УДК 004.75+004.4 DOI: 10.33310/2524-0978-2019-1-7-20-25

Сергій ЄВДОКИМОВ
serge.evdokimov2015@gmail.com
ORCID: 0000-0001-7213-0259
Сергій УСТЕНКО
ustenko.s.a@gmail.com
ORCID: 0000-0003-4968-1233
м. Миколаїв

РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ МЕРЕЖІ ПІДПРИЄМСТВА

Сьогодні постає необхідність правильно обирати засоби і заходи забезпечення захищеності інформації від несанкціонованого до неї доступу. У цій роботі пропонуються можливість використання найбільш ефективної та перспективної архітектури DLP-системи для захисту даних від сучасних загроз в локальній мережі підприємства. Сучасні системи DLP (англ. Data Leak Prevention) – це технології, за допомогою яких можна запобігти витоку з підприємства саме конфіденційної інформації, а також можна використовувати для вирішення ряду інших завдань, наприклад, пов'язаних з контролем дій персоналу.

З урахуванням вищевказаного, зрозуміло, що цим обумовлюється затребуваність і актуальність сучасних DLP-систем для будь-якого підприємства.

Проаналізовано можливість використання DLP-системи для захисту інформації у локальній мережі підприємства. Розроблено програму для виконання моніторингу системних подій у додатках, визначених політиками інформаційної безпеки.

***Ключові слова**: локальна мережа, DLP-система, системи захисту даних, заходи безпеки інформації, цілісність інформації.*

Постановка проблеми

Витоки інформації з підприємств перетворюються сьогодні в одну з найбільш серйозних загроз для інформаційної безпеки. Різноманіття загроз породжує різноманіття методів захисту.

Судячи зі зростаючої кількості публікацій компаній, які професійно займаються захистом інформації в комп'ютерних системах, вирішення цього завдання надається велике значення [1]. Зокрема, для їх вирішення пропонується програмний продукт, створений для запобігання витоку конфіденційної інформації за межі корпоративної мережі (рис. 1). Будується система на аналізі потоків даних, що особливо перспективний для локальної мережі підприємства.

Захист даних – це комплекс заходів, які проводять з метою запобігти витоку інформації, яка захищається, а також несанкціонованих дій з інформацією [2, стр. 13]. Захист інформації в локальних мережах (з англ. Local Area Network, LAN), об'єднання певного числа комп'ютерів на відносно невеликій території, має низку специфічних особливостей, пов'язаних з тим, що інформація може легко і швидко копіюватися та передаватися по каналах зв'язку [3, стр. 28].

Відомо, що розголошення або витік інформації здійснюється від джерела інформації через середу до зловмисника. Джерелами інформації можуть бути: люди, документи, вироби, системи обробки інформації, відходи. Носієм інформації може бути або поле (електромагнітне, акустичне), або речовина (папір, матеріал, виріб і т.д.). Середовищем є повітряний простір, жорсткі середовища (стіни, комунікації).

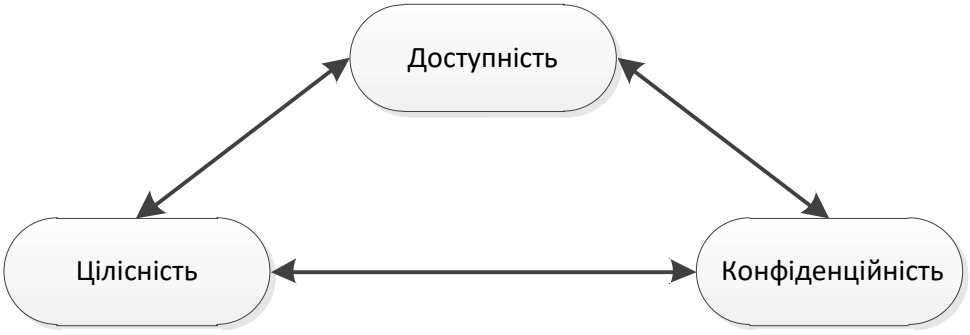

Рис. 1. Основні вимоги до безпеки мережі будь-якого підприємства

Аналіз останніх досліджень і публікацій

Небачені раніше «інформаційні катастрофи» дають уявлення про те, які жахливі обсяги даних можуть бути викрадені з використанням сучасних технологій і до яких наслідків це може призвести.

За останній час проблема витоків інформації з самих різних комерційних та некомерційних підприємств стають фактично щоденними. Наприклад, в березні 2019 року Компанія Tesla подала два судових позови проти п'ятьох колишніх співробітників, звинувачуючи їх в передачі конфіденційної інформації конкуруючим компаніям. Про це пише портал TechCrunch [4]. Ще один випадок, медичний університет Вашингтона повідомив про велику кількість витоку даних пацієнтів. Витік захищеної інформації майже мільйона пацієнтів, включаючи імена і медичні записи, трапилася в грудні 2018 року [5].

В результаті загрози витоку конфіденційної інформації та несанкціонованого доступу до даних входять до числа критичних проблем сучасності, а для протистояння їм пропонуються в тому числі кошти запобігання витоку даних (Data Leak Prevention, DLP). У зв’язку з постійним зростанням потреб у застосуванні.

Постановка завдання

Сьогодні DLP-системи значно розширили коло розв'язуваних завдань, які постійно розвиваються.

Для створення системи захисту інформації в локальній мережі необхідно проаналізувати потоки інформації, які будуть циркулювати всередині неї. Також бажано по можливості мінімізувати витрати на реалізацію даного проекту, але в той же час намагатися не нехтувати якістю використовуваних матеріалів і устаткування.

Мета даної роботи – розробка DLP-системи захисту інформації для локальної мережі підприємства та підготувати проект програмного засобу для захисту мережі від зовнішніх загроз, яка буде вирішувати наступні завдання:

– налаштування політики безпеки в локальній мережі;

– захист інформації від витоку шляхом контролю виведення даних на друк;

– блокування спроб пересилання/ збереження конфіденційних даних;

– відстеження даних у використанні та генерування попереджувальних повідомлень у разі порушення політик безпеки;

– запобігання витокам інформації шляхом контролю життєвого циклу і руху конфіденційних відомостей.

Тому – актуальне завдання створення систем захисту конфіденційних даних від

несанкціонованої передачі і використання. Такі системи повинні виконувати моніторинг системних подій, аналізувати використовувані дані, на предмет їх конфіденційності і, за деяких умов, виконувати дії певні в політиках інформаційної безпеки.

Виклад основного матеріалу

На території підприємства основними джерелами інформації є люди і документи. В якості носіїв інформації істотно переважають паперові, але в той же час робляться активні спроби інформатизації робочого процесу підприємства, в тому числі введення електронного документообігу. Використання паперових носіїв інформації до певної міри ускладнює збір та обробку інформації, але з іншого боку робить її менш вразливою для зловмисника, враховуючи той факт, що кошти програмно-апаратного захисту електронних носіїв не впроваджено в повному обсязі і на належному рівні [4].

Весь потік інформації, що циркулює всередині підприємства можна класифікувати наступним чином:

– інформація юридичного характеру (накази, статути, договори);

– інформація фінансового характеру (бухгалтерська документація, рахунки, уявлення, платіжні доручення, зарплатні відомості і т.д.);

Захист конфіденційної інформації включає в себе організаційні заходи з пошуку і класифікації наявних в компанії даних. У процесі класифікації дані поділяються на 3 категорії:

– секретна інформація;

– інформація для службового користування;

– загальнодоступна інформація.

Захист конфіденційної інформації за допомогою розробленого програмного забезпечення для моніторингу мережі заснована на використанні функціоналу і технологій системи із захисту даних від витоків. До складу DLP-системи входять два типи модулів: хост модуль і мережний модуль.

Хост модулі встановлюються на робочі станції користувачів і забезпечують контроль дій, вироблених користувачем щодо класифікованих даних (конфіденційної інформації).

Мережний модуль здійснює аналіз інформації, що передається по локальній мережі і контролює трафік виходить за межі інформаційної системи. У разі виявлення в переданому трафіку конфіденційної інформації мережний модуль присікає передачу даних [3].

Структура DLP-системи має клієнтську та серверну архітектуру (рис. 2).

Створений програмний продукт побудований на базі архітектури DLP-системи. Реалізовано функції моніторингу системних подій в операційній системі Windows на прикладі платформи JVET Framework і мови програмування C #.

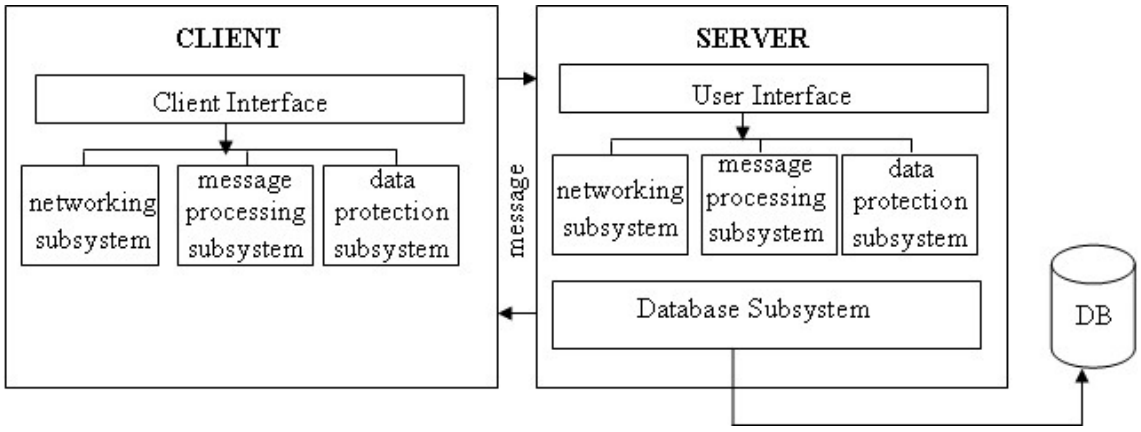

Рис. 2. Структура DLP-системи

Розроблена система захисту поєднує в собі набір технологій запобігання витоку даних по локальних каналах. У серверному додатку формуються політики безпеки, в яких зазначається ім'я виконуваного файлу програми та дії, що застосовуються при виконанні операцій з буфером обміну. Клієнтський додаток працює у фоновому режимі, виконуючи моніторинг системних подій.

Проаналізуємо, результати роботи розробленого програмного продукту на прикладі захисту інформації від витоку шляхом контролю виведення даних на друк:

Для блокування можливості друку документів додаток повинен відслідковувати чергу принтера і скасовувати її. Реалізувати ці функції можна за допомогою технології WMI, Місце властивостей об'єктів WMI називається репозиторієм і розташоване в системній папці операційної системи Windows: `%SystemRoot%\System32\WBEM\Repository\FS`

Оскільки WMI побудований за принципами ООП, то всі дані операційної системи представлені у вигляді об'єктів, їх властивостей та методів. Приклад скасування роботи принтера, що здійснюється шляхом виклику методу *Delete* для об'єкта зі списку поточних робіт. Приклад функції *CancelPrintJob*, що скасовує роботу принтера, показаний у лістінгу 1.

Висновки і перспективи досліджень

На закінчення хотілося б підкреслити, що ніякі апаратні, програмні і будь-які інші рішення не зможуть гарантувати абсолютну надійність і безпека даних у комп'ютерних мережах. У той же час звести ризик втрат до мінімуму можливо лише при комплексному підході до питань безпеки [6].

На основі DLP-системи та розробленого оригінального алгоритму створена нова програма для виконання моніторингу системних подій Windows в додатках, визначених політиками інформаційної безпеки. Проведені експерименти показали високу ефективність даного підходу при вирішенні завдань обмеження несанкціонованого доступу до конфіденційної інформації. Для IT-відділів і фахівців з інформаційної безпеки запропонований програмний продукт дозволяє поглянути на задачу контролю над діями з конфіденційними документами, мінімізувати недоліки на рівні технології.

Лістінг 1

```
public bool Cancel_PrintJOB(string Print_Name, int printJobId)
{
    bool Action_Performed = false;
    string searchQuery = "SELECT * FROM Win32_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)[1]);
        string documentName = PrintJOB.Properties["Document"].Value.ToString();
        if (jobPrinterName == Print_Name)
        {
            PrintJOB.Delete();
            Action_Performed = true;
            break;
        }
    }
    return Action_Performed;
}
```

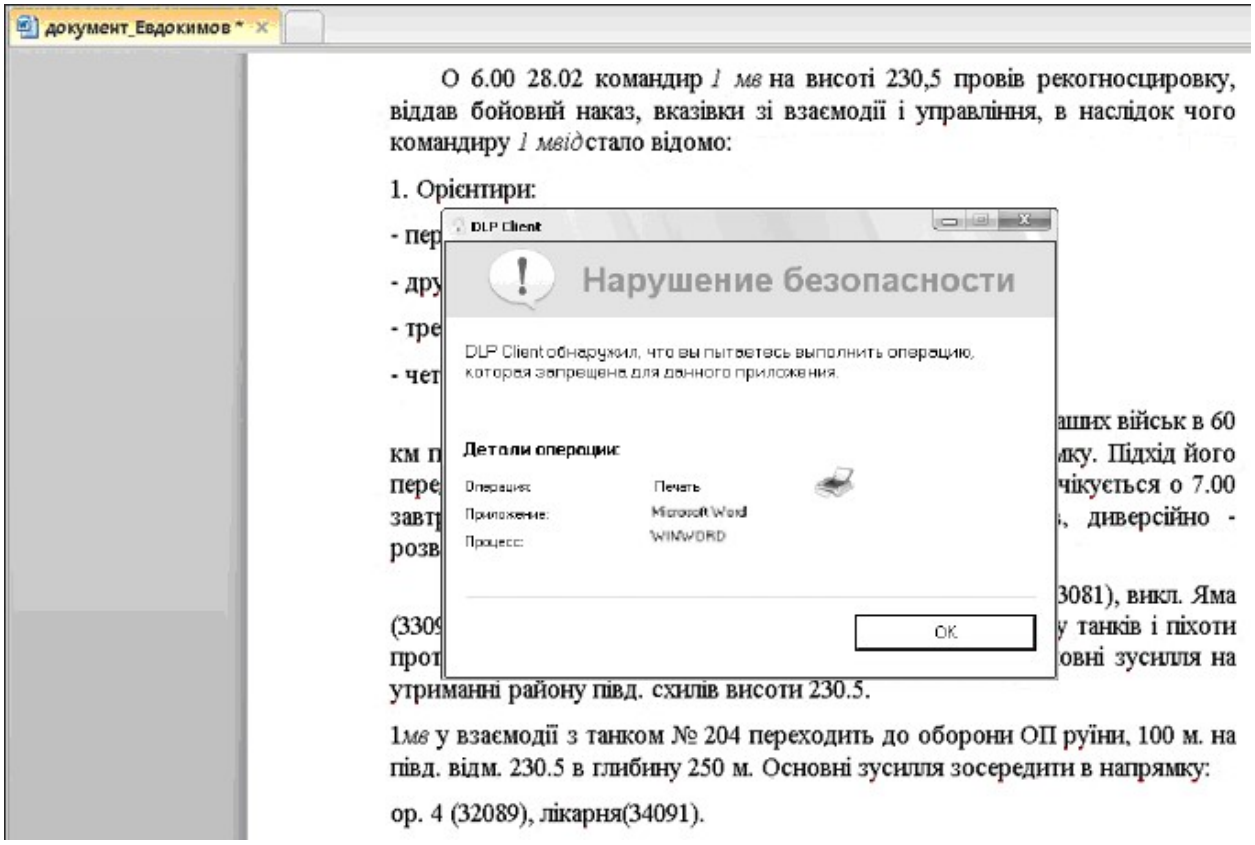

Рис. 3. Повідомлення про блокування файлу на друк

Проведене дослідження в перспективі відкриває можливості створення компактних, швидкодіючих та енергонезалежних систем штучного інтелекту. При всьому цьому відзначимо, що системи DLP на сьогоднішній день досить ефективний інструмент для захисту конфіденційної інформації тільки в інтеграції з іншими сервісами безпеки і актуальність інтегрованих рішень буде з часом тільки збільшуватися. Тому, впровадження DLP-систем є необхідністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Habimana N., Muhoza D., Nyirimanzi J.C. та ін. Statistical YearBook 2017. *National Institute of Statics of Rwanda*. URL: http://www.statistics.gov.rw/publication/statistical-yearbook-2017 (дата звернення 31.03.2019).
2. Нестеров С. А. Информационная безопасность и защита информации: Учеб. пособие. Санкт-Петербург: Изд-во Политехн. ун-та, 2009. 126 с.
3. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. Санкт-Петербург: Питер, 2016. 992 с.
4. Korosec K. Tesla подає в суд на колишніх співробітників за крадіжку комерційних секретів. TechCrunch. 2019. URL: https://techcrunch.com/2019/03/21/tesla-sues-former-employees-zoox-for-alleged-trade-secret-theft/ (дата звернення 31.03.2019).
5. Infowatch. Глобальні дослідження витоків інформації починаючи з 2007 року. 2018. URL: https://www.infowatch.ru/analytics/leaks_monitoring (дата звернення 31.03.2019).
6. Євдокимов С.О., Лукьянчіков С.Д. Актуальні проблеми кібербезпеки автоматизованої банківської системи. *Інформаційні технології в моделюванні*: Матеріали ІІІ-ої всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (22-23 березня 2018 р., м. Миколаїв). Миколаїв: МНУ імені В.О. Сухомлинського, 2018. С. 122.

Serhii EVDOKIMOV, Serhii USTENKO
Mykolayiv

DEVELOPMENT OF A SYSTEM OF PROTECTION OF INFORMATION IN THE LOCAL NETWORK OF THE ENTERPRISE

Today there is a need to choose the right means and measures to ensure the security of information from unauthorized access to it. This paper proposes the possibility of using the most efficient and promising DLP system architecture to protect data from threats in the local area network. Modern DLP systems (Data Leak Prevention) are technologies that can help prevent confidential information from being leaked from an enterprise, and can also be used to solve a number of other tasks, for example, personnel-related control actions.

Given the above, it is clear that this explains the relevance and relevance of modern DLP systems for any enterprise.

Analyzed the possibility of using DLP-system to protect information in the local network of the enterprise. A program has been developed for monitoring system events in applications defined by information security policies.

Keywords: *local healty, DLP-system, system for Danish, come bezin information, information, information.*

Сергей ЕВДОКИМОВ, Сергей УСТЕНКО
Николаев

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

Сегодня возникает необходимость правильно выбирать средства и меры обеспечения защищенности информации от несанкционированного к ней доступа. В этой работе предлагаются возможность использования наиболее эффективной и перспективной архитектуры DLP-системы для защиты данных от угроз в локальной сети предприятия. Современные системы DLP (англ. Data Leak Prevention) – это технологии, с помощью которых можно предотвратить утечки с предприятия именно конфиденциальной информации, а также можно использовать для решения ряда других задач, например, связанных с контролем действий персонала.

С учетом вышеуказанного, понятно, что этим объясняется востребованность и актуальность современных DLP-систем для любого предприятия.

Проанализирована возможность использования DLP-системы для защиты информации в локальной сети предприятия. Разработана программа для выполнения мониторинга системных событий в приложениях, определенных политиками информационной безопасности.

Ключевые слова: *локальная сеть, DLP-система, системы защиты данных, меры безопасности информации, целостность информации.*

Стаття надійшла до редколегії 31.03.2019