реалізації загроз зловмисником відносять:

- безпосереднє звернення до об'єктів доступу;
- створення програмних та технічних засобів, що виконують звернення до об'єктів доступу в обхід засобів захисту;
- модифікація засобів захисту, що дозволяє реалізовувати загрози інформаційній безпеці;
- упровадження в технічні засоби автоматизованої системи програмних або технічних механізмів, що порушують передбачувану структуру та функції автоматизованої системи.

До основних методів реалізації загроз інформаційній безпеці системи зазвичай відносять:

- визначення зловмисником типу та параметрів носіїв інформації;
- одержання зловмисником всієї необхідної інформації щодо програмно-апаратного середовища, типу та параметрів засобів обчислювальної техніки, типу та версії операційної системи, складу прикладного програмного забезпечення;
- одержання зловмисником детальної інформації щодо функцій, які виконуються автоматизованою системою;
- одержання зловмисником даних щодо системи захисту, яка застосовується в інформаційній системі;
- визначення способу подання інформації;
- визначення зловмисником змісту даних, що оброблюються в системі, на якісному рівні (застосовується для моніторингу автоматизованої системи і для дешифрування повідомлень);
- викрадення (копіювання) машинних носіїв інформації, які містять конфіденційні дані;
- використання спеціальних технічних засобів для перехоплення побічних електромагнітних випромінювань та наведень (ПЕМВН) – конфіденційні дані перехоплюються зловмисником шляхом виділення інформативних сигналів з електромагнітного випромінювання та наведень колами живлення засобів обчислювальної техніки, що входять до автоматизованої системи;
- знищення засобів обчислювальної техніки та носіїв інформації;
- викрадення (копіювання) носіїв інформації;
- несанкціонований доступ користувача до ресурсів автоматизованої системи в обхід, або шляхом подолання систем захисту з використанням спеціальних засобів, прийомів, методів;
- несанкціоноване перевищення користувачем своїх повноважень;
- несанкціоноване копіювання програмного забезпечення;
- перехоплення даних, що передаються каналами зв'язку;
- візуальне спостереження – конфіденційні дані зчитуються з екранів терміналів, роздруківок у процесі їх друку і т. п.;
- розкриття змісту інформації на семантичному рівні – доступ до смислової складової інформації, яка зберігається а автоматизованій системі;
- знищення машинних носіїв інформації;
- внесення користувачем несанкціонованих змін у програмно-апаратні компоненти автоматизовані системи та дані, які оброблюються;
- установка та використання нештатного апаратного і/або програмного забезпечення;
- зараження комп'ютерними вірусами;

- внесення спотворень в подання даних, знищення даних на рівні подання, спотворення інформації при передаванні лініями зв'язку;

- упровадження дезінформації;

- виведення з ладу машинних носіїв інформації без знищення інформації – виведення з ладу електронних блоків нагромаджувачів на жорстких дисках та інше;

- прояв помилок проектування та розробки апаратних і програмних компонентів автоматизованої системи;

- обхід (відключення) механізмів захисту – завантаження зловмисником нештатної операційної системи з флешки, використання налагоджувальних режимів програмно-апаратних компонент автоматизованої системи та інше;

- спотворення відповідності синтаксичних та семантичних конструкцій мови – встановлення нових значень слів, виразів і т. п.;

- заборона на використання інформації – наявна інформація за будь- яких причин не може бути використаною.

Однак, як вже зазначалось раніше, перед проведенням детального аналізу загроз інформаційної безпеки, спершу необхідно виділити їх та здійснити повний перелік.

Література.

Бурячок, В. Л. (2013). Модель формування дерева атак для одержання інформації в інформаційно-телекомунікаційних системах і мережах при вилученому доступі. *Інформатика та математичні методи в моделюванні,* 2, 123–131.

Бурячок, В. Л., Толюпа, С. В., Семко, В. В., Бурячок, Л. В., Складанний, П. М., & Лукова-Чуйко, Н. В. (2016). *Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник*. Київ: ДУТ – КНУ.

Гулак, Г. М. Мухачов, В. А., Хорошко, В. О., & Яремчук, Ю. Є. (2011*). Основи криптографічного захисту інформації: підручник*. Вінниця: ВНТУ.

Законі України «Про інформацію».

Законом України «Про захист персональних даних».

Закону України «Про основні засади забезпечення кібербезпеки України».

Кодекс України «Про адміністративні правопорушення».

Кримінальний кодекс України.

Кузьменко, Б. В. & Чайковська, О. А. (2009). *Захист інформації.* Київ: Видавничий відділ КНУКіМ.

Остапов, С. Е., Євсеєв, С. П., & Король, О. Г. (2013). *Технології захисту інформації: навчальний посібник*. Харків: ХНЕУ.