МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ЗАХИСТ ІНФОРМАЦІЇ В ПОЛІГРАФІЇ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ

*Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня магістра за освітньою
програмою «Технології друкованих і електронних видань»
спеціальності 186 «Видавництво та поліграфія»*

Київ
КПІ ім. Ігоря Сікорського
2020

Захист інформації в поліграфії: Комп’ютерний практикум [Електронний ресурс] : навч. посіб. для студ. спеціальності 186 «Видавництво та поліграфія» / КПІ ім. Ігоря Сікорського ; уклад.: Т. Ю. Киричок, Т. Є. Клименко, О. В. Коротенко. – Електронні текстові дані (1 файл: 2,1 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 27 с.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 9 від 30.04.2020 р.) за поданням Вченої ради Видавничо-поліграфічного інституту (протокол № 9 від 27.04.2020 р.)

Електронне мережне навчальне видання

ЗАХИСТ ІНФОРМАЦІЇ В ПОЛІГРАФІЇ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ

Укладачі: *Киричок Тетяна Юріївна,* докт. техн. наук, проф.
Клименко Тетяна Євгенівна, канд. техн. наук
Коротенко Олена Володимирівна, канд. техн. наук

Відповідальний редактор: *Т. А. Роїк*, д-р техн. наук, проф., (в. о. завідувача кафедри ТПВ) КПІ ім. Ігоря Сікорського

Рецензент: *В. М. Скиба*, канд. техн. наук, доц.

Навчальний посібник відповідає навчальній програмі дисципліни «Захист інформації в поліграфії. Комп’ютерний практикум» спеціальності 186 «Видавництво та поліграфія» освітньо-професійної програми «Технології друкованих та електронних видань» підготовки магістрів Видавничо-поліграфічного інституту. Наведено перелік робіт як індивідуальних завдань комп’ютерного практикуму за розділами «Система захисту друкованої продукції» та «Захищені від підроблення матеріали» та «Захист ЦПДСО та іншої друкованої продукції інформаційними методами». Показано застосування теоретичного матеріалу до розв’язування поставлених практичних задач у відповідності до робот з комп’ютерного практикуму.

Для студентів ВПІ КПІ ім. Ігоря Сікорського та інших факультетів, інститутів, які вивчають виробництво захищеної від підроблення продукції, та зацікавлених осіб.

ЗМІСТ

1. Загальні відомості

Кредитний модуль визначає дисципліну «Захист інформації в поліграфії», яка входить до циклу дисциплін професійної підготовки магістрів відповідно до освітньої програми «Технології друкованих та електронних видань» спеціальності 186 Видавництво та поліграфія. Курс присвячений вивченню технологій поліграфічної продукції, що потребує захисту від підроблення, зокрема ЦПДСО, та відповідає нагальній ринковій потребі підготовки сучасних фахівців. Знання і розуміння технологій захисту друкованої продукції дозволяє успішно працевлаштовуватися на підприємствах, що випускають захищену від підроблення продукцію.

Навчальний посібник «Захист інформації в поліграфії. Комп'ютерний практикум» охоплює основні поняття, засоби та технології виготовлення, а саме вивчення методів захисту поліграфічної продукції, графічних елементів для захисту, видів штрихового кодування, дослідження їх специфікації, способи встановлення нумерації та персоніфікації та внесення змінної інформації в документи, здобуття практичних навичок роботи у спеціальних комп'ютерних програмах.

Посібник призначено для студентів денної та заочної форми навчання технічних спеціальностей. Його можна використати також для підготовки до занять, заліків, екзаменів студентам всіх форм навчання, які вивчають подібний матеріал.

Мета комп'ютерного практикуму полягає в закріпленні знань, одержаних студентами під час вивчення дисципліни «Захист інформації в поліграфії», їх застосуванні для вирішення конкретних завдань, сприянні самостійності у аналізі та прийнятті важливих професійних рішень, які є необхідною складовою підвищення технічного рівня підготовки студента.

Основні завдання циклу робіт з комп'ютерного практикуму – формування у студентів вмінь розробляти захисний комплекс, обирати технології для виготовлення цінних паперів та документів суворого обліку, а також іншої друкованої продукції, застосовувати відповідне комп'ютерне програмне забезпечення.

2. Основні вимоги до виконання робіт з комп'ютерного практикуму

Комп'ютерний практикум з дисципліни «Захист інформації в поліграфії» для кожного студента містять відповідні завдання. При виконанні робіт з комп'ютерного практикуму необхідно дотримуватися наведених нижче правил. Роботи, виконані без дотримання цих правил, можуть бути повернені студенту для доопрацювання.

Протокол роботи комп'ютерного практикуму оформлюється у вигляді роздрукованих сторінок формату А4, оформлення якої здійснюється із дотриманням вимог ДСТУ 3008-2015.

Типова структура роботи містить: титульний аркуш (оформлення у додатку); аркуш завдання; основна частина; додатки (за необхідністю); макет зразка виконаного завдання.

Оформлення звіту та порядок захисту

Звіт роботи з комп'ютерного практикуму виконується на аркушах А4, в протоколі стисло відображається хід роботи, отримані результати та висновки. Зміст виконаної роботи ілюструється на електронних носіях. При захисті студент повинен розуміти зміст роботи, а також знати відповіді на контрольні запитання та запитання щодо можливостей використання основних функцій застосованих програмних засобів.

3. Зміст та перелік робіт з комп'ютерного практикуму

3.1. Робота з комп'ютерного практикуму № 1
ЗАХИСТ ДОКУМЕНТІВ MICROSOFT WORD

Мета роботи: вивчити способи захисту документів в пакеті Microsoft Word, дослідити стійкість захистів електронних документів до злому.

Теоретичні відомості

Програмний пакет Microsoft Word є найбільш популярним і часто використовуваним пакетом при підготовці електронних документів, зокрема електронних видань. При роботі з додатками Microsoft Word виникає проблема забезпечення захисту інформації, що міститься в документі, для чого в пакет Microsoft Word були введені різні методи захисту.

Microsoft Word підтримує три рівні захисту при збереженні документів.

Для доступу до параметрів захисту потрібно відкрити меню *Файл (File)* - *Зберегти як (Save As)*, розкрити список *Сервіс (Tools)* і вибрати пункт *Загальні параметри (General Options)* (рис. 1.1).

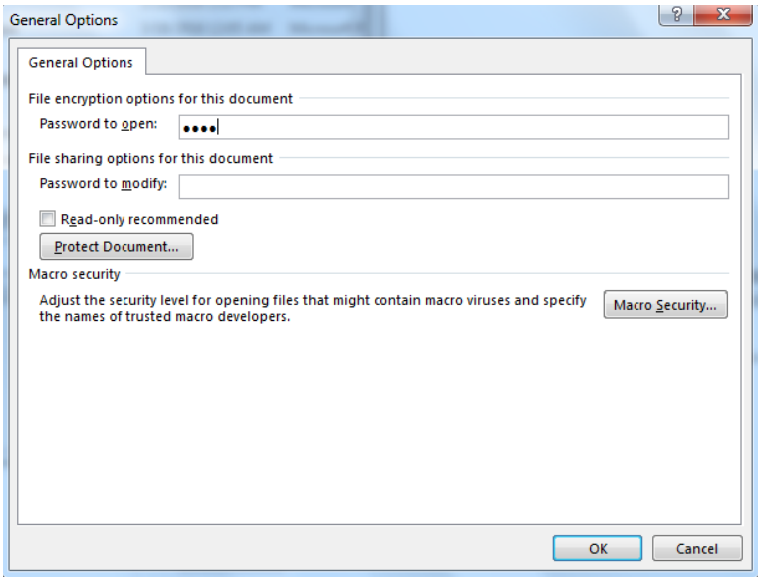


Рисунок 1.1 – Вибір параметрів в програмі Microsoft Word

Ці параметри можуть використовуватися як разом, так і окремо:

1. *Пароль для відкриття файлу (Password to open)*

Для відкриття документа користувач повинен ввести пароль, який є кодом, за допомогою якого був зашифрований файл.

2. *Пароль дозволу запису (Password to modify)*

Для відкриття документа в режимі редагування, користувач повинен ввести пароль. Чи не вводячи пароль, користувач може відкрити документ в режимі тільки для читання. Якщо Ви задали пароль дозволу запису, параметр Рекомендувати доступ лише для читання (Read-only recommended) ігнорується.

3. Рекомендувати доступ лише для читання (Read-only recommended)

Користувачеві пропонується відкрити документ в режимі тільки для читання в тому випадку, якщо йому не потрібно змінювати вміст документа. Незважаючи на те, що цей параметр знаходиться в меню завдання паролів на відкриття та зміна документа, сам по собі він не забезпечує ніякого захисту. Якщо документ відкритий в режимі тільки для читання, він захищений від випадкового або автоматичного збереження. Якщо не використовується будь-який додатковий метод захисту, користувач може відмовитися від запропонованого режиму відкриття документа, натиснувши кнопку Ні (No) в діалоговому вікні. У цьому випадку документ Word відкривається в режимі редагування.

На додаток до захисту всього документа Microsoft Word Ви також можете в деякій мірі захистити документ від несанкціонованих змін його окремих областей. Коли Ви застосовуєте захист до окремих областей документа, шифрування не проводиться. Тому рівень безпеки при використанні параметра Захистити документ (Protect Document) є нижчим, ніж той, який забезпечує шифрування всього документа Microsoft Word. Цей метод скоріше служить для більш зручної спільної роботи з документом, ніж для забезпечення його захисту. Захист окремих областей документа не захищає інтелектуальну власність від зловмисників.

У відомостях про документ Microsoft Word дозволяє також здійснити:

- захист документа від редагування;
- захист документа від форматування;
- захист документа від відкриття (паролем).

Захист документа від редагування (рис. 1.2) (FILE → Info → Protect document → Restrict Edition → Editing restrictions → ☑ → Allow only this type of editing in the document (No changes (Read only)/Filling in forms/Comments/Tracked changes) → Yes, Start Enforcing Protection → Enter new password → Reenter password → OK) / (Файл → Інформація → Захистити документ → Обмеження на редагування → ☑ → Дозволити тільки вказаний спосіб редагування документу (Тільки читання/Введення даних в поля форм/Примітки/Запис виправлень) → Так, ввімкнути захист → Ввести новий пароль → Повторити пароль→ OK).

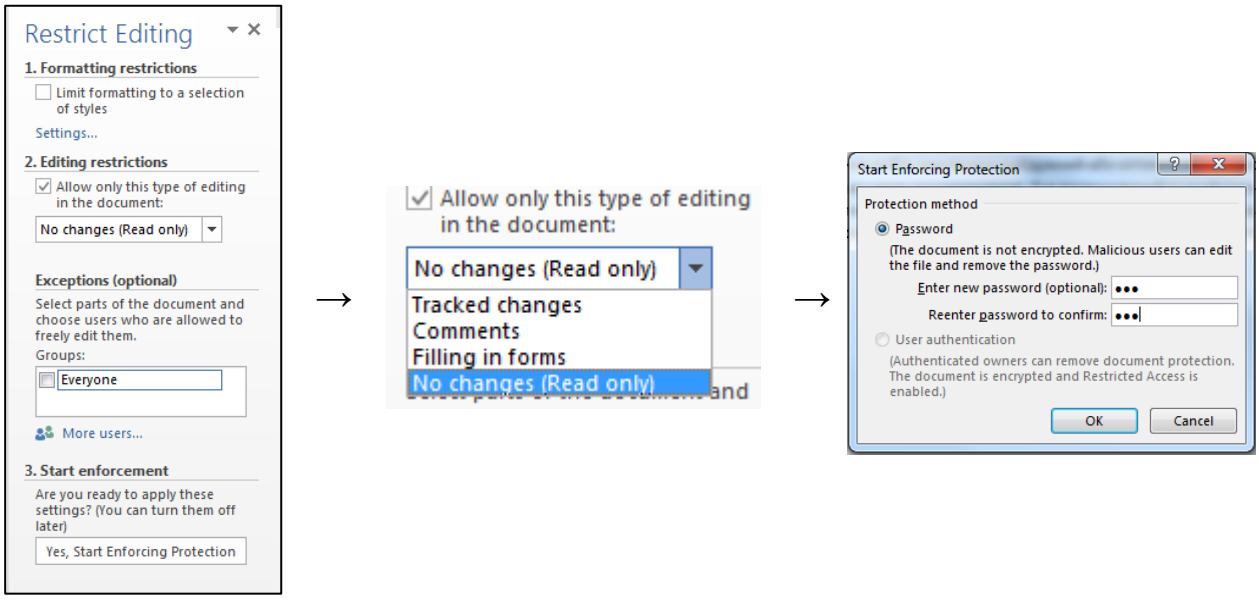


Рисунок 1.2 – Вибір параметрів захисту документу від редагування

Захист від редагування потрібний для убезпечення документів від несанкціонованого редагування. Користувачу також тут дозволено обрати один із типів редагування: введення даних в поля форм, примітки, запис виправлень перегляду обраної області.

У разі установки даного типу захисту, необхідно ввести відповідний пароль, який дозволяє запис документа. Зняти захист може той, хто володіє паролем (Stop protection → Password → OK) (Зняти захист→ Пароль → OK).

Захист документа від форматування (рис. 1.3) (FILE → Info → Protect document → Restrict Edition → Formatting restrictions → ☑ → Yes, Start Enforcing Protection → Enter new password → Reenter password → OK) / (Файл → Інформація → Захистити документ → Обмеження на форматування → ☑ → Так, ввімкнути захист → Ввести новий пароль → Повторити пароль→ OK).

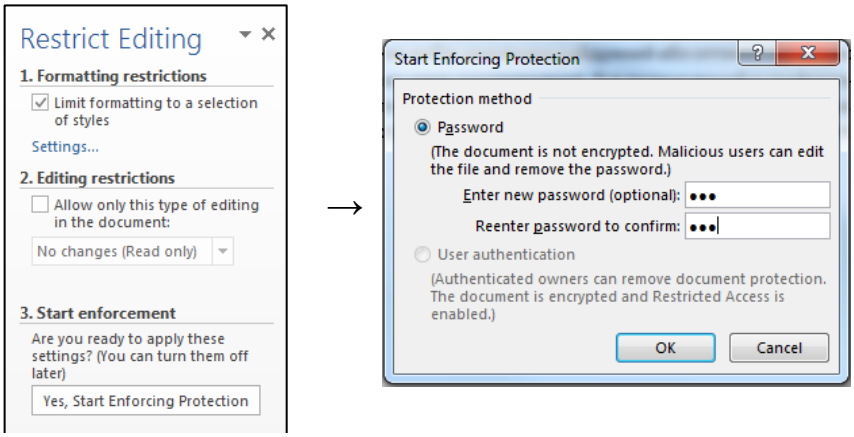


Рисунок 1.3 – Вибір параметрів захисту документу від форматування

Захист від форматування потрібний для убезпечення документів від несанкціонованого форматування. Користувачу дозволено редагувати обрану область, проте із визначеним набором дозволених стилей, змінити форматування яких неможливо.

Зняти захист може той, хто володіє паролем (Stop protection → Password → OK) (Зняти захист→ Пароль → OK)

Методи захисту від редагування та форматування є найслабшими. Пароль захисту запису зберігається в документі у відкритому вигляді. Його можна знайти будь-яким редактором коду. Цей пароль не піддається хешуванню. Захищати документ цим типом захисту вкрай не рекомендується, його криптостійкість дорівнює нулю. Порада - якщо користуватися цим методом захисту, то пароль краще ставити українською/російською мовою, в цьому випадку його дещо складніше виявити.

Захист документа від відкриття (паролем) (рис. 1.4) шляхом FILE → Info → Protect document → Encrypt with Password → Password → Reenter password → OK) / (Файл → Інформація → Захистити документ → Зашифрувати паролем → Підвердження → Пароль → OK).

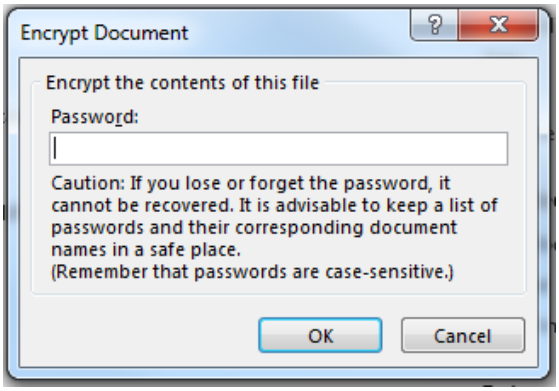


Рисунок 1.4 – Вибір параметрів захисту документа від відкриття

Важливо, що забутий пароль відновити неможливо.

З усіх розглянутих способів захисту в Word, даний метод є найстійкішим. При установці пароля, документ використовується 128-бітне шифрування AES. У документі зберігається зашифрований хеш-образ пароля, який використовується при перевірці. Єдиний спосіб знаходження пароля - повний перебір. Якщо довжина пароля велика, і пароль обраний у відповідність до вимог, то зламати даний тип захисту за прийнятний час досить складно.

Атаки на паролі Microsoft Word

Відомі різні методи атаки на паролі Microsoft Word. Одні методи атакують власне алгоритм шифрування, інші – людський фактор. Найпоширеніші із них:

1. *Атака методом повного перебору (Bruteforce Attack)* – найбільш трудомісткий метод, але дозволяє розкрити всі архіви. При атаці методом послідовного перебору згенеровані пробні паролі є випадковими комбінації

символів (типу 6F7drts78). Атака здійснюється на підставі заданої довжини пароля і набору символів, які перебираються. Швидкість атаки залежить від алгоритму перевірки пароля, а також від кількості символів в наборі і довжини.

Методом послідовного перебору підібрати пароль можна завжди - це лише питання часу, яке може тривати роками, століттями або навіть тисячоліттями. Тому ефективність такого методу досить низька. Природно, якщо заздалегідь відомий набір символів, який використовується для пароля (наприклад, тільки англійські букви і цифри, або тільки російські букви, або тільки цифри), а також приблизна довжина пароля, то це істотно спрощує завдання його підбору і робить її цілком вирішуваною. Якщо ж заздалегідь про пароль нічого не відомо, то підібрати його методом послідовного перебору практично неможливо.

2. *Атака по словнику (Dictionary Attack)* – атака на людський фактор. Алгоритм знаходження пароля, заснований на припущенні, що паролем є деяке слово, або вираз, введене на будь-якій мові. При атаці по словнику в утиліти використовується зовнішній словник і для кожного з слів, що містяться в ньому, послідовно обчислюються хеші, які потім порівнюються з хешем пароля. У порівнянні з методом прямого перебору, швидкість злому значно зростає, оскільки будь-яка мова світу містить менше слів, ніж всі можливі комбінації символів. Для застосування цієї атаки необхідний словник. Недоліком є велика ймовірність відсутності пароля в словнику. Для збільшення ефективності атаки по словнику в деяких утилітах передбачена можливість виробляти додаткові налаштування такої атаки. Зокрема, до словника можна додавати поєднання сусідніх клавіш (типу послідовностей QWERT і ін.), Перевіряти двічі записане слово (наприклад, useruser), зворотний порядок символів в словах (наприклад, RESU), конкатенацію на протилежне символів (зокрема, userresu), слова без голосних, транслітерацію літер (типу Parol). Крім того, можна перевіряти заміну локалізованої розкладки латинської (слово «пароль» в латинській розкладці буде виглядати як «gfhjkm») і заміну латинської розкладки локалізованої (слово «password» в російській розкладці - «зфиицщкв»). Крім цього при атаці по словнику можливе підключення декількох словників.

3. *Атака по масці (Mask Attack)* є варіацією атаки перебором, за тим лише винятком, що деякі символи для знаходження пароля залишаються незмінними, а змінюється тільки певна частина пароля. Ця атака корисна лише тоді, коли відома будь-яка інформація про шуканий пароль. Наприклад, перші чотири символи в паролі - латинські букви, за якими слідує тризначне число. Для завдання маски або правила перебування пароля, використовується спеціально розроблений синтаксис.

4. *Гібридна атака (Hybrid Attack)* – атака, яку можна розглядати як варіант атаки по словнику. При підборі пароля методом гібридної атаки до кожного слова або до модифікації слова словника додається по кілька символів з

визначеного набору справа і / або зліва. Для кожної отриманої комбінації обчислюється хеш, який порівнюється з хешем пароля.

Програми для підбору паролів

Сьогодні можна знайти досить багато як платних, так і безкоштовних програм для підбору паролів до офісних документів. Більш того, деякі компанії пропонують навіть онлайн-сервіс з підбору пароля до документа.

Принцип роботи всіх програм, що дозволяють зламувати паролі, практично однаковий – відмінності лише в деталях. Існують два базових алгоритми злому паролів. Перший полягає в тому, щоб підбирати не саме пароль до документа, а саме секретний ключ і відповідно розшифровувати документ без знання його пароля. Такий тип атаки по ключу називається атакою ключового простору. Другий алгоритм – це підбір пароля. Різні утиліти забезпечують різну швидкість перебору пробних паролів, в них можуть бути реалізовані різні алгоритми генерації пробних паролів (типи атак).

Утиліти підбору паролів можна умовно розбити на два класи: багатоцільові програмні пакети, що дозволяють підбирати паролі до різного типу файлів, і спеціалізовані утиліти, які орієнтовані на підбір паролів до файлів, створеним яким-небудь одним додатком. Фактично багатоцільові програмні пакети становлять собою збірник окремих утиліт (іноді такі пакети передбачають використання єдиної програмної оболонки для доступу до окремих утиліт).

Серед багатоцільових програмних пакетів можна виділити:

- Accent Office Password Recovery v.6.1 від компанії AccentSoft (www.passwordrecoverytools.com);
- Passware Kit 11.1 від компанії Passware (www.lostpassword.com);
- Advanced Office Password Recovery 5.4.547 від компанії ElcomSoft (www.elcomsoft.com, www.passwords.ru);
- Office Password Recovery Magic 6.1.1.0290 від компанії Password Recovery Magic Студія (www.password-recovery-magic.com).

Всі перераховані вище пакети - це зібрання безлічі утиліт, об'єднаних єдиним інтерфейсом. Всі утиліти, що входять в ці пакети, можна придбати і окремо.

Об'єкти дослідження, обладнання, інструменти: програмне забезпечення Microsoft Word, Advanced Office Password Recovery.

Хід роботи

1. Вивчити теоретичні відомості (п. 2).
2. Включити ПК. Перевірити чи встановлене програмне забезпечення на ПК (при необхідності встановити).
3. Виконати завдання, відповіді на питання внести до звіту.

4. Дослідити всі типи захистів в Microsoft Word – захист від запису, від виправлень і захист на відкриття документа. Вивчити функції даних захистів.

5. Сформувати в Microsoft Word довільний документ і поставити на нього захист від запису. В якості пароля вибрати легку послідовність символів англійською мовою. Збережіть даний документ на диску і вийдіть з Word.

6. Запустити програму підбору паролів Advanced Office Password Recovery і з'ясувати введений пароль. Чи перебирає комп'ютер паролі в цьому випадку? Чому? *(Слід зазначити, що обмеження, закладені в демо-версії програми, не дозволяють виводити на екран паролі довжиною понад 4 символів.)*

7. Захистити документ від запису виправлень і спробувати з'ясувати пароль за допомогою програми Advanced Office Password Recovery. Чи здійснюється перебір в цьому випадку? Чому?

8. Поставити захист на відкриття документа (4 символи) і розкрити його за допомогою Advanced Office Password Recovery. Чи здійснюється перебір в цьому випадку? Яка швидкість перебору паролей? Поекспериментувати з різними наборами символів. Якщо Ви не володієте ніякими апріорними знаннями про пароль, то який набір символів необхідно використовувати? Скільки часу зайняв перебір паролів з 1, 2, 3 та 4 символів (при переборі всіх друкованих символів пароля)?

9. Дати рекомендації щодо захисту документів Office. Який захист необхідно ставити? Який пароль вибирати?

10. Спробувати ввести в якості пароля якесь словникове англійське слово, наприклад, «like», і спробувати здійснити атаку по словнику. Як швидко програма зуміла підібрати пароль? Наскільки безпечно використовувати словникові слова в якості пароля?

11. Здійснити узагальнений висновок проведеної роботи.

Контрольні запитання

1. Перерахувати методи захисту документа Microsoft Word. Яка з них найстійкіша до зламування?

2. Перерахувати типи атак на паролі Microsoft Word. Пояснити принципи їх здійснення.

3.2. Робота з комп'ютерного практикуму № 2
ЗАХИСТ ПОЛІГРАФІЧНОЇ ПРОДУКЦІЇ ГРАФІЧНИМИ ЕЛЕМЕНТАМИ

Мета роботи: створення графічних елементів для захисту поліграфічної продукції за допомогою ПЗ Cerber або Adobe Illustrator.

Теоретичні відомості

Одним із найважливіших методів захисту від підроблення є захист на стадії розроблення конструкції, дизайну та формування зображення оригіналу ЦПДСО із застосуванням тонких графічних елементів – сіток, розеток, віньєток, прихованих елементів, мікрографіки тощо [1, 2]. Захист базується на складності відтворення та репродуціювання, які пов'язані з геометричною структурою та мінімально можливою товщиною ліній. Візуально порівнюючи підробки з оригіналом, вже за 5–10-кратного збільшення можна побачити значні перекривлення зображення – потовщення ліній, рвані та перервані лінії, нечіткість окремих елементів, здвоєність зображення тощо [3, 4].

Для захисту бланків ЦПДСО застосовують такі основні графічні елементи:

1. Гільйошні елементи – графічні елементи, утворені тонкими неперервними лініями, які побудовані за певними геометричними законами (рис. 2.1). Як правило, вони складаються з різнокольорових ліній, що перехрещуються, захисних сіток, орнаментів, розеток, бордюрів, віньєток тощо. Найчастіше застосовують типовий орнамент – набір універсальних гільйошних елементів, що відрізняються кольоровим рішенням та змістом, а також клієнтський орнамент, який створено спеціально під певну продукцію. Відповідно до чинних нормативів, гільйошні елементи повинні охоплювати не менше 70 % площі цінних паперів, з яких більша частина – це багатоколірні гільйошні композиції.

Рисунок 2.1 – Гільйошні елементи

Під час створення оригіналів ЦПДСО передбачено застосування позитивних ліній завтовшки 40–70 мкм та негативних – 50–90 мкм. Викреслювання потрібних ліній та побудова композицій гільйошних елементів будь-якої складності, нерегулярних сіток, у т. ч. з використанням об'ємних моделей та накладанням растрових зображень, виконуються за спеціальними векторними програмами та математичними формулами.

2. Тангірні сітки. Це система ліній, яка створює фон бланка ЦПДСО та побудована за геометричними законами. До цієї групи також відносять

псевдорельєфні сітки, що являють собою рисунок фонової сітки, яка імітує рельєфне зображення. Найефективнішим захистом від копіювання є подвійні двоколірні сітки нерегулярної структури.

Для тангірних сіток при друкуванні обирають м'які пастельні тони, що створює перепони для копіювання. У документах тангірні сітки, як правило, наносять на лицьовий та зворотний боки. Рекомендована товщина ліній – 40 мкм для позитивного зображення та 70 мкм для негативного.

3. Спеціальні лінійні растри. Для відтворення півтонового зображення використовують спеціальні лінійні растри зі стандартними формами растрової точки у вигляді кола, еліпса, ромба та ін. За формою розрізняють лінійний, концентричний та інші растри. Створюючи за їх допомогою зображення використовують сітку, що складається з концентричних кіл, прямих чи кривих ліній. Елементи зображення при цьому формуються зміною товщини цих ліній (рис. 2.2). Існує також стохастичне растрування зображення, що складається із багатьох хаотично розкиданих по площі аркуша малих крапок (15–30 мкм), причому їх концентрація на будь-якій ділянці аркуша відповідає кольоровій щільності зображення.

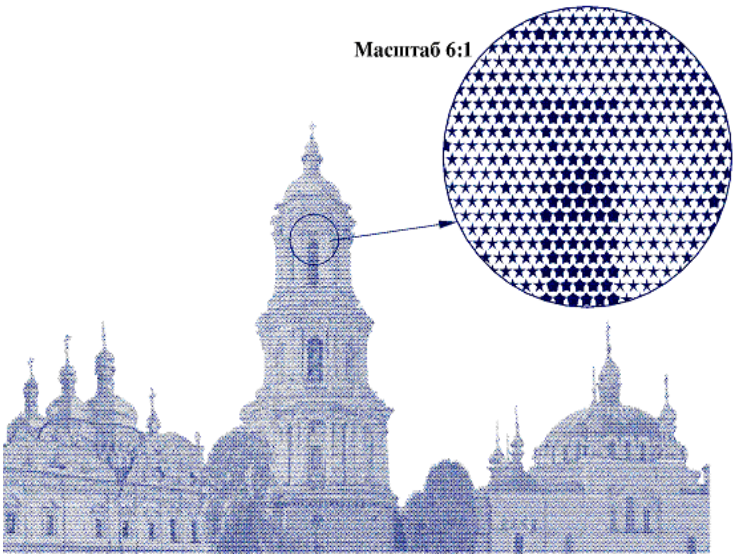


Рисунок 2.2 – Спеціальні растри

4. Наскрізні та регістрові елементи. Наскрізними називають зображення, одна частина яких розташована з лицьового боку бланка ЦПДСО, а інша – на зворотному. Під час розглядання документа на просвіт разом вони утворюють єдине ціле зображення (рис. 2.3).

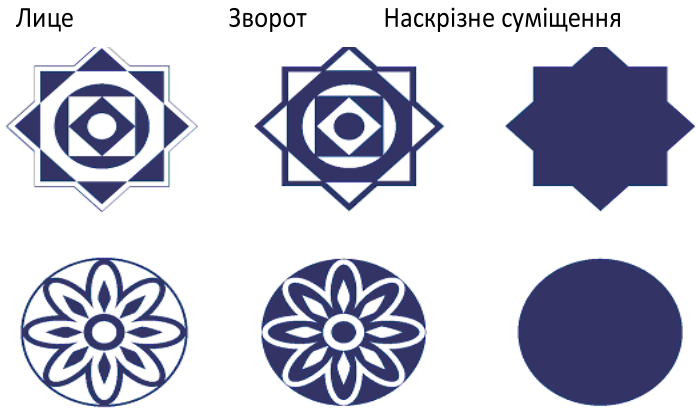


Рисунок 2.3 – Наскрізні елементи

Регістрові зображення («регістр на просвіт») – це ідентичні друковані елементи, розташовані по краях бланка ЦПДСО з лицьового та зворотного боків, які збігаються під час розглядання документа на просвіт.

5. Мікрографіка (мікротекст) – це зображення, що складається з літер тексту з висотою мікрошрифту для позитивного зображення – 200–300 мкм та

для негативного – 300–400 мкм, а також зі знаків, символів тощо, які сприймаються неозброєним людським оком у вигляді тонкої суцільної лінії. Прочитати їх можна за допомогою збільшувальних пристроїв, лупи чи мікроскопу із кратністю збільшення у 4–7 разів. Мікрографіка – це штрихові зображення, але в деяких випадках щоб підвищити складність застосовують також багатотоновий мікротекст. Під час ксерокопіювання окремі елементи мікрографіки (мікротексту) втрачаються, і це дозволяє відрізнити справжні документи від підроблених. Приклад трансформованого (збільшеного) мікротексту наведено на рис. 2.4.

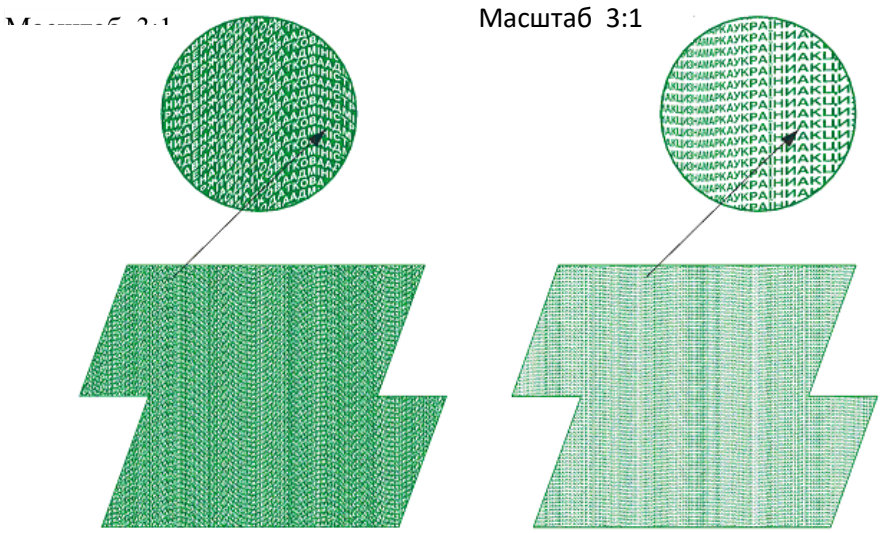


Рисунок 2.4 – Трансформований негативний та позитивний мікротекст

6. Скриті (приховані) елементи – це друковані елементи, які візуалізуються за допомогою спеціальних приладів, методів тощо. До цієї групи відносять такі захисні елементи:

- *антисканерні* елементи – це зображення, побудовані за певними законами геометрії або надруковані з використанням спеціальних матеріалів та технологій, які запобігають відтворенню засобами оргтехніки. Приховані елементи, які мають складну геометричну сукупність, є невід'ємними атрибутами рамок, бордюрів, віньєток (рис. 2.5);
- *скриті* (латентні, «примарні» чи «фантомні») зображення – це зображення, замасковані іншими графічними об'єктами, які можна розпізнати тільки під визначеним кутом зору до світла. Ефект прихованого зображення полягає у тому, що якщо повернути аркуш паперу під визначеним кутом, то в ньому з'являються нові елементи. Зображення може бути створене з рівнобіжних, однакових по ширині ліній на передньому і задньому планах малюнка. Причому лінії переднього плану на зображенні будуть більш рельєфними, ніж лінії заднього плану. При звичайному освітленні передній і

задній план нічим не відрізняються один від одного, і тільки під певним кутом зору видно, що задній план світліший.

Суть методу прихованих зображень полягає в тому, що під час копіювання сигнальний напис, схований у фоновій сітці, проявляється яскравим кольором. Текст прихованого напису може бути довільним, але, як правило, це слова «КОПІЯ», «ДУБЛІКАТ», «ПІДРОБЛЕННЯ». Зображення має регулярний системний характер. На оригіналі прихований надпис виявити неможливо. Технологічно метод базується на специфічній поведінці растрової точки при офсетному способі друку (растрове зображення тангірної сітки, задане різновеликими крапками на першому етапі друкування, робить схований напис видимим. На другому етапі у процесі розтискування растрових точок приховане зображення зливається з тангіром і стає таким, що візуально не виявляється. Під час копіювання зображення проступає).

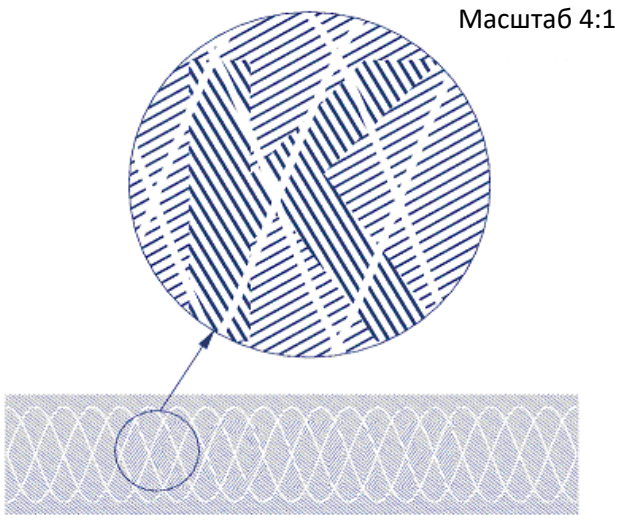


Рисунок 2.5 – Приховане зображення

Сучасні кольорові копіювальні апарати у змозі обійти «Void Pantograf», тому в одному виробі часто застосовують дві сітки «Void». Для такої комбінації можливість цифрової фальсифікації зменшується. Товщина ліній та випуклий рельєф, характерні для кольорового копіювального апарата, видадуть підробку. Більш сучасною модифікацією «Void Pantograf» є «Copy ban +». На відміну від аналога, ця захисна сітка має нерегулярну структуру, яку не в змозі «обійти» сучасні копіювальні апарати. Зазвичай захисний напис багаторазово повторюється в межах поля захисної сітки. Нерегулярна структура цієї сітки забезпечує проявлення прихованих написів хоча б в одному місці копії [5, 6].

7. Призматичний друк є випадком застосування тангірних двоколірних нерегулярних сіток із плавним переходом кольорів у межах зображення. Такий перехід не відтворюється копіюванням на ксероксі чи скануванням. Способом призматичного друку створюють багатоколірний пантографічний фон, який перешкоджає кольоровому ксерокопіюванню чи скануванню.

Об'єкти дослідження, обладнання, інструменти: програмне забезпечення Cerber, Adobe Illustrator, зразки захищеної поліграфічної продукції: бланки цінних паперів та державні папери, документарні бланки, квиткова продукція, лотерейна продукція, етикетко-пакувальна продукція тощо.

Хід роботи

1. Ознайомитися з програмами, за допомогою яких можна створювати графічні елементи: SecureDraw, Cerber v.3.0, Гравер, SecuriDesign 1.0, Barco Graphics, AestronDesign, HCC Security Graphics, SecuritySoft Co, Orell Fussli Security Documents AG, JSP Jura, або векторний редактор Adobe Illustrator. Встановити Cerber v.3.0.

2. Створити в Cerber v.3.0. або Adobe Illustrator макет захищеної поліграфічної продукції використавши наступні графічні елементи: гільйошні елементи, тангірні сітки, спеціальні лінійні растри, наскрізні та регістрові елементи, мікрографіка (мікротекст), скриті (приховані) елементи, призматичний друк.

**Самостійно обрати продукцію, яка потребує захисту графічними елементами.*

3. Вивести на друк.

4. Відповісти на контрольні запитання.

Контрольні запитання

1. Які види поліграфічної продукції потребують захисту графічними елементами? Перерахуйте.

2. Які основні графічні елементи застосовують для захисту поліграфічної продукції?

3. У чому різниця між гільйошними елементами та тангірними сітками?

4. Які існують різновиди гільйошних елементів?

5. Яке програмне забезпечення необхідно для створення гільйошних елементів?

6. З яких технологічних операцій складається процес створення гільйошних елементів?

3.3. Робота з комп'ютерного практикуму №3
ШТРИХОВЕ ТА QR КОДУВАННЯ ЗАХИЩЕНОЇ ДРУКОВАНОЇ ПРОДУКЦІЇ

Мета роботи: вивчення видів штрихового кодування, дослідження їх специфікації, виготовлення штрихового кодування за допомогою програмного забезпечення TechnoRiverStudio.

Теоретичні відомості

Штрих-код або штриховий код – графічна інформація, яка наноситься на поверхню, маркування і пакування виробів, що представляє можливість зчитування її технічними засобами – послідовність чорних і білих смуг або інших геометричних фігур. Штрихи в штрих-коді можуть бути і інших кольорів, головне, щоб ці кольори були контрастними, тому що сканери штрих-кодів розпізнають власне контрастні переходи від штриха до штриха. Технічно простіше і економічно вигідніше виготовляти чорно-білі штрих-коди, тому вони і набули такого поширення [6, 7].

Основною функцією штрих-кодів є автоматизація процесу ідентифікації товарів (штрих коди на товарах, пакуваннях, цінниках тощо). Однак, в даний час штрих код отримав застосування і в документообігу, інвентаризації, в системах контролю доступу.

Якщо говорити в загальному сенсі, то в штрих-код закодований ідентифікатор з бази даних, за яким можна запросити всю інформацію про об'єкт, на який нанесений відповідний штрих-код. Якщо немає доступу до бази даних, використовуваної при кодуванні об'єкта, то ідентифікатор є марним набором цифр і букв.

Види штрих-кодів

Штрихові коди бувають двох типів: лінійні та двомірні [8, 9].

Лінійними (звичайними) називаються штрих коди, які читаються в одному напрямку (по горизонталі). Лінійні символіки дозволяють кодувати невеликий об'єм інформації (до 20-30 символів, зазвичай цифр).

Двомірними називаються символіки, розроблені для кодування великого обсягу інформації. Розшифровка такого коду проводиться у двох вимірах (по горизонталі і по вертикалі).

Програми для створення штрих-кодів

Сьогодні можна знайти досить багато як платних, так і безкоштовних програм для створення штрих кодів різних видів. Більш того, існують онлайн-сервіси для генерації штрих-кодів.

Серед багатоцільових програмних пакетів можна виділити:

- Barcoder;

- Zoner Barcode Studio;
- Labeljoy;
- TechnoRiverStudio.

Генерування штрих-кодів є додатковою опцією таких програм як Corel Draw, PrintShop Mail та ін.

Об'єкти дослідження, обладнання, інструменти: програмне забезпечення TechnoRiverStudio, Adobe Illustrator, Adobe Photoshop, Microsoft Excel.

Хід роботи

1. Вивчити теоретичні відомості (п. 2).
2. Включити ПК. Перевірити чи встановлене програмне забезпечення на ПК (при необхідності встановити).
3. Виконати завдання, відповіді на питання внести до звіту.
4. Дослідити всі типи штрихового кодування в TechnoRiverStudio [10]. Вивчити технічні особливості даних штрих-кодів.
5. Створити в Adobe Illustrator, Adobe Photoshop, TechnoRiverStudio макет з дизайном довільної продукції, що вимагає персоналізації за допомогою змінного штрихового кодування.
6. Створити в Microsoft Excel базу даних для персоналізації (*як мінімум, 3 стовпчика, в перший з них, наприклад, ввести номера документу, в другий – цифрове представлення штрих-коду, в третій – прізвище власника документу*).
7. Підключаємо створену базу даних до програми TechnoRiverStudio *(File → Setup Database Connection → Add → Data Source Type → файл Microsoft Excel)*.
8. Розміщуємо дані із бази даних (*Database → [F1] ([F2, F3])*). Обираємо потрібний тип штрих-коду *(як мінімум, два – лінійний та двомірний)*.
9. Дати рекомендації щодо вибору типу штрих-коду. Які фактори впливають на вибір штрих-коду?
10. Здійснити узагальнений висновок проведеної роботи.

Контрольні запитання

1. Перерахувати всі види штрих-кодів. Описати їх основні технічні особливості.
2. Перерахувати фактори впливу на вибір виду штрих-коду.
3. Перерахувати методи генерування штрих-кодів. Пояснити принципи їх створення.
4. Вкажіть особливості штрихових кодів для книжково-журнальної та пакувальної продукції.
5. Опишіть вимоги до показників якості штрихових кодів.
6. Наведіть недоліки, які викликають спотворення елементів штрихових кодів в процесі друкування.

3.4. Робота з комп'ютерного практикуму № 4
ТЕХНОЛОГІЧНІ ПРОЦЕСИ НУМЕРАЦІЇ ТА ПЕРСОНІФІКАЦІЇ. ВНЕСЕННЯ ЗМІННОЇ ІНФОРМАЦІЇ В ДОКУМЕНТИ

Мета роботи: вивчити способи встановлення нумерації та персоніфікації ЦПДСО та внесення змінної інформації в документи.

Теоретичні відомості

Нумерація – це технологічний процес нанесення номерів на поліграфічні вироби. Нумерація має широку сферу застосування від друку рахунків, необхідних в бухгалтерії до друку цінних паперів та документів суворого обліку (ЦПДСО): паспорти різних видів, посвідчення, документи ДАІ та пенсійно-страхувальні документи, акції, сертифікати, дипломи, атестати, поштові марки. лотерейна та білетна продукція, етикеткова продукція. Нумерація документів необхідна для зручності, а й часто обов'язкова, згідно з вимогами податкових органів, оскільки ці документи форми суворої звітності. Нумерація захищає ЦПДСО від підробок. Нанесення номерів на етикетках, бланках спрощує контроль та облік документації. Нанесення серійного номеру на кожній банкноті, що дає можливість її ідентифікувати.

Кожен виріб має серію та окремий номер. Серію визначають найчастіше двома літерами чи цифрами, а номер може мати від 3 до 10 цифр. Алгоритм внесення номеру нумерації найчастіше задається формулою n + 1, де n – це початкова цифра, а кожна наступна збільшується на 1. Крім того, нумерація може бути в зворотній послідовності або через певний інтервал.

Наприклад, для акцизних марок, які виготовляють мільярдами штук, розроблено таку систему: акцизні марки повинні мати наскрізну нумерацію, яка складається з двох цифр індексу регіону (для України від 1 до 27), серії та окремого для кожної марки номера. Таку нумерацію наносять паралельно до довшої сторони марки. Нумерація акцизних марок, крім функцій саме захисту, дозволяє організувати їх облік. Нумерацію виконують високим друком фарбами, що проникають іншим кольором на зворотний бік марки.

Нумерацію виконують видимим, невидимим або видимим тільки в УФ-, ІЧ- діапазоні. Для нумерації багатотиражної продукції в сучасній поліграфії використовують такі технології: нумерацію з використанням механічних нумераторів на друкарських машинах високого друку, у т. ч. із застосуванням захисних фарб із різним механізмом захисту та методом механічної перфорації, нумерацію на фарбо-струминних друкарських машинах та нумерацію на лазерних нумераторах із синхронною перфорацією – пропалюванням – декількох сторінок документа [1, 9].

Персоналізація – це процес нанесення змінних даних на поліграфічні вироби або на паперову чи картонну упаковку.

При персоналізації можливе нанесення на кожний окремий екземпляр тиражу індивідуальних цифрових, текстових, ілюстраційних або графічних даних. Може бути нанесений унікальний серійний номер, штрих-код, QR-код, поштова адреса, ім’я одержувача, звернення до адресата у листі тощо. В основі технології персоніфікації лежить об'єднання інформації, запитуваної з бази даних і статичного шаблону.

Поліграфічна продукція персоналізується за допомогою цифрового друку, однак, якщо необхідний великий тираж, то оптимально буде використовувати комбінований друк – спочатку офсетним друкуються макет майбутньої продукції без змінних даних, після цифровим способом віддрукуються змінні дані в потрібному місці [2, 11].

Персоналізація підвищує рівень безпеки виданих документів, оскільки вона виключає можливість функціонування заготовок, тобто документів, які не пройшли персоналізацію. Крім того, застосовуються методи персоналізації, які тісно пов'язані з процесами виготовлення ЦПДСО.

Методи нанесення персоналізації:

1. Лазерний друк.
2. Термотрансферний (термосублімаційний) друк.
3. Лазерне гравіювання. Даний метод використовується в кольоровій гамі від чорного до сірого. Вигравірувана інформація не може бути видалена або змінена за допомогою механічних або хімічних методів, не залишаючи видимих ознак втручання. Лазерне гравірування не пов'язане з процесом виготовлення документа, тому для цього методу здійснюється персоналізація готових, раніше підготовлених бланків документів.

4. Прозоре лазерне гравіювання. Технологічний процес нанесення на поверхню документа прозорих, опуклих позначень у вигляді рядка цифр і символів. Нанесення знаків не погіршує читабельність документа при його щоденному використанні, оскільки ці символи прозорі. У той же час, це є ефективним елементом захисту, не вдаючись до використання спеціальних інструментів. Розробка застосовується в пластикових посвідченнях водія нового зразка, в модифікованому бланку посвідчення особи, а також в службових посвідченнях.

5. Технологія кольорової персоналізації. Дана технологія дозволяє розміщувати кольорову фотографію в структурі багатошарової пластикової карти. Розміщення кольорової фотографії на одному з шарів, а потім його інтеграція в структуру всієї карти, унеможливлює підробку документа без слідів видимого втручання.

Внесення змінної інформації в документи можна виконати за допомогою програмного забезпечення PrintShop Mail Suite [12]. При використанні даного продукту деякі елементи, наприклад зображення або текст, змінюються на

кожному новому друкованому аркуші на основі інформації з бази даних. Програма PrintShop Mail Suite оптимізує процес друку змінних даних за рахунок мінімального часу налаштувань і максимальної швидкості друку. PrintShop Mail Suite дозволяє об'єднувати різні формати шаблонів з різними базами даних і роздруковувати документи на будь-якому цифровому обладнанні.

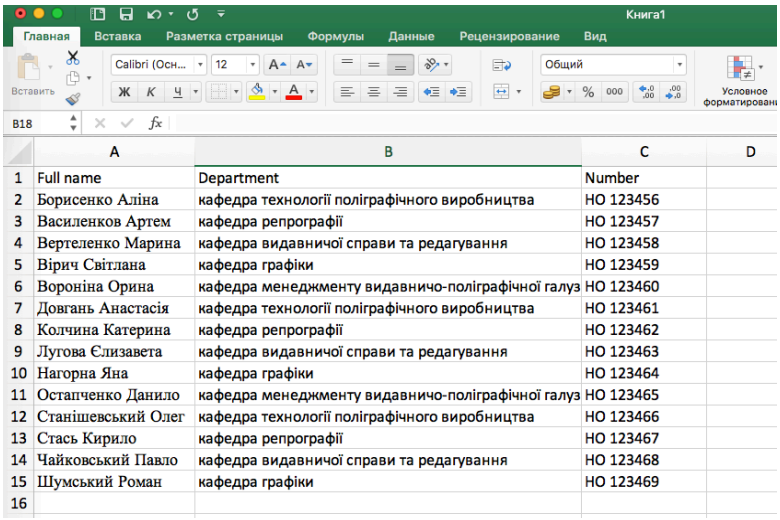
Об'єкти дослідження, обладнання, інструменти: програмне забезпечення PrintShop Mail, Adobe Illustrator, Adobe Photoshop, Microsoft Excel.

Хід роботи

1. Створити макет диплому форматом А4 (210х297 мм) в графічному редакторі та зберегти в форматі .pdf.

2. Створити базу даних в Microsoft Excel (програма PrintShop Mail підтримує файли Excel 2003 і нижче, в форматі .xls).

2.1. Створити новий файл Excel, задавши три стовпця, в першому – вказати прізвища та ім’я, в другому – назву кафедри, в третьому – шестизначні числа (рис. 4.1).



	A	B	C	D
1	Full name	Department	Number	
2	Борисенко Аліна	кафедра технології поліграфічного виробництва	НО 123456	
3	Василенков Артем	кафедра репрографії	НО 123457	
4	Вертеленко Марина	кафедра видавничої справи та редагування	НО 123458	
5	Вірич Світлана	кафедра графіки	НО 123459	
6	Вороніна Орина	кафедра менеджменту видавничо-поліграфічної галуз	НО 123460	
7	Довгань Анастасія	кафедра технології поліграфічного виробництва	НО 123461	
8	Колчина Катерина	кафедра репрографії	НО 123462	
9	Лугова Єлизавета	кафедра видавничої справи та редагування	НО 123463	
10	Нагорна Яна	кафедра графіки	НО 123464	
11	Остапченко Данило	кафедра менеджменту видавничо-поліграфічної галуз	НО 123465	
12	Станішевський Олег	кафедра технології поліграфічного виробництва	НО 123466	
13	Стась Кирило	кафедра репрографії	НО 123467	
14	Чайковський Павло	кафедра видавничої справи та редагування	НО 123468	
15	Шумський Роман	кафедра графіки	НО 123469	
16				

Рисунок 4.1 – Створення бази даних в Microsoft Excel

3. Відкрити програму PrintShop Mail, створити новий документ у PrintShop Mail, визначити формат аркуша: Меню - Файл - Параметри сторінки. Вказати формат паперу А4, орієнтація книжкова. Вставити розроблений макет диплому (файл шаблону документа, як на рис. 4.2): Меню - Вставити - Файл рисунка. Вставити

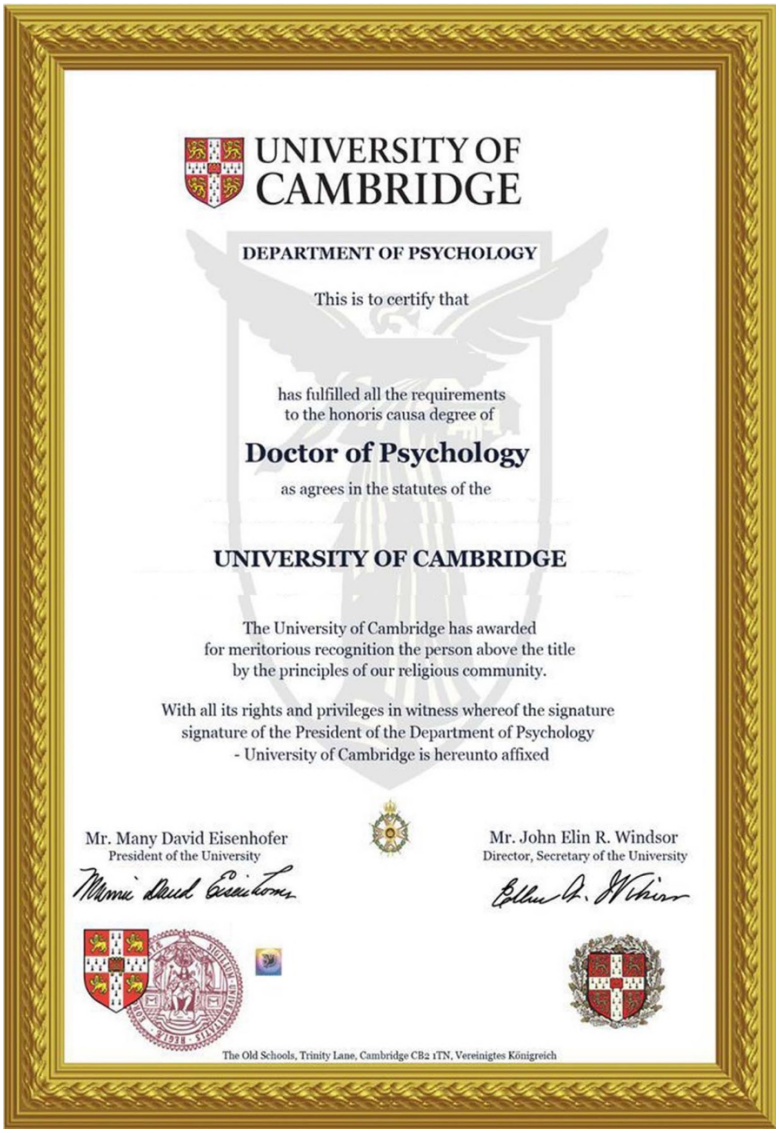


Рисунок 4.2 – Приклад шаблону документа

* На даному етапі можна зробити спуск полос, якщо планується виготовлення малоформатної друкованої продукції, як етикетки, білети, поштові марки тощо: Меню - Правка - Параметри - Повторювання. Можна встановлювати порядок виробу саме так, як потрібно: Повторення макетів - по вертикалі і горизонталі - цими цифрами виставляється кількість виробів на аркуші - 3 по вертикалі, 3 по горизонталі тощо, задається відстань між макетами та розділ пріоритетів (рис. 4.3).

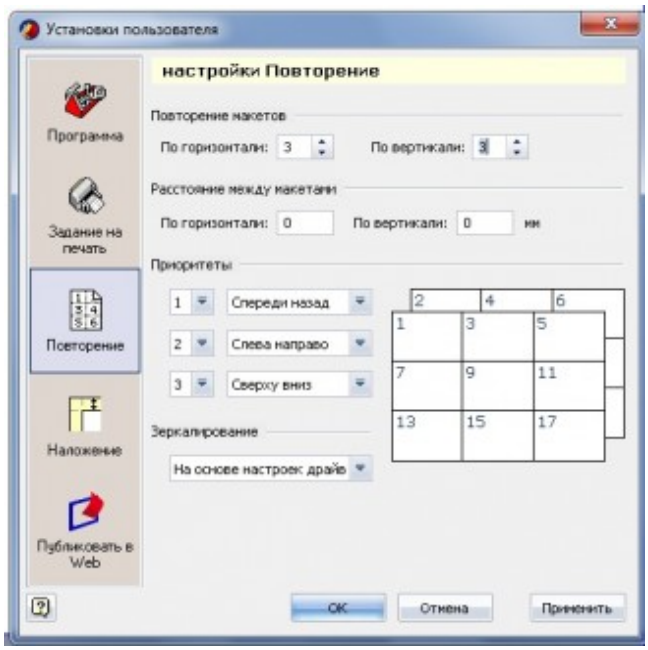


Рисунок 4.3 – Вибір параметрів спуску шпальт в програмі PrintShop Mail

3.1. Для встановлення персоналізації розробленому документу підключаємо базу даних: Меню - База даних - Відкрити. Відкриваємо файл Excel. Він відкриється на екрані праворуч. Для зручності збільшуємо масштаб, і звертаємо увагу на віконце в нижньому правому куті: Вкладка Макети, де можна побачити вставлені макети для персоналізації. У вашому файлі там тільки один макет диплом.pdf. Відкрити вкладку - Поля даних, де вказано список всіх ваших змінних даних. Їх кількість повинна збігатися з кількістю стовпців в Microsoft Excel. У даному макеті тільки три зміні, тому саме їх беремо і перетягуємо правою кнопкою миші на макет, так званий принцип Drag & Drop. Переносимо в потрібні місця шаблону документа (див. рис. 4.4) тільки перший рядок, назву стовпця (Прізвище, Назва кафедри, Номер).

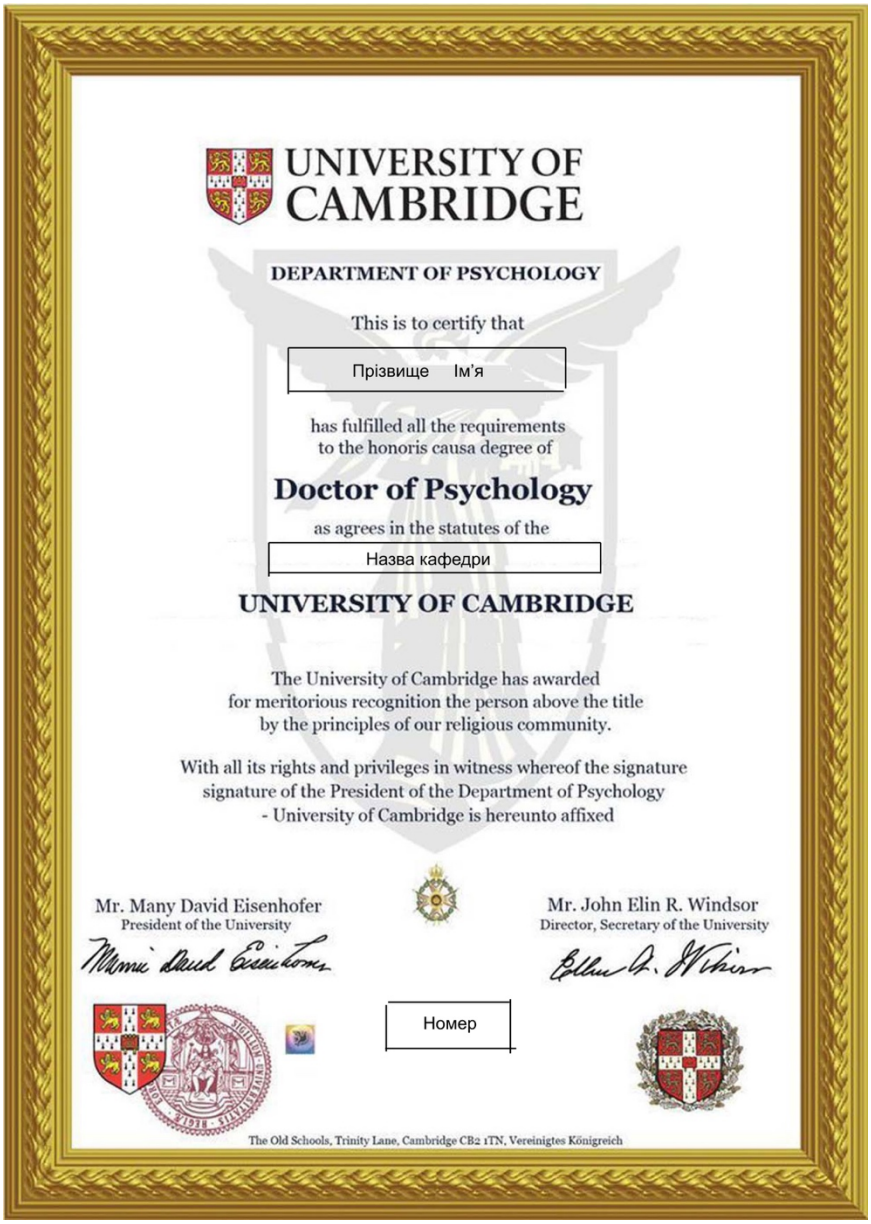


Рисунок 4.4 – Приклад віконців із внесенням змінних даних

3.2. Виділяємо вставлений об'єкт, працюємо з ним як зі звичайним текстовим об'єктом, вибираємо гарнітуру та кегль шрифта, вирівнюємо на сторінці, ставимо в потрібне місце в макеті.

4. Макет зі внесеними змінними даними готовий до друку, стрілочками знизу можна перегорнути всі задані данні або подивитись Print Preview.

Контрольні запитання

1. Поясніть, що таке нумерація та персоніфікація?
2. Наведіть приклади захищеної продукції, де вони зустрічаються.
3. Вкажіть можливості програмного забезпечення PrintShop Mail. Яким чином відбувається внесення змінних даних у документ?

4. Список літератури

1. Киричок П.О. Методи захисту цінних паперів та документів суворого обліку / П.О. Киричок, Ю.М. Коростіль, А.В. Шевчук. – К.: НТУУ „КПІ”, 2008. – 368 с.

2. Киричок Т. Ю. Зносостійкість банкнотної продукції : монографія / Т. Ю. Киричок. – К. : НТУУ «КПІ», 2014. – 308 с.

3. ДСТУ 4010-2001. Бланки цінних паперів і документів сурового обліку та звітності. Загальні технічні вимоги.

4. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Державний стандарт України. Чинний від 01.07.1997 р.

5. Технології захисту цінних паперів [Текст] : навч. посіб. / В. Й. Запоточний ; Нац. ун-т «Львів.політехніка». – 2-ге вид., допов. – Л. : Вид-во Львів. політехніки, 2013. – 152с.

6. Коншин А. А. Защита полиграфической продукции от фальсификации, 1999. М.: Синус, 1999. – 160 с.

7. Van Renesse R. L. Optical document security / R. L. van Renesse. – Third edition. – Boston–London : Artech House, 2005. – 368 p.

8. Лазаренко Е.Т. Захист друкованої продукції / Е.Т. Лазаренко, В.З. Маїк, А.В. Шевчук, С.В. Жидецький. – Л.: УАД, 2007. – 104 с.

9. Дичка І. А. Зберігання інформації у вигляді багатокольорових штрихових кодів та їх обробка. – Київ: ІВЦ «Видавництво «Політехніка», 2003. – 340 с.

10. Інформаційний портал technoriversoft [Электронный ресурс]. – Режим доступа:https://www.technoriversoft.com/products.html

11. Дурняк Б. В. Інформаційна технологія формування графічних засобів захисту документів / Б. В. Дурняк, В. З. Пашкевич, В. І. Сабат, О. В. Тимченко. – Львів : Вид-во Української академії друкарства, 2011. – 152 с.

12. Інформаційний портал printshopmail [Электронный ресурс]. – Режим доступа: https://printshopmail.objectiflune.com.

Додаток А

Приклад оформлення титульного аркуша

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Видавничо-поліграфічний інститут
Кафедра технології поліграфічного виробництва

Комп'ютерний практикум

Робота з комп'ютерного практикуму № 1
з дисципліни «Захист інформації в поліграфії»

«_____»

Виконав студент групи _____
_____

Перевірив
_____

КИЇВ – 20__