МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_А.В. Ільєнко

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ р.

На правах рукопису

УДК 004.772, 004.056.55

**Магістерська атестаціна РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«Магістр»**

**Тема:** Система захищеного корпоративного документообігу

**Автор:** А.І. Цвєтков

**Науковий керівник:** к.т.н., доц. М.Б. Гумен

**Нормоконтролер**: асист. С.В. Єгоров

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Комп’ютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:**  125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Цвєткова Андрія Ігоровича**

1. Тема: Система захищеного корпоративного документообігу затверджена наказом ректора від «02» жовтня 2019 № 2265/ст*.*
2. Термін виконання з 14.10.2019р. по 09.02.2020р*.*
3. Вихідні дані: зібрати інформацію щодо зберігання та обробки документів; проаналізувати розвиток документообігу як галузі прикладного значення; дослідити існуючі стандарти і протоколи електронного документообігу; розробити та реалізувати алгоритм обміну файлами із автентифікацією та шифруванням.
4. Зміст пояснювальної записки: аналіз розвитку поняття «документообіг»; огляд існуючих протоколів електронного обміну даними; оцінка ризиків та загроз; реалізація серверної та клієнтської частини програмного забезпечення, що реалізує захищений обмін файлами; демонстрація роботи.

**КАЛЕНДАРНИЙ ПЛАН**

**виконання магістерської роботи**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Етапи виконання магістерської роботи** | **Термін виконання етапів** | **Примітка** |
|  | Уточнення постановки задачі | 14.10.2019 | *Виконано* |
|  | Аналіз літературних джерел | 15.10.2019 – 22.10.2019 | *Виконано* |
|  | Обґрунтування вибору рішення | 23.10.2019 – 30.10.2019 | *Виконано* |
|  | Збір інформації | 31.10.2019 – 15.11.2019 | *Виконано* |
|  | Дослідження історичного аспекту розвитку поняття «документ» | 16.11.2019 – 10.12.2019 | *Виконано* |
|  | Аналіз сучасних реалізацій документообігу | 10.12.2019 – 01.01.2020 | *Виконано* |
|  | Розробка алгоритму та програмного забезпечення, що реалізує захищений обмін файлами | 02.01.2020 – 12.01.2020 | *Виконано* |
|  | Підготовка тестового полігону та перевірка роботи | 13.01.2020 | *Виконано* |
|  | Перевірка на антиплагіат | 02.02.2020 | *Виконано* |
|  | Оформлення і друк пояснювальної записки | 04.02.2020 | *Виконано* |
|  | Оформлення презентації | 05.02.2020 | *Виконано* |
|  | Отримання рецензій від рецензента | 08.02.2020 | *Виконано* |
|  | Захист в ЕК | 09.02.2020 | *Виконано* |

Магістрант А. Цвєтков

(підпис, дата)

Науковий керівник М. Гумен

(підпис, дата)

**Реферат**

Магістерська атестаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 114 сторінки основного тексту, 9 рисунків, 1 таблицю, 13 сторінок додатків. Список використаних джерел містить 58 найменування і займає 6 сторінок. Загальний обсяг роботи 142 сторінки.

Метою роботи є підвищення захисту інформації, що передається комп’ютерними мережами.

В роботі вирішено задачу зберігання, шифрування, доставку мережею та дешифрування файлів.

В роботі розроблено алгоритм обробки даних, що включає шифрування, дешифрування файлів та передачу від сервера до клієнта з обмеження доступу до файлів відповідно до групи користувача Unix-системи, а також практична реалізація даної системи.

Розроблений метод та програмне забезпечення відносяться до галузі інформаційної безпеки і можуть бути використані в цілях корпоративного підвищення рівня захищеності даних.

Можливі напрямки розвитку цієї роботи пов’язані із розширенням функціоналу додатку, наприклад, реалізації асиметричного шифрування.

Ключові слова: документ, документообіг, шифрування, інформаційна безпека, TCP-сокет, ключ, файл.

**Зміст**

[Перелік умовних позначень та скорочень 8](#_Toc30373721)

[Вступ 9](#_Toc30373722)

[Розділ 1](#_Toc30373723). [Документи в історії людства](#_Toc30373724). [Підгрунтя розвитку технологій документообігу 11](#_Toc30373725)

[1.1. Історія документу 11](#_Toc30373726)

[1.1.1. Від документа до "документації" 12](#_Toc30373727)

[1.1.2. Повернення від документації назад до "документа" 13](#_Toc30373728)

[1.1.3. Пол Отлет: об'єкти як документи 14](#_Toc30373729)

[1.1.4. Сюзанна Бріт: фізичні докази як документ 15](#_Toc30373730)

[1.1.5. Донкер Дуйвіс: духовний вимір для документів 16](#_Toc30373731)

[1.1.6. Ранганатан: мікро-думка на рівній поверхні 17](#_Toc30373732)

[1.1.7. Антропологія: матеріальна культура 18](#_Toc30373733)

[1.1.8. Семіотика: "Текст" і "об'єкт як знак" 18](#_Toc30373734)

[1.1.9. Цифрові документи 20](#_Toc30373735)

[1.2. Система управління документами 21](#_Toc30373736)

[1.2.1. Основи поняття СУД 22](#_Toc30373737)

[1.2.2. Роль СУД 22](#_Toc30373738)

[1.3. Висновки до розділу 27](#_Toc30373739)

[Розділ 2](#_Toc30373740). [Існуючі концепції та реалізації документообігу 30](#_Toc30373741)

[2.1. Відстеження документів 30](#_Toc30373742)

[2.1.1. Ролі відстеження 31](#_Toc30373743)

[2.1.2. Приклади відстеження документів на робочому місці 32](#_Toc30373744)

[2.1.3. Стандартна операційна процедура 33](#_Toc30373745)

[2.2. Управління документообігом 33](#_Toc30373746)

[2.2.1. Програмне забезпечення для управління документами 35](#_Toc30373747)

[2.3. Electronic Data Interchange 38](#_Toc30373748)

[2.3.1. Стандарти, необхідні для EDI 39](#_Toc30373749)

[2.3.2. Обмежене охоплення цього стандарту. 40](#_Toc30373750)

[2.3.3. Довгострокова перспектива для стандартів EDI 40](#_Toc30373751)

[2.4. Керівництво щодо розгортання EDI 41](#_Toc30373752)

[2.4.1. Що таке EDI? 42](#_Toc30373753)

[2.4.2. Процес EDI 45](#_Toc30373754)

[2.4.3. Використання EDI 45](#_Toc30373755)

[2.4.4. Переваги EDI 46](#_Toc30373756)

[2.4.5. Алгоритм EDI 48](#_Toc30373757)

[2.4.6. Впровадження EDI 51](#_Toc30373758)

[2.4.7. Інфраструктура EDI 51](#_Toc30373759)

[2.5. Стандарти EDI 53](#_Toc30373760)

[2.5.1. EANCOM 53](#_Toc30373761)

[2.5.2. EDIFACT 57](#_Toc30373762)

[2.5.3. EDIG@S 61](#_Toc30373763)

[2.5.4. HL7 63](#_Toc30373764)

[2.5.5. IATA Cargo-IMP 64](#_Toc30373765)

[2.5.6. IATA Cargo XML 66](#_Toc30373766)

[2.5.7. IATA (IATA PADIS) 66](#_Toc30373767)

[2.5.8. National Council for Prescription Drug Programs 67](#_Toc30373768)

[2.5.9. RosettaNet EDI Standard 68](#_Toc30373769)

[2.5.10. SAP IDoc EDI 69](#_Toc30373770)

[2.5.11. Standard Exchange Format (SEF) 70](#_Toc30373771)

[2.5.12. Tradacoms 71](#_Toc30373772)

[2.5.13. X12 EDI Standard 71](#_Toc30373773)

[2.6. Криптографія 77](#_Toc30373774)

[2.6.1. Історія криптографії 78](#_Toc30373775)

[2.6.2. Сучасна криптографія 79](#_Toc30373776)

[2.7 Види шифрування 89](#_Toc30373777)

[2.7.1. Data Encryption Standard 92](#_Toc30373778)

[2.7.2. TripleDES 92](#_Toc30373779)

[2.7.3. RC4, RC5 і RC6 93](#_Toc30373780)

[2.7.4. AES 93](#_Toc30373781)

[2.8. Програми для шифрування 94](#_Toc30373782)

[2.8.1. Хеш 94](#_Toc30373783)

[2.8.2. Цифрові сертифікати 94](#_Toc30373784)

[2.9. Протоколи шифрування 95](#_Toc30373785)

[2.9.1. IPsec 95](#_Toc30373786)

[2.9.2. Point-to-Point Tunneling Protocol 97](#_Toc30373787)

[2.9.3. Layer Two Tunneling Protocol 97](#_Toc30373788)

[2.9.4. Secure Socket Layer 98](#_Toc30373789)

[2.10. Модель загроз 98](#_Toc30373790)

[2.10.1. Поняття моделі загроз 98](#_Toc30373791)

[2.10.2. Реалізація моделі загроз 99](#_Toc30373792)

[2.11. Модель порушника 101](#_Toc30373793)

[2.11.1. Ступені деталізації 102](#_Toc30373794)

[2.11.2. Способи класифікацій порушників 102](#_Toc30373795)

[2.11.3. Реалізація моделі порушника 104](#_Toc30373796)

[2.12. Висновки до розділу 105](#_Toc30373797)

[Розділ 3](#_Toc30373798). [Авторська реалізація ПЗ для захищеного обміну інформацією 108](#_Toc30373799)

[3.1 Мова програмування Python 108](#_Toc30373800)

[3.2. Характеристики створеного програмного продукту 109](#_Toc30373801)

[3.3. Перевірка роботи 112](#_Toc30373802)

[3.3.1. Робота із додатком 114](#_Toc30373803)

[3.4. Висновок до розділу 118](#_Toc30373804)

[Висновки 120](#_Toc30373805)

[Список бібліографічних посилань 125](#_Toc30373806)

[Додаток А 131](#_Toc30373807)

[Додаток Б 136](#_Toc30373808)

Перелік умовних позначень та скорочень

AES – Advanced Encryption Standard

ANSI – American National Standards Institute

DES – Data Encryption Standard

DMS – Document Management System (див. СУД)

EDI – Electronic data interchange

ERP – Enterprise Resource Planning System

FIPS – Federal Information Processing Standards

HIPAA – Health Insurance Portability and Accountability Act

IDC – International Data Corporation

VAN – Value Added Network

АС – Автоматизована система

ЄЕК ООН – Європейська Економічна Комісія ООН

ІР – Інформаційні ресурси

ІС – Інформаційна система

КСЗІ – Комплексна система захисту інформації

НСД – Несанкціонований доступ

ПЗ – Програмне забезпечення

ПК – Персональний комп’ютер

СОП – Стандартна операційна процедура

СУД – Система управління документами

Вступ

Стрімкий розвиток інформаційних технологій та їх впровадження в усі сфери діяльності призводить до появи чинників, що несуть загрозу інформаційним ресурсам. Особливо це стосується властивостей інформації, серед яких – конфіденційність, доступність, цілісність. Незважаючи на існування численних методів, засобів та інструментів по збереженню кожного з трьох названих аспектів, цю роботу присвячено реалізації забезпечення в першу чергу доступності та конфіденційності.

Відповідно до цього, випливає завдання створення нових прикладних інструментів та засобів захищеного обміну файлами.

Об’єктом дослідження є захищений обмін файлами при передачі мережею.

Предмет дослідження: програмна реалізація алгоритму, що дозволяє виконання шифрованого обміну файлами від сервера до клієнта.

Метою роботи є створення програмного комплексу, що дозволяє виконувати передачу файлів від сервера до клієнта із шифруванням та попередньою автентифікацією.

Завдання роботи: проаналізувати розвиток поняття «документообіг»; розглянути існуючі методи електронного документообігу, його протоколи та стандарти; провести аналіз загроз щодо цілісності, доступності та створити відповідні моделі (загроз та порушника); створити програмний продукт (клієнтська та серверна частина) для шифрування та передачі даних.

Метод дослідження (технічні та програмні засоби) – проведення аналізу; створення програмного продукту з використанням мови програмування Python, середовища розробки IDLE і текстового редактора vim.

Практична значимість визначається необхідністю створення національного програмного забезпечення, а також реалізацію захищенної передачі файлів в корпоративних та відкритих мережах.

Даний програмний продукт буде ефективний при використанні як у приватних умовах, так і в державних установах та організаціях.

В подальшому можливе удосконалення розробленого продукту з метою покращення його характеристик: введення можливості використання асиметричного шифрування, створення власної інфраструктури обміну ключами, тунельний режим з’єднання, асинхронний сервер.

Розділ 1

Документи в історії людства.

Підгрунтя розвитку технологій документообігу

Запитання "Що таке електронний документ" розглядається як окремий випадок питання "Що таке документ". Зазвичай, слово "документ" позначає текстовий запис. На початку минулого століття спроби забезпечити доступ до швидкозростаючої кількості доступних документів викликали питання щодо того, які саме слід вважати "документом". В результаті Пол Отлет розробив функціональний погляд на "документ". Сюзанна Бріт визначила «документ» таким, що має організований фізичний відповідник. Ці ідеї нагадують поняття "матеріальна культура" в культурній антропології та "об'єкт як знак" у семіотиці.

Інші, особливо в США (наприклад, Джессі Шера та Луї Шорс), мали більш вузьку точку зору.

Безлад в поняттях «засіб», «повідомлення», «значення» знову стає актуальною проблемою через активний розвиток цифрових технологій, бо із представленням інформації в бітах технічне визначення поняття «документ» стало ще більш розпливчатим.

1.1. Історія документу

Посилання на паперовий документ, папірусний документ або мікрофільмований документ, значення є зрозумілим. Однак ідея "цифрового документа" більш складна. Ми можемо визнати електронну пошту та технічний звіт, створений текстовим процесором, як цифрові документи, але поза цими простими прикладами поняття "документ" стає менш зрозумілим. Чи є програмне забезпечення документом? Він має рядки мовоподібного тексту. Чи є операційна система документом? Можна перераховувати різні типи цифрових документів, оскільки існує необхідність уточнення стандартів для досягнення ефективності та сумісності. Але якщо прямувати до завершеності, процес стає примхливим та інтелектуально незадовільним, оскільки незрозуміло, де має бути межа між документами та недокументами.

Паперовий документ відрізняється, в першу чергу, тим, що він знаходиться на папері. Але аспект носія менш корисний для цифрових документів. Повідомлення електронної пошти та технічний звіт фізично існують у цифровому середовищі як рядок бітів. Слово "Мультимедіа", яке раніше позначало декілька фізично різних медіа (як способів представлення інформації), зараз викликає інтерес, оскільки, за іронією долі, декілька медіа можуть бути зведені в одному середовищі у вигляді електронно збережених бітів.

Для практичних цілей люди розробляють прагматичні визначення, такі як "все, що може мати ім'я файлу та збережено на електронних носіях" або "колекція даних плюс властивості тих даних, що є для користувача логічною одиницею". І, як це часто трапляється, можна знайти визначення "документа", які зосереджуються на одному аспекті і часто є високо метафоричними, наприклад "захоплені знання", "дані в контексті" та "організований погляд на інформацію".

Цифрові системи стосувалися в основному текстових записів (наприклад, імена, цифри та буквено-цифрові коди), але сучасна зацікавленість у піктограмах та графіці нагадує, що нам може знадобитися мати справу з будь-якими явищами, які будь-хто може спостерігати: події, процеси, зображення, предмети, а також тексти [1].

1.1.1. Від документа до "документації"

Цифрові документи відносно нові, але обговорення більш широкого питання "Що таке документ?" не є новим. В кінці 19 століття зростала стурбованість швидким збільшенням кількості публікацій, особливо науково-технічної літератури та соціальних "фактів". Постійна ефективність у створенні, розповсюдженні, використанні записаних знань розглядалася як необхідність у новій методиці управління зростаючим потоком документів.

«Управління», яке було потрібно, мало кілька аспектів. Для збирання, збереження, організації (упорядкування), представлення (опису), вибору (вилучення), відтворення (копіювання) та розповсюдження документів були потрібні ефективні та надійні методи. Традиційною назвою цієї діяльності була "бібліографія". Однак цей термін виявився не зовсім доречним. Відчувалося, що потрібно щось більше, ніж традиційна «бібліографія». Наприклад, методики відтворення документів та «бібліографії» мали також інші усталені значення, пов’язані з традиційними прийомами книговидання.

На початку XX століття в Європі все частіше було використовувалося слово "документація" замість "бібліографія" для позначення набору методів, необхідних для управління цим потоком документів. Починаючи з 1920 р. "документація" (і споріднені слова англійською, французькою та німецькою мовами) все частіше сприймалася як загальний термін, який охоплює бібліографію, наукові інформаційні послуги, управління документацією та архівну роботу. Після приблизно 1950 р. більш досконала термінологія, така як "інформатика (наука про інформацію)", "зберігання та пошук інформації" та "управління інформацією", поступово замінювала слово "документація".

1.1.2. Повернення від документації назад до "документа"

Проблеми, викликані збільшенням друкованих документів (і їх кількості), призвели до розробки методик, покликаних для управління важливими (або потенційно значущими) документами, тобто на практиці надрукованими текстами. Але не було жодної теоретичної причини, по якій документацію слід обмежувати лише текстами, не кажучи вже про лише друковані тексти. Окрім них існує багато інших видів означувальних об’єктів. І якщо документація може стосуватися текстів, які не є надрукованими, чи не може вона також стосуватися документів, які взагалі не є текстами? Наскільки широко можна застосувати термін “документація”? Зазначимо інакше: якщо термін "документ" використовувався в спеціалізованому значенні як технічний термін для позначення об'єктів, для яких можна застосувати методи документації, то наскільки можна було б розширити обсяг документації. Що може (чи не може) бути документом? Однак питання нечасто формулювалося в цьому значенні.

Ранньою розробкою було розширення поняття «документ» за межі письмових текстів, яке можна знайти в тлумачних словниках. "Будь-яке вираження людської думки" найбільш часто використовувалося як визначення "документа" серед документалістів. У США широко використовувались фрази «графічний запис» та «книга загального призначення». Це було зручно для розширення сфери застосування на зображення та інші графічні та аудіовізуальні матеріали. Бельгієць Пол Отлет (1868-1944рр.) відомий своїм спостереженням, що документи можуть бути тривимірними і включати скульптуру. Починаючи з 1928 року, музейні предмети, ймовірно, будуть включені документалістами у визначення "документа" [2]. Переважне практичне занепокоєння документалістів стосувалося друкованих документів. Тому питання про те, наскільки можна визначити поняття "документ", мало отримати більше безпосередньої уваги. Інколи вдумливий письменник обговорював би цю тему, можливо, тому що цікавиться якоюсь новою формою означеного предмета.

1.1.3. Пол Отлет: об'єкти як документи

Отлет розширив визначення "документа" в своїй роботі Traité de documentation 1934 р. [3]. Графічні та письмові записи – це уявлення про ідеї чи об’єкти, писав він, але самі об'єкти можна вважати "документами", якщо вас інформують про спостереження за ними. В якості прикладів таких "документів" Отлет наводить природні предмети, артефакти, предмети, що мають сліди людської діяльності (наприклад, археологічні знахідки), пояснювальні моделі, навчальні ігри та твори мистецтва [4].

У 1935 році Вальтер Шурмейер писав: "Сьогодні під документом розуміється будь-яка матеріальна основа для розширення наших знань, яка доступна для вивчення або порівняння". ("Man versteht heute unter einem Dokument jede materielle Unterlage zur Erweiterung unserer Kenntnisse, die einem Studium oder Vergleich zugänglich ist." [5]).

Аналогічно, Міжнародний інститут інтелектуального співробітництва, агентство Ліги Націй, у співпраці з Французьким союзом організації документації розробило технічні визначення поняття "документ" та пов'язані з ним технічні терміни англійською, французькою та німецькою версіями:

Документ – будь-яке джерело інформації у матеріальній формі, яке може бути використане для довідок чи дослідження або як доказ. Приклади: рукописи, друковані видання, ілюстрації, схеми, музейні зразки тощо [6].

1.1.4. Сюзанна Бріт: фізичні докази як документ

Прониклива французька бібліотекарка Сюзанна Бріт (1894-1989) розширила значення терміну "документ". У 1951 р. Бріт опублікувала маніфест про природу документації «Qu'est-ce que la documentation», який починається з твердження, що «Документ є доказом на підтвердження факту». ("Un document est une preuve à l'appui d'un fait" [7]. Потім вона уточнює: документ – це "будь-який фізичний або символічний знак, збережений або записаний, призначений представляти, реконструювати або демонструвати фізичне або концептуальне явище" (“Tout indice concret ou symbolique, conservé ou enregistré, aux fins de représenter, de reconstituer ou de prouver un phénomène ou physique ou intellectuel»). Отже, слід вважати, що документація стосується доступу до доказів, а не доступу до текстів.

Бріт наводить приклади: зірка на небі – це не документ, а його фотографія; камінь у річці – це не документ, але камінь, виставлений у музеї, був би; тварина в дикій природі не є документом, але дика тварина, представлена ​​в зоопарку, була б. Антилопа, що дико біжить рівнинами Африки, не повинна вважатися документом, вона є даними, першоджерелом. Але якщо її схопити, відвезти в зоопарк і зробити об’єктом вивчення, то вона стала б своєрідним документом. Таким чином, вона стала фізичним доказом, яким користуються ті, хто її вивчають. Дійсно, наукові статті, написані про антилопу, є вторинними документами, оскільки сама антилопа є первинним документом.

Правила Бріт щодо визначення того, коли об’єкт став документом, не з'ясовані, але її обговорення, схоже, свідчить наступне:

1. Матеріальність: документи можуть бути лише фізичними об'єктами [1];

2. Навмисність: до об'єкта слід ставитися як до доказів;

3. Об'єкти підлягають обробці;

4. Існує феноменологічна позиція: об’єкт сприймається як документ.

Ця ситуація нагадує дискусії про те, як образ стає мистецтвом, при обрамленні його як об’єкт мистецтва. Чи Бріт мала на увазі, що подібно до того, як «мистецтво» стає мистецтвом, «обрамлюючи» (тобто трактуючи) його як мистецтво, таким чином, об’єкт стає «документом», коли він трактується як документ, тобто як фізичний або символічний знак, що збережено чи записано, призначено для репрезентації, реконструкції чи демонстрації фізичного чи концептуального явища?

Рон Дей припустив, що вживання Бріт слова "індекс" є важливим, що індексованість – ознака того, що вони були розташовані в організованому, змістовному взаємозв'язку з іншими даними. І саме це надає об’єкту його документальний статус.

1.1.5. Донкер Дуйвіс: духовний вимір для документів

Фрітс Донкер Дювіс (1894-1961), який після Поля Отлета очолив Міжнародну федерацію документації, уособлював технологічний модернізм документалістів у його відданості триєдності наукового управління, стандартизації та бібліографічного контролю як взаємодоповнюючого зміцнення основ для досягнення прогресу [8]. І все ж Донкер Дювіс не був матеріалістом. Він прийняв концепцію Отлета, що документ є вираженням людської думки. Та він зробив це з точки зору антропософії – духовного руху, заснованого на уявленні, що існує духовний світ, зрозумілий чистій думці і доступний лише найбільш розумним представникам суспільства. Як результат, Донкер Дювіс став чутливим до того, що ми можемо зараз назвати когнітивними аспектами середовища повідомлення. Він написав, що "…документ є сховищем висловленої думки. Отже, його зміст має духовний характер. Але небезпека того, що бездумна уніфікація зовнішньої форми впливає на зміст, роблячи останній безликим і безособовим, не є ілюзорною.... Стандартизуючи форму та макет документів, потрібно обмежити діяльність тією, яка не впливає на духовний зміст і яка служить для вилучення ірраціональної різноманітності " [9].

1.1.6. Ранганатан: мікро-думка на рівній поверхні

Індійський теоретик С. Р. Ранганатан, як і завжди надзвичайно метафізичний, займав цікаво вузьку і прагматичну позицію щодо визначення поняття "документ", не визнаючи навіть включення аудіовізуальних матеріалів, таких як радіо- і телевізійні комунікації. "Але це не документи, тому що вони не є записами на матеріалах, придатних для обробки чи збереження. Статуї, шматки порцеляни та матеріальні експонати в музеї були згадані, оскільки вони передають думки, виражені певним чином. Але жодний з них не є документом, оскільки це не запис на більш-менш рівній поверхні" [10].

Погляд Ранганатана на "документ" як синонім "втіленої мікродумки" на папері "чи іншому матеріалі, придатному для фізичного користування, транспортування через простір та збереження у часі" було прийнято Індійським інститутом стандартів [11]. Інші також мали обмежений погляд на те, чим є документ. У США два дуже впливові автори обрали варіант перегляду документів, який був лише розширенням текстових записів, щоб включити аудіовізуальні комунікації. Луї Шорс популяризував поняття "універсальна книга (The generic book)" [12], а Джессі Х. Шера використовував термін "графічний запис" з таким же значенням [13].

1.1.7. Антропологія: матеріальна культура

Отлет явно визначив, що його погляд на "документ" включає археологічні знахідки, сліди людської діяльності та інші предмети, не призначені для комунікацій. "Колекції предметів, зібрані для збереження, для науки та освіти, по суті мають документальний характер (Музеї та шафи, колекції моделей, прикладів та зразків). Ці колекції створюються з предметів, що зустрічаються в природі, а не окреслені або описані словами; це тривимірні документи " [14].

Поняття предметів як документів нагадує поняття "матеріальної культури" серед культурних антропологів, "для яких артефакти внесли важливі докази в документацію та інтерпретацію американського досвіду" [15].

1.1.8. Семіотика: "Текст" і "об'єкт як знак"

Ідеї Бріт щодо природи "документа" викликають дискусії стосовно семіотики. У цьому контексті ми відзначимо дискусію Дюфрена про відмінність естетичних об'єктів від знакових об'єктів:

"Функція таких [знакових] об'єктів полягає не в тому, щоб стримувати якусь дію чи задовольнити якусь потребу, а щоб розповсюджувати знання. Ми, звичайно, можемо називати всі об'єкти знаковими в якомусь сенсі. Однак ми повинні виділити ті об'єкти, які роблять більше, ніж означають, лише для того, щоб підготувати нас до певних дій, які не використовуються лише для виконання завдання. Наукові тексти, катехізиси, фотоальбоми та покажчики – це все знаки, значення яких залучає нас до діяльності лише після того, як ми забезпечили себе інформацією" [16].

Ми можемо спостерігати, що завдяки включенню музейних та інших «знайдених» предметів «будь-який фізичний чи символічний знак» Бріт включає як людські, так і природні знаки. Інші розробили поняття «предмет-як-знак». Наприклад, Роланд Бартс, обговорюючи "семантику об'єкта", писав, що об'єкти "функціонують як рушій значення: іншими словами, об'єкт ефективно служить певному призначенню, але він також виконує функцію передачі інформації. Можемо підсумувати, що завжди є значення, яке виходить за межі використання об’єкта" [17]. Відзначимо широке використання слова "текст" для охарактеризування зразків соціальних явищ, що не містять слів чи цифр, але, схоже, було приділено недостатньо уваги до співпадінь між семіотикою та управлінням інформацією [18].

Однією із відмінностей поглядів документалістів, про яких згадувалося вище, та сучасними поглядами є акцент, зроблений на соціальну конструкцію значення та сприйняття споглядачем значущості і доказового характеру документів.

"... знаки ніколи не є природними об'єктами ... Причина полягає просто в тому, що властивість бути знаком – це не природна властивість, яку можна шукати і знаходити, а властивість, яка надається об'єктам, незалежно від того, природні вони або штучні за способом створення. Знаки, як предмети і засоби, мають трактуватися як щось винайдене, і в цьому сенсі вони співвідносяться з діями " [19].

Концепція Бріт щодо документів як доказів може бути представлена щонайменше двома способами. Одним із призначень інформаційних систем є зберігання та підтримка доступу до тих чи інших доказів, які були вказані як докази певного твердження. Інший підхід полягає в тому, що людина, яка має можливість класифікувати та організовувати артефакти, зразки, тексти чи інші предмети, повинна враховувати те, що вони можуть розповісти про світ, який їх створив, а потім, розробивши певну теорію його значення для визнання предмета доказом, пропонувати його як доказ у порядку їх організації, індексації чи подання. Таким чином, інформаційні системи можуть використовуватися не тільки для пошуку матеріалів, які вже є доказами, але й для упорядкування матеріалів, щоб існувала можливість застосування їх як (нових) доказів з певною метою.

1.1.9. Цифрові документи

Поступова зміна поняття "документ" в роботах Отлета, Бріт, Шурмейєра та інших документалістів все частіше підкреслювала те, що більше функціонує власне документ, а не його традиційна фізична форма. Перехід до цифрових технологій робить цю відмінність ще важливішою. Глибокий аналіз Девіда М. Леві (професор вашингтонського університету) показав, що акцент на технологіях цифрових документів перешкоджає нашому розумінню цифрових документів як документів [20]. Кожна річ у цифровій технології зберігається у вигляді бітів, тому звичайна фізична форма (на папері, у вигляді мікрофільму) вже не допомагає. У цьому сенсі будь-яка відмінність документа як фізичної форми ще більше зменшується.

П'ятдесят років тому необхідно було шукати логарифмічні значення у друкованій книзі "Журнал таблиць" для виконання обчислень. Сьогодні можна уявити кількість таблиць, що зберігаються в інтернеті, і які можна використовувати як цифрову версію друкованих таблиць. Однак є більш імовірним те, що можна використовувати алгоритм для обчислення значень таблиць за потребою. Надана відповідь повинна бути однаковою. Можливо, ніхто не дізнається, використовував комп'ютер таблицю або алгоритм. Таблиця та алгоритм здаються функціонально еквівалентними. Що сталося з поняттям "документ"? Одна з відповідей полягає в тому, що все, що відображається на екрані або роздруковується, – це документ. Можна сказати, що алгоритм функціонує як документ або як динамічний вид документа, який нагадує нам ідею Отлета про те, що навчальну іграшку слід вважати своєрідним документом. Це відповідало б описаній вище тенденції до визначення документа з точки зору функціонування, а не фізичного формату.

Кожна інша технологія має різні можливості, різні обмеження. Якщо ми підтримуємо функціональне уявлення про те, що становить документ, слід очікувати, що документи прийматимуть різні форми в контекстах різних технологій, і тому слід очікувати, що діапазон того, що можна вважати документом, відрізняється в цифровому та паперовому середовищах. Алгоритм генерування логарифмів, як і механічна навчальна іграшка, може розглядатися як динамічний вид документа на відміну від звичайних паперових документів, але все ще відповідає етимологічному походженню поняття "документ".

Спроби визначити цифрові документи, ймовірно, залишаться безуспішними, якщо потрібно більш прагматичне визначення. В свою чергу, визначення на основі форми, формату та носія виглядають менш задовільними, ніж функціональний підхід, наслідуючи шлях міркувань, що лежить в основі забутих дискусій про об'єкти Отлета та антилопи Бріт.

1.2. Система управління документами

Система управління документами (СУД) (англ. Document Management System – DMS) – обов’язковий інструмент у сучасному цифровому світі. Необхідно з’ясувати, що саме являє собою система управління документами, чому вона є обов'язковою та які системи управління документами вважаються найкращими на ринку.

Документи – основа будь-якої справи, процесу. Вони відіграють центральну роль у сприянні належному функціонуванню та загальному успіху будь-якого бізнесу. На Землі немає компанії, яка могла б існувати без перегляду та обміну документами. Сюди входять маркетингові брошури, проектні пропозиції, технічні документи, вказівки з персоналу та навчальні матеріали.

Проблема полягає в тому, що чим більше створюється документів та чим більше на них покладено роботи, тим критичнішою стає наявність систем для відслідковування та контролю за документами. Саме ці функції виконують так звані системи управління документами [21].

1.2.1. Основи поняття СУД

Найкращим визначенням системи управління документами або DMS є система або програмне забезпечення, яке дозволяє створювати, зберігати, керувати, індексувати, захищати та отримувати цифрові документи. Хоча більшість систем управління документами зберігають усі ваші цифрові документи у хмарі, вони набагато функціональніші, ніж просте хмарне зберігання. Система управління документами – це структура, яка сприяє легкому потоку критичної інформації по всій організації.

Ефективна система управління документами може допомогти впорядкувати всі ваші файли та дані в одному місці, відстежити всі критичні документи, прискорити робочий процес, підвищити точність роботи та забезпечити цілодобовий доступ до документів з будь-якої частини світу.

Таким чином, вибір надійної системи управління документацією дозволяє вам бути на крок попереду конкурентів та надавати всю інформацію, необхідну вашим працівникам для забезпечення ефективності роботи.

1.2.2. Роль СУД

Швидке оцифрування нашого світу призвело до експоненційного зростання кількості даних та ресурсів. Щодня будь-яка компанія створює та керує великою кількістю ділових документів, контрактів, пропозицій, маркетингових матеріалів, публікацій в блогах, інструкцій по роботі із персоналом, навчальних посібників тощо.

Ці документи часто розкидані по всіх доступних місцях на цифрових пристроях. У вас можуть бути файли Word, файли, що зберігаються в хмарних додатках, таких як Dropbox, Google Drive, OneDrive, SkyDrive, файли, що зберігаються на робочому столі, вкладення електронної пошти тощо. Що станеться, коли неможливо знайти потрібний файл посеред наради? Або коли менеджеру негайно знадобиться саме той важливий документ, але невідомо, де саме він зберігається?

Організація цифрових файлів завжди була непомітним аспектом ведення роботи в організації. Оскільки ви насправді не можете побачити або відчути створений вами цифровий безлад на відміну від паперового безладу у шафах із старими документами, ви можете не відчувати, що у вас є проблеми, поки ви не зможете знайти конкретний файл.

Управління цим цифровим безладом, яке часто буває неструктурованим, та надання доступу до нього вашим співробітникам, клієнтам, партнерам чи іншим зацікавленим сторонам – непросте завдання. Глобальне опитування працівників та ІТ-фахівців у 2012 році, проведене International Data Corporation (IDC), показало, що пошуки документів становлять 21,3% втрати продуктивності праці. Співробітники часто не можуть знайти потрібні документи в потрібний час або не можуть отримати доступ до документа через брак часу чи невдале місцезнаходження. Все це створює великі втрати продуктивності та робочого часу.

СУД відіграє величезну роль у тому, щоб зробити всі завдання, пов'язані з управлінням документацією, простішими, швидшими та ефективнішими. Є багато причин, чому організації потрібно негайно розгорнути систему управління документами. Деякі з них розглянуто нижче.

Прибирання цифрового безладу.

Система управління документами дозволяє позбутися масового цифрового безладу, який ви створили несвідомо. У всіх нас документи розкидані на різноманітних електронних пристроях: ноутбуках, персональних комп’ютерах (ПК), мобільних пристроях, робочих станціях, хмарних сховищах, вкладеннях електронної пошти, папках на робочому столі тощо. Виявити конкретний файл та місце його знаходження стає надзвичайно важко. Система управління документами дозволяє виконувати задачу по зберіганню та пошуку документів централізовано. Ефективна система управління документами також допомагає оцифровувати документи та приводити їх до єдиної форми. Наявність рішення "все в одному" допомагає при створенні централізованого сховища існуючого контенту та у співпраці команди над новим. Таким чином, не потрібно покладатися на використання Word чи інших редакторів документів для створення цифрових файлів, а потім зберігати вміст в іншому місці.

Зменшення залежності від паперу

Якщо компанія все ще використовує паперові документи, перехід на систему управління документами може допомогти зменшити залежність від паперу та заощадити витрати на друк, зберігання, обслуговування, витратні матеріали тощо. За даними RegisteredRep.com, компанії із щорічним доходом від 500 000 доларів до 1 мільйону доларів США можуть заощадити цілих 40 000 доларів на рік, перейшовши на управління цифровими документами. Laserfiche оцінює економію часу у 20% за рахунок автоматизації створення та використання контенту, а також зменшення вірогідності помилки. Підвищення ефективності, а також підвищення продуктивності персоналу можуть економити до 6000 годин щорічно або 2,4 штатні посади [22].

Абсолютна відсутність паперу також допомагає зменшити величезну кількість паперових відходів. Це не лише допомагає зробити етично правильний вибір, але й надає соціальну місію, до якої хочуть приєднатися і клієнти, і працівники, і уряди, і клієнти.

Підвищення загальної ефективність роботи офісу

Робочий день співробітників надзвичайно неефективний, коли більша частина часу витрачається на пошук цифрових документів на різних платформах і пристроях. Також, зменшується підсумковий внесок кожного в діяльність компанії. Перевантаження роботою знижує продуктивність праці на 68% у працівників, які відчувають, що мають недостатньо часу в добі для виконання своїх завдань. Ефективний спосіб звільнити робочий час співробітників – це розгортання системи управління документами для легкого створення, подання, редагування, спільної роботи в команді та затвердження ваших документів.

Інформація повинна бути доступною

Оскільки всі важливі робочі документи розкидані по Google Drive, OneDrive, вкладеннях електронної пошти, папках ПК та USB-накопичувачах, дуже складно розраховувати на своєчасне знаходження актуальних документів.

Згідно з доповіддю МакКінсі [23], працівники витрачають 1,8 години щодня – в середньому 9,3 години на тиждень – на пошук та збирання інформації. Майже 20% робочого часу, що еквівалентно одному дню на робочий тиждень, витрачають працівники, які шукають інформацію для ефективної роботи.

Дані IDC [24] показують, що спеціаліст з пошуку витрачає близько 2,5 годин на день, або приблизно 30% робочого дня, шукаючи інформацію.

Основною перевагою наявності системи управління документами є легкість доступу до інформації. Системи управління документами забезпечують централізоване місце зберігання для всіх файлів, документів, веб-посилань та інших мультимедійних матеріалів. Завдяки цьому члени команди мають надзвичайно легкий та швидкий доступ до інформації з будь-якого пристрою.

Безпечно і захищено

Найкращий спосіб зберегти важливі ділові документи в безпеці – це зберігання їх у цифровій формі в системі управління документами. Таким чином, не потрібно турбуватися про можливості захисту сотень додатків, де перебувають ваші дані, і не потрібно пам’ятати дані про вхід у кожний із них.

Грамотна система управління документами оснащена такими функціями, як контроль доступу до документів, відстеження документів, захист паролем, контроль версій, співпраця в режимі реального часу, сповіщення в режимі реального часу тощо. Зберігання файлів у хмарі допомагає гарантувати, що документи вашої компанії не будуть замінені та є доступними тільки для тих, хто має підтверджений доступ до них.

Масштабованість

По мірі того, як бізнес зростає і стає більш успішним, з часом збільшуватиметься кількість документів, які створюються та опрацьовуються. Більше документів – більше безладу, більше папок для перегляду, більше хмарних служб зберігання даних та більше вкладень електронної пошти для пошуку. Система управління документами дуже важлива, оскільки її легко масштабувати. Ви завжди можете налаштувати або придбати більше можливостей для зберігання даних у хмарі та переконатися, що ваші робочі процеси не порушені через розвиток бізнесу.

Швидкий пошук

Якщо у вас немає системи управління документами, пошук потрібного документа забирає забагато часу. Пошук потрібної хмарної служби, потрібної папки на робочому столі або того самого листа в електронній пошті може зайняти години цінного часу. Тому здатність системи управління документами здійснювати швидкий пошук є одним з найважливіших елементів.

Ефективна система управління документами має чудові можливості пошуку та індексації, щоб знайти точний файл, назву документа та вміст у документі. Незалежно від того, наскільки великий ваш каталог документів, система управління документами може знаходити потрібний документ зі швидкістю світла.

Висока точність

Цифрові документи повинні бути більш точними завдяки можливості редагування та співпраці в процесі створення документа. Ефективна система управління документами забезпечує всі інструменти, необхідні для створення, редагування та співпраці над документами для забезпечення якості та зменшення кількості неточностей. З такими функціями, як контроль версій та відстеження документів, усі зміни, внесені до документа, будуть видимі для решти групи / команди. Ви завжди можете повернутися до попередньої версії або запропонувати корективи, якщо вас не влаштовують внесені зміни.

Зменшення витрат на зберігання та постачання

Без системи управління документами вартість створення та управління документами може бути досить високою. Вартість паперу, друку, офісних приміщень, складських приміщень, шаф та найму працівників може скласти досить значну суму [25].

Навіть якщо всі документи зберігаються в цифровому вигляді, індивідуальна вартість кожної хмарної служби зберігання даних, яку ви використовуєте, може бути значною. При переході на систему управління документами можна позбутися усіх паперових файлів, зменшити обсяг пам’яті та використати офісний простір для більш продуктивної роботи, позбутися великих та потворних файлів, заощадити на папері, друку, чорнилі та інших канцелярських товарах і, нарешті, зекономити витрати на наймання нових співробітників для зберігання, пошуку та отримання цих документів.

Забезпечення конкурентної переваги

Компанія, що використовує систему управління документами, очевидно має конкурентну перевагу для тих, хто все ще зберігає свої важливі документи у папках на робочому столі, жорстких дисках, хмарних місцях зберігання та безлічі інших місць. Є багато переваг, які має компанія цифрового рівня перед їх еволюційними попередниками та старомодними конкурентами:

* Економія витрат на поставку та зберігання;
* Економія фінансів на нових працівниках для управління паперовими документами;
* Цифрові документи, як правило, більш точні;
* Співробітники можуть отримати доступ до інформації швидко та легко, заощаджуючи на них час та сили;
* Співробітники можуть надати кращі послуги клієнтам та запропонувати менші терміни виконання;
* Оскільки співробітники заощаджують багато часу, вони можуть зосередитись на речах, які насправді мають значення, та ефективніше сприяти успіху бізнесу.

1.3. Висновки до розділу

Запитання "Що таке електронний документ" розглядається як окремий випадок питання "Що таке документ". На початку минулого століття спроби забезпечити доступ до швидкозростаючої кількості доступних документів викликали питання щодо того, які саме слід вважати "документом". В результаті було розроблено функціональний погляд на "документ" і його визначено таким, що має організований фізичний відповідник.

Для практичних цілей люди розробляють прагматичні визначення, такі як "все, що може мати ім'я файлу та збережено на електронних носіях" або "колекція даних плюс властивості тих даних, що є для користувача логічною одиницею".

Поняття предметів як документів нагадує поняття "матеріальної культури" серед культурних антропологів, "для яких артефакти внесли важливі докази в документацію та інтерпретацію американського досвіду".

Одним із призначень інформаційних систем є зберігання та підтримка доступу до тих чи інших доказів, які були вказані як докази певного твердження. Інший підхід полягає в тому, що людина, яка має можливість класифікувати та організовувати артефакти, зразки, тексти чи інші предмети, повинна враховувати те, що вони можуть розповісти про світ, який їх створив, а потім, розробивши певну теорію його значення для визнання предмета доказом, пропонувати його як доказ у порядку їх організації, індексації чи подання.

Користувачі повинні мати єдине джерело інформації, що об'єднує цифровий контент з усіх куточків в одне місце, і воно має реалізовувати:

* Масштабованість і можливість забезпечити достатньо місця, оскільки кількість документів компанії зростає в результаті її успіху та розвитку;
* Забезпечення спільним простіром для співробітників, щоб вони збиралися разом і співпрацювали, створювали, керували та редагували документи та інші важливі файли;
* Надійну систему управління вмістом, щоб зберігати всі файли компанії та документи PDF, ексклюзивні аркуші, путівники, навчальні документи, відео, зображення тощо;
* Сильні можливості пошуку для швидкого перегляду заголовків документів та вмісту в документах, щоб працівники могли швидко та легко знаходити саме те, що шукають;
* Надійні засоби захисту інформації, що зберігається в системі, від сторонніх осіб або когось без належної згоди на доступ до цієї інформації.

Розділ 2

Існуючі концепції та реалізації документообігу

Коли можна відстежувати кожен аспект своєї ділової активності в Інтернеті з веб-сайтів, блогів, публікацій у соціальних медіа, електронних листів, відео тощо, чому б не використати цю можливість і до документів?

В цифрову епоху дані – основний аспект будь-якої діяльності. При наявності багатьох корисних даних про своїх клієнтів, потенційних клієнтів, інвесторів та навіть конкурентів, існує можливість налагодити те, що не працює і значно зменшити витрати у вже існуючих процесах та механізмах. Ось чому компанії відстежують велику кількість аспектів своєї діяльності. Підприємства та професіонали використовують передову аналітику, щоб вивчити, як їх роботу приймають, і зрозуміти, що вони роблять правильно та, особливо, неправильно [26].

2.1. Відстеження документів

Сьогодні можна відстежувати всі аспекти ділової активності в Інтернеті: веб-сайт, блог, соціальні медіа, електронну пошту, відео, аудіо тощо. Але в той же час, коли більшість роботи полягає у створенні та обміні документами, відсутність належних інструментів для вимірювання рівнів залучення до документа виглядає несподівано. Відсутнє відстеження документів. Відсутній спосіб швидко дізнатися, що сталося з вашим документом після того, як ви поділилися ним з кимось. Ефективна система може надати відповіді на наступні питання стосовно кожного з документів, що перебувають в обробці:

* Інша сторона його відкрила?
* Коли?
* Як далеко його прокручували перед тим, як закрити?
* Як часто його відкривали?

Ці дані є надзвичайно важливими для прийняття обґрунтованих бізнес-рішень у майбутньому, вивчаючи дієві та недієві аспекти. Аналіз цих важливих даних дозволяє використовувати їх із користю та отримувати перевагу перед конкурентами.

2.1.1. Ролі відстеження

Часто створюються ділові документи, щоб закрити угоду, руху бізнесу вперед, оновлення або повідомлення важливого клієнта, розділення досліджень. Створені документи надсилаються у вигляді вкладених файлів електронною поштою або в таких додатках для зв'язку, як Slack або Skype.

Незважаючи на те, що є інструменти для відстеження кількості звернень електронною поштою, не існує простого способу з’ясувати взаємодію з додатками в цих електронних листах. Навіть якщо хтось відкрив електронне або slack-повідомлення, не можна дізнатися, чи переглядали презентацію, яку їм надіслали, або наскільки її прочитали перш, ніж втратили інтерес.

Отримання критичної інформації про спільні документи, наприклад, хто їх відкрив, коли їх відкрили, як далеко їх прокрутили або скільки часу було витрачено на його перегляд, може змінити правила гри на користь того, хто отримує ці дані [27].

Інформація про відстеження документів допоможе зрозуміти:

* Чи дійсно клієнт, потенційний інвестор або власні працівники читають те, що їм надіслали;
* Чи потрібно зробити вміст документів більш привабливим;
* Чи потрібно реплікувати вміст на різні аудиторії;
* Як слід спостерігати за перспективою;
* Коли слід звертатися до клієнта.

2.1.2. Приклади відстеження документів на робочому місці

Маркетологи відстежують електронні книги, що розповсюджуються цільовим ринком. Колосальні 38% контент-маркетологів[?] розглядають електронні книги як найважливішу тактику маркетингу та створення потенційних клієнтів (лідів). Ще краще, що споживачі не відмовляються від своїх електронних адрес для цих електронних книг. За інформацією ImpactBND, 80% користувачів стверджували, що нададуть електронну пошту для «білого паперу» чи електронної книги. Важливо дізнатися, чи підходить вміст вашої електронної книги цій аудиторії, або потрібно досягати кращих результатів наступного разу. Єдиний спосіб пізнати його корисність – відстеження електронних книг.

Забезпечення та підтримка при використанні відстеження документів

Торгове забезпечення включає будь-який тип друкованого або цифрового ресурсу інформації, медіа чи контенту, який допомагає підтримувати процес продажу. Мета цих матеріалів – надати потенційним клієнтам необхідну для прийняття рішення, купувати ваш товар чи послугу, інформацію. Це зручний спосіб для продавців отримати додаткову підтримку в процесі продажу. Багато видів забезпечення продажів варіюються від брошур, цінових аркушів, блогу, торгових палаток, бюлетенів тощо. Можливість відстежувати забезпечення ваших продажів дає критичну інформацію про те, як реагують потенційні клієнти на вміст, який створюється, і як можна його вдосконалити, щоб краще продати в майбутньому.

Значні 40% працівників з поганою підготовкою залишають роботу протягом першого року [28]. Крім наставників та занять, новим співробітникам часто надається значна кількість навчальних матеріалів, таких як рекомендації, контрольні списки, інструкції з експлуатації, матеріали підтримки клієнтів, навчальні документи, бізнес-політика тощо. Якби була можливість відстежувати час, витрачений на ці документи, частоту їх перегляду і чи взагалі вони переглядалися. Таким чином, можна контролювати, чи дійсно нові працівники ознайомилися із наданим навчальним матеріалом.

Відстеження стану пропозицій щодо роботи

Рекрутери часто розсилають оффери високоефективним кандидатам в інших фірмах для їх найму. Було б доречно, якби вони могли відслідковувати, чи перевіряв потенційний кандидат публікацію або скільки часу він витратив на читання документа. Це допоможе рекрутерам визначити недоліки у своїх вакантних місцях та внести зміни до пропозиції, щоб залучити якісних кандидатів.

2.1.3. Стандартна операційна процедура

Стандартна операційна процедура (СОП) – це набір покрокових інструкцій, який компанія дає своїм працівникам, щоб допомогти їм виконувати складні рутинні операції. Оскільки СОП видаються менеджерами, щоб забезпечити послідовний та якісний результат, членам групи важливо ретельно виконувати ці інструкції. Маючи можливість відслідковувати ці документи на СОП, можна переконатись, що всі члени команди прочитали ці процедури та досконало зрозуміли процес.

Необхідність у інструменті відстеження документів, який може допомогти вам приймати розумні та обґрунтовані рішення та уникати дорогих помилок, є надзвичайно високою.

2.2. Управління документообігом

Документи – це значна частина нашого щоденного трудового життя. Незалежно від того, про яку галузь – охорону здоров’я, технології, автомобілі, фінанси чи будь-яку іншу – йде мова. Всі вони створюють та використовують документи щодня.

Насправді, професіоналу було б майже неможливо працювати цілий день без взаємодії (прямої чи опосередкованої) з документом. Це включає в себе проектні пропозиції, фінансові звіти, програмну документацію, вказівки щодо управління персоналом, маркетингові матеріали, навчальні посібники. Документи відіграють вирішальну роль у забезпеченні належного робочого процесу будь-якого бізнесу.

Однак проблема виникає тоді, коли доводиться керувати цими документами та ефективно працювати. Чим більше ми створюємо та покладаємось на ці документи для своєї щоденної роботи, тим важливішим є наявність надійних систем для управління ними.

Це те, про що йдеться в документообігу. Робочий процес управління документацією забезпечує впорядкування всіх документів на робочому місці, щоб кожен користувач міг швидко отримати доступ до документів і виконати свою роботу якісно. Без налаштування робочого процесу управління документами робота стає неефективною та повторюваною.

Незважаючи на те, що документи незамінні для нашої роботи, вони несуть відповідальність за значну неефективність у нашому робочому процесі. Всім знайома ситуація – витрата дорогоцінного часу на пошук документа на комп’ютері, на жорстких дисках, у хмарних папках, у чатових повідомленнях, у поштових скриньках тощо. Глобальне опитування працівників та ІТ-фахівців у 2012 році, проведене IDC, показало, що звернення до документів становлять 21,3% втрати продуктивності праці. Часто не можна знайти потрібні документи чи файли, коли вони вкрай потрібні або неможливо отримати доступ до документа через брак часу чи перешкоди місцезнаходження [29].

Ще одна причина уповільнення робочого процесу – це необхідність їх затвердження або валідації іншими співробітниками та менеджерами. Процес подання, перегляду та затвердження документа займає набагато більше часу, ніж повинен. Паперові документи часто подорожують від письмового до робочого столу, і їх можна проігнорувати або не помітити. Тож не дивно, чому наші документи втрачаються в цьому перебої та сповільнюють нашу роботу.

Саме з цієї причини багато компаній у всьому світі приймають поняття документообігу та управління документами, що часто досягається за допомогою програмного забезпечення для управління документами.

2.2.1. Програмне забезпечення для управління документами

Як випливає з назви, програмне забезпечення для управління документами – це інструмент, що дозволяє створювати, зберігати, керувати, захищати та отримувати цифрові документи.

Система управління документами – це набагато більше, ніж просто хмарний інструмент для зберігання цифрових документів. По суті, це основа, яка упорядковує робочі процеси та стимулює співпрацю, сприяючи вільному потоку критичної інформації по всій організації.

Управляючи документообігом, підвищується загальна ефективність роботи офісу, що в кінцевому рахунку позитивно впливає на прибуток компанії. Існує безліч переваг робочого процесу управління документами та переходу на програмне забезпечення для управління цифровими документами. Деякі з них перелічені нижче.

Основні переваги робочого процесу управління документами:

1. Позбутися неефективності паперових документів

Перехід з паперу на цифрові документи не тільки позбавляє від неефективності, пов’язаної з паперовими документами, але також допомагає заощадити додаткові експлуатаційні витрати, такі як обслуговування, друк, подача та зберігання паперу. Порівнюючи витрати середнього офісу (близько 25 000 доларів) на заповнення картотеки з чотирма ящиками та 2000 доларів на його підтримку, можна усвідомити вигідність цифрових документів.

2. Файли з паперами / документами

Відповідно до звіту Registeredrep.com, компанії з щорічним доходом від $ 500 000 до 1 мільйона доларів можуть заощадити близько 40 тисяч доларів на рік, перейшовши на управління цифровими документами. У той час як служба управління контентом Laserfiche оцінює економію 20% часу, засновану на ефективності подачі та пошуку, виключаючи помилки та ефективність робочого процесу [30].

Перехід до цифрових даних також означає, що ви допомагаєте навколишньому середовищу, зменшуючи кількість паперових відходів, створених офісом.

3. Значно підвищує ефективність роботи офісу

У сучасному швидкому світі, де щодня з’являються нові конкуренти, не можна витрачати свій дорогоцінний час на пошук файлі на комп’ютері. Оскільки більша частина часу витрачається на збирання інформації, не дивно, що 68% працівників вважають, що у них не вистачає годин на день, щоб виконати завдання [31].

Чудовий спосіб звільнити робочий час – використовувати систему управління документами для зручного створення, обміну, редагування та затвердження ваших документів. Таким чином, бізнес-процеси різко прискорюються, і працівники можуть витрачати час на виконання роботи.

4. Надійний і точний

Цифрові документи є більш надійними та точними відносно своїх паперових аналогів, тим більше, що редагування цифрового документа набагато простіше. Ефективна система управління документами постачається з усіма інструментами, необхідними для створення, редагування та співпраці над документами для впорядкування робочого процесу.

Такі функції, як керування версіями, гарантують, що буде можливість бачити всю часову шкалу документа та історію його появи. Якщо потрібно, користувачі можуть повернути документ до старішої версії, що неможливо зробити за допомогою паперових документів.

5. Активний пошук

Як відомо, пошук документа у картотеках – це не найкраще використання часу. Навіть якщо шукається цифровий документ, пошук потрібної хмарної програми, тої самої папки вхідних повідомлень або потрібної папки може зайняти багато часу.

Робочий процес управління документами гарантує швидкий пошук усіх потрібних документів та файлів, так що буде витрачено більше часу на роботу, ніж на пошук. Незалежно від того, наскільки великий каталог документів, робочий процес управління документами допоможе знайти файл за лічені секунди.

6. Економний

Gartner підрахував, що компанія може заощадити до 40% витрат, пов'язаних з документами, якщо розгорнути систему управління документами [32].

Вартість створення, зберігання та управління паперовими документами може бути досить високою, особливо, коли компанія зростає. Склади, шафи, вартість паперу, друк, офісні приміщення, сховища та наймання працівників, які всім цим керують – все це може бути досить недешевим.

Перейшовши на систему управління документами, можна позбутися від усіх паперових файлів, зменшити місце для зберігання, заощадити гроші на друк, чорнило та інші канцелярські товари, а також зекономити на винайманні нових працівників для управління цими документами.

7. Безпечний

Відомо, як важко захистити паперове документування, а потім запам'ятати, де знаходиться кожен документ. Система управління документами зберігає всі ваші файли в цілості та безпеці. З такими функціями, як відстеження документів, контроль версій паролів, сповіщення в режимі реального часу, захист паролем тощо, завжди легко дізнатися про етап життєвого циклу документа: хто його переглядав, коли, з якого місця та які зміни відбулися.

8. Масштабованість відповідно до конкретної компанії

Кількість документів, яка виробляється, безпосередньо пов'язана з кількістю працюючих або обсягом роботи. Коли компанія росте і стає успішною, кількість документів, які виробляються, також збільшується разом із нею. Більше документів призведе до більшого скупчення, що врешті-решт призводить до втрати продуктивності.

СУД не повинна ускладнювати її експлуатацію через зростання компанії, оскільки однією із найважливіших властивостей є масштабованість. Просто необхідно більше хмарного сховища для продовження операції без збоїв.

2.3. Electronic Data Interchange

Електронний Обмін Документами (англ. Electronic Data Interchange – EDI) – це обмін строго відформатованими повідомленнями, які представляють собою документи (крім грошових інструментів та документів) між комп'ютером та комп'ютером. EDI являє собою послідовність повідомлень між двома сторонами, кожна з яких може виступати в ролі як ініціатора, так і одержувача. Відформатовані дані, що представляють документи, можуть передаватися від відправника до одержувача за допомогою телекомунікаційних мереж або фізично транспортуватися на електронних носіях.

У EDI звичайна обробка отриманих повідомлень здійснюється лише за допомогою комп'ютера. Втручання людини в обробку отриманого повідомлення, як правило, призначене лише для помилок, для перевірки якості та для особливих ситуацій. Наприклад, передача бінарних або текстових даних не є EDI, як визначено тут, якщо ці дані не розглядаються як один або кілька елементів даних повідомлення EDI і зазвичай не призначені для інтерпретації людиною як частина онлайн обробки даних.

Приклад EDI – це набір обмінів між покупцем і продавцем. Повідомлення від покупця до продавця можуть включати, наприклад, запит на котирування (RFQ), замовлення на покупку, отримання консультацій та консультацій щодо оплати; повідомлення продавця до покупця можуть, зокрема, включати в себе ставки у відповідь на запитання, підтвердження замовлення на покупку, повідомлення про доставку та рахунок-фактуру [33]. Ці повідомлення можуть просто надавати інформацію, наприклад, отримувати поради або повідомлення про доставку, або вони можуть включати дані, які можуть бути інтерпретовані як юридично обов'язкове зобов'язання, наприклад, подання пропозицій у відповідь на запит про замовлення або замовлення на купівлю.

EDI використовується також для рішення все більш різноманітних задач, наприклад, для обміну між постачальниками медичних послуг та страховиками, для подорожей та бронювання готелів, для управління освітою, а також для державної регуляторної, статистичної та податкової звітності.

2.3.1. Стандарти, необхідні для EDI

З точки зору необхідних стандартів, EDI може бути визначений як обмін між комп'ютерами послідовності стандартизованих повідомлень, взятих із заздалегідь визначеного набору типів повідомлень. Кожне повідомлення складається, відповідно до стандартизованого синтаксису, з послідовності стандартизованих елементів даних. Саме стандартизація форматів повідомлень за допомогою стандартного синтаксису та стандартизація елементів даних всередині повідомлень робить можливим збирання, розбирання та обробку повідомлень комп'ютером.

Впровадження EDI вимагає використання сімейства взаємозалежних стандартів. Стандарти необхідні як мінімум:

1. синтаксису, який використовується для складання повідомлень та розділення різних частин повідомлення;
2. типів та визначень елементів даних програми, більшість з яких змінної довжини;
3. типів повідомлень, визначається ідентифікацією та послідовністю елементів даних, що утворюють кожне повідомлення;
4. визначення та послідовність елементів керування даними в заголовках повідомлень та трейлерах.

Додаткові стандарти можуть визначати:

1. набір коротких послідовностей елементів даних, що називаються сегментами даних;
2. спосіб, яким може бути включено більше ніж одне повідомлення в одну передачу;
3. спосіб додавання захисних засобів для цілісності, конфіденційності та автентифікації переданих повідомлень.

2.3.2. Обмежене охоплення цього стандарту.

Федеральні стандарти обробки інформації (англ. FIPS, Federal Information Processing Standards) охоплюють лише EDI. Вони не охоплюють інші форми електронних обмінів, наприклад, такі, що не складаються з повідомлень, взятих із заздалегідь визначеного набору. Крім того, додаток, що включає лише один або два заздалегідь визначені типи повідомлень, що використовують лише елементи даних фіксованої довжини, виключається з покриття цих FIPS. Він також не призначений для покриття передач з медичних, лабораторних або чутливих до змін в навколишньому середовищі приладів [34].

2.3.3. Довгострокова перспектива для стандартів EDI

На сьогоднішній день існує декілька різних стандартів EDI, але досягнення єдиної загальнодержавної родини стандартів EDI є цільовим завданням на довгий час. Єдине загальновживане сімейство стандартів дозволило б використовувати EDI ефективніше і мінімізувати сукупні витрати на використання. Зокрема, це

1. мінімізувало б потреби у навчанні персоналу для використання та підтримки стандартів EDI;
2. усувало б дублювання функціональності та витрати на досягнення цього дублювання, яке зараз існує у різних системах стандартів;
3. мінімізувало б вимоги до різних видів програмного забезпечення для перекладу;
4. дозволило б створити універсальний набір елементів даних, який полегшив би потік даних між різними, але взаємопов'язаними додатками, і тим самим максимізував обмін корисною інформацією.

FIPS визнають реальність того, що деякі сімейства стандартів EDI були розроблені для вирішення негайних потреб, і що включення мети універсальності у їх розвиток неприпустимо затримало б їх доступність. Однак передбачається майбутнє, в якому переваги універсальності переважають зависокі витрати на спеціалізовані рішення, що веде спочатку до співпраці між розробниками стандартів, потім до гармонізації стандартів і, зрештою, до єдиної загальновизнаної родини стандартів EDI.

2.4. Керівництво щодо розгортання EDI

EDI – це технологія, яка допомагає торговим партнерам та організаціям зробити більше, пришвидшити графіки логістики та усунути помилки вручну за допомогою автоматизації комунікацій рівня «бізнес-бізнес» (B2B). EDI допомагає багатьом організаціям, які виробляють, доставляють, купують та продають товари чи надають догляд, від торгових мереж та виробників до логістичних фірм, авіакомпаній, медичних працівників, страховиків тощо.

Незважаючи на те, що він застосовується з 1960-х років, EDI сьогодні знаходить нове застосування, що дозволяє автоматизувати ланцюги поставок, цифрову трансформацію і навіть як ключову частину робочого процесу та автоматизації бізнес-процесів. В цьому розділі надано чітке розуміння EDI для швидкого ознайомлення із усіма основами EDI, включаючи:

* Що таке EDI;
* Випадки використання EDI;
* Переваги EDI;
* Як працює EDI;
* Документи EDI;
* Впровадження EDI.

2.4.1. Що таке EDI?

EDI – це автоматизований обмін з комп'ютера на комп'ютер стандартних електронних ділових документів між діловими партнерами через безпечне, стандартизоване з'єднання.

Необхідно розбити це визначення EDI по частинах, щоб дати повне уявлення про дане поняття.

Комп'ютер-комп’ютер

EDI замінює ручні B2B-комунікації, такі як паперова пошта, факс та електронна пошта. Документи надходять безпосередньо від комп’ютерної програми відправника (наприклад, логістичної системи) до комп’ютерної програми одержувача (наприклад, системи управління замовленнями).

Ділові документи

Тисячі стандартних документів, пов’язаних із бізнес-транзакціями, можна автоматично надсилати за допомогою EDI.

Деякі поширені приклади включають:

* замовлення на купівлю;
* рахунки-фактури;
* статуси доставки;
* митні дані;
* документи про запаси;
* підтвердження платежів.

Стандартний формат EDI

Документи EDI обробляються на комп’ютерах і використовують стандартні, зручні для комп'ютера формати.

Стандарти описують кожен фрагмент даних та його формат (наприклад, тип документа, залучені сторони, дії, які слід вжити, дати створення та терміни виконання). Стандарти усувають відхилення від компанії до компанії, дозволяючи комп'ютерній системі кожного бізнес-партнера розмовляти загальною мовою.

Існують різноманітні стандарти EDI для різних галузей, регіонів та випадків використання – кожен з різними версіями, тому партнери EDI повинні використовувати той самий стандарт та версію.

Популярні стандарти включають: ANSI X12 в США, UN / EDIFACT в усьому світі та стандарти, що відповідають конкретним галузям, наприклад, акту про мобільність та підзвітність медичного страхування (Health Insurance Portability and Accountability Act HIPAA) [35].

Обмін документами EDI зазвичай відбувається між двома різними організаціями, які називаються діловими партнерами або торговими партнерами.

Приклад: компанія A може купувати товари у компанії B. Компанія A надсилає ордер про замовлення до компанії B, яка надсилає рахунки-фактури та повідомлення про відвантаження компанії A.

Безпечне, стандартизоване з'єднання

EDI використовує цілий спектр захищених протоколів для полегшення безпечного обміну документами EDI.

Партнери повинні використовувати той самий узгоджений протокол для обміну файлами EDI або працювати з посередником, який може полегшити обмін, якщо партнери використовують різні протоколи.

Протоколи варіюються від давно встановлених технологій, таких як FTP, до веб-EDI через AS2 (Applicability Statement 2), на основі API-систем, таких як AS4, та інших варіантів, таких як мобільний EDI.

Автоматизація

Повідомлення EDI можна надсилати автоматично за допомогою попередньо налаштованих робочих процесів.

Компанії зазвичай використовують перекладачі EDI – як програмне забезпечення, так і через постачальника послуг EDI – для перекладу документів EDI для використання у внутрішніх додатках, що дозволяє автоматизовану обробку.

Процеси можуть бути розширені для роботи з інтеграцією даних та робочими потоками в організації.

Приклад: щойно компанія отримує замовлення на закупівлю EDI, система логістики формує завдання для складського персоналу переміщати товари з товарних запасів до доставки.

Щоб проілюструвати значення EDI або електронного обміну даними, треба порівняти, як типова операція із закупівлі проходитиме між двома торговими партнерами, використовуючи традиційні паперові комунікації (або електронну пошту) порівняно з використанням EDI.

Традиційні методи:

* Покупець або отримує сповіщення у своїй системі про замовлення, або, запитуючи товарний запас, визначає, що йому потрібно зробити замовлення;
* Покупець вносить дані на екран системи закупівлі для створення ордеру, роздруковує та надсилає поштою або надсилає електронний лист постачальнику;
* Постачальник отримує пошту через декілька днів, або електронний лист (разом із довгим списком інших комунікацій) та вручну вводить в систему замовлень;
* Постачальник роздруковує рахунок-фактуру і додає його до вантажу та / або надсилає окремо поштою чи електронною поштою.
* Покупець вручну вносить рахунок-фактуру в систему кредиторської заборгованості.

У цьому прикладі паперова система може додати тиждень часу на комунікації до процесу. І електронна пошта, і папір вразливі до помилок при введенні даних вручну, подовжуючи час замовлення.

2.4.2. Процес EDI

* Система закупівель покупця, яка використовує EDI, автоматично генерує та відправляє ордер про замовлення у форматі EDI, коли товарний запас досягне заздалегідь заданого рівня;
* За лічені хвилини система замовлень продавця, використовуючи програмне забезпечення EDI, отримує даний ордер системою EDI;
* Система постачальника автоматично повідомляє їх відділ доставки про відправлення товару;
* Після того, як товар упакований і готовий до відправки, система доставки генерує розширені повідомлення про доставку (ASN) для відправки до відділу прийому покупців;
* ERP-система постачальника потім генерує рахунок-фактуру EDI для передачі до системи кредиторської заборгованості покупця.

Весь процес EDI може бути завершений за годину.

2.4.3. Використання EDI

Жодне визначення EDI не є повним без прикладу застосування в реальному світі. Електронний обмін даними корисний для широкого спектру функцій, що охоплюють багато тисяч конкретних обмінів інформацією. Ось лише декілька найпоширеніших сценаріїв, коли EDI є корисним через значну кількість типів транзакцій, які EDI обробляє щодня.

Ланцюги поставок (Роздріб, виробництво, автомобільна індустрія)

* Придбання;
* Виконання замовлення;
* Підтвердження доставки;
* Міжнародні замовлення;
* Виконання замовлення на запчастини;

Охорона здоров'я

* Обмін інформацією про стан здоров'я пацієнта;
* Обробка даних щодо медичного страхування;
* Обмін інформацією за рецептом;

Логістика

* Планування відправлень;
* Відстеження товарів;

Бухгалтерський облік

* Створення рахунків-фактур;
* Забезпечення аудиторських маршрутів;

Авіація

* Обмін інформацією про рейс;
* Записи імен пасажирів (Passenger name records – PNR);
* Міжнародна відповідність та стандартизація.

2.4.4. Переваги EDI

EDI допомагає компаніям покращити швидкість, точність, ефективність та витрати, а деякі найбільші переваги EDI припадають на стратегічний рівень бізнесу [36]. Тут розкривається роль EDI для бізнесу:

Швидша обробка

* EDI може пришвидшити ділові цикли на 61%;
* EDI дозволяє здійснювати транзакції за лічені хвилини замість днів або тижнів, проведених на пошті або у листуванні електронною поштою;
* Автоматизація завдань на паперовій основі звільняє ваш персонал від завдань з більш високою цінністю та надає їм інструменти для підвищення продуктивності;
* Швидка обробка точних ділових документів призводить до меншої кількості перероблених замовлень, розпродажів запасів та скасування;
* Автоматизація обміну даними додатків через ланцюжки постачання забезпечує критичну передачу важливих даних вчасно та відстеження в режимі реального часу;
* Скорочення обробки та доставки замовлень допомагає організаціям зменшити товарний запас;

Зниження витрат

* EDI зменшує трансакційні витрати на папір, друк, відтворення, зберігання, подачу документів, відправлення поштових відправлень та отримання документів, економлячи підприємствам більше 35 % від транзакційних витрат;
* Для покупців, які здійснюють численні транзакції, використання EDI також може призвести до отримання мільйонів доларів щорічних заощаджень через знижки дострокового платежу;
* У деяких випадках EDI становить лише 1/20 витрат часу порівняно із традиційними способами на обробку замовлень вручну, зменшуючи витрати в 20 разів;
* EDI також усуває дорогі помилки через нерозбірливі факси, втрачені замовлення або неправильно прийняті замовлення на телефон;

Більше точності, менше помилок

* EDI знижує помилки угод на 30-40%;
* EDI усуває людські помилки через нерозбірливі почерки, втрачену пошту та помилки при натисканні клавіш;

Кращі стосунки

* Продавці виграють від покращеного грошового потоку та скорочення циклів операцій на замовлення;
* Насправді EDI може скоротити час циклу операцій на замовлення більш, ніж на 20%, покращуючи транзакції та відносини ділових партнерів;
* Зменшення помилок також економить партнерам цінний час та розчарування при вирішенні суперечок;

Стратегічні переваги

* EDI забезпечує в режимі реального часу видимість стану транзакцій, що дозволяє швидше приймати рішення та краще реагувати на вимоги клієнтів та ринку, допомагаючи бізнесу приймати підхід, орієнтований на попит;
* Покращення продукту та доставка мають менший термін використання;
* Упорядковує процес введення нових територій, оскільки EDI надає загальну світову ділову мову;

Екологічні переваги

* EDI сприяє стійкості та зменшує викиди СО2 шляхом заміни процесів на паперовій основі електронними альтернативами;
* EDI збільшує експлуатаційну ефективність, що призводить до меншої кількості помилок та менших витрат енергії.

2.4.5. Алгоритм EDI

У процесі надсилання документів EDI є три етапи: підготувати документи, перевести їх у формат EDI та надіслати їх партнеру [37].

Один загальний процес, автоматизований за допомогою EDI, – це обмін замовленнями на купівлю та рахунками-фактурами. Щоб надати вам хороший приклад того, як працює EDI, ми проілюструємо процес EDI для ордерів замовлення та рахунків-фактур.

Підготовка документа

На прикладі покупок і накладних саме тут покупець готує замовлення в системі закупівлі:

* Покупець збирає та впорядковує дані для того, щоб в нього була можливість працювати з EDI;
* Наприклад, замість друку ордеру про замовлення система створює електронний файл з необхідною інформацією для складання документа EDI.

Існує кілька підходів щодо підготовки документів:

* Експорт даних на основі комп'ютера з електронних таблиць або баз даних;
* Переформатовані електронні звіти у файли даних;
* Покращення програм для створення вихідних файлів, готових до стандартного перекладу EDI;
* Придбання програмного забезпечення EDI, яке може перетворити документи із ваших систем у файли EDI;
* Введення даних про людину.

Ідеальна система має усунути якомога більше людських даних, щоб заощадити час та підвищити точність.

Переклад документів EDI

Наступним кроком є ​​подача документа через програмне забезпечення для перекладу і перетворення внутрішнього формату даних у стандартний формат EDI, використовуючи відповідні сегменти та елементи даних. Крім того, ви можете надіслати свої дані постачальнику послуг EDI, який обробляє переклад у та від формату EDI від вашого імені.

Підключення та передача документів EDI

Після того, як ордер переведено у формат замовлення, він готовий для передачі постачальнику. Існує кілька способів підключитися до партнера за допомогою EDI. До найбільш поширених належать:

* Пряме з'єднання EDI від точки до точки через захищений Інтернет-протокол, наприклад, AS2;
* Підключення до постачальника мереж EDI, який також називається провайдером мережі з доданою вартістю – Value Added Network (VAN);
* Поєднання Direct EDI та VAN, залежно від залучених партнерів та обсягу транзакцій.

У випадку постачальника мережі EDI або VAN, покупець використовує їх протокол зв'язку, забезпечуючи надійну і безпечну передачу EDI. Потім постачальник мережі підключається, використовуючи уподобаний протокол зв'язку постачальника, гарантуючи, що постачальник отримує замовлення. VAN можуть зменшити налаштування та обслуговування в деяких випадках, але, як правило, дорожчі, ніж інтеграція «точка-точка-точка» для багатьох випадків використання, оскільки вони стягують плату за кожну транзакцію або навіть позицію.

Безпека та контроль даних підтримуються протягом усього процесу передачі за допомогою паролів, ідентифікації користувача та шифрування. Як покупець, так і постачальник EDI-програми автоматично редагують та перевіряють документи на точність.

Документи EDI

Для кращого розуміння EDI потрібно розглянути ключові процеси обробки EDI. Документ EDI складається з трьох основних фрагментів: конверт, сегмент та елементи даних. Він відформатований відповідно до конкретного стандарту EDI.

Документи EDI, такі як ордери, повинні відповідати строгим правилам форматування, які точно визначають, куди і як надходить кожен фрагмент даних у документі, щоб перекладач EDI на комп’ютері, що приймає, миттєво знаходив усі ключові дані, наприклад, назву компанію покупця, поштовий номер, придбані товари та вартість. Потім дані будуть надходити у систему введення замовлення постачальника у відповідному внутрішньому форматі, не вимагаючи жодного ручного введення.

Для передачі документів EDI використовується система з трьох конвертів для розміщення наборів транзакцій:

* Конверт для повідомлень;
* Груповий конверт;
* Обмінний конверт.

Сегмент у наборі транзакцій EDI – це група подібних елементів даних.

Елементи даних у наборі транзакцій EDI – це окремі дані в документі, такі як товар, що купується, кількість придбаних предметів тощо.

2.4.6. Впровадження EDI

Досягнення відповідності EDI в кінцевому рахунку означає наступне:

* Налаштування інфраструктури EDI;
* Вирівнювання налаштування EDI із системами EDI торгових партнерів;
* Дотримання загальних стандартів.

2.4.7. Інфраструктура EDI

Щоб розпочати роботу з EDI, потрібно або придбати і налаштувати, або передати такі ключові компоненти:

* Програмне забезпечення EDI для зв'язку, поштового боксу транзакцій EDI, картографування EDI та перекладу EDI;
* Інтернет-комунікації, VAN тощо, як того вимагають різні партнери;
* Обладнання: сервер або ПК, пристрої зв'язку та периферійні пристрої;
* Забезпечити приміщенням належного рівня безпеки;
* Резервне копіювання даних та надмірна потужність для надійності;
* Програмне забезпечення для будь-якої інтеграції транзакцій EDI із системами бек-офісу;
* Карти для кожного типу документів EDI, що обмінюються з кожним партнером, для відображення записів EDI у ділових документах, що використовуються.

Крім того, потрібно навчити команду щодо використання програмного забезпечення та комунікаційних пристроїв EDI або вибору партнера з інтеграції EDI, щоб налаштувати все це та навчити команду [38].

EDI компанії є настільки ж цінним, як і інтеграція з системами партнерів. До основних моментів можна віднести:

* Визначення протоколів EDI, які використовуються для надсилання та прийому документів EDI (наприклад, AS2, SFTP тощо);
* Вибір та впровадження обмінів на правильні документи або транзакції EDI ;
* Включення EDI в інші оперативні, логістичні або 3PL, системи обліку та виконання замовлень;
* Грамотна інтеграція карт EDI, переклад та тестування із партнерами.

Залежно від налаштувань, це може включати взаємний вибір рішень EDI та постачальників інтеграції EDI. Зрештою, вам знадобляться правильні рішення, які допоможуть вам максимально покращити ваше партнерство. Чим простіше налаштування (за допомогою найбільш універсальних інструментів), тим швидше можна впровадити EDI і почати економити час і гроші під час покращення відносин зі своїм партнером.

Загальні, сертифіковані стандарти – це своєрідний клей, який тримає EDI разом. Ключові сертифікаційні органи регулюють ці стандарти та можуть допомогти оцінити різні рішення.

* ANSI – сертифікує стандарт X12 EDI, який використовується в США;
* UN / CEFACT – сертифікує популярний міжнародний стандарт EDIFACT;
* GS1 – сертифікує декілька галузевих міжнародних стандартів EDI (побудований на EDIFACT);
* Drummond – сертифікує програмне забезпечення EDI шляхом суворих тестів на сумісність, гарантуючи, що різні інструменти EDI можуть успішно спілкуватися між собою.

2.5. Стандарти EDI

З моменту появи EDI в 1960-х роках організації намагалися стандартизувати обмін повідомленнями на рівні організацій/компаній. Завдяки різноманітним вимогам бізнесу, галузі оптимізували формати обміну повідомленнями для власного використання, в результаті чого на сьогоднішній день використовуються понад десяти популярних стандартів EDI. Популярні формати, такі як X12, EDIFACT, TRADACOMS та ebXML, використовуються в різних галузях для полегшення ділового спілкування, тоді як варіації форматів EDI визначають транзакції в унікальних галузевих сценаріях.

2.5.1. EANCOM

EANCOM – стандарт EDI, який використовується для інтеграції інформації, що надсилається в електронному вигляді, з фізичним потоком товарів по всьому ланцюгу поставок. Це підмножина стандарту UN / EDIFACT EDI і містить лише повідомлення, що використовуються в бізнес-програмах, виключаючи багато зайвих, необов'язкових повідомлень від EDIFACT.

Стандартні повідомлення, доступні в EANCOM, можна розділити на такі категорії: Основні дані, Комерційні операції, Звіт і Планування та Транспортні.

Повідомлення, доступні в EANCOM, охоплюють усі функції, необхідні для завершення торгової операції між партнерами, що обмінюють товари.

Кожне повідомлення EANCOM містить стандарти GS1 для таких аспектів:

* Фізична ідентифікація товарних позицій;
* Одиниці логістики;
* Глобальні номери локації (GLN), що ідентифікують торгових партнерів.

Комерційні організації вибирають повідомлення та сценарії залежно від своїх особистих виробничих потреб.

Спочатку EANCOM був створений для роздрібної торгівлі та споживчих товарів і став одним з найпопулярніших, найбільш важливих стандартів EDI в європейській галузі споживчих товарів. У наступні роки він почав використовуватися у галузях охорони здоров'я та будівництва [39].

* Розроблений у 1987 році;
* Поглинуто GS1 у 2015 році;
* Оновлено завдяки GS1 у 2016 році.

Керується GS1, міжнародною організацією зі стандартів, яка також керує EDIFACT.

Переваги EANCOM

У EDI важливо чітко визначити продукти, послуги та залучені сторони, а кодування інформації, що обмінюється EDI, має високе значення для автоматичної обробки. Повідомлення EANCOM визначають кожен продукт та партію відповідно до унікального номера статті EAN та номера EAN.

Ці стандарти EAN дають значні переваги, включаючи наступне:

* Конвенція про стандартну нумерацію – ідентифікатори EAN є унікальними та визнаними у всьому світі, тому організаціям не потрібно вести складні довідкові листи для партнерів та коди;
* Стандартні повідомлення прості та точні. Чітке кодування продуктів та місць спрощує повідомлення EDI, економлячи час та ресурси на обробку;
* Багатопромисловий стандарт. Оскільки будь-який предмет може бути визначений унікальними ідентифікаторами EANCOM, будь-який бізнес може використовувати EANCOM для торгівлі;
* Технічне обслуговування та підтримка. Стандарт EANCOM постійно підтримується та підтримується GS1 (раніше відомий як EAN International);
* Міжнародна та мовна підтримка. Повідомлення EANCOM використовуються у всьому світі. GS1 охоплює понад 80 країн та надає підтримку EANCOM багатьма місцевими мовами.

Типи транзакцій EANCOM

Найчастіше використовуються типи повідомлень – замовлення на купівлю (orders), поради щодо доставки транспорту (DESADV) та рахунки-фактури (INVOIC), але повідомлення EANCOM охоплюють усі функції, необхідні для управління повноцінною торговою транзакцією.

Повідомлення EANCOM можна розділити на чотири категорії:

* Основні повідомлення даних: містять дані, які відповідають усім транзакціям;
* Повідомлення про комерційні транзакції: використовуються для банківських операцій;
* Повідомлення щодо транспорту та логістики: інструктуйте транспортні послуги щодо того, як і куди переміщувати вантажі;
* Повідомлення звітів та планування: надають корисну інформацію для звітності.

Основні повідомлення даних можна розділити на дві підкатегорії послідовної інформації:

* Інформаційне повідомлення учасника: визначені всі фізичні та віртуальні місця (ім’я, адреса, контакти, фінансові рахунки тощо), які використовуються при транзакціях;
* Інформаційні повідомлення про товар: надають інформацію, що містить описову, логістичну та фінансову інформацію про товар чи послугу.

Повідомлення про комерційні операції охоплюють фінансовий цикл торгівлі та поділяються на три підкатегорії:

* Котирування повідомлень: містять фінансовий запит від потенційного покупця (умови доставки, умови оплати, каталоги цін, надбавки, збори тощо);
* Повідомлення про замовлення: стосуються процесу замовлення від запропонованого замовлення до подальших змін та підтвердження замовлення (відповідні кількості, дати, місце доставки тощо);
* Повідомлення рахунків-фактур та переказів: покриття оплати за доставлені товари; покупець може автоматично узгодити рахунок-фактуру постачальників, використовуючи інформацію про отримання товару.

Транспортно-логістичні повідомлення: надають інформацію про консультацію щодо відправки (DESADV), транспортування та отримання замовленої продукції.

Повідомлення звітів та планування надають звіти про торгівлю, що дозволяють партнерам планувати стратегії, обмінюватися інформацією про вимоги з актуальними звітами та прогнозами щодо доставки, продажу та запасів. Існує два типи:

* Синтаксис та сервісний звіт: одержувач будь-якого повідомлення EANCOM може надіслати його, щоб підтвердити або відмовитися від обміну або участі у функціональній групі;
* Загальне повідомлення: використовується для надсилання даних, які не вписуються в якесь конкретне стандартне повідомлення.

2.5.2. EDIFACT

EDIFACT розшифровується як Electronic Data Interchange For Administration, Commerce and Transport (електронний обмін даними для адміністрації, торгівлі та транспорту). Це прийнятий стандарт EDI для міжнародної торгівлі за межами США і включає в себе:

* Правила синтаксису для структуризації даних;
* Протокол інтерактивного обміну (I-EDI);
* Стандартні повідомлення (набори документаційних транзакцій) для обміну між країнами та галузями;
* Каталоги елементів даних;
* Вказівки щодо електронного обміну структурованими даними між комп'ютерними системами.

Переваги EDIFACT

EDIFACT став загальноприйнятим стандартом EDI через його здатність передавати всі типи транзакцій в єдиний файл зі стандартизацією, автоматичним введенням та автоматичною обробкою. Автоматизовані процеси зменшують потребу в ручних процедурах, схильних до помилок.

Ці широкі можливості підвищують ефективність при надсиланні більшого обсягу транзакцій. Компанії можуть легко координувати безпаперові передачі даних з невеликими обмеженнями стосовно галузі чи країни, що отримує повідомлення.

Багато компаній виграють від комплексних наборів транзакцій EDIFACT, які пропонують безліч типів повідомлень, включаючи транзакції щодо співпраці постачальників, фінансів, циклу замовлень, складських складів, управління логістикою, обробки матеріалів, а також інших категорій ділового спілкування.

Підмножини EDIFACT

Комплексні набори транзакцій в рамках стандарту EDIFACT були створені майже для кожної ділової транзакції та галузі. Широта можливостей комунікації призвела до розробки підмножини (або підстандартів), що впорядковує комунікації та дозволяє компаніям обробляти повідомлення з більшою легкістю та розумінням [40].

Приклади галузевих стандартів підмножини EDIFACT включають:

* CEFIC – Хімічна промисловість;
* EANCOM – промисловість споживчих товарів;
* Edi@Energy – Електрика та газ (діє лише для Німеччини);
* EDIBDB – Промисловість будівельних матеріалів;
* EDIFICE – Електроніка, програмне забезпечення та телекомунікаційна галузь;
* EDIFOR – Експедиторська галузь;
* EDIFURN – Меблева промисловість;
* EDIGAS – газопередача та торгівля;
* EDILEKTRO – Електротехнічна промисловість / Оптова торгівля електротехнікою;
* EDILIBE – Продавці книг;
* EDIPAP – Виробник паперу / оптовий продаж паперу / переробка паперу;
* EDITEC – Санітарна промисловість;
* EDITEX – Текстильна промисловість;
* EDITRANS – Транспортна економіка;
* EDIWHEEL – виробник шин і коліс (включаючи різне EDI);
* ETIS – Телекомунікації (тільки для рахунків-фактур);
* ODA / ODIF – загальні формати документів;
* ODETTE – Автомобільна промисловість;
* RINET – Страхова галузь.

Операції та схеми

EDIFACT охоплює понад 10 тис. конкретних бізнес-операцій, починаючи від простих замовлень на придбання та рахунків-фактур, до розширеної документації по доставці, логістичної інформації та повідомлень, що стосуються галузей.

EDIFACT EDI визначається його щільно сплетеною структурою, яка сприяє організації та ефективності. Ось деякі його основні особливості.

Правила синтаксису дозволяють забезпечити більшу однаковість у структурі повідомлень, забезпечуючи однаково зрозуміле повідомлення для всіх приймачів даних, незалежно від програмного забезпечення або обладнання, яким вони користуються. Крім того, стандартизована структура дозволяє користувачам включати лише необхідний вміст для оптимізації передачі файлів.

Протокол інтерактивного обміну дозволяє компаніям спілкуватися через динамічний та прямий діалог під час обміну повідомленнями, що стосуються ділової транзакції. Інтерактивний обмін призводить до скорочення часу реакції та покращення комунікацій для обох сторін.

Перевага стандартизованих повідомлень залишається однією з найпомітніших особливостей EDIFACT EDI. Її єдині повідомлення оптимізують потік даних між підприємствами в галузях та на міжнародних кордонах, зберігаючи чітку комунікацію.

Якщо синтаксис являє собою граматику стандартних повідомлень EDIFACT, то елементи даних – це його словниковий запас (необроблені дані транзакції). Елементи даних функціонують як поле даних, представляючи інформацію, таку як номери статті. Вони живуть у межах сегменту і визначаються за своїм станом. Каталоги елементів даних оновлюються та публікуються кожні півроку ЄЕК ООН (Європейська Економічна Комісія ООН).

За даними ЄЕК ООН, EDIFACT EDI продовжує регулюватися "набором міжнародних узгоджених стандартів, каталогів та вказівок для електронного обміну структурованими даними між незалежними комп'ютеризованими інформаційними системами". Положення та опубліковані вказівки (UNTDID – Директорія обміну даними про торгівлю ООН) захищає єдиний, універсальний характер стандарту EDIFACT від корупції та внутрішнього злому.

Структура EDIFACT

Сегменти даних в рамках EDIFACT – це просто дані, організовані в логічні сегменти, що утворюють повідомлення.

Існує два типи сегментів даних:

* Сегменти обслуговування (починаючи з ООН);
* Сегменти даних користувачів (усі інші).

Обмін може включати такі сегменти даних:

* Сегменти обслуговування:
  + UNA – сервісні строкові поради;
  + UNB – заголовок обміну;
  + UNF – функціональний груповий заголовок;
  + UNH – заголовок повідомлення;
* Сегменти даних користувачів:
  + UNT – трейлер повідомлення;
  + UNE – функціональний груповий трейлер;
  + UNZ – трейлер обміну.

Рядок сегментів даних містить повідомлення EDIFACT, а в реальному розумінні повідомлення є єдиним бізнес-документом, підготовленим для передачі EDI. Хоча сегменти сервісу необхідні для стандартної форми та передачі, сегменти даних користувачів містять дані, специфічні для користувача, по суті, інформацію, що потребує передачі. Сегменти даних користувачів включають такі значення, як кількість, адреси та іншу конкретну інформацію, необхідну для повідомлення.

Найвища одиниця в повідомленні EDIFACT – обмін. Це як конверт для повідомлення. Він включає в себе одержувача повідомлення, відправника, номер, дату тощо. Його стандартизована форма дозволяє передавати повідомлення в електронній формі.

Пари даних визначають початок і кінець конверта, будь то конверт набору транзакцій для кожного пов'язаного документа, конверт групи, що містить декілька пов'язаних документів, або конверт обміну, що містить усі необхідні дані для передачі одному відправнику.

Кожен з цих конвертів використовує конкретні сегменти даних, як UNH та UNT (транзакційний набір конвертів) для позначення початку та кінця конверта. Цей високоорганізований формат сприяє чіткій та впорядкованій передачі декількох наборів транзакцій за один обмін.

Використання EDIFACT

EDIFACT служить світовим стандартом електронного обміну даними (EDI). Організація Об'єднаних Націй спочатку розробила EDIFACT у 1987 році та продовжує керувати стандартом EDI через Центр сприяння торгівлі та електронному бізнесу (UN / CEFACT), які входять до UNTDID (Каталог обміну даними про торговельні дані ООН).

Організації, що активно залучаються до міжнародної торгівлі, першими прийняли стандарт EDIFACT. Багато з них були багатонаціональними корпораціями, які прагнули впорядкувати свої транзакції між країнами. Врешті-решт, інші компанії у їх ланцюжку поставок впровадили EDIFACT EDI, включаючи страхові, банківські та урядові організації.

У Сполучених Штатах однією з перших компаній, що застосували стандарт EDIFACT, був General Motors, який, в свою чергу, скеровував своїх постачальників слідувати цьому. З часом американські організації зі стандартів, а саме ANSI, розробили конверсії, які сприяли переходу на новий міжнародний стандарт EDI для багатьох компаній.

2.5.3. EDIG@S

EDIG@S або EDIGAS – це рішення EDI, розроблене спеціально для обміну інформацією між партнерами в газовому секторі.

Цей стандарт EDI походить від стандарту EDIFACT ООН, використовуючи підмножину повідомлень EDIFACT. Спочатку створений чотирма газовими компаніями як незалежний стандарт угод, тепер EDIGAS має 14 компаній-членів, які керують його застосуванням, і використовується усіма транснаціональними газовими та енергетичними компаніями. Сьогодні EDIGAS також підтримує транзакції XML.

Типи транзакцій EDIG@S

EDIGAS охоплює широкий спектр обміну інформацією для газових компаній та їх партнерів, включаючи закупівлю, транспорт, розподіл, розрахунки, торгівлю тощо.

Стандарт було створено у 1983 році і удосконалено у 1996 році та оновлено для можливості використання стандартних транзакцій ООН / EDIFACT [41].

HIPAA EDI є прямим результатом прийняття в США Акта про переносимість та підзвітність медичного страхування (HIPAA), закону, що регулює, окрім всього, електронний обмін даними про охорону здоров'я, включаючи документи EDI, безпеку та управління даними.

HIPAA EDI охоплює обмін електронними документами між медичними працівниками та страховиками. Медична практика та інші постачальники медичних послуг зобов'язані використовувати HIPAA EDI під час електронного обміну будь-якою конфіденційною адміністративною інформацією

Завдання HIPAA EDI полягає в тому, щоб звести сотні форматів даних про охорону здоров'я до загальноприйнятого стандарту даних про охорону здоров'я. Така уніфікованість значно збільшує портативність та доступність інформації, пов’язаної зі здоров’ям, та зменшує адміністративні витрати.

Закон про переносимість та підзвітність медичного страхування (HIPAA), прийнятий в 1996 році в США, вимагає мільйонів медичних установ, які передають в електронному вигляді дані для використання EDI у стандартному форматі HIPAA.

Використовується в наступних галузях:

* Охорона здоров'я;
* Медична страховка.

HIPAA EDI керує майже всіма видами електронних транзакцій, включаючи:

* Медичні претензії;
* Стан претензій;
* Поради щодо переказів (RA);
* Перевірка відповідності та відповіді;
* Координація переваг (COB).

В 1991 році були встановлені стандарти передачі даних про охорону здоров'я. У 1996 році американський федеральний закон HIPAA ухвалив стандартні транзакції даних в галузі охорони здоров'я. У 2001 році лікарі, лікарні, медичні плани почали впроваджувати EDI. У 2003 році всі медичні сторони повинні були повністю впровадити EDI.

Федеральний закон США зобов’язує використовувати HIPAA EDI в галузі охорони здоров'я. Американський національний інститут стандартів (ANSI) керує X12, прийнятим стандартним форматом для транзакцій HIPAA EDI

2.5.4. HL7

Health Level Seven або HL7 – це сукупність міжнародних стандартів для передачі клінічних та адміністративних даних між програмними комплексами, які використовуються постачальниками медичних послуг. Ці стандарти орієнтуються на прикладний рівень, який є "рівнем 7" у моделі стандартизації Міжнародної організації стандартів (ISO).

Лікарі та інші медичні працівники, як правило, мають різноманітні комп’ютерні системи, що застосовуються для всього, починаючи від виставлення рахунків і до відстеження пацієнтів. HL7 допомагає всім цим системам взаємодіяти, коли вони отримують або потребують отримання нової інформації. HL7 визначає різноманітні гнучкі стандарти, вказівки та методології, які системи охорони здоров’я можуть використовувати для обміну інформацією та обробки даних у єдиний, послідовний спосіб. Цей обмін інформацією допоміг зробити медичну допомогу менш географічно ізольованою [42].

Галузі, що використовують HL7:

* Охорона здоров'я;
* Лікарні та клініки.

Типи транзакцій HL7

HL7 забезпечує стандартизацію сотень заходів охорони здоров’я в лікарняних системах. Невеликий список цих транзакцій включає:

* Сповіщення про пацієнтів;
* Передача пацієнтів;
* Виписка пацієнта;
* Інформація про клінічне дослідження;
* Основні файли;
* Аптечні замовлення;
* Дієтичні рецепти.

Створений у 1987 році разом із заснуванням International Health Seven International. Постійно оновлюється та підтримується.

2.5.5. IATA Cargo-IMP

IATA Cargo-IMP розшифровується як International Air Transport Association Cargo Interchange Message Procedures (Міжнародна асоціація повітряного транспорту). Це стандарт EDI, заснований на EDIFACT, створений для автоматизації та стандартизації обміну даними між авіакомпаніями та іншими сторонами.

Cargo-IMP IATA – це застарілий стандарт для обміну критичною інформацією про вантажні операції. Але IATA перестала підтримувати Cargo-IMP після 34-го видання в 2014 році. Метою цього було повністю зосередити увагу на розширенні можливостей Cargo-XML (розширювана мова розмітки вантажів), нового сучасного формату обміну повідомленнями [43].

Cargo-XML полегшує вантажні бізнес-процеси, виконує власні вимоги щодо подання розширеної інформації про вантажі (Advanced Cargo Information – ACI) та відповідає таким правилам безпеки, як e-CSD. Цей новий формат, в кінцевому рахунку, допомагає галузі вантажних авіаперевезень рухатися до вдосконалення своїх процесів шляхом оцифрування всього ланцюжка поставок.

Тим не менш, Cargo-IMP все ще широко використовується для електронних повідомлень у галузі, незалежно від відсутності вдосконалення від IATA. Триває міграція зі старого формату Cargo-IMP до Cargo-XML.

Типи транзакцій

IATA Cargo-IMP визначає процедури автоматичного обміну та розподілу: місця, авіанакладних, маніфестів рейсів, обліку, статусу, розбіжностей, ембарго, митних процедур, виставлення рахунків CASS, небезпечних вантажів.

Створений у 1983 р., доопрацьований у 1996 році та оновлений для використання стандартних транзакцій UN / EDIFACT

Розроблявся IATA спільно із її авіакомпаніями-членами та авіакомпаніями Airlines for America (A4A). Він також схвалений Комітетом з вантажів, вантажними перевізниками та конференціями вантажних агентств.

Міжнародна асоціація повітряного транспорту (IATA) – торгова асоціація світових авіакомпаній, що становить близько 290 авіакомпаній або 82% загального авіаперевезення.

Авіакомпанії Америки (A4A) виступають від імені своїх членів для формування важливих політик та заходів, що сприяють безпеці американських авіакомпаній.

2.5.6. IATA Cargo XML

У 2012 році IATA створила стандарт IATA Cargo XML для заміни стандарту IATA Cargo-IMP. У 2014 році IATA випустила своє 34-е видання IATA Cargo-IMP та оголосила, що це останнє оновлення протоколу, а всі подальші оновлення переходять на IATA Cargo XML.

Запуск IATA Cargo XML був приурочений завершенню залежності авіаційної галузі від системи на базі EDIFACT та оновленню до більш сучасного стандарту. IATA CARGO XML із лозунгом «Нова здатність до розповсюдження», є частиною ширшої ініціативи IATA «Спрощення бізнесу», що виникла в 2004 році для підвищення ефективності в авіації. Він включає інновації, такі як електронні квитки, посадкові талони з штрих-кодом та нові варіанти самообслуговування багажу.

Стандарт IATA Cargo XML дозволяє пропонувати ті ж самі варіанти, що пропонують покупцям подорожей на високих вулицях, як і тим, хто бронює безпосередньо через веб-сторінки авіакомпаній [44].

2.5.7. IATA (IATA PADIS)

Стандарти обміну даними про пасажирів та аеропортів IATA (IATA PADIS - Passenger and Airport Data Interchange Standards) – це підмножина повідомлень EDI, призначених для використання як із синтаксисами EDIFACT, так і з XML. IATA створила його спеціально як стандартизований засіб обміну інформацією про пасажирів між авіакомпаніями, аеропортами, урядами та іншими в авіаційній галузі. Цей стандарт більш вузькоспеціалізований, ніж більш широкі стандарти IATA Cargo-IMP та Cargo XML.

IATA PADIS охоплює всі стандартні взаємодії з пасажирами, такі як оновлення посадки на рейс, передрук посадки на борт, перевезення багажу, запити на цінові маршрути та запити контролю квитків.

Розроблявся IATA спільно із її авіакомпаніями-членами та авіакомпаніями Airlines for America (A4A).

2.5.8. National Council for Prescription Drug Programs

NCPDP SCRIPT – це стандарт, розроблений та підтримуваний Національною радою з лікарських препаратів за рецептом (NCPDP). Стандарт визначає документи для електронної передачі медичних рецептів у США [45].

Галузі, що використовують NCPDP SCRIPT:

* Охорона здоров'я
* Фармацевтичні препарати
* Довгий догляд
* Медична страховка
* Уряд

Види транзакцій SCRIPT NCPDP

Стандарт SCRIPT забезпечує стандартні формати документів EDI для обміну інформацією між лікарськими препаратами, аптеками, посередниками та платниками. Деякі приклади включають:

* Новий запит на рецепт;
* Зміна нового рецепта;
* Скасування рецепту;
* Поповнення / поновлення;
* Постачання в довготривалий догляд;
* Заповнення сповіщення про статус;
* Обмін історії медикаментозного лікування.

Вік

* NCPDP була заснована у 1976 році;
* Організація отримала акредитацію ANSI в 1996 році;
* У 2010 році основний випуск сценарію NCPDP отримав законодавче визнання;
* Стандарт SCRIPT поновлюється та оновлюється регулярно NCPDP.

Керуючі органи

* NCPDP, організація з розробки стандартів, акредитованої ANSI, керує стандартом SCRIPT:
  + NCPDP – фармацевтична галузь, організація, що керується членами, яка відіграла головну роль у важливих законодавчих актах, таких як HIPAA, пільги за лікарськими препаратами за рецептом Medicare та Закон про доступну допомогу.

2.5.9. RosettaNet EDI Standard

RosettaNet – це стандарт GS1 для електронної торгівлі інформацією серед галузей, таких як галузь високих технологій та побутова електроніка, напівпровідники, телекомунікації та логістика.

RosettaNet – це відкритий стандарт, який використовується для формування загальної мови електронного бізнесу, вирівнюючи процеси між партнерами ланцюга поставок на глобальній основі. Він заснований на стандарті XML.

Галузі, що використовують RosettaNet

* Високі технології;
* Побутова електроніка;
* Напівпровідник;
* Телекомунікації;
* Логістика.

RosettaNet охоплює широкий спектр логістичних та фінансових операцій, включаючи замовлення на купівлю, повідомлення про відвантаження, рахунки-фактури, запити на повернення, котирування тощо.

Керується RosettaNet, дочірньою компанією GS1.

RosettaNet – це некомерційний консорціум, спрямований на встановлення стандартних процесів обміну діловою інформацією (B2B). RosettaNet включає основні комп'ютерні та побутові електроніки, електронні компоненти, виробництво напівпровідників, телекомунікації та логістику [46].

2.5.10. SAP IDoc EDI

SAP IDocs (intermediate documents – проміжні документи) – це стандартизовані документи або контейнери даних, які використовуються для зв'язку з системами SAP та обміну інформацією. Вони нагадують документи EDI і зазвичай використовуються для передачі в електронному вигляді інформації, наприклад, замовлення на купівлю, рахунки-фактури, повідомлення про доставку тощо.

IDocs базується на двох стандартах EDI: X12 та EDIFACT. У випадку будь-якого конфлікту за розміром даних він приймає формат з більшою довжиною – немає офіційного відображення IDocs до EDIFACT або X12.

IDOC складається з трьох структурних елементів:

* Запис управління – тип IDOC, тип повідомлення, статус, відправник, одержувач та інша інформація про повідомлення;
* Запис даних – фактичний вміст повідомлення;
* Запис статусу – надає інформацію про стани, за якими дотримувався IDOC.

SAP IDocs використовуються мільйонами компаній, що використовують системи SAP, і не обов'язково специфічні для будь-якої галузі, оскільки SAP обслуговує компанії від хімічних до освітніх, а також спортивні і розважальні.

IDocs використовуються для різноманітних взаємодій, насамперед, у сферах фінансових, логістичних та торгових операцій.

SAP IDocs керується SAP, однією з найбільших і провідних технологічних компаній у всьому світі, заснованою в 1972 році.

2.5.11. Standard Exchange Format (SEF)

Стандартний формат обміну (SEF) – це формат відкритого стандарту – файли, що закінчуються розширенням .sef, що визначає формат та вказівки щодо реалізації патентованих та стандартних документів EDI.

SEF має ключові переваги перед іншими форматами файлів (наприклад, PDF, .docx, rft, html та папір), наприклад:

* Файли SEF можуть бути використані як користувачами, так і комп'ютерами;
* Представляє собою невеликі файли і легко передаються через Інтернет;
* Ви можете редагувати їх за допомогою текстового редактора або менеджера SEF;
* SEF – це відкритий стандарт, тому можна створювати та розповсюджувати файли SEF без спеціальних дозволів чи роялті.

SEF широко використовується у багатьох галузях промисловості для власних потреб у обміні повідомленнями EDI, а також у логістиці та мережах постачання.

SEF може використовуватися для будь-якого типу транзакцій EDI, оскільки він використовується для створення фірмових, спеціальних повідомлень про EDI підприємствами та галузями. Він також підтримує багато стандартних повідомлень X12 та UN / EDIFACT, таких як логістика, транспортні та фінансові повідомлення, включаючи замовлення на купівлю, рахунки-фактури тощо [47].

Стандарт SEF був розроблений корпорацією Foresight, яка зараз належить технічному гіганту Tibco, щоб кодувати будь-які специфікації EDI і передати їх у загальнодоступне надбання.

2.5.12. Tradacoms

Tradacoms – ранній стандарт EDI, розроблений для роздрібної торгівлі. Сьогодні його в основному використовують у секторі роздрібної торгівлі Великобританії, незважаючи на те, що він по суті замінений на весь світ EDIFACT. Спочатку він був одним із попередників стандарту UN / EDIFACT і з тих пір застарів, йому на заміну прийшов EDIFACT EANCOM. Незважаючи на це, TRADACOMS все ще використовується для більшості специфічних для Великобританії роздрібних сценаріїв.

TRADACOMS охоплює широкий набір обміну даними для роздрібної торгівлі, включаючи наступне:

* Інформація про замовлення та підтвердження;
* Повідомлення про доставку та комунікації;
* Рахунки та платіжні доручення;
* Інформація про ціни;
* Інформація про продукт;
* Корегування запасів та знімки;
* Комунальні рахунки.

Створений у 1982 році як реалізація синтаксису ООН / GTDI, ранньої версії EDIFACT. Розвиток фактично припинився в 1995 році, потім був замінений EDIFACT. Керуючий орган і донині – ООН [48].

2.5.13. X12 EDI Standard

X12 є основним стандартом EDI в США. Поза межами США EDIFACT є еквівалентом X12. Угоди EDI у США повинні відповідати стандарту X12 EDI та вимагати сумісного, якісного програмного забезпечення для перекладу.

X12 офіційно відомий як ASC X12 EDI (Комітет з акредитованих стандартів X12, Електронний обмін даними) і є стандартом, створеним для управління використанням EDI для електронного обміну інформацією між організаціями. X12 EDI включає набір стандартів та відповідних повідомлень, що визначають конкретні ділові документи, які широко використовуються сьогодні в галузях.

Переваги X12 EDI

Стандарт X12 дозволяє американським компаніям передавати інформацію та передавати документи з бізнесу в бізнес без перешкод несумісного програмного забезпечення або незахищених з'єднань, що залишають власні дані вразливими для сторонніх. X12 розроблений для забезпечення стандартизованої системи передачі даних, яка створює ефективність у діловому спілкуванні.

Як найпоширеніший стандарт EDI у США, користувачі X12 представляють величезну кількість підприємств та численних галузей. Він особливо відомий у галузі охорони здоров’я завдяки правилам HIPPA (Закон про переносність медичного страхування та підзвітності), прийнятим у 1996 році. Закон вимагає національного стандарту електронних операцій із охороною здоров'я. Набори транзакцій для HIPAA EDI засновані на X12.

Одним з найцінніших активів X12 є його комплексний набір транзакцій, який включає загальновживані господарські операції або документи, такі як рахунки-фактури, повідомлення про відвантаження або замовлення на купівлю. X12 може похвалитися понад 300 стандартами транзакцій у п'яти галузевих підмножинах або підстандартах.

Підмножини X12 EDI

Через поширене використання X12 у різних галузях промисловості, це вважається кореневим стандартом із п’ятьма підгалузями або підмножинами, що відповідають певній галузі, для підвищення ефективності.

П’ять функціональних наборів транзакцій або підмножини включають:

* Зв'язок та управління;
* Фінанси;
* Транспорт;
* Ланцюг постачання;
* Страхування.

Кожна галузь використовує певну підмножину, що базується на стандарті X12. Наприклад, продуктова промисловість використовує підмножину UCS для своїх комунікаційних технологій EDI, а роздрібна торгівля одягом – VICS.

Специфічні для галузі підмножини X12:

* HIPAA – Закон про переносність та підзвітність медичного страхування;
* UCS – Єдиний стандарт зв'язку;
* VICS – добровільні стандарти міжіндустріальної торгівлі;
* AIAG – Група дій з автомобільної промисловості;
* CIDX – Обмін даними про хімічну промисловість;
* EIDX – Група обміну даними електроніки (CompTIA);
* PIDX – Американський інститут нафти.

Правила синтаксису

Правила синтаксису регулюють структуру повідомлення та забезпечують однаковість незалежно від компанії, галузі чи документа. В результаті є транзакція даних, яка доставляє чітке повідомлення всім приймачам, незалежно від використовуваних програмних платформ. Стандартизована структура оптимізує передачу файлів за рахунок зменшення непотрібного вмісту.

Стандарт X12 EDI використовує протокол інтерактивного обміну, який дозволяє компаніям безпосередньо обмінюватися повідомленнями та документами, пов'язаними з бізнесом. Цей динамічний обмін покращує комунікацію обох сторін, забезпечуючи скорочення часу реагування та усунення проблеми затримки відповідей та неефективного з'єднання даних.

Стандартизоване повідомлення X12 оптимізує обмін даними не тільки між бізнесом, але і між галузями та країнами. Багато транзакцій є спільними для X12 та UN / EDIFACT (використовується на міжнародному рівні), що дозволяє чітко спілкуватися між двома стандартами EDI.

Поширені типи повідомлень X12 (набори транзакцій):

* 204 Тендер на завантаження автомобільного перевізника;
* 276 Запит про статус претензії;
* 277 Відповідь щодо статусу претензії;
* 383 Профіль торгового партнера;
* 753 Запит на інструкції щодо маршрутизації;
* 754 Інструкції щодо маршрутизації;
* 810 Рахунок-фактура;
* 820 Платіжне доручення / Довідка про переказ коштів (EFT);
* 830 План планування / Випуск матеріалів;
* 834 Зарахування виплат та обслуговування;
* 846 Інвентаризаційний запит / Поради;
* 848 Інформаційний лист про безпеку матеріалів;
* 850 Замовлення на купівлю;
* 852 Дані про активність у продукті;
* 855 Підтвердження замовлення;
* 856 Повідомлення про судно / маніфест (ASN);
* 858 Інформація про відправлення;
* 859 Вантажна накладна;
* 861 Отримання поради;
* 990 Завантаження відповіді на тендер;
* 997 Функціональне підтвердження.

Каталоги елементів даних

Елементи даних – це просто необроблені дані кожної транзакції, і вони функціонують як поля даних, що містять сегменти в наборі транзакцій. Стандарт X12 ідентифікує кожен елемент даних з посилальним номером, як зазначено у словнику елементів даних. Крім того, ЄЕК ООН кожні півроку оновлюється та публікується каталоги елементів даних для EDIFACT. Коли американська компанія спілкується на міжнародному рівні, ці оновлення каталогів мають вирішальне значення для рівномірності та розширення обсягу наборів транзакцій між X12 та UN / EDIFACT.

Кожна стандартизована система повинна дотримуватися суворих рекомендацій щодо ефективного регулювання та уніфікованості. Нинішній стандарт X12 EDI керується взаємозалежними публікаціями, включаючи:

* Словник набору транзакцій;
* Сегментний словник;
* Словник елементів даних;
* Структури управління обміном;
* Взаємозв'язок структур управління поштовою сумкою;
* Структури безпеки;
* Впровадження структур EDI;
* Структура управління додатками;
* Правила та рекомендації щодо дизайну ASC X12.

Стандарт X12 EDI характеризується дуже специфічною структурою для кожного з наборів транзакцій або документів. Хоча елементи даних змінюватимуться між документами EDI, такими як замовлення на придбання, рахунки-фактури або повідомлення про доставку, загальна структура документа залишається тією ж, що сприяє рівномірності та послідовності [49].

Сегменти даних

Сегменти даних у X12 – це категорії, які організовують дані, направляючи інформацію у відповідні місця, подібно до контуру. Наприклад, у наборі транзакцій «замовлення на купівлю» необхідна інформація для документа викладається (публікується), та надається унікальний ідентифікатор.

Назви ідентифікаторів сегментів даних:

* ST: Transaction Set Header – заголовок набору транзакцій;
* BEG: Beginning Segment for Purchase Order – початковий сегмент для замовлення на купівлю;
* CUR: Currency – валюта;
* REF: Reference Identification – ідентифікація посилання;
* PER: Administrative Communications Contract – договір адміністративного зв’язку;
* TAX: Tax Reference – податковий довідник;
* FOB: Free On Board – інформація про переміщення вантажу за межі судна і зміну відповідальних за вантаж;
* CTP: Pricing Information – інформація про ціни;
* PAM: Period Amount – сума за період;
* CSH: Sales Requirements – вимоги до продажів;
* TC2: Commodity – товар;
* SE: Transaction Set Trailer – трейлер набору транзакцій.

Після того, як набір транзакцій (або документ) побудований з використанням необхідних сегментів даних та елементів, його можна організувати для передачі. X12 використовує трирівневу систему обгортання, яка дозволяє ретельно переносити кілька наборів транзакцій за одну передачу даних. Конверт набору транзакцій – це найглибший конверт, який містить інформацію про передачу для одного набору транзакцій (або одного документа).

Середній конверт або конверт функціональної групи об'єднує подібні типи транзакцій разом для однієї передачі. Кожна передача даних може містити кілька функціональних конвертів груп, кожна група містить один або більше документів подібного типу.

Конверт обміну – це зовнішній конверт, в якому розміщені всі конверти функціональних груп для однієї передачі даних. Він містить дані для остаточної передачі і включає інформацію, таку як:

* Обмінні контрольні номери;
* Структуровані адреси поштової скриньки відправника та одержувача;
* Розрахунки функціональних груп у межах обміну;
* Версія конверта обміну;
* Штамп часу / дати.

Конверт обміну дозволяє ефективно передавати декілька різних документів або повідомлень однією передачею.

Початок і кінець кожного конверта визначаються парами даних або певними сегментами даних, які призначені для цієї мети. Обволікаючі пари даних забезпечують організацію між конвертами, сприяючи чіткому та впорядкованому обміну даними.

У 1979 році ANSI створила організацію стандартів, відому як Accredited Standards Committee (ASC X12) – Комітет з акредитованих стандартів X12. Вони мали на меті створити та підтримувати стандарти EDI та схеми XML. X12 набула популярності наприкінці 1980-х, коли більшість стандартних груп у США прийняли його як свій стандарт EDI. Сьогодні ASC X12 складається з 3000 стандартних експертів, які представляють понад 600 компаній у різних галузях. X12 залишається найбільш широко використовуваним стандартом EDI в США.

2.6. Криптографія

Ми живемо у світі, де комп’ютери та Інтернет є майже скрізь. З огляду на це, випливає той факт, що фізичні особи та компанії стикаються із швидко зростаючою онлайн-загрозою: кіберзлочинністю.

Великий ринок (більший, ніж будь-коли) робить Інтернет новою (і вигідною) територією для кіберзлочинців. Це означає, що захист нашої цифрової присутності має надзвичайно високе значення, а шифрування – чи не найважливіший захід безпеки.

Наприклад, програмне забезпечення електронної пошти, інтернет-банкінг, веб-магазини, веб-сайти готелів та веб-сайти з новинами – лише кілька прикладів величезної кількості платформ, які використовують шифрування для захисту даних.

Метод захисту інформації шляхом шифрування не є новим. Греки та єгиптяни використовували криптографію тисячі років тому, щоб захистити важливі повідомлення від небажаних очей. При цьому, інструменти та методи дуже різні та вдосконалені в сучасному цифровому світі з метою захисту та захисту даних. Шифрування використовується, щоб переконатися, що важливі дані не можуть бути викрадені або зловживати хакерами для шахрайських дій.

Наука про шифрування та методи шифрування називається криптографією.

2.6.1. Історія криптографії

Перш, ніж більшість людей навіть змогли писати чи читати, схеми шифрування вже були розроблені для перетворення повідомлень та інформації у нечитабельний фрагмент тексту.

Слово «крипторафія» походить від "крипто". Греки використовували "крипто", щоб описати щось приховане або таємне.

Перші задокументовані приклади писемної криптографії датуються 1900 р. до н.е., коли єгиптяни застосовували прості методи шифрування, такі як нестандартні ієрогліфи.

У 700 році до н.е. спартанці написали важливі повідомлення на шкіру, яку намотали на палиці. Повідомлення міг прочитати лише той, хто мав паличку точно такого ж діаметра. Не знаючи точного розміру, людина не змогла б розшифрувати (перетворити код у письмовий текст) повідомлення.

Пізніше єврейські переписувачі розробили модель шифрування під назвою "ATBASH". Цей тип шифрування використовував простий код підстановки із зворотним алфавітом. Це означає, що "A" стає "Z", "B" стає "Y" і т.д.

За часів Юлія Цезаря (100-44 до н.е.) римляни застосовували подібну заміну. Замість того, щоб перевернути алфавіт, римляни застосували заздалегідь узгоджене зміщення літер по алфавіту: розшифрувати повідомлення може лише людина, яка знала про необхідність зміщення.

Протягом середньовіччя спостерігався бурхливий розвиток моделей шифрування з використанням поліалфавітної заміни (кілька алфавітів заміщення, що використовуються для мінімізації успіху дешифрування).

Пізніше відбулася ще одна велика розробка в шифруванні: між 1933 та 1945 роками, коли німецькі криптологи створили всесвітньо відому машину Enigma. До цього періоду всі моделі шифрування використовували симетричний ключ [50].

У 1976 р. IBM створила модель шифрування, яка згодом була прийнята як американський стандарт шифрування даних DES (Data Encryption Standard). Він досяг світового визнання значною мірою тому, що витримав 20 років атак. Пізніше його було замінено шифруванням AES.

Того ж року Вітфілд Діффі та Мартін Хеллман опублікували «Нові напрямки в криптографії». Вони заклали основу для вирішення однієї з основних (на той час) проблем шифрування: як розподілити ключ шифрування на передбачувану особу безпечним способом.

Нові напрямки в криптографії вважалися проривом і започаткували еру нових схем криптографії, використовуючи відкритий ключ із асиметричними алгоритмами та новими методами аутентифікації.

2.6.2. Сучасна криптографія

Шифрування – сучасний варіант давніх схем криптографії. Він заснований на складному алгоритмі, який називається "шифр".

Його мета – приховати важливу інформацію від інших шляхом перетворення даних прямого тексту в ряд випадкових шифротекстів, що унеможливлює читання простого тексту без розшифровки даних спеціальним ключем дешифрування.

У криптографії простий текст (незашифрована інформація) – це дані, які представляються тому вигляді, в якому їх розуміє користувач, наприклад, електронний лист начальнику.

Протилежність простому тексту називається шифротекстом. Шифротекст (зашифрована інформація) – це дані, що містять форму оригіналу та зашифрованого простого тексту, але вони не читаються для людей та комп'ютерів.

Простіше кажучи, шифрування – це процес перетворення конфіденційних даних або інформації в нерозбірливі дані.

Ключі шифрування розроблені так, щоб вони були абсолютно єдиними, використовуючи набір різних алгоритмів. Ключ шифрування використовується для кодування або декодування даних.

Це в основному означає, що ключ шифрування здатний змішувати дані в нечитабельні символи, а також може повернути ці нечитабельні символи назад у відкритий текст.

Один унікальний ключ, який використовується як для шифрування, так і для дешифрування даних, стосується лише симетричного шифрування, тоді як асиметричне шифрування працює за допомогою окремих ключів на шифрування і на дешифрування.

Машинна криптографія (роторна машина) стала відома громадськості під час Другої світової війни, коли німці використовували код та машину Enigma для шифрування всіх своїх комунікацій. Машинна криптографія складається з електромеханічної системи, яка використовується для шифрування та дешифрування секретної інформації. Німці зашифрували всі свої канали комунікації, від координації атаки та планування стратегії до звітування. Це стало одним з найважливіших та таємних завдань Великобританії – розшифрувати апарат Enigma, щоб знати, що планують зробити німці [50].

Британський математик Алан Тьюрінг вирішив (серед інших у групі найбільш відомих британських математиків) розшифрувати код Енігми у тодішньому секретному місці в парку Блетчлі в Англії. У парку Блетчлі Алану Тьюрінгу та Гордону Велчману вдалося побудувати машину для розбиття коду, яка отримала назву "Колосс".

Колосс став першим програмованим цифровим комп’ютером, який міг генерувати унікальні та сильні ключі шифрування та дешифрування, що стало масовим переломним явищем як у Другій світовій світовій, так і у процесі розвитку шифрування та дешифрування.

Використання шифрування

Як показано вище, схеми шифрування використовувались важливими людьми у воєнний час або з політичних міркувань. Хоча шифрування в основному використовувалося урядами та великими корпораціями до 1970-х років, новаторське впровадження Вітфілда Діффі та "Нових напрямків криптографії" Вітфілда Діффі та Мартина Хеллмана змінило це в 1976 році.

Їх робота призвела до впровадження алгоритму RSA на персональних комп'ютерах. Врешті-решт шифрування набуло широкого впровадження у веб-браузерах та сервісах для захисту даних.

У сучасному світі шифрування використовується у багатьох сферах для захисту даних, наприклад, електронної комерції, онлайн-платежів та банківських операцій, програмного забезпечення електронної пошти, криптовалюти, зберігання даних клієнтів та багато іншого. Крім того, у SIM-картках та Wi-Fi модемах використовуються протоколи алгоритму шифрування для шифрування та захисту конфіденційних даних.

Шифрування також захищає дані, що передаються між двома сторонами. Наприклад, дані кредитної картки клієнта, коли він здійснює онлайн-покупку. Незважаючи на те, що дані все-таки можуть бути перехоплені, це було б не зрозумілим і, таким чином, марним для шпигунів чи хакерів.

Усі види пристроїв у широкому спектрі різних мереж шифрують канали зв’язку. Шифрування використовується не тільки для інтернет-операцій, але також для транзакцій банкоматів або дзвінків на мобільний телефон.

Алгоритми шифрування захищають всі передані дані.

Алгоритм шифрування

У своїй найпростішій формі програма шифрування запускає формулу, щоб перетворити ваші дані (простий текст) у шифротекст – секретні та нечитабельні дані. Цей процес працює і в протилежний бік. Отже, шифротекст можна повернути до простого тексту (який людина може прочитати). Перетворюючи дані або простий текст у шифротекст, небажані очі хакерів чи інших людей, швидше за все, не зможуть прочитати інформацію.

Кожен окремий алгоритм шифрування використовує рядок біт, широко відомий як "ключ", для виконання обчислень. Чим довше ключ шифрування (чим більше містить біт), тим більше можливих шаблонів обчислення можна створити, і тим важче буде розшифрувати шифротекст без ключа.

Більшість алгоритмів шифрування використовують метод «блочного шифрування». Цей метод застосовує випадковий алгоритм у поєднанні з симетричним ключем для шифрування блоку тексту. Таким чином можна зашифровати нерухомі блоки введення, які зазвичай становлять від 64 до 128 або 256 біт у довжину [51].

Менш популярним і періодично використовуваним методом є "метод потоку". Цей метод застосовується до цифр простого тексту, які поєднуються з псевдовипадковим шифровим цифровим, або "ключовим потоком". Алгоритм застосовується до кожної бінарної цифри в потоці даних.

Роль ключа

Ключ шифрування / дешифрування можна порівняти зі звичайним паролем – тим, який використовується для електронної пошти. Ключ – важлива частина процесу кодування та декодування даних.

Зазвичай ключ – це випадкова двійкова або фактична парольна фраза. Клавіша "повідомляє" алгоритму, яким шаблонам він повинен слідувати, щоб перетворити простий текст у шифротекст (і навпаки). Відповідно, ключ є основним елементом захисту конфіденційної інформації, повідомлення або даних. Процес шифрування та дешифрування можна ініціювати лише за допомогою ключа.

Через те, що алгоритми є загальнодоступними та до них може отримати доступ будь-хто, як тільки зловмисник отримає ключ шифрування, зашифровані дані можуть легко розшифруватися до простого тексту. Хакер може зламати випадкову бінарну або парольну фразу ключа або вашу систему та отримати ключ, викравши її.

Тому надзвичайно важливо створити дуже сильне поєднання різних літер (малі та великі регістри), цифр та спеціальних символів. Або, ще краще, регулярно змінювати комбінацію ключа.

Для прикладу, сервіси чату Telegram і WhatsApp шифрують кожне повідомлення, яке надсилає користувач. Програмне забезпечення розроблене таким чином, що кожне повідомлення в прямому тексті перетворюється в шифротекст і може бути розшифровано – переглянуто в простому тексті – одержувачем. Крім того, цифрове шифрування є дуже складним і вважається, що його важко зламати.

Щоб додати ще один рівень складності (та безпеки) для шифрування смартфонів, кожного разу, коли пара смартфонів встановлює канал зв'язку, навколо цього каналу створюється додаткова оболонка захисту. Оболонка – це в основному новий набір алгоритмів, що встановлюють безпечне з'єднання.

Багато постачальників електронної пошти та служб чату, орієнтованих на безпеку та конфіденційність, захищають дані своїх користувачів, здійснюючи шифрування в кінці. Як і інші типи шифрування, він перетворює повідомлення в шифротекст.

У той час, як одні методи шифрування працюють у парах, один ключ шифрує дані, а другий ключ може використовуватися та розповсюджуватися іншим сторонам для дешифрування даних, шифрування end-to-end (також відоме як наскрізне) працює інакше.

Наскрізне шифрування означає, що читати його може лише той, хто надсилає повідомлення, і той, хто його отримує. Простіше кажучи, коли надсилається електронний лист, використовуючи наскрізне шифрування, навіть постачальник послуг електронної пошти не може прочитати ваше повідомлення, оскільки воно вже зашифровано на їх сервері.

Типи ключових алгоритмів

Фундаментальний стовп для встановлення безпечного спілкування базується на міцності ключа.

Існує два способи шифрування:

* Алгоритми симетричних ключів: симетричні алгоритми використовують подібні або абсолютно однакові ключі шифрування як для шифрування простого тексту, так і для дешифрування шифротексту;
* Асиметричні ключові алгоритми: асиметричні алгоритми використовують різні (унікальні) ключі для шифрування простого тексту та дешифрування шифротексту.

Метод асиметричного алгоритму часто називають «криптографією з відкритим ключем».

Симетричні ключові алгоритми

Симетричні алгоритми використовують точно такий же ключ для шифрування простого тексту та розшифровки шифротексту. Симетричні ключові алгоритми часто встановлюються на зразок наступного прикладу: коли дві сторони хочуть надійно та безпечно повідомляти певні дані чи інформацію, обидві сторони можуть обмінятись парольною фразою ключа перед обміном даними. Це, наприклад, можна зробити телефоном або при зустрічі віч-на-віч. Тоді обидві сторони погоджуються, що конкретний ключ (пароль) буде використовуватися для захисту всієї інформації та повідомлень, які обмінюються в майбутньому.

Цей тип шифрування є простим у використанні для всіх учасників, оскільки їм потрібно лише один раз обміняти ключ шифрування та дешифрування. З цього моменту все спілкування захищено.

На відміну від цього, асиметричні алгоритми вимагають нового ключа для кожного сесії зв'язку між двома сторонами.

Крім того, алгоритми симетричних ключів швидші, ніж асиметричні, тому що є лише один ключ. Асиметричні алгоритми використовують пару ключів, які математично пов'язані – збільшуючи математичну складність.

Основним недоліком симетричних ключових алгоритмів є те, що якщо той, хто не має права переглядати дані або інформацію, в змозі отримати ключ, ця людина може легко розшифрувати перехоплене повідомлення, надіслане між двома сторонами.

При створенні багатьох сесій з різними сторонами може бути складним керування кожним унікальним ключем, який належить певній особі.

Асиметричні ключові алгоритми

На відміну від симетричних алгоритмів з одним ключем, асиметричні ключові алгоритми використовують пару двох ключів для виконання алгоритму.

Один ключ використовується для шифрування простого тексту, а інший використовується для розшифровки шифротексту.

Два ключі – це комбінація букв, цифр та спеціальних символів, які створюють випадково створені рядки.

Асиметричний ключ шифрування використовує приватний ключ і відкритий ключ. Це означає, що той, хто надсилає повідомлення, може зашифрувати його приватним ключем, який не було надано спільноті отримувача. Натомість, відкритий ключ доступний для будь-якого користувача, однак він забезпечує доступ лише до обмеженої кількості інформації [52].

Асиметричне шифрування передбачає автентифікацію. Під час процесу автентифікації функцією відкритого ключа є перевірка того, що повідомлення надсилається власником пари приватних ключів. Натомість, лише власник парного приватного ключа може розшифрувати повідомлення, зашифроване відкритим парним ключем.

Суттєвою перевагою тут є те, що викрадення ключа від однієї із сесій не призведе до компрометації всіх повідомлень в інших сесіях. Дані будуть в безпеці, оскільки інші абоненти, яким надсилались повідомлення, надавали різні ключі.

Приватний ключ створюється на основі високоскладних математичних обчислень, які пов'язані з парою відкритих ключів. Простіше кажучи, якщо повідомлення або набір даних шифрується відкритим ключем, лише його приватна пара ключів може розшифрувати його – і навпаки.

Найбільшою перевагою використання алгоритмів асиметричного ключа є те, що ніколи не потрібно ділитися або надсилати свій ключ шифрування або фразу фрази через незахищений канал. Отже, це різко зменшує можливість зламу.

Відкритим ключем можна ділитися з будь-ким, не порушуючи безпеку, оскільки будь-яка людина може зашифрувати повідомлення, використовуючи відкритий ключ одержувача. Але зашифроване повідомлення може бути розшифровано до простого тексту власником приватного ключа.

Алгоритми асиметричного ключа мають три недоліки:

* Потрібно завершити процес автентифікації відкритим ключем щоразу, коли повідомлення надсилається;
* Якщо приватний ключ втрачено, шифротекст неможливо розшифрувати;
* Обробка асиметричного алгоритму відбувається набагато повільніше порівняно з симетричним алгоритмом через його математичну складність, і тому він не підходить для обчислення великої кількості даних.

Advanced Encryption Standart (AES)

Advanced Encryption Standart (розширений стандарт шифрування) – це симетричний блок-шифр і підмножина шифру Рінддейла.

Цей метод симетричного шифрування був обраний Національним інститутом стандартів і технологій США як головний стандарт шифрування безпеки. Таким чином, уряд США прийняв AES, який зараз використовується у всьому світі для захисту секретної інформації та шифрування конфіденційних даних у програмному та апаратному забезпеченні.

AES використовує три різні блок-шифри:

* AES-128;
* AES-192;
* AES-256.

Кожен окремий блоковий шифр здатний шифрувати та дешифрувати дані у фіксованому розмірі блоку 128-біт. Розмір ключа – 128, 192 або 256 біт відповідно.

Різниця між шифром Рінддейла і шифром AES полягає в тому, що шифр Рінддейла прийняв додаткові розміри блоків і ключових розмірів, але шифр AES цих функцій не реалізував.

Кожен алгоритм обробляє блоки шифрів у певному розмірі. Іншими словами, алгоритм "розбиває" дані або простий текст на блоки та обробляє обчислення блок за блоком. Кожен блок містить фіксований розмір бітів: наприклад (як показано вище), 128, 192 або 256 біт. Повний рядок вхідного тексту буде розділений на точно однакові за розмірами блоки, поки алгоритм обробляє шифрування або дешифрування даних. Кожен блок простого тексту має відповідний блок шифротексту для конкретного ключа (і навпаки).

Розмір ключа означає кількість бітів у ключі. Для AES розмір ключа безпосередньо пов'язаний із силою алгоритму. Чим більша кількість бітів, тим сильніше її безпека.

Отже, 256 біт забезпечує додаткову безпеку порівняно з 128 бітами. Короткі ключі можуть бути вразливими для грубої атаки (наприклад, методом перебору). При цьому, шифрування AES майже неможливо зламати методом перебору.

Відповідно до цікавого прикладу розрахунку, взятого з технологічного документу Seagate "128-бітове версію 256-бітного шифрування AES" (128-Bit Versus 256-Bit AES Encryption).

* Кожна людина планети володіє 10 комп’ютерами;
* На планеті живе 7 мільярдів людей;
* Кожен з цих комп'ютерів може випробувати 1 мільярд комбінацій ключів в секунду;
* У середньому ви можете зламати ключ після тестування 50% можливостей.

Тоді, зважаючи на ці умови, населення Землі може зламати один ключ шифрування за 77 000 000 000 000 000 000 000 000 років! І це лише для 128-бітного шифрування AES[53].

Слабкі сторони шифрування

Особливо, побачивши наведений вище розрахунок, можна повірити, що алгоритми шифрування абсолютно незламні.

На жаль, це не так. По мірі використання нових слабких місць створюються нові методи шифрування для протидії цим діям з метою створення нових шарів безпеки. Найбільша слабкість алгоритмів шифрування полягає в тому, що деякі алгоритми не можуть генерувати, здавалося б, випадкові рядки шифротексту, а натомість, генерують розпізнавані шаблони.

Наприклад, коли зловмисник здатний ідентифікувати візерунок шаблону, це допомагає їм сильно зламати шифротекст. Це питання стосується також алгоритмів, які генерують передбачені закономірності в результаті повторюваних та певних тестів для введення даних. Навряд чи хакер може зламати всі блоки шифрів, але виявлення лише декількох блоків вже може призвести до витоку важливих, чутливих даних – і наслідки можуть бути катастрофічними.

Однак час, зусилля та обчислювальні витрати, необхідні для розгортання такого алгоритму, як AES, роблять це надзвичайно дорогим починанням, і спроба є досить безглуздою.

Найбільші загрози безпеці зашифрованих даних здебільшого не пов’язані безпосередньо із загрозою безпосередньо зламу. Слід пам’ятати про кейлоггери, які записують який ключ або пароль вводить користувач, а також про бекдори та інші форми шкідливих програм, які використовуються для отримання ключів шифрування.{тут буде доповнено про шифрування}

2.7 Види шифрування

Сьогодні існує два основні способи шифрування. Перший вид шифрування, званий симетричною криптографією або загальним таємним шифруванням, застосовувався ще з давніх єгипетських часів. Ця форма шифрування використовує секретний ключ, який називається загальним ключем, для того, щоб перетворити дані на беззмістовний потік символів. Людині на іншому кінці потрібен загальний (ключ), щоб розблокувати дані – алгоритм шифрування. Ви можете змінити ключ і змінити результати шифрування. Його називають симетричною криптографією, оскільки однаковий ключ використовується з обох кінців як для шифрування, так і для розшифрування.

Проблема цього методу полягає в тому, що потрібно надійно повідомити секретний ключ передбачуваним одержувачем. Якщо ворог перехопить ключ, він може прочитати повідомлення. Всілякі системи були винайдені, щоб спробувати подолати цю основну слабкість, але факт залишився фактом: доводиться передавати секретний ключ до призначеного одержувача, перш ніж розпочинати безпечні комунікації.

Революція в шифруванні почалася, коли Вітфілд Діффі, Мартін Гелман та Ральф Меркле винайшли криптографію відкритого ключа. (Насправді, існують певні дискусії, чи дійсно британський державний службовець Джеймс Елліс винайшов це раніше і тримав це в таємниці, але Діффі, Хеллман та Меркле були першими, хто оприлюднив це в 1976 році.) Вони намагалися вирішити одвічну проблему обміну ключами. Діффі поцікавився, як двоє людей, які хочуть здійснити фінансову операцію через електронну мережу, можуть зробити це надійно. Тут він думав далеко заздалегідь, адже Інтернет на той час був у зародковому стані, а електронна комерція ще не існувала. Якщо у великих урядів виникли проблеми з вирішенням ключової проблеми обміну, то як пересічна людина із цим впорається? Він хотів створити систему, за допомогою якої дві сторони могли легко вести захищені розмови та захищати транзакції, не потребуючи щоразу обмінюватися ключами. Він знав, що якщо він зможе вирішити ключову проблему обміну, це буде величезний прогрес в криптографії.

Діффі співпрацював з Мартіном Хеллманом та Ральфом Меркле. Минуло кілька років, але нарешті вони придумали систему під назвою шифрування відкритого ключа (англ. public key encryption – PKE), також відому як асиметрична криптографія [54].

Асиметрична криптографія використовує шифрування, яке розбиває ключ на дві менші ключі. Один з ключів оприлюднюється, а один зберігається приватним. Суб’єкт шифрує повідомлення відкритим ключем одержувача. Потім одержувач може розшифрувати його своїм приватним ключем. І він можуть зробити те ж саме, зашифрувавши повідомлення своїм відкритим ключем, щоб перший відправник міг розшифрувати його своїм приватним ключем. Різниця тут полягає в тому, що не потрібен чийсь приватний ключ, щоб надіслати певному абоненту захищене повідомлення. Ви використовуєте його відкритий ключ, який не повинен бути захищеним (насправді він може бути опублікований як номер телефону). Використовуючи відкритий ключ вашого одержувача, ви знаєте, що тільки ця людина може зашифрувати його за допомогою свого приватного ключа. Ця система дозволяє двом об'єктам безпечно спілкуватися без попереднього обміну ключами.

Асиметрична криптографія зазвичай реалізується за допомогою використання односторонніх функцій. Математично це функції, які легко обчислити в одному напрямку, але дуже важко обчислити в зворотному напрямку. Саме це дозволяє опублікувати відкритий ключ, який походить від приватного ключа. Але дуже складно виконувати зворотнє обчислення і визначати приватний ключ. Загальна одностороння функція, яка використовується сьогодні, – це множення великих простих чисел. Легко помножити два простих числа разом і отримати добуток. Однак визначити, які з багатьох можливих чисел є саме тими числами, що використовувалися при створенні ключа – одна з великих математичних проблем.. На щастя, для цього додатка працюють інші односторонні функції, такі як обчислення еліптичних кривих або обчислення зворотних логарифмів над скінченним полем.

Незабаром після виходу статті Діффі, Геллмана та Меркле іншою групою з трьох чоловіків було опубліковано практичне застосування теорії. Їх система шифрування відкритими ключами отримала назву RSA за їхніми іменами: Рональд Рівест, Аді Шамір та Леонард Адлеман. Вони створили компанію і почали ліцензувати свою систему. Швидкість прийняття була повільною, і їхня компанія майже припинила свою діяльність, поки вони не уклали угоду, щоб скористатися розростаючись сферою інтернет-торгівлі з маловідомою на той час компанією під назвою Netscape. Решта – це історія, і RSA зараз є найбільш широко використовуваним алгоритмом шифрування відкритих ключів. Діффі і Хеллман врешті-решт випустили власне практичне застосування, але воно може бути використане лише для обміну ключами, тоді як RSA може проводити аутентифікацію.

Шифрування відкритих ключів тепер обов’язкове для кожного веб-сервера, який пропонує вам безпечну покупку. Ваша транзакція шифрується, не даючи та не беручи секретний ключ, і все це відбувається у фоновому режимі. Все, що бачать користувачі, – це маленький символ блокування SSL, що відображається у браузері, і вони почувають себе в безпеці. Очевидно, що електронна комерція не могла б існувати, як сьогодні, без криптографії відкритого ключа.

На основі цих двох основних типів шифрування існує багато різних алгоритмів шифрування, протоколів та додатків. У наступних розділах представлено деякі з них.

Сьогодні ефективність шифрування зазвичай вимірюється розміром ключа. Незалежно від того, наскільки сильний алгоритм, зашифровані дані можуть бути піддані жорстоким атакам, в яких пробуються всі можливі комбінації ключів. Врешті-решт шифрування може бути зламано. Для більшості сучасних шифрів із значною довжиною ключів час грубого зламу вимірюється тисячоліттями. Однак нерозкритий недолік в алгоритмі або просування в обчислювальній техніці чи математичних методах може цей час різко зменшити.

Як правило, думка полягає в тому, що довжина ключа повинна бути придатною для збереження даних в безпеці протягом розумної кількості часу. Якщо предмет є дуже актуальним, наприклад, повідомленням на полі бою або щоденною інформацією про запаси, то шифр, який захищає його протягом декількох тижнів чи місяців, є просто чудовим. Однак щось на зразок номера вашої кредитної картки або секретів національної безпеки потрібно зберігати в безпеці протягом більш тривалого періоду, фактично назавжди. Тож використання слабших алгоритмів шифрування або скорочення довжини ключів для деяких речей добре, доки термін корисності інформації для сторонніх людей закінчується за короткий проміжок часу.

2.7.1. Data Encryption Standard

Стандарт шифрування даних (англ. Data Encryption Standard – DES) – оригінальний стандарт, який американський уряд почав просувати як для уряду, так і для бізнесу. Спочатку вважалося, що це було практично непорушним у 1970-х роках, збільшення потужності та зниження витрат на обчислення зробили його 56-бітний ключ функціонально застарілим для високочутливої ​​інформації. Однак він все ще використовується у багатьох комерційних продуктах і вважається прийнятним для застосувань із нижчим рівнем безпеки. Він також використовується в продуктах, які мають повільні процесори, наприклад, смарт-карти та пристрої приладів, які не можуть обробити більший розмір ключа [55].

2.7.2. TripleDES

TripleDES або 3DES – це нова, вдосконалена версія DES, а її назва описує, що вона робить. Він запускає DES тричі на даних у три фази: шифрувати, дешифрувати та знову шифрувати. Насправді це не дає втричі збільшити ефективність шифру (оскільки перший ключ шифрування використовується два рази для шифрування даних, а потім другий ключ використовується для шифрування результатів цього процесу), але він все одно дає ефективну довжину ключа у 168 біт, що є досить сильним для майже всіх випадків.

2.7.3. RC4, RC5 і RC6

Це алгоритм шифрування, розроблений Рональдом Рівестом, одним із розробників RSA, першого комерційного застосування криптографії відкритого ключа. З часом було внесено удосконалення, щоб посилити його та виправити незначні проблеми. Поточна версія RC6 дозволяє використовувати розмір ключа до 2040 біт та змінний розмір блоку до 128 біт [56].

2.7.4. AES

Коли уряд США зрозумів, що в DES зрештою закінчиться термін корисного використання, він розпочав пошук заміни. Національний інститут стандартів і технологій (NIST), орган урядових стандартів, оголосив відкритий конкурс на новий алгоритм, який стане новим урядовим стандартом. Було багато конкурентів, серед яких RC6, Blowfish відомого криптографа Брюса Шнейера та інші гідні алгоритми. В результаті, вони запинилися на AES, який базується на алгоритмі під назвою Рейндал (Rijndael), розробленому двома бельгійськими криптографами. Це важливо, оскільки вони використовували відкритий конкурс для визначення стандарту. Крім того, вибір алгоритму двома неамериканськими розробниками, що не мають значних комерційних інтересів, допоміг узаконити цей вибір у всьому світі. AES швидко стає новим стандартом шифрування. Він пропонує до 256 біт ключа шифру, що є більш ніж достатньою потужністю для передбачуваного майбутнього. Зазвичай AES реалізується в 128- або 192-бітному режимі з міркувань продуктивності.

2.8. Програми для шифрування

2.8.1. Хеш

Хеш – це спеціальне використання односторонніх функцій для забезпечення автентифікації та перевірки за допомогою шифрування. Хеш-функція бере файл і передає його через функцію, щоб він створював значно менший файл заданого розміру. Хешуванні файлу створюється унікальний відбиток. Це дає можливість переконатися, що файл жодним чином не змінено. При хешуванні підозрілого файлу і порівнюючи хеш з відомим хешем цього файлу, можна визначити, чи були внесені якісь зміни. Надзвичайно мала вірогідність того, що файл з іншим вмістом створив би ідентичний хеш. Навіть зміни одного символу суттєво змінює хеш.

Хеші часто надаються у завантажених версіях програмного забезпечення, щоб переконатися, що ви отримуєте дійсно саме це ПЗ. Це важливо, особливо з ПЗ з відкритим кодом. На офіційному веб-сайті зазвичай розміщується правильний хеш останньої версії. Якщо вони не збігаються, ви знаєте, що деякі зміни були внесені, можливо, без дозволу чи відома розробників програмного забезпечення. Найпопулярніший алгоритм хешування називається MD5 [57].

2.8.2. Цифрові сертифікати

Цифрові сертифікати є "підписом" світу інтернет-комерції. Вони використовують комбінацію типів шифрування для забезпечення автентифікації. Вони доводять, що хто з ким ви підключаєтесь, це справді ті, хто кажуть, що вони є. Простіше кажучи, сертифікат – це підтвердження істинності відправника інформації. Сертифікат містить відкритий ключ організації, зашифрований або приватним ключем, або приватним ключем органу, що підписує. Якщо можна розшифрувати сертифікат за допомогою їх відкритого ключа, то можна обгрунтовано припустити, що веб-сайт належить цій організації.

Сертифікати зазвичай прив’язані до певного домену. Вони можуть бути видані центральною особою, які називаються органом з сертифікації (Certificate Authority – CA), або створюватися та підписуватися локально, як описано вище. Є кілька таких організацій, найбільша з яких – VeriSign, компанія, яка також управляє системою доменних імен. Вони санкціонували багато інших компаній пропонувати сертифікати під їх владою. Отримати сертифікат від VeriSign або однієї з авторизованих компаній – це як би хтось поручив за вас. Як правило, вони не видадуть вам сертифікат, поки вони не підтвердять інформацію, яку ви вводите в сертифікат, або по телефону, або через якусь паперову документацію, наприклад корпоративний статут. Після того, як вони вас "засвідчать", вони візьмуть цю інформацію, включаючи URL-адреси, для яких ви будете використовувати сертифікат, і цифровим чином "підпишіть" її, зашифрувавши її своїм приватним ключем. Тоді веб-сервер або інша програма може використовувати цей сертифікат. Коли зовнішні користувачі отримують деякі дані, наприклад веб-сторінку від сервера, і до неї додається сертифікат, вони можуть використовувати криптографію відкритого ключа для розшифрування сертифіката та підтвердження вашої особи. Сертифікати використовуються найчастіше на веб-сайтах електронної комерції, але вони також можуть використовуватися для будь-якої форми зв'язку. SSH і Nessus можуть використовувати сертифікати для аутентифікації. VPN також можуть використовувати сертифікати для автентифікації замість паролів [58].

2.9. Протоколи шифрування

2.9.1. IPsec

Загальновідомий факт, що протокол IP, розроблений спочатку, був не дуже захищеним. IP-версія 4 (IPv4), яка використовується у більшості країн світу для IP-комунікацій, не забезпечує жодної аутентифікації та конфіденційності. Корисні навантаження пакетів надсилаються чітко, і заголовки пакетів легко змінюються, оскільки вони не перевірені в пункті призначення. Багато інтернет-атак покладаються на цю основну незахищеність в Інтернет-інфраструктурі. Новий стандарт IP, званий IPv6, був розроблений для забезпечення автентичності та конфіденційності за допомогою шифрування. Він також розширив простір IP-адрес, використовуючи 128-бітну адресу, а не 32-бітну в даний час, а також вдосконалено для ряду інших речей.

Повна реалізація стандарту IPv6 потребує широкого оновлення обладнання, тому розгортання IPv6 проходить досить повільно. Однак була розроблена реалізація безпеки для IP, яка називається IPsec, яка не потребує великих змін у схемі адресації. Постачальники обладнання перескочили це, і IPsec поступово став фактичним стандартом для створення Інтернет-VPN.

IPsec не є специфічним алгоритмом шифрування, а скоріше рамкою для шифрування та перевірки пакетів в протоколі IP. IPsec може використовувати різні алгоритми і може бути реалізований повністю або лише частково. Комбінація криптографії відкритого ключа та приватного ключа використовується для шифрування вмісту пакету, а також хеші додають аутентифікацію. Ця функція називається заголовком аутентифікації (Authentication Header – AH). З AH складається хеш із заголовка IP та передається вздовж. Коли пакет прибуває до пункту призначення, з кожного заголовка робиться новий хеш. Якщо він не порівнюється з надісланим, то можна визначити, що заголовок був якось змінений під час руху. Це забезпечує високий рівень впевненості, що пакет прийшов звідти, звідки в ньому вказано. можете зробити шифрування корисної навантаження пакетів, але не робити AH, оскільки це може уповільнити пропускну здатність. AH також може «забруднитися» в деяких середовищах з NAT або брандмауерами. Існують також різні два режими роботи, в яких можна запускати IPsec: тунельний режим або транспортний режим.

У тунельному режимі весь пакет – заголовок і вміст – інкапсулюється та шифрується, поміщається в інший пакет і передається центральному процесору VPN. Кінцеві точки розшифровують пакети, а потім пересилають їх до правильної IP-адреси. Перевага цього методу полягає в тому, що сторонні люди навіть не можуть сказати, що є кінцевим пунктом призначення зашифрованого пакету. Ще одна перевага полягає в тому, що VPN можна контролювати та керувати з декількох центральних точок. Мінусом є те, що для тунелювання потрібне спеціальне обладнання з обох кінців.

У транспортному режимі шифрується лише вміст пакетів; заголовки надсилаються неушкодженими. Це полегшує розгортання та потребує меншої інфраструктури. Все ще можна використовувати AH у транспортному та перевіряючи адресу джерела пакетів

2.9.2. Point-to-Point Tunneling Protocol

Протокол тунелювання "точка-точка" (англ. Point-to-Point Tunneling Protocol – PPTP) – це стандарт, розроблений Microsoft, 3Com та іншими великими компаніями для забезпечення шифрування. Microsoft додала його до Windows 98 та пізніших версій. Це зробило його кандидатом на роль головного стандарту для широко розповсюдженої технології шифрування. Однак у PPTP було виявлено деякі основні недоліки, які обмежили його прийняття. Коли Microsoft постачала IPsec з Windows 2000, це здавалося негласним визнанням, що IPsec виграв як новий стандарт шифрування. Однак PPTP все ще є корисним і недорогим протоколом для встановлення VPN між старими ПК Windows.

2.9.3. Layer Two Tunneling Protocol

Протокол тунелювання другого рівня (L2TP) – це ще один розроблений в галузі протокол і його схвалюють Microsoft та Cisco. Хоча використовується часто на апаратних пристроях шифрування, його використання в програмному забезпеченні порівняно обмежене.

2.9.4. Secure Socket Layer

SSL був розроблений спеціально для використання в Інтернеті, хоча його можна використовувати майже для будь-якого типу комунікацій TCP. Спочатку Netscape розробила його для свого браузера, щоб сприяти стимулюванню електронної комерції. SSL забезпечує шифрування даних, аутентифікацію на обох кінцях та цілісність повідомлення за допомогою сертифікатів. Більшу частину часу SSL використовується під час підключення до веб-сервера, щоб було відомо, що інформація, яка надсилається, захищена. Більшість людей навіть не розуміють, що SSL працює у фоновому режимі. Зазвичай він автентифікує лише одну сторону, сервер, оскільки більшість кінцевих користувачів не мають сертифікатів.

2.10. Модель загроз

Модель загроз – документ, що описує можливі методи та засоби реалізації загроз для інформації в конкретних умовах функціонування автоматизованої системи (АС).

2.10.1. Поняття моделі загроз

Формування моделі загроз є одним з головних чинників забезпечення безпеки інформації АС, оскільки безпосередньо пов'язано з вибором необхідного переліку послуг безпеки, заходів і засобів захисту, що реалізуються в системі.

Всебічність та повнота аналізу загроз дає необхідну впевненість, що враховано всі суттєві загрози безпеки інформації.

Конструктивним шляхом створення моделі загроз є формування окремих моделей загроз для кожного типового компоненту системи (зокрема для локально обчислювальних мереж підрозділів, вузла Інтернет, вузлів зв'язку з Інтернет, каналів зв'язку і вузлів зв'язку з підрозділами) та типових об'єктів захисту (робочих станцій, серверів, мережевого обладнання локальних обчислювальних мереж тощо).

Формування окремих моделей загроз повинно здійснюватись на підставі загальної класифікації загроз інформації, загальної моделі порушника, моделі загроз.

Протягом життєвого циклу АС модель загроз необхідно переглядати у зв'язку з модернізацією та розвитком АС, а також з удосконаленням технічних та програмних засобів подолання механізмів захисту.

Під час створення моделі загроз виконується оцінка, у процесі здійснення якої, фахівці у галузі ІБ одержують інформацію для її використання на всіх наступних етапах побудови комплексної системи забезпечення ІБ. А саме:

* + - 1. Класифікація та опис ресурсів АС: операційних систем, засобів зв'язку і комунікацій, інформації, її категорій, виду подання, технології обробки тощо, обслуговуючого персоналу і користувачів, території і приміщень тощо.
      2. Аналіз інформаційної моделі існуючої АС, тобто неформальний опис інформаційних потоків АС.
      3. Визначення переліку загроз і можливих каналів витоку інформації.
      4. Визначення послуг безпеки, які треба реалізувати.
      5. Визначення вимог до нормативно-правових, організаційних, інженерно-Технічних, та інших заходів захисту, що реалізуються у доповнення до комплексу програмно-апаратних засобів захисту.
      6. Прийняття остаточного рішення про склад КСЗІ.

2.10.2. Реалізація моделі загроз

Виходячи із вищесказаного, модель порушника для систем відновлення цілісності виглядатиме наступним чином (табл. 2.1):

*Таблиця 2.1.*

Модель загроз цілісності інформації

|  |  |  |  |
| --- | --- | --- | --- |
| **№ за п/п** | **Вид загрози** | **Механізм** | **Джерело** |
| **1** | **2** | **3** | **4** |
| 1 | Помилка | Виконання помилок при роботі з додатками | Користувач |
| 2 | Хакінг | Виконання несанкціонованих дій на пристрої клієнта | Зловмисник |
| 3 | Вірусне зараження | Зараження кінцевого пристрою  шкідливим ПЗ | Зловмисник |
| 4 | Соціальна інженерія | Незаконне отримання конфіденційних даних  клієнта | Зловмисник |
| 5 | Перехвати | Типові помилки клієнта під час зберігання та  зміни інформації персональної ідентифікації. | Користувач |
| 6 | Збої в каналах зв’язку | Забезпечення неможливості відмови | Середовище комунікації |
| 7 | Відмова в обслуговуванні | Виведення з ладу/пошкодження/перехід в  нештатний режим роботи. | Персонал, клієнт, зловмисник, програма |
| 8 | Недоліки | Помилки під час конфігурації, використання  та підключення засобів захисті | Зловмисник |

*Закінчення таблиці 2.1.*

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **2** | **3** | **4** |
| 9 | Комп’ютерна неграмотність | Помилкові дії персоналу | Персонал, користувач |

*.*

2.11. Модель порушника

Модель порушника представляє собою опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушників прийнято поділяти на зовнішніх і внутрішніх. До внутрішніх належать співробітники, користувачі інформаційної системи (ІС), які можуть наносити шкоду інформаційним ресурсам (ІР) як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі і приміщення (електрики, сантехніки, прибиральниці тощо); персонал, який обслуговує технічні засоби (інженери, техніки). Зовнішні порушники — це сторонні особи, які знаходяться поза контрольованою зоною організації або не авторизовані для використання даної КС. Це означає, що вони не мають в системі облікового запису і згідно системної політики безпеки взагалі не можуть працювати в даній системі. Приклад зовнішніх порушників: відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих обмежень; кваліфіковані хакери; особи, яких найняли конкуренти для отримання необхідної інформації; порушники пропускного режиму.

При розробці моделі порушника необхідно визначитись, що і у якій мірі має відображати отримана модель. Для цього необхідно визначитись з необхідним ступенем деталізації моделі порушника.

2.11.1. Ступені деталізації

* + - 1. Змістовна модель порушників — відображає причини й мотивацію дій порушників, переслідувані ними цілі і загальний характер дій у процесі підготовки і здійснення порушення ІБ. Побудувавши змістовну модель, адміністратори безпеки можуть визначити мету порушника, його рівень знань, кваліфікацію, розташування та т.п.;
      2. Сценарії впливу порушників — визначають класифіковані типи порушень з конкретизацією алгоритмів і етапів, а також способи дії на кожному етапі. Розробивши сценарії впливу, адміністратори безпеки отримають можливу послідовність дій зловмисника для нанесення збитків ІР;
      3. Математична модель впливу порушників представляє собою формалізований опис сценаріїв у вигляді логіко-алгоритмічної послідовності дій порушників, кількісних значень, що параметрично характеризують результати дій, і функціональних (аналітичних, числових чи алгоритмічних) залежностей, які описують процеси взаємодії порушників з елементами об’єкту і системи охорони. Цей вид моделі слід використовувати для кількісних оцінок вразливості об’єкту і ефективності охорони.

Для того, щоб модель порушника найбільш точно і детально характеризувала порушників, алгоритм їх дій і давала кількісні оцінки вразливості об’єкту і ефективності охорони рекомендується розробляти комплексну модель з урахуванням усіх ступенів деталізації.[?]

2.11.2. Способи класифікацій порушників

Під час побудови моделі порушника спочатку необхідно проаналізувати усіх користувачів системи, розподілити їх за категоріями та визначити найбільш критичні. Користувачі таких категорій будуть прийняті як можливі внутрішні порушники системи. Далі необхідно визначитись, які категорії відвідувачів можуть бути зовнішніми порушниками.

Усіх можливих порушників необхідно класифікувати за різними показниками для того, щоб надалі скласти модель порушника. Нижче наведені можливі види класифікацій:

* + - 1. Класифікація порушників ІБ за метою порушення. Класифікація за метою порушення проводиться для визначення мотивів порушника. Дії порушника в залежності від мети можуть бути спрямовані як на інформацію, так і на матеріальні носії інформації. Знаючи мету порушника, адміністратори безпеки будуть орієнтуватись, на захист якого ресурсу необхідно приділити більше уваги першочергово;
      2. Класифікація порушників інформаційної безпеки за рівнем знань про АС. Кожен порушник має певний рівень кваліфікації та поінформованості відносно організації функціонування лабораторії зовнішніх та внутрішніх мереж інформаційного комп’ютерного комплексу. В залежності від рівня знань, якими володіє порушник, може бути нанесений певний рівень збитків ІР організації. В класифікації враховуються знання можливого порушника та його практичні навички у роботі з КС та ІТ;
      3. Класифікація порушника за місцем дії. Ця класифікація проводиться для визначення розташування порушника відносно організації під час здійснення спроби несанкціонованого доступу до ІР;
      4. Класифікація порушників за методами і способами, якими вони користуються. Порушник може отримати конфіденційну інформацію та інформацію з обмеженим доступом, користуючись при цьому різними методами та засобами. Порушення може бути скоєне або з використанням певних засобів для отримання інформації, або без них. Методи можуть бути різними, як дозволеними, так і забороненими. Дозволеним вважається отримання інформації без порушення прав власності. Як приклад можна привести використання методів соціальної інженерії;
      5. Класифікація порушників за рівнем можливостей, які надані їм засобами АС та обчислювальної техніки. Внутрішніх порушників можна класифікувати за наданим рівнем повноважень у системі. Адже чим більше повноважень, там більше можливостей доступу до інформації з обмеженим доступом;
      6. Класифікація порушників за мотивом порушень. Зловмисники можуть порушувати ІБ з різних причин. Порушення можна розбити на дві групи — навмисні та ненавмисні. Особи, які ненавмисно наносять збитків ІР, порушуючи конфіденційність, цілісність або доступність інформації, не складають плану дій, не мають мети та спеціальних методів та засобів реалізації запланованого порушення. Ненавмисні порушення частіше всього здійснюються в результаті недостатньої кваліфікації, неуважності персоналу. Порушники, які наносять збитків ІР навмисно, мають певну мету, готують план реалізації атаки на ІР. Навмисні порушення ІБ здійснюються для нанесення збитків організації (матеріальних чи моральних), для власного збагачення за рахунок отриманої інформації, а також для нейтралізації конкурентів.

2.11.3. Реалізація моделі порушника

Відповідно до вищенаведеної класифікації, модель порушників цілісності можна представити наступним чином:

1. За розміщенням:
   1. Внутрішні;
   2. Зовнішні;
2. За рівнем кваліфікації:
   1. Знайомий із структурою і принципом роботи ІС (абсолютний рівень знань);
   2. Досвідчений спеціаліст;
   3. Користувач;
   4. Некваліфікований користувач;
3. За методами і способами:
   1. З використанням спеціалізованого ПЗ;
   2. Без використання спеціалізованого ПЗ;
4. За рівнем доступу:
   1. Обмежений;
   2. Необмежений;
5. За мотивом порушення:
   1. Ненавмисні (випадкові);
   2. Навмисні (сплановані).

2.12. Висновки до розділу

Документи – це значна частина нашого щоденного трудового життя. Незалежно від того, про яку галузь – охорону здоров’я, технології, автомобілі, фінанси чи будь-яку іншу – йде мова. Всі вони створюють та використовують документи щодня. Документи відіграють вирішальну роль у забезпеченні належного робочого процесу будь-якого бізнесу.

Сьогодні можна відстежувати всі аспекти ділової активності в Інтернеті: веб-сайт, блог, соціальні медіа, електронну пошту, відео, аудіо тощо. Ефективна система може надати відповіді на багато питань стосовно кожного з документів, що перебувають в обробці. Отримання критичної інформації про спільні документи, наприклад, хто їх відкрив, коли їх відкрили, як далеко їх прокрутили або скільки часу було витрачено на його перегляд, може змінити правила гри на користь того, хто отримує ці дані.

Система управління документами – це набагато більше, ніж просто хмарний інструмент для зберігання цифрових документів. По суті, це основа, яка упорядковує робочі процеси та стимулює співпрацю, сприяючи вільному потоку критичної інформації по всій організації.

Електронний обмін даними (EDI) – це автоматизований обмін з комп'ютера на комп'ютер стандартних електронних ділових документів між діловими партнерами через безпечне, стандартизоване з'єднання.

Управляючи документообігом, підвищується загальна ефективність роботи офісу, що в кінцевому рахунку позитивно впливає на прибуток компанії. EDI використовується також для рішення все більш різноманітних задач, наприклад, для обміну між постачальниками медичних послуг та страховиками, для подорожей та бронювання готелів, для управління освітою, а також для державної регуляторної, статистичної та податкової звітності.

Жодне визначення EDI не є повним без прикладу застосування в реальному світі. Електронний обмін даними корисний для широкого спектру функцій, що охоплюють багато тисяч конкретних обмінів інформацією. Ось лише декілька найпоширеніших сценаріїв, коли EDI є корисним через значну кількість типів транзакцій, які EDI обробляє щодня.

Залежно від налаштувань, це може включати взаємний вибір рішень EDI та постачальників інтеграції EDI. Зрештою, вам знадобляться правильні рішення, які допоможуть вам максимально покращити ваше партнерство. Чим простіше налаштування (за допомогою найбільш універсальних інструментів), тим швидше можна впровадити EDI і почати економити час і гроші під час покращення відносин зі своїм партнером.

Загальні, сертифіковані стандарти – це своєрідний клей, який тримає EDI разом. Ключові сертифікаційні органи регулюють ці стандарти та можуть допомогти оцінити різні рішення.

Сьогодні ефективність шифрування зазвичай вимірюється розміром ключа. Незалежно від того, наскільки сильний алгоритм, зашифровані дані можуть бути піддані жорстоким атакам, в яких пробуються всі можливі комбінації ключів. Врешті-решт шифрування може бути зламано. Для більшості сучасних шифрів із значною довжиною ключів час грубого зламу вимірюється тисячоліттями. Однак нерозкритий недолік в алгоритмі або просування в обчислювальній техніці чи математичних методах може цей час різко зменшити.

Як правило, думка полягає в тому, що довжина ключа повинна бути придатною для збереження даних в безпеці протягом розумної кількості часу. Якщо предмет є дуже актуальним, наприклад, повідомленням на полі бою або щоденною інформацією про запаси, то шифр, який захищає його протягом декількох тижнів чи місяців, є просто чудовим. Однак щось на зразок номера вашої кредитної картки або секретів національної безпеки потрібно зберігати в безпеці протягом більш тривалого періоду, фактично назавжди. Тож використання слабших алгоритмів шифрування або скорочення довжини ключів для деяких речей добре, доки термін корисності інформації для сторонніх людей закінчується за короткий проміжок часу.

Розділ 3

Авторська реалізація ПЗ для захищеного обміну інформацією

В якості практичної частини даної дипломної роботи було обрано створення ПЗ для обміну файлами локальною мережею в АС. Реалізовано мовою Python версії 3.7.5 та з використанням середовища розробки IDLE (клієнтська частина, Windows 10) та багатофункціональний текстовий редактор vim (серверна частина, Ubuntu 19.10).

3.1 Мова програмування Python

Python - інтерпретована мова програмування високого рівня загального призначення. Створена Гвідо ван Россумом та вперше випущена в 1991 році, філософія дизайну Python підкреслює читабельність коду завдяки використанню значного пробілу. Його мовні конструкції та об'єктно-орієнтований підхід мають на меті допомогти програмістам написати чіткий логічний код для малих та масштабних проектів.

Python динамічно типізується та вміє збирати сміття. Він підтримує декілька парадигм програмування, включаючи процедурне, об'єктно-орієнтоване та функціональне програмування. Python часто описується словосполученням "містить батарейки" завдяки своїм всебічним стандартним бібліотекам.

Пітон був задуманий наприкінці 1980-х років як наступник мови ABC. Python 2.0, випущений у 2000 році, представив такі функції, як розуміння списків та систему збору сміття, здатну збирати еталонні цикли. Python 3.0, випущений у 2008 році, був значною змінений, і не є повністю сумісним із кодом попередніх версій.

Підтримка мови Python 2, тобто Python 2.7.x, була офіційно припинена 1 січня 2020 року (вперше заплановано на 2015 рік), після чого патчі безпеки та інші вдосконалення для неї не будуть випущені. З закінченням терміну служби Python 2 підтримується лише Python 3.5.x та пізніші версії.

Інтерпретатори Python доступні для багатьох операційних систем. Глобальне співтовариство програмістів розробляє та підтримує CPython із відкритим вихідним кодом. Некомерційна організація, програмний фонд Python, керує та спрямовує ресурси для розробки Python та CPython.

3.2. Характеристики створеного програмного продукту

Функціонал додатку базується на python3 бібліотеках socket (мережеві функції), simplepam (авторизація Linux-користувачів), os, pwd, (робота із файловою системою), grp (робота із групами користувачів Linux-систем), aes128 (симетричне блокове шифрування). Для реалізації користувацького інтерфейсу використовується бібліотека tk.

Автентифікацію та авторизацію реалізовано стандартними засобами Unix: текстовий файл /etc/passwd, в якому зберігаються основні дані користувачів (логін, uid, gid), текстовий файл /etc/group, де визначена прив’язка імені групи до guid, а також /etc/shadow, де зберігається хешовані користувацькі паролі. Слід зазначити, що розмежування по доступах до файлів реалізовано на рівні саме груп. Таким чином, представники однієї групи матимуть доступи до одних і тих самих файлів, що зберігаються в директоріях /var/secdoc/[назва групи].

Слід зазначити, що на даному етапі шифруванню підлягають лише окремі повідомлення: користувацький пароль, список файлів, безпосередньо файл, щоб зменшити вірогідність зламу симетричного шифру на ідентичних службових повідомленнях (наприклад, запит на дані користувача чи список файлів).

Програмний комплекс працює за наступним алгоритмом:

1. Запуск серверу: створення TCP-сокету на порту 33123. На даному етапі порт фіксований у програмному коді і сервера, і клієнта. Подальший розвиток ПЗ передбачає зміну порту у клієнтському вікні і в налаштуваннях серверу. З цього моменту сервер очікує підключень;
2. Запуск клієнта: створюється основне робоче вікно, на якому можливо введення наступних даних:
   1. IPv4-адреса сервера (на етапі розробки автоматично підставляється «10.1.31.99», де розміщено тестовий сервер);
   2. Ім’я користувача;
   3. Пароль користувача;
   4. Ключ користувача;
3. Також у вікні наявні елементи виду «кнопка»: вхід до системи, скасування підключення (при другому натисканні очищуються поля введення) і завантаження обраного файлу із сервера. І поле, де після авторизації виводиться список доступних для завантаження файлів;
4. Введення користувачем даних для авторизації і натискання кнопки «Увійти»;
5. Шифрування пароля ключем;
6. Спроба TCP-з’єднання із заданим користувачем сервером на порт 33123:
   1. При успішному з’єднанні сервер відправить до клієнта запит «11 Hello.WaitForUsername»
   2. При помилці з’єднання клієнт за 10 секунд закриває з’єднання і видає вікно щодо помилки і недоступності сервера.
7. Після обробки статус-коду «11» клієнта надсилає ім’я користувача;
8. Сервер обробляє ім’я і встановлює актуальний ключ для даного користувача (на даному етапі /etc/secdoc/keys);
9. Сервер відповідає «12 WaitForPassword»;
10. Клієнт надсилає зашифрований користувацький пароль;
11. Розшифрування сервером пароля із використання відомого попередньо відомого ключа як пари до імені користувача;
12. Автентифікація користувача за ім’ям та розшифрованим паролем за допомогою simplepam:
    1. При підтвердженні існування пари «ім’я-пароль» simplepam повертає значення «Істинна», сервер передає клієнту «21 Succesful»;
    2. Якщо simplepam не підтвердив дану пару «ім’я-пароль» і повернув «Хибно», сервер передає клієнту «31 Auth error: wrong credentials.» і закриває з’єднання. Клієнт при обробці статус коду «31» видає вікно з описом помилки щодо невірних даних.
13. Клієнт після отримання статус коду «21» надсилає запит на список доступних для нього (його групи) файлів: «22 filesForGroup»;
14. Сервер перевіряє належність облікового запису до певної групи і зберігає вміст директорії /var/secdoc/[назва групи] в змінну типу «список» із наступних перетворення в змінну типу «рядок» (розділювач елементів «::»), після чого шифрує його і відправляє;
15. Клієнт розшифровує список та показує у вікні;
16. Користувач обирає один із файлів для завантаження, після натискання на кнопку «Завантажити» на сервер передається зашифроване «23 [ім’я файлу]»;
17. Після отримання та опрацювання запиту «23» сервер надсилає в зашифрованому вигляді розмір файлу, після чого надсилає власне зашифрований файл.
18. Користувач може обрати інший файл для завантаження або в будь-який момент завершити роботу кнопкою «Скасувати», вона ініціалізує розрив з’єднання.
19. Після завершення з’єднання сервер переходить в режим очікування нового з’єднання.

3.3. Перевірка роботи

В процесі розгортання системи було створено віртуальну машину із ОС Ubuntu 19.10 і створено 5 тестових груп, в кожну з яких увійшло від 1-го до 3-х користувачів (див. рис. 3.1.):

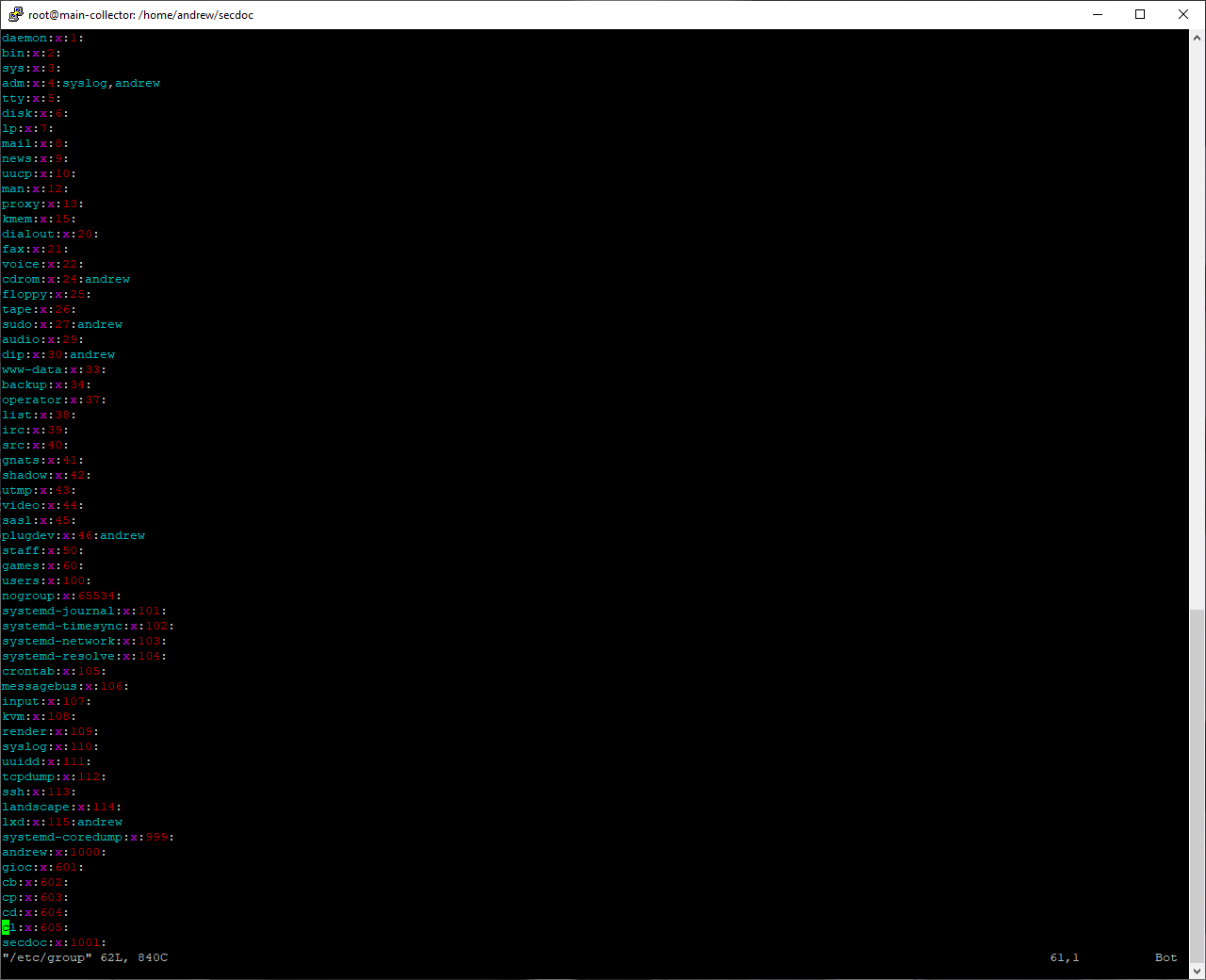


Рис 3.1. Фрагмент файлу /etc/group

* gioc:x:601:
* cb:x:602:
* cp:x:603:
* cd:x:604:
* cl:x:605:
* secdoc:x:1001:

Групи із GID від 601 до 605 – тестові групи.

Для цих груп було створено 11 користувачів безпосередньо для роботи із системою (див. рис. 3.2.). По 3 користувача в групах gioc, cb, cp; по одному в групах cd і cl. Користувач secdoc вводився з метою надання йому прав на всі робочі файли (група-господар визначається групою призначення). Дані користувачі не мають можливості входу до ОС, оскільки в них відсутні інтерпретатори, через які вони могли б працювати. Також в них відсутні домашні директорії.



Рис. 3.2. Фрагмент файлу /etc/passwd

Також було створено 5 директорій за назвами груп за шляхом /var/secdoc, в кожну з яких додано по 5 текстових файлів (див. рис. 3.3 та 3.4.):

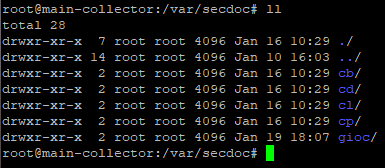


Рис. 3.3. Вміст директорії /var/secdoc

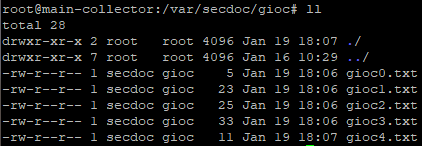


Рис. 3.4. Вміст директорії /var/secdoc/gioc

* gioc
  + gioc0.txt
  + gioc1.txt
  + gioc2.txt
  + gioc3.txt
  + gioc4.txt
* cb
  + cb0.txt
  + cb1.txt
  + cb2.txt
  + cbr.txt
  + cb4.txt
* cd
  + cd0.txt
  + cd1.txt.
  + cd2.txt
  + cd3.txt
  + cd4.txt
* cl
  + cl0.txt
  + cl1.txt
  + cl2.txt
  + cl3.txt
  + cl4.txt
* cp
  + cp0.txt
  + cp1.txt
  + cp2.txt
  + cp3.txt
  + cp4.txt

3.3.1. Робота із додатком

Після запуску сервер переходить в режим очікування підключення клієнта (див. рис. 3.5.)

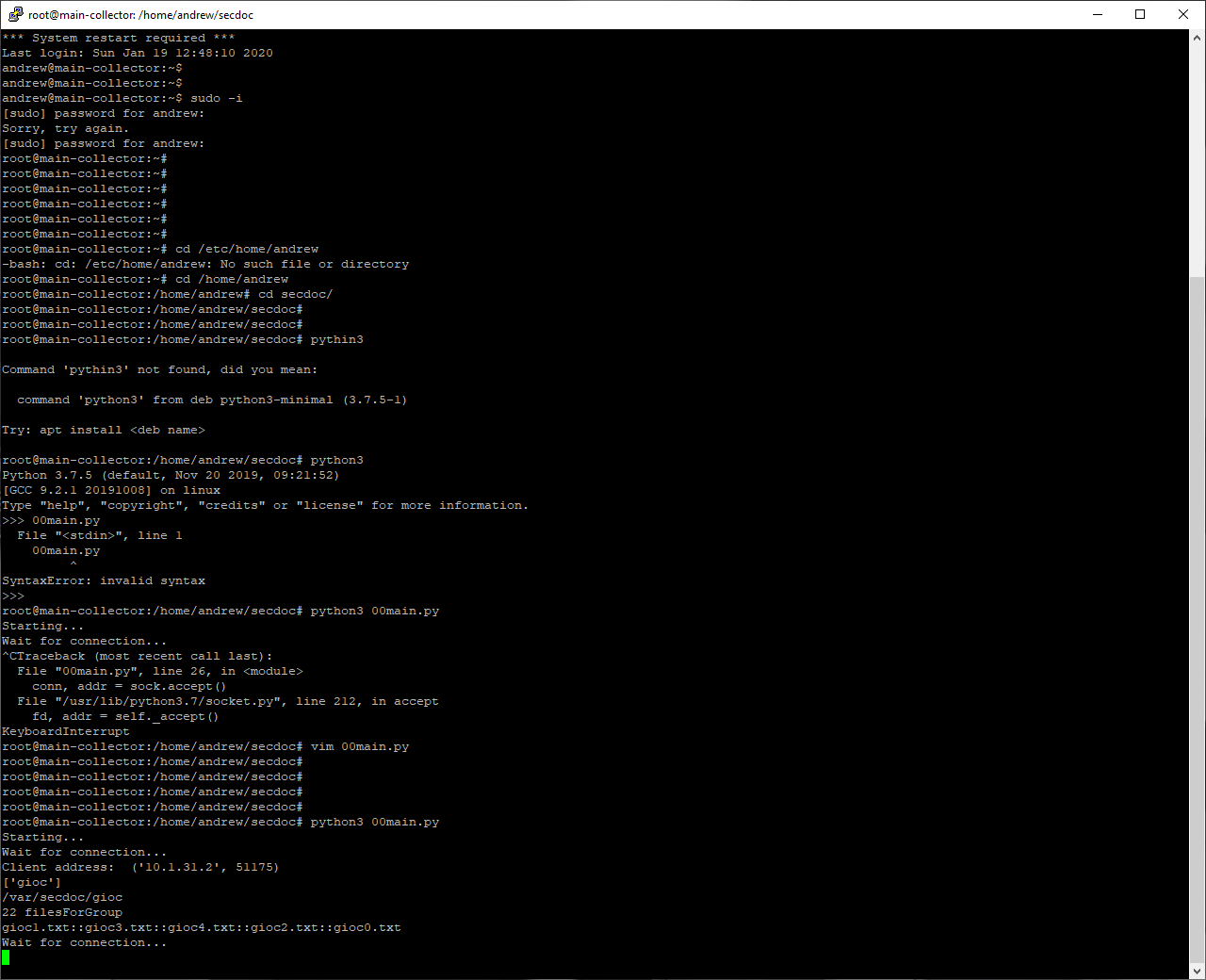


Рис. 3.5. Сервер очікує підключень

Запуск клієнтської частини додатку (див. рис. 3.6.):

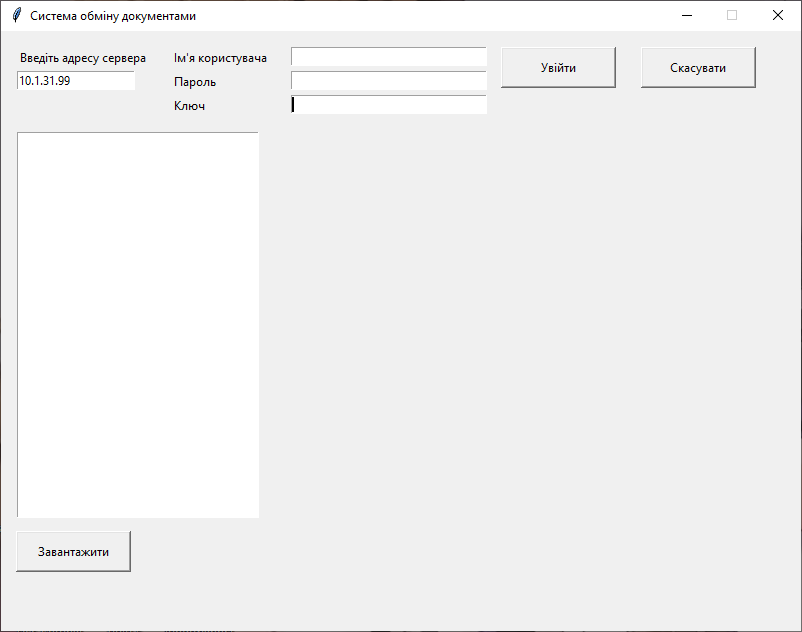


Рис. 3.6. Вікно клієнта відразу після запуску

Користувач вводить дані для автентифікації (рис. 3.7):

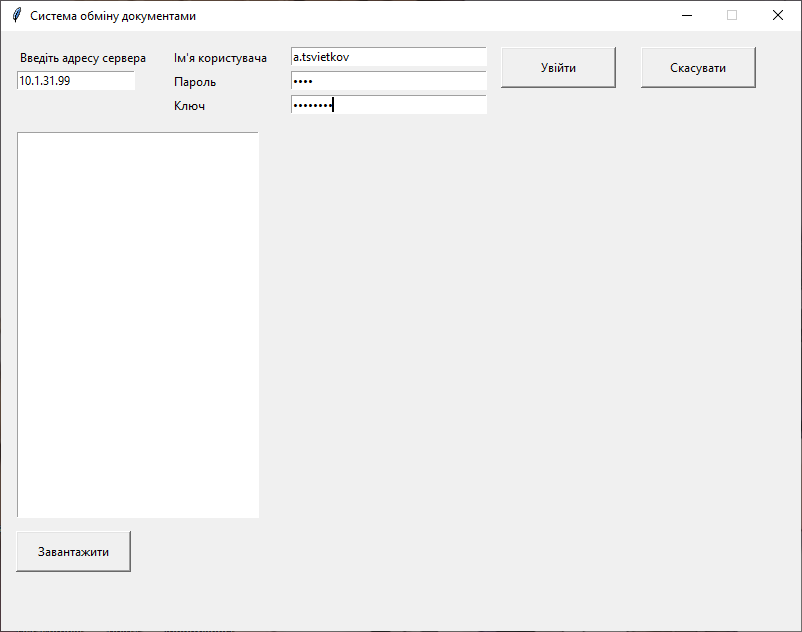


Рис. 3.7. Користувачем введено дані перед підключенням.

Після підключення користувач відразу отримує список файлів, доступних для завантаження (див. рис. 3.8):

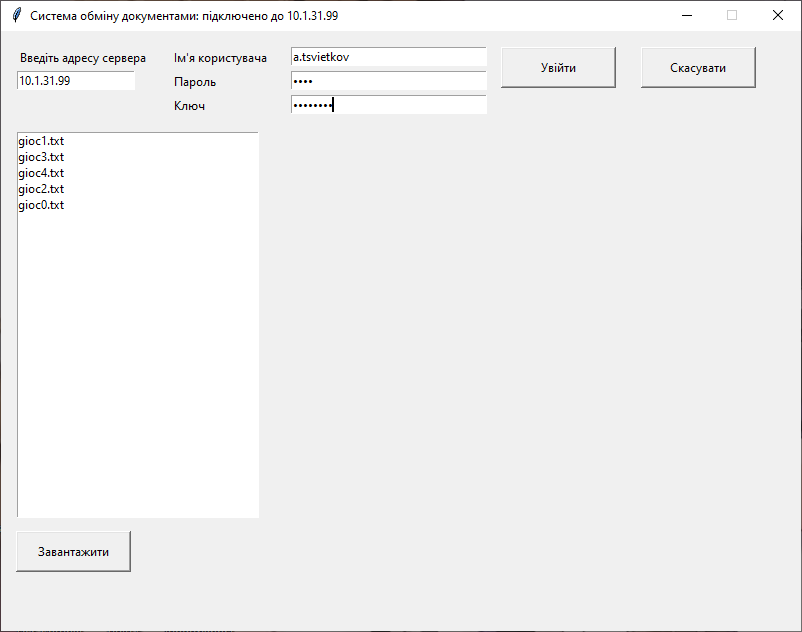


Рис. 3.8. Успішне підключення до серверу

Після підключення користувач може обрати файл для завантаження, або відразу відключитися.

В командному рядку сервера буде відображена деяка інформація: адреса і порт клієнта, його група, директорія із файлами, запит від клієнта на отримання файлів та список файлів у вигляді рядку із розділювачем у вигляді подвійної двокрапки (::). Після завантаження файла клієнт відключився і сервер очікує на нове підключення (див. рис. 3.9):

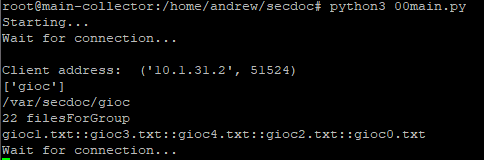


Рис. 3.9. Виведення службової інформаціїї

3.4. Висновок до розділу

Розгляд можливостей різних мов програмування і аналіз їх бібліотек дозволив зупинити вибір на Python3.

Пітон (Python) - це потужна мова програмування, якою легко оволодіти. Вона має ефективні структури даних високого рівня та простий, але ефективний підхід до об'єктно-орієнтованого програмування. Елегантний синтаксис Пітона, динамічна обробка типів, а також те, що це інтерпретована мова, роблять його ідеальним для написання скриптів та швидкої розробки прикладних програм у багатьох галузях на більшості платформ.

Інтерпретатор мови Пітон і багата стандартна бібліотека (як код-джерело, так і бінарні дистрибутиви для усіх головних операційних систем) можуть бути отримані з сайту Пітона, і можуть вільно розповсюджуватися. Цей самий сайт має дистрибутиви та посилання на численні модулі, програми, утиліти та додаткову документацію.

Інтерпретатор мови Пітон може бути легко розширений функціями та типами даних, розробленими на C чи C++ (або на іншій мові, яку можна викликати із C). Пітон також зручний як мова розширення для прикладних програм, що потребують подальшого налагодження.

Створений за допомогою даної мови додаток простий у використанні (за рахунок простого інтерфейсу, який не дозволяє помилитися або виконати щось, що може загрожувати АС чи інформації), займає мінімально можливий об’єм пам’яті та не потребує попередньої інсталяції (клієнтська частина). Ефективність було підтверджено шляхом тесту. Його використання рекомендується як у домашніх умовах, так і на будь-яких підприємствах як для самостійного використання, так і в комплексі заходів із попередження НСД. Слід зазначити низькі системні вимоги: сервер можна розгорнути на будь-якій Linux-машині із підтримкою python3, потребує до 12 МБ пам’яті, для клієнта достатньо 4 МБ оперативної пам’яті.

Висновки

Запитання "Що таке електронний документ" розглядається як окремий випадок питання "Що таке документ". На початку минулого століття спроби забезпечити доступ до швидкозростаючої кількості доступних документів викликали питання щодо того, які саме слід вважати "документом". В результаті було розроблено функціональний погляд на "документ" і його визначено таким, що має організований фізичний відповідник.

Для практичних цілей люди розробляють прагматичні визначення, такі як "все, що може мати ім'я файлу та збережено на електронних носіях" або "колекція даних плюс властивості тих даних, що є для користувача логічною одиницею".

Поняття предметів як документів нагадує поняття "матеріальної культури" серед культурних антропологів, "для яких артефакти внесли важливі докази в документацію та інтерпретацію американського досвіду".

Одним із призначень інформаційних систем є зберігання та підтримка доступу до тих чи інших доказів, які були вказані як докази певного твердження. Інший підхід полягає в тому, що людина, яка має можливість класифікувати та організовувати артефакти, зразки, тексти чи інші предмети, повинна враховувати те, що вони можуть розповісти про світ, який їх створив, а потім, розробивши певну теорію його значення для визнання предмета доказом, пропонувати його як доказ у порядку їх організації, індексації чи подання.

Користувачі повинні мати єдине джерело інформації, що об'єднує цифровий контент з усіх куточків в одне місце, і воно має реалізовувати:

* Масштабованість і можливість забезпечити достатньо місця, оскільки кількість документів компанії зростає в результаті її успіху та розвитку;
* Забезпечення спільним простіром для співробітників, щоб вони збиралися разом і співпрацювали, створювали, керували та редагували документи та інші важливі файли;
* Надійну систему управління вмістом, щоб зберігати всі файли компанії та документи PDF, ексклюзивні аркуші, путівники, навчальні документи, відео, зображення тощо;
* Сильні можливості пошуку для швидкого перегляду заголовків документів та вмісту в документах, щоб працівники могли швидко та легко знаходити саме те, що шукають;
* Надійні засоби захисту інформації, що зберігається в системі, від сторонніх осіб або когось без належної згоди на доступ до цієї інформації.

Документи – це значна частина нашого щоденного трудового життя. Незалежно від того, про яку галузь – охорону здоров’я, технології, автомобілі, фінанси чи будь-яку іншу – йде мова. Всі вони створюють та використовують документи щодня. Документи відіграють вирішальну роль у забезпеченні належного робочого процесу будь-якого бізнесу.

Сьогодні можна відстежувати всі аспекти ділової активності в Інтернеті: веб-сайт, блог, соціальні медіа, електронну пошту, відео, аудіо тощо. Ефективна система може надати відповіді на багато питань стосовно кожного з документів, що перебувають в обробці. Отримання критичної інформації про спільні документи, наприклад, хто їх відкрив, коли їх відкрили, як далеко їх прокрутили або скільки часу було витрачено на його перегляд, може змінити правила гри на користь того, хто отримує ці дані.

Система управління документами – це набагато більше, ніж просто хмарний інструмент для зберігання цифрових документів. По суті, це основа, яка упорядковує робочі процеси та стимулює співпрацю, сприяючи вільному потоку критичної інформації по всій організації.

Електронний обмін даними (EDI) – це автоматизований обмін з комп'ютера на комп'ютер стандартних електронних ділових документів між діловими партнерами через безпечне, стандартизоване з'єднання.

Управляючи документообігом, підвищується загальна ефективність роботи офісу, що в кінцевому рахунку позитивно впливає на прибуток компанії. EDI використовується також для рішення все більш різноманітних задач, наприклад, для обміну між постачальниками медичних послуг та страховиками, для подорожей та бронювання готелів, для управління освітою, а також для державної регуляторної, статистичної та податкової звітності.

Жодне визначення EDI не є повним без прикладу застосування в реальному світі. Електронний обмін даними корисний для широкого спектру функцій, що охоплюють багато тисяч конкретних обмінів інформацією. Ось лише декілька найпоширеніших сценаріїв, коли EDI є корисним через значну кількість типів транзакцій, які EDI обробляє щодня.

Залежно від налаштувань, це може включати взаємний вибір рішень EDI та постачальників інтеграції EDI. Зрештою, вам знадобляться правильні рішення, які допоможуть вам максимально покращити ваше партнерство. Чим простіше налаштування (за допомогою найбільш універсальних інструментів), тим швидше можна впровадити EDI і почати економити час і гроші під час покращення відносин зі своїм партнером.

Загальні, сертифіковані стандарти – це своєрідний клей, який тримає EDI разом. Ключові сертифікаційні органи регулюють ці стандарти та можуть допомогти оцінити різні рішення.

Сьогодні ефективність шифрування зазвичай вимірюється розміром ключа. Незалежно від того, наскільки сильний алгоритм, зашифровані дані можуть бути піддані жорстоким атакам, в яких пробуються всі можливі комбінації ключів. Врешті-решт шифрування може бути зламано. Для більшості сучасних шифрів із значною довжиною ключів час грубого зламу вимірюється тисячоліттями. Однак нерозкритий недолік в алгоритмі або просування в обчислювальній техніці чи математичних методах може цей час різко зменшити.

Як правило, думка полягає в тому, що довжина ключа повинна бути придатною для збереження даних в безпеці протягом розумної кількості часу. Якщо предмет є дуже актуальним, наприклад, повідомленням на полі бою або щоденною інформацією про запаси, то шифр, який захищає його протягом декількох тижнів чи місяців, є просто чудовим. Однак щось на зразок номера вашої кредитної картки або секретів національної безпеки потрібно зберігати в безпеці протягом більш тривалого періоду, фактично назавжди. Тож використання слабших алгоритмів шифрування або скорочення довжини ключів для деяких речей добре, доки термін корисності інформації для сторонніх людей закінчується за короткий проміжок часу.

Розгляд можливостей різних мов програмування і аналіз їх бібліотек дозволив зупинити вибір на Python3.

Пітон (Python) - це потужна мова програмування, якою легко оволодіти. Вона має ефективні структури даних високого рівня та простий, але ефективний підхід до об'єктно-орієнтованого програмування. Елегантний синтаксис Пітона, динамічна обробка типів, а також те, що це інтерпретована мова, роблять його ідеальним для написання скриптів та швидкої розробки прикладних програм у багатьох галузях на більшості платформ.

Інтерпретатор мови Пітон і багата стандартна бібліотека (як код-джерело, так і бінарні дистрибутиви для усіх головних операційних систем) можуть бути отримані з сайту Пітона, і можуть вільно розповсюджуватися. Цей самий сайт має дистрибутиви та посилання на численні модулі, програми, утиліти та додаткову документацію.

Інтерпретатор мови Пітон може бути легко розширений функціями та типами даних, розробленими на C чи C++ (або на іншій мові, яку можна викликати із C). Пітон також зручний як мова розширення для прикладних програм, що потребують подальшого налагодження.

Створений за допомогою даної мови додаток простий у використанні (за рахунок простого інтерфейсу, який не дозволяє помилитися або виконати щось, що може загрожувати АС чи інформації), займає мінімально можливий об’єм пам’яті та не потребує попередньої інсталяції (клієнтська частина). Ефективність було підтверджено шляхом тесту. Його використання рекомендується як у домашніх умовах, так і на будь-яких підприємствах як для самостійного використання, так і в комплексі заходів із попередження НСД. Слід зазначити низькі системні вимоги: сервер можна розгорнути на будь-якій Linux-машині із підтримкою python3, потребує до 12 МБ пам’яті, для клієнта достатньо 4 МБ оперативної пам’яті.

Список бібліографічних посилань

1. Buckland M. K. Information as thing. Journal of the American Society of Information Science v, 42, pp. 351-360, 1991.
2. Dupuy-Briet S. Rapport présenté à la Commission de terminologie. In: International Institute for Documentation. XIIe Conférence. Rapport. Bruxelles, 1933. (IID publication 172a), pp. 187-192, IID: Brussels, 1933.
3. Otlet P. Traité de documentation. Editiones Mundaneum, Brussels, 1934. Reprinted 1989, Liège: Centre de Lecture Publique de la Communauté Française.
4. Izquierdo Arroyo J. M. La organizacion documental del conocimiento. Tecnidoc, Madrid, 1995.
5. Schürmeyer W. Aufgaben und Methoden der Dokumentation, Zentralblatt für Bibliothekswesen, 52, pp. 533-543, 1935.
6. Anon. La terminologie de la documentation, Coopération Intellectuelle, 77, pp. 228-240, 1937.
7. Briet S. Qu'est-ce que la documentation. EDIT, Paris, 1951.
8. Anon. F. Donker Duyvis: His life and work, (NIDER publ. ser. 2, no. 45), Netherlands Institute for Documentation and Filing, The Hague, Netherlands, pp. 39-50, 1964.
9. Voorhoeve N. A. J. F. Donker Duyvis and standardization. In: F. Donker Duyvis: His life and work, (NIDER publ. ser. 2, no. 45). Netherlands Institute for Documentation and Filing, The Hague, pp. 39-50, 1964.
10. Ranganathan S. R. ed. Documentation and its facets, Asia Publishing House, London, 1963.
11. Indian Standards Institute. Indian standard glossary of classification terms. IS : 2550 – 1963, Indian Standards Institute, New Delhi, 1963.
12. *Shores L.*The generic book: What is it and how it works*, Library-College Associates, Norman, Oklahoma, 1977.*
13. Shera J. H. The foundations of education for librarianship, Becker and Hayes, New York, 1972.
14. Otlet P. International organization and dissemination of knowledge: Selected essays. (FID 684). Elsevier, Amsterdam, 1990.
15. Ames K. L. et al. Material culture: a research guide, ed. by T. J. Schlereth. University Press of Kansas, Lawrence, Kansas, 1985.
16. Dufrenne M. The phenomenology of aesthetic experience, Northwestern University Press, Evanston, Illinois, 1973.
17. Barthes R. The semiotic challenge. Hall & Wang, New York, 1988.
18. Warner J. Semiotics, information science, documents and computers. Journal of Documentation, 46, pp. 16-32, 1990.
19. Sebeok T. A., ed. Encyclopedic dictionary of semiotics. 2nd ed., Mouton de Gruyter, Berlin, 1994.
20. Levy D. M. Fixed or fluid? Document stability and new media. In: European Conference on Hypertext Technology 1994 Proceedings. (Pp. 24-31). Association for Computing Machinery, New York, 1994.
21. Document Management Policy: 10 Step Development Process // [Електронний ресурс]. – Режим доступу: https://www.lbmc.com/blog/document-management-policy-development/
22. Workflow Assessments: Are you paying far too much for little to no efficiency? // [Електронний ресурс]. – Режим доступу: https://www.datamaxtexas.com/workflow-assessments
23. The social economy: Unlocking value and productivity through social technologies // [Електронний ресурс]. – Режим доступу: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-social-economy
24. Do workers still waste time searching for information? // [Електронний ресурс]. – Режим доступу: https://blog.xenit.eu/blog/do-workers-still-waste-time-searching-for-information
25. 10 Task Management Skills and Tips to Manage Workload Like a Boss // [Електронний ресурс]. – Режим доступу: https://dzone.com/articles/10-task-management-skills-amp-tips-to-manage-workl
26. Why Document Tracking is Critical for Every Business // [Електронний ресурс]. – Режим доступу: https://blog.bit.ai/document-tracking/
27. What is the Best Way to Share Research with Your Team? // [Електронний ресурс]. – Режим доступу: https://blog.bit.ai/share-research/
28. 5 Surprising Employee Development Statistics You Don't Know // [Електронний ресурс]. – Режим доступу: https://blog.clearcompany.com/5-surprising-employee-development-statistics-you-dont-know
29. 7 Stats That Will Make You Rethink Your Document Management Strategy // [Електронний ресурс]. – Режим доступу: https://www.business.com/articles/7-statistics-that-will-make-you-rethink-your-document-management-strategy/
30. How to Increase Productivity and Efficiency with Document Management Software // [Електронний ресурс]. – Режим доступу: https://www.imagemicrographics.com/blog/2015/10/7/document-management-software-increase-productivity-efficiency
31. 8 Free Easy-to-Use Online Collaboration Tools // [Електронний ресурс]. – Режим доступу: https://blog.elink.io/online-collaboration-tools/
32. Shifts Corporate Strategy Must Make for the Future // [Електронний ресурс]. – Режим доступу: https://www.gartner.com/en/innovation-strategy/trends/strategy-in-2020
33. Electronic Data Interchange // [Електронний ресурс]. – Режим доступу: https://web.archive.org/web/20080511043940/https:/www.itl.nist.gov/fipspubs/fip161-2.htm#FORE\_SEC
34. Security Testing, Validation and Measurement // [Електронний ресурс]. – Режим доступу: https://www.nist.gov/itl/csd/security-testing-validation-and-measurement
35. What is HIPAA Compliance? 2019 HIPAA Requirements // [Електронний ресурс]. – Режим доступу: https://digitalguardian.com/blog/what-hipaa-compliance
36. Electronic data interchange (EDI) Global Market and its Applications in Industries // [Електронний ресурс]. – Режим доступу: https://www.dartconsulting.co.in/market-news/electronic-data-interchange-edi-global-market-and-its-applications-in-industries/
37. EXSMAL: EDI/XML semi-automatic schema matching algorithm // [Електронний ресурс]. – Режим доступу: https://ieeexplore.ieee.org/document/1524079?section=abstract
38. EDI Communication: simple and secure exchange of business documents // [Електронний ресурс]. – Режим доступу: https://www.editel.eu/solutions/edi-communication/
39. GS1 EANCOM // [Електронний ресурс]. – Режим доступу: https://www.gs1.org/standards/eancom
40. EDIFACT: The universal message standard // [Електронний ресурс]. – Режим доступу: https://www.seeburger.com/info/what-is-edifact/
41. How Edigas may satisfy the gas processes // [Електронний ресурс]. – Режим доступу: <https://easee-gas.eu/uploads/kcFinder/files/what> %20is%20EDIGAS%20V3.pdf
42. Health Level Seven (HL7) // [Електронний ресурс]. – Режим доступу: https://www.siemens-healthineers.com/ua/services/it-standards/hl7
43. Advancing the e-Freight Initiative // [Електронний ресурс]. – Режим доступу: https://www.descartes.com/de/knowledge-center/e-freight
44. Why does the air cargo industry need to go from Cargo-IMP to Cargo-XML? // [Електронний ресурс]. – Режим доступу: https://www.youredi.com/blog/air-cargo-needs-to-overcome-cargo-imp
45. NCPDP SCRIPT // [Електронний ресурс]. – Режим доступу: http://xmlpipelineserver.com/data-sources/edi-standards/ncpdp-script/
46. RosettaNet B2B Protocol Standard // [Електронний ресурс]. – Режим доступу: https://docs.oracle.com/cd/B10463\_01/integrate.904/b12121/b2bstandards.htm
47. The Standard Exchange Format (SEF) // [Електронний ресурс]. – Режим доступу: https://www.edidev.com/eval\_SefFile.html
48. TRADACOMS // [Електронний ресурс]. – Режим доступу: https://docs.axway.com/bundle/B2Bi\_230\_AdministratorsGuide\_allOS\_en\_HTML5/page/Content/Objects/agrmnt\_fields\_tradacoms.htm
49. EDI (X12) // [Електронний ресурс]. – Режим доступу: https://docs.actian.com/dataconnect/11.5/index.html#page/User/EDI\_(X12).htm
50. Technical Details of the Enigma Machine // [Електронний ресурс]. – Режим доступу: http://users.telenet.be/d.rijmenants/en/enigmatech.htm
51. Block Cipher modes of Operation // [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/block-cipher-modes-of-operation/
52. What is Asymmetric Encryption? Understand with Simple Examples // [Електронний ресурс]. – Режим доступу: https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/
53. 128-Bit Versus 256-Bit AES Encryption Examples // [Електронний ресурс]. – <http://dator8.info/pdf/AES/3.pdf>
54. What is Public-key Cryptography? // [Електронний ресурс]. – Режим доступу: https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/
55. Data Encryption Standard (DES) // [Електронний ресурс]. – Режим доступу: https://academic.csuohio.edu/yuc/security/Chapter\_06\_Data\_Encription\_Standard.pdf
56. Простая реализация RC4 на C# // [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/111510/
57. MD5 encryption // [Електронний ресурс]. – Режим доступу: https://indianwebs.com/en/producto/encriptacion-md5/
58. Using Digital Certificates for IPsec // [Електронний ресурс]. – Режим доступу: <https://www.juniper.net/documentation/en_US/junos/topics/topic-map/using-digital-certificates-for-ipsec.html>

Додаток А

Фрагменти програмного коду серверної частини

#!/usr/bin/env python3

import socket

from simplepam import authenticate

import grp

import os

import pwd

import aes128

def encrypt(input\_bytes, key):

state = [[] for j in range(4)]

for r in range(4):

for c in range(nb):

state[r].append(input\_bytes[r + 4\*c])

key\_schedule = key\_expansion(key)

state = add\_round\_key(state, key\_schedule)

for rnd in range(1, nr):

state = sub\_bytes(state)

state = shift\_rows(state)

state = mix\_columns(state)

state = add\_round\_key(state, key\_schedule, rnd)

state = sub\_bytes(state)

state = shift\_rows(state)

state = add\_round\_key(state, key\_schedule, rnd + 1)

output = [None for i in range(4\*nb)]

for r in range(4):

for c in range(nb):

output[r + 4\*c] = state[r][c]

return output

def decrypt(cipher, key):

state = [[] for i in range(nb)]

for r in range(4):

for c in range(nb):

state[r].append(cipher[r + 4\*c])

key\_schedule = key\_expansion(key)

state = add\_round\_key(state, key\_schedule, nr)

rnd = nr - 1

while rnd >= 1:

state = shift\_rows(state, inv=True)

state = sub\_bytes(state, inv=True)

state = add\_round\_key(state, key\_schedule, rnd)

state = mix\_columns(state, inv=True)

rnd -= 1

state = shift\_rows(state, inv=True)

state = sub\_bytes(state, inv=True)

state = add\_round\_key(state, key\_schedule, rnd)

output = [None for i in range(4\*nb)]

for r in range(4):

for c in range(nb):

output[r + 4\*c] = state[r][c]

return output

host = ``

port = 33123

addr = (host,port)

sock = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

sock.bind(addr)

sock.listen(1)

print('Starting...')

while 1:

print('Wait for connection...')

conn, addr = sock.accept()

print('Client address: ', addr)

conn.send(b'11 Hello.WaitForUsername ')

username = conn.recv(1024)

conn.send(b'12 WaitForPassword ')

password = conn.recv(1024)

username = username.decode("utf-8")

password = password.decode("utf-8")

username = username.strip()

password = password.strip()

password = decrypt(password,key)

if authenticate(username,password) == True:

conn.send(b'21 Succesful\n')

group = [g.gr\_name for g in grp.getgrall() if username in g.gr\_mem]

gid = pwd.getpwnam(username).pw\_gid

group.append(grp.getgrgid(gid).gr\_name)

print (group)

path = '/var/secdoc/' + group[0]

print(path)

data = conn.recv(1024)

data = data.decode("utf-8")

data = data.strip()

data = decrypt(data,key)

print(data)

data = data.split()

data = data[0]

if data == '22':

fileList = os.listdir(path)

fileListStr = ''

fileListStr = '::'.join(fileList)

print(fileListStr)

conn.send(bytes(fileListStr,encoding='utf-8'))

filename=filename

f = open(filename,'rb')

l = f.read(1024)

while (l):

conn.send(l)

print('Sent ',repr(l))

l = f.read(1024)

f.close()

else:

conn.send(b'31 Auth error: wrong username / password.')

conn.close()

sock.close()

Додаток Б

Фрагменти програмного коду клієнтської частини

#!/usr/bin/env python3

from tkinter import \*

from tkinter import messagebox as mb

import socket

def debug():

host = hostEntry.get()

uname = usernameEntry.get()

pword = passwordEntry.get()

statusLabel.config(text=host+' '+uname+' '+pword)

def encrypt(input\_bytes, key):

# let's prepare our input data: State array and KeySchedule

state = [[] for j in range(4)]

for r in range(4):

for c in range(nb):

state[r].append(input\_bytes[r + 4\*c])

key\_schedule = key\_expansion(key)

state = add\_round\_key(state, key\_schedule)

for rnd in range(1, nr):

state = sub\_bytes(state)

state = shift\_rows(state)

state = mix\_columns(state)

state = add\_round\_key(state, key\_schedule, rnd)

state = sub\_bytes(state)

state = shift\_rows(state)

state = add\_round\_key(state, key\_schedule, rnd + 1)

output = [None for i in range(4\*nb)]

for r in range(4):

for c in range(nb):

output[r + 4\*c] = state[r][c]

return output

def decrypt(cipher, key):

# let's prepare our algorithm enter data: State array and KeySchedule

state = [[] for i in range(nb)]

for r in range(4):

for c in range(nb):

state[r].append(cipher[r + 4\*c])

key\_schedule = key\_expansion(key)

state = add\_round\_key(state, key\_schedule, nr)

rnd = nr - 1

while rnd >= 1:

state = shift\_rows(state, inv=True)

state = sub\_bytes(state, inv=True)

state = add\_round\_key(state, key\_schedule, rnd)

state = mix\_columns(state, inv=True)

rnd -= 1

state = shift\_rows(state, inv=True)

state = sub\_bytes(state, inv=True)

state = add\_round\_key(state, key\_schedule, rnd)

output = [None for i in range(4\*nb)]

for r in range(4):

for c in range(nb):

output[r + 4\*c] = state[r][c]

return output

def connect():

global status

status = '0'

global sock

port = 33123

host = hostEntry.get()

uname = usernameEntry.get()

pword = passwordEntry.get()

if host and uname and pword != '':

sock = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

sock.connect((host, port))

print('Connected.')

global data

data = sock.recv(1024)

data = data.decode("utf-8")

data = data.strip()

print(status)

data = data.split()

status = data[0]

if status == '11':

sock.send(bytes(uname,encoding='utf-8'))

print('Uname')

data = sock.recv(1024)

data = data.decode("utf-8")

data = data.strip()

print(status)

data = data.split()

status = data[0]

if status == '12':

sock.send(bytes(pword,encoding='utf-8'))

print('pword')

data = sock.recv(1024)

data = data.decode("utf-8")

data = data.strip()

print(status)

data = data.split()

status = data[0]

if status == '21':

root.title("Система обміну документами: підключено до {}".format(host))

sock.send(b'22 filesForGroup')

fileList = ''

print(fileList)

fileListBox.delete(0,END)

fileList = sock.recv(1024)

print(fileList)

fileList = fileList.decode("utf-8")

fileList = fileList.split('::')

print(fileList)

for fileList in fileList:

fileListBox.insert(END, fileList)

elif status == '31':

root.title("Система обміну документами: помилка підключення до {}".format(host))

mb.showerror("Помилка авторизації", "Перевірте облікові дані")

sock.close()

else:

status=5

root.destroy()

else:

status=6

mb.showerror("Помилка підключення", "Перевірте адресу та доступність сервера")

root.title('Система обміну документами')

print(status)

def disconnect(status):

if status == '11' or '12' or '21':

sock.close()

else :

hostEntry.delete(END)

usernameEntry.delete(END)

passwordEntry.delete(END)

root=Tk()

root.title('Система обміну документами')

root.resizable(False, False)

root.geometry('800x600+80+30')

hostLabel = Label(text='Введіть адресу сервера')

hostLabel.place(x=16,y=16)

hostEntry = Entry(root,

width=19

)

hostEntry.place(x=16,y=40)

hostEntry.insert(END, '10.1.31.99')

usernameLabel = Label(root,

text='Ім\'я користувача')

usernameLabel.place(x=170,y=16)

passwordLabel = Label(root,

text='Пароль')

passwordLabel.place(x=170,y=40)

keyLabel = Label(root,

text='Ключ')

keyLabel.place(x=170,y=64)

usernameEntry = Entry(root,

width=32)

usernameEntry.place(x=290,y=16)

passwordEntry = Entry(root,

width=32,

show="\u2022")

passwordEntry.place(x=290,y=40)

keyEntry = Entry(root,

width=32,

show="\u2022")

keyEntry.place(x=290,y=64)

fileList = ['']

fileListBox = Listbox(root,

height=24,

width=40,

selectmode=SINGLE)

for filelist in fileList:

fileListBox.insert(END, fileList)

fileListBox.place(x=15, y=100)

authOk = Button(root,

text='Увійти',

width=15,

height=2,

command=connect

)

authOk.place(x=500,y=16)

authCancel = Button(root,

text='Скасувати',

width=15,

height=2,

command=fileListBox.delete(END),

command=disconnect

)

authCancel.place(x=640,y=16)

downloadFileButton = Button(root,

text='Завантажити',

width=15,

height=2,

command=download

)

downloadFileButton.place(x=15,y=500)

root.mainloop()