УДК 004.93

РОЗРОБЛЕННЯ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Євдокимов Сергій

Науковий керівник: доктор педагогічних наук, професор Шерман М.І.

Херсонський державний університет, м. Херсон, Україна

У статті досліджено можливості використання засобів захисту інформації для виявлення несанкціонованого втручання в роботу електронного документообігу та запобігання витоку інформації в локальній мережі, також для використання вирішення ряду інших завдань, які пов'язані з контролем дій персоналу. В ході роботи, розроблений алгоритм шифрування даних, на основі якого використовуються ключі на основі сучасної криптографії. З огляду на це, дане дослідження характеризується актуальністю. Для досягнення зазначеної мети вивчалася література з електронного документообігу, комп'ютерних систем, мов програмування: Python, C Sharp.

Ключові слова: система захисту інформації, конфіденційна інформація, моніторинг витоків, мережевий екран, алгоритм шифрування, несанкціонований доступ, штучні нейронні мережі.

Development of information security tools for electronic document management systems

S. Yevdokymov

Scientific supervisor: Doctor of Pedagogical Sciences, Professor

Sherman M. I.

Kherson State University, Kherson, Ukraine

The article examines the possibilities of using information security tools to detect unauthorized interference in the operation of electronic document management and prevent information leakage in the local network, as well as to use the solution of a number of other tasks related to monitoring the actions of personnel. In the course of the work, a data encryption algorithm was developed, on the basis of which keys based on modern cryptography are used. Given this, this study is characterized by relevance. To achieve this goal, we studied literature on electronic document management, computer systems, programming languages: Python, With Sharp.

Keywords: information security system, confidential information, leak monitoring, network screen, encryption algorithm, unauthorized access, artificial neural networks.

Сьогодні, будь-яка установа чи підприємство зацікавлені у збереженні інформації, тому потребує необхідного програмного забезпечення для локальній мережі, так як інформація яка знаходиться в документообігу – як правило, важливі договори, списки клієнтів, бази даних бухгалтерських програм, паролі і ключі системи "клієнт-банк", канали зв'язку з підрозділами та ін., що може становити інтерес для зловмисника, наприклад, для продажу цієї інформації у всесвітній мережі «DarkNet», «Deep Web», чи використання цієї

інформації для доступу до банківських рахунків, можливості зламу сайтів та використання цієї інформації для рефайлінгу або навіть дані будуть знищені в особистих цілях, але зазвичай – в політичних. Для державних установ така інформація носить гриф "Таємно", для комерційних підприємств –"Комерційна таємниця" або "Цінна інформація" [1].

На локальному рівні загроз інформаційної безпеки (наприклад, для приміщень, які вони займають установою, організацією, підприємством) виділяють канали витоку інформації, під якими розуміють – сукупність джерел інформації, матеріальних носіїв або середовища поширення несучих цю інформацію сигналів і засобів виділення інформації з сигналів або носіїв [2]. Об'єктивне існування даних каналів витоку передбачає їх можливе використання зловмисниками для несанкціонованого доступу до інформації, її модифікації, блокування та інших неправомірних маніпуляцій, тобто наявність каналів витоку інформації впливає на обрання способу вчинення злочину [1].

Типові види інформації, що містяться в переліку конфіденційної інформації:

- перелік конфіденційної документації;
- персональні дані співробітників;
- перелік ПІБ співробітників;
- електронні ключі.

Надалі, при використанні системи контролю та захисту електронного документообігу, відповідальна особа за безпеку інформації в середині підприємства використовує даний перелік для задання необхідних правил та шаблонів цих систем з використанням методів, розглянутих вище. Канали витоку інформації – це методи та шляхи витоку інформації з інформаційної системи. Відіграють основну роль у захисті інформації, як фактор інформаційної безпеки [3]. Велика частина витоків інформації, реалізованих в середині підприємства,що пов'язана з особистою користю і характеризується більш вузькою зоною інтересу і, отже, значно меншими обсягами викрадених даних.Зокрема, більшість витоків проводяться через мережу підприємства.

Тому, постає необхідність розробки таких засобів для системи захисту інформації, що обумовлювало би можливу вразливість локальної мережі від несанкціонованого доступу та втручання в роботу електронного документообігу [2].

Метою даного дослідження є розробка і реалізація політики безпеки в локальній мережі, до прикладу взяту мережу державної установи ЗВО.

Для досягнення зазначеної мети необхідно виконати ряд завдань:

- виявлення можливих джерел загроз об'єктів атаки в мережі ЗВО;
- проектування політики безпеки корпоративної мережі;
- розробка комплексу заходів щодо захисту інформації в мережі;
- аналіз ефективності реалізації політики безпеки в мережі підприємства.

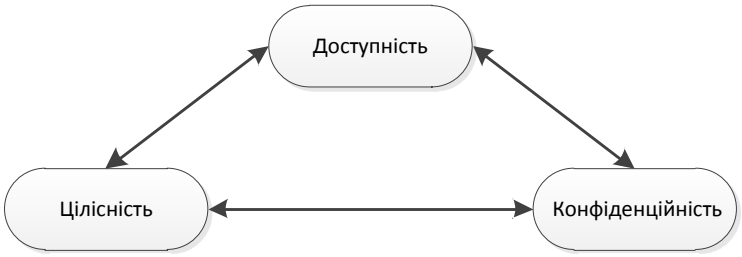

Рис. 1. Основні вимоги до безпеки мережі будь-якого підприємства

Безперервний контроль над роботою локальної мережі, нині складової основу будь-якої корпоративної мережі, необхідний для підтримки її в постійному працездатному стані [4]. Контроль – це головний етап, який повинен виконуватися при управлінні мережею в першу чергу. Використання автономних засобів контролю допомагає адміністратору мережі виявити проблемні ділянки і влаштування мережі, а їх відключення або реконфігурацію він може виконувати в цьому випадку вручну [5]. Специфікація програмного модуля складається з функціональної специфікації модуля, яка описує семантику функцій, які виконуються цим модулем по кожному з його входів, і синтаксичної специфікації його входів, що дозволяє побудувати на використовувану мову програмування синтаксично правильне звертання до

нього. Функціональна специфікація модуля визначається тими ж принципами, що та функціональна специфікація програмної системи (Рис. 2).

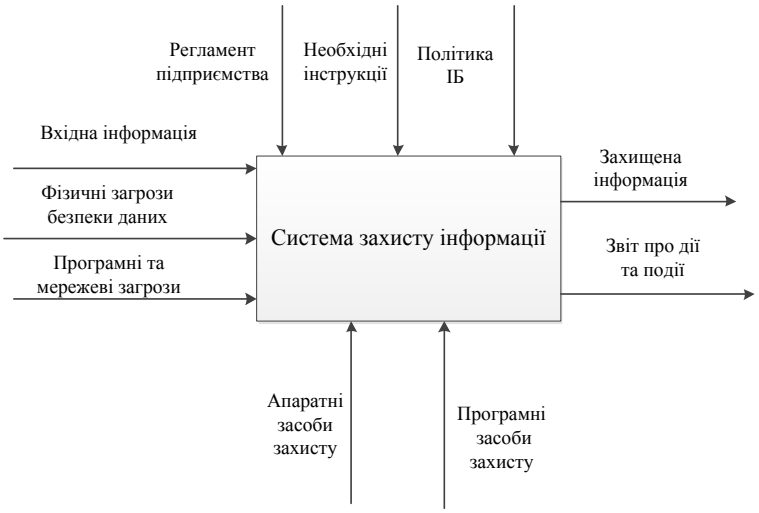

Рис. 2. Специфікація процесів системи

За даними клієнта системи, менеджера здійснюється пошук в базі користувачів, визначаючи його за категоріями. За визначеною категорією відповідно встановлюється повноваження, які будуть надаватись клієнту (користувачу) системи. Далі – здійснюється процедура доступу до системи, що перевіряє відповідність ім'я, пароль, логін та додаткові дані, зазначні адміністратором системи, для доступу в систему чи відповідно до електронно-обчислювальної машини на якому вона встановлена. Для користувача формується набір дозволених дій, об'єднуючи інформацію на повноваження та рівні доступу до системи, чи дією з відповідною документацією. Тому, визначення рівня доступу до системи мє бути, як показано на рис. 3.

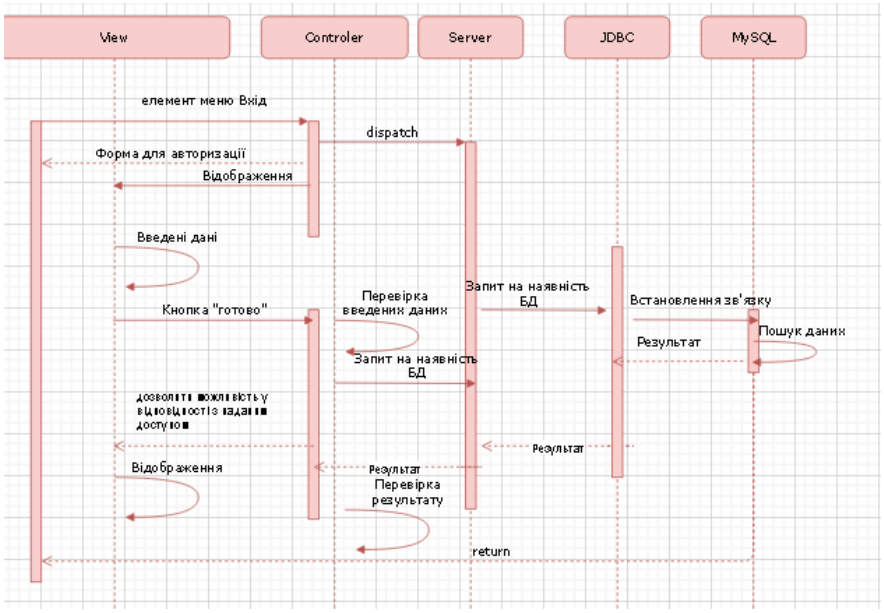

Рис.3. UML-діаграма станів

Зокрема, в подальшому, процес пошуку та тестувань на виявлення уразливих точок доступу до локальної мережі вищевказаної організації було здійснено за допомогою різних програм, в тому числі «Armitage» (графічний інструмент управління кібератакою), «nmap» (сканер портів), Wireshark (аналізатор трафіку) [6], брутфорс паролів «John the Ripper, Aircrack-ng» (програмний пакет для тестування локальних мереж), та «routerscan»(вміє знаходити і визначати різні пристрої з великого числа відомих роутерів / маршрутизаторів, отримує з них корисну інформацію, зокрема характеристики мережі).

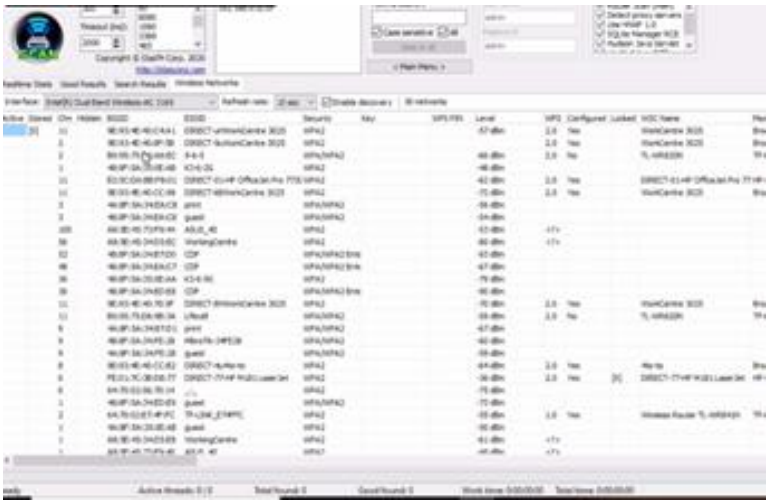

Рис. 4. Робота в додатку «Router Scan»

Всі вищевказані додатки були встановленні на ОС «Kali Linux» та при неодноразовому моніторингу внутрішньої мережі державної установи ЗВО

були отримані результати які в подальшому, використані для розробки ПЗ щодо захисту цієї мережі, використовуючи в подальшому – можливість застосування нейронних мереж.

Програма написана мовою програмування «C Sharp» та «Python» на основі розробленого алгоритму для Windows додатків, визначених політиками інформаційної безпеки. Проаналізовано можливості роботи даної системи для підприємства. Проведені експерименти показали високу ефективність даного підходу при вирішенні завдань обмеження несанкціонованого доступу до конфіденційної інформації.

Програмне забезпечення написане мовою програмування C# та Python на основі розробленого алгоритму для Windows додатків, визначених політиками інформаційної безпеки. Криптографічний алгоритм RSA (з англ. **R**ivest, **S**hamir та **A**dleman) був реалізований на формах, які інтегровані з програмуванням для Windows і використовують компонентну технологію. Крім того, C Sharp забезпечує ефективну і не витратну за часом розробку без необхідності писати вставки на C# або займатися написанням коду вручну (хоча це можливо). Проаналізовано можливості роботи даної СЗІ для підприємства. Проведені експерименти показали високу ефективність даного підходу при вирішенні завдань обмеження несанкціонованого доступу до конфіденційної інформації.

Для шифрування даних застосовується наступний код, написаний на мові Python на середовищі Microsoft Visual Studio 2019. Код програми:

```
# Зашифруем файл и записываем его
f = Fernet(key)
if ent1.get().split('.')[1] == 'docx':

    doc = docx.Document(ent1.get())
    ff = open(ent1.get().split('.')[0]+'.txt','w',encoding='utf-8')
    all_paras = doc.paragraphs
    text = ''
    for i in all_paras:
        text += i.text + '\n'
        text = (text)
    ff.write(text)
    ff.close()
```

```
        # Зашифровать данные
```

Приклад функції *CancelPrintJob*, що скасовує роботу принтера, застосований наступний код (C#):

```
public bool Cancel_PrintJOB(int PrintJobId1, string Print_Name)
{
    bool Action_Performed = false;
    string SearchQuer = "SELECT * FROM Win_PrintJOB";
    ManagementObjectSearcher PrintSearchJOB = new ManagementObjectSearcher(searchQuery);
    ManagementObjectCollection PrintJOB_Collect = PrintSearchJOB.Get();
    foreach (ManagementObject PrintJOB in PrintJOB_Collect)
    {
        string NAME_JOB = PrintJOB.Properties["Name"].Value.ToString();
        char[] ListARR = new char[] { ',' };
        string jobPrinterName = NAME_JOB.Split(ListARR)[0];
        int JOB_ID = Convert.ToInt32(NAME_JOB.Split(ListARR));
        string documentName = PrintJOB.Properties["Document"].Value.ToString();
        if (jobPrinterName == Print_Name)
        {
            PrintJOB.Delete();
            Action_Performed = true;
            break;
        }
    }
    return Action_Performed;
```

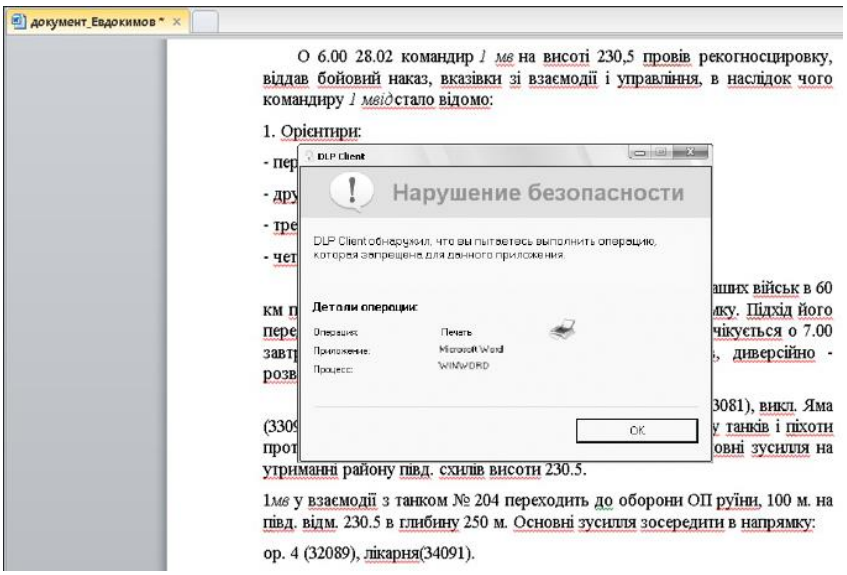

Рис. 5. Повідомлення про блокування файлу на друк

Для ІТ-відділів і фахівців з інформаційної безпеки запропонований програмний продукт дозволяє поглянути на задачу контролю над діями з конфіденційними документами, мінімізувати недоліки на рівні технології. [7].

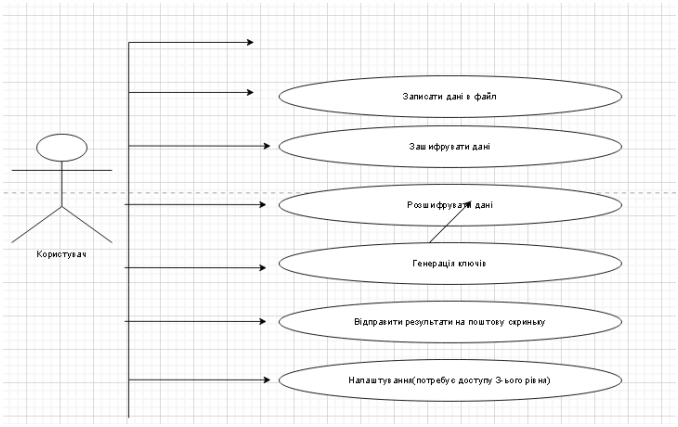

Рис. 6. Діаграма варіантів використання

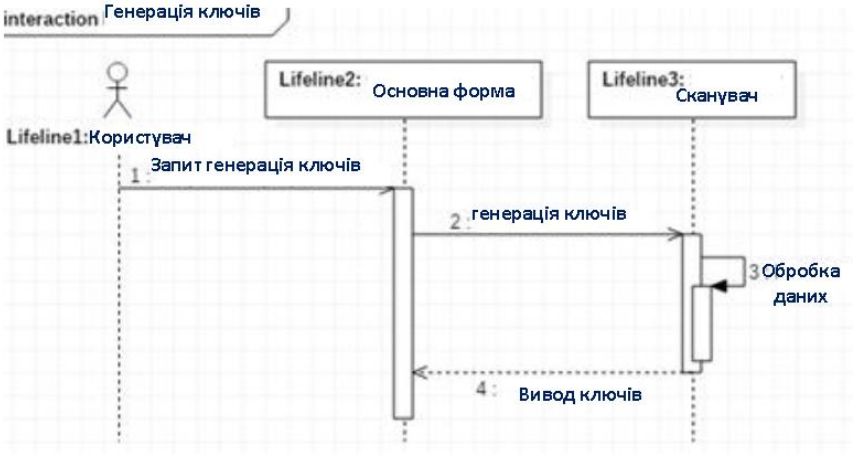

Рис.7. Блок-схема «Генерація ключів»

Тестування даного програмного продукту показало, що програмне забезпечення успішно справляється з поставленими перед ним задачами щодо захисту інформації в локальній мережі установи. Для ІТ-відділів та фахівців з інформаційної безпеки запропонований програмний продукт дозволяє поглянути на задачу контролю над діями з конфіденційними документами, мінімізувати недоліки на рівні технології.

Коли виникає необхідність забезпечити інформаційну безпеку компанії, керівництво, як правило, звертається до системних інтеграторів. Вони проводять комплексний аналіз і розробляють проект із захисту інформації. В остаточному підсумку це обертається купівлею дорогих програмних та

апаратних засобів, таких як Cisco PIX, Checkpoint, Microsoft ISA. Такі великі комплексні проекти коштують більше 15 тис. доларів [6;7]. Не є виключенням те, що доведеться з часом модифікувати з урахуванням вимог безпеки деякі протоколи програми, але на сьогодні – досить ефективний спосіб для застосування на фоні інших програмних продуктів [7].

Удосконалення процесу документообігу за допомогою впровадження електронної бази даних вже охопило низку державних структур, і стає все більш необхідним у вищих навчальних закладах [7; 8]. У перспективі розглядається можливість розробки спільних рекомендацій щодо захисту інформації електронного документообігу для подібних організацій, заводів, установ, та створення типової інструкції щодо забезпечення безпеки інформації в системах обробки даних. Проведене дослідження в перспективі відкриває можливості створення компактних, швидкодіючих та енергонезалежних систем штучного інтелекту. Зокрема, в подальшому постає необхідність в розробці алгоритму штучних нейронних мереж, які будуть більш детально і краще посилювати швидкість розпізнання образів мережевого екрану СЗІ та якість програмного забезпечення вказаного в даному дослідженні.

Список літератури

1. Євдокимов С.О., Лукьянчиков С.Д. Актуальні проблеми кібербезпеки автоматизованої банківської системи // Інформаційні технології в моделюванні: науковий журнал / за ред. Сергія Устенка. – № 1 (5), квітень 2018. – Миколаїв: МНУ імені В.О. Сухомлинського, 2018. С. – 120 с.
2. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб.: Питер, 2016. — 992 с.: ил. — (Серия «Учебник для вузов»).
3. Філоненко, С. Ф. Система попередження витоку персональних даних мережевими каналами [Текст] / С. Ф. Філоненко, І. М. Мужик, Т. В. Німченко // Ukrainian Scientific Jornal of Information Security. — 2014. — Vol. 20, № 3. — P. 279–285.
4. Саидерс, Крис., Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях, 3-е изд. : Пер. с англ. - СПб. : ООО "Диалектика", 2019 - 448 с. : ил. - Парал. тит. англ.
5. Євдокимов С.О., Устенко С.А. . Розробка системи захисту інформації в локальній мережі підприємства // Геометричне моделювання та інформаційні технології: науковий журнал / за ред. Сергія Устенка. – № 1 (7), квітень 2019. – Миколаїв: МНУ імені В.О. Сухомлинського, 2019. С. – 103 с.
6. Шерман М.І., Степаненко Н.В. Електронний документ як об’єкт інформаційної діяльності посадової особи органів місцевого самоврядування/ Державна політика щодо місцевого самоврядування: стан, проблеми та перспективи : збірник матеріалів конференції / за заг. ред. Ю.М. Бардачова, І.П. Лопушинського, О.А. Тертишної. – Херсон: Олді-плюс, 2012. – с. 185-186

7. Шерман М.І. Навчальна дисципліна «Електронний документообіг та захист інформації» як складова системи формування комп'ютерно-інформаційної компетентності магістрів державної служби/ Інформаційні технології в освіті: Збірник наукових праць. Випуск 15. – Херсон: ХДУ, 2013. – С. 96-102

8. Несторенко Т.П. Роль електронного урядування в розвитку інституціональної інфраструктури міста: вітчизняний та зарубіжний досвід. Зб. матеріалів Всеукраїнської конференції „Інформаційні технології та розвиток місцевого самоврядування". Чернівці: ДрукАрт, 2008. 15-17 грудня 2008. – С.62-69.