МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
_____Завідувач кафедри
С. В. Казмірчук

«____»_____ 20__ р.

На правах рукопису
УДК 004.451.36:681.5

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«МАГІСТР»

Тема: «Програмний модуль захисту інформаційних потоків в автоматизованій системі документообігу»

Автор: Н. Д. Гайдич

Науковий керівник: к. т. н., доц. А. Б. Єлізаров

Нормоконтролер: к. т. н., доц. А. Б. Єлізаров

Київ 2020

ВСТУП

Актуальність. Асоціація бізнесу з доходами не є новизною в сучасному світі. Загроза бізнесу – банкрутство, відсутність попиту на пропоновану продукцію, висока конкуренція. Такі основні думки з'являються при вживанні цього словосполучення, та потрібно розуміти, основною і прямою загрозою бізнесу, будь-то приватне підприємництво чи державні установи є інформація яка циркулює на підприємстві. Зі зростанням бізнесу, його розвитком також зростає цінність інформації якою володіє дана компанія: комерційна таємниця, бази даних поставок, особисті дані, говорячи про державні установи – це державна таємниця та інше. Втрата або недоступність такої інформації може привести до величезних збитків, а також можливого тиску та вимагання з боку зловмисника.

З потужним розвитком комп'ютерних технологій, по експоненціальній кривій та в час загально-світової інформатизації, найкращим методом ведення підприємницької документації або діяльності державних структур є виключно автоматизована система документообігу, що в свою чергу дає ряд переваг та недоліків. Основною перевагою є великий відсоток виключення людського фактору з рівняння передачі документів між підрозділами та реалізація комфортної взаємодії. На противагу перевагам, основним недоліком є недостатня стійкість до загроз інформації, що циркулює в системі.

Аналізуючи останні новини про збитки в галузі інформаційної безпеки завдані викраденням інформації, зломом систем безпеки та іншим, можна сказати, що число ризиків пов'язаних із загрозою інформаційній безпеці зросло. Зловмисником в таких випадка може виступати як працівник компанії так і компанія конкурент, що цілеспрямовано фінансує злочинні дії задля особистої вигоди. Нажаль, більшість компаній починають згадувати про забезпечення інформаційної безпеки для власного підприємства вже після завданого збитку в даній області.

Для вирішення задачі забезпечення захисту інформації в автоматизованій системі документообігу необхідний аналіз програмного забезпечення з АСДО, що пропонується на ринку. Визначення та оцінка його методів захисту, пошук можливих загроз з боку зловмисника. Для забезпечення повної захищеності системи документообігу потрібно використовувати новітні методи захисту, спроектовані спеціалізовано і відповідно до потреб і інформаційної структури компанії. Тому в даній роботі проводиться АСДО, розкривається в повній мірі загальна структура та методи взаємодій компонентів АСДО. Отримані дані використовуються для розробки програмної надбудови, що забезпечить захист інформаційних потоків в автоматизованій системі документообігу.

Відомі підходи до вирішення поставленої задачі. На сьогоднішній день існує багато методів та засобів забезпечення інформаційної безпеки АСДО. Найбільшу захищуваність системи забезпечує шифрування, при застосуванні якого інформація стає недоступною для читання та сприйняття, хоча часто це не забезпечує можливого спотворення інформації або її недоступність. Фахівець із безпеки інформації зустрічається із питанням вибору системи безпеки для відповідного підприємства, враховуючи всі деталі та характеристики інформації, що циркулює. Ті чи інші програмні рішення, що існують на ринку можуть не задовольняти підприємство як в методах захисту, так і у витратах на таке ПЗ та його вплив на ефективність роботи системи захисту. Ці та інші фактори створюють труднощі при виборі рішення захисту інформації в АСДО.

Метою роботи є підвищення рівня захищеності АСДО за рахунок розробки програмного модуля захисту.

Для досягнення даної мети вирішуються такі **задачі:**

- загальний аналіз законодавчої бази щодо інформаційної безпеки;
- аналіз програмного забезпечення АСДО, принципи роботи, загрозостійкість;
- розробка алгоритмів та програмної надбудови, що забезпечить захищеність інформаційних потоків в АСДО;

Галузь застосування. Розроблений програмний продукт відноситься до галузі до галузі інформаційної безпеки і може бути використаним для забезпечення захищеності інформаційних потоків в АСДО, за рахунок використання новітніх методів захисту.

Об’єктом дослідження є процес захисту інформації в АСДО.

Предметом дослідження є методи, моделі, та система аналізу ризиків інформаційної безпеки АСД та їх вирішення.

Методи дослідження базуються на основі точного аналізу систем захисту та самих АСДО, об’єктно-орієнтованого програмування.

Новизна одержаних результатів полягає в наступному:

- вперше на основі аналітичних даних систем захисту АСДО, розроблена програмна надбудова для забезпечення безпеки інформаційних потоків в системах документообігу в якій використовуються новітні методи захисту.

Практичне значення отриманих результатів:

- проаналізовано внутрішній спосіб взаємодії елементів АСДО, викладені аналітичні оцінки;
- розроблено програмну надбудову забезпечення безпеки інформаційних потоків систем документообігу.

Апробація. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- XVI Міжнародна науково-практична конференція:«Наука и образование без границ – 2020».

Розділ 1. ЗАГАЛЬНИЙ АНАЛІЗ ЗАКОНОДАВЧОЇ БАЗИ УКРАЇНИ ЩОДО АВТОМАТИЗОВАНИХ СИСТЕМ ДОКУМЕНТООБІГУ, ЕЛЕКТРОННИХ ДОКУМЕНТІВ ТА ВІДПОВІДАЛЬНОСТІ

1.1. Регулювання захисту інформації в Україні, законодавча база, нормативно-правові документи

Розглядаючи наукові праці щодо законодавства України, правового регулювання, правової регламентації інформаційної та кібернетичної державної безпеки, узагальненими шляхами розвитку даних напрямків є:

- правове регулювання захисту інформації та її обігу;
- правові основи захисту інформаційних технологій;
- правові основи безпеки інформаційної інфраструктури;
- правове регулювання безпеки інформаційного розвитку; [1-3]

Таким чином, визначивши основні напрями розвитку законодавства щодо інформаційного простору та захисту інформації як в особистих цілях окремих громадян держави, так і в масштабах захисту інформаційних структур України, потрібно зазначити, що дана сукупність документації правового регулювання, представляє собою закони, норми, постанови, нормативні документи та державні стандарти, що регулюють взаємовідносини в захисту інформації, інформатики та загалом інформаційного простору держави. Нормативно-правова база регулювання відносин в сфері інформаційного простору невпинно розвивається і розширюється відповідно до розвитку інформаційних технологій, і несе в собі поняття, тлумачення та встановлення відповідальності суб’єктів інформаційних відносин, також встановлює правовий статус

технічних засобів та способів захисту інформації. Сукупність узагальнених правил наслідування законів веде за собою розвиток морально-етичних норм в області захисту інформації.

Захист інформації та простору її циркулювання тягне за собою правові відносини, таким чином будуючи систему захисту для інформації, потрібно опиратися саме на повну, структуровану базу законів, постанов та правових норм. Дане регулювання дозволить узаконити, сертифікувати засоби захисту інформації, а також на законних підставах притягнути до відповідальності зловмисників, які неправомірно отримають доступ до закритої інформації.

Умовою забезпечення інформаційної безпеки України є пріоритетний розвиток інформаційної сфери та загальної інформатизації, а також закріплення цілі нормативної протидії загрозам національної безпеки. Звісно Україна як країна, що розвивається має на меті інтеграцію в міжнародне співтовариство, що суттєво розширює можливості закріплення інформаційної безпеки держави за рахунок участі в розвитку норм міжнародного права, створення міжнародної системи забезпечення безпеки інформаційної сфери як світу в цілому, так і кожної окремої держави.

За дисертацією Ю. Максименко щодо аналізу стану нормативно-правового регулювання інформаційної безпеки її становлять три структурні елементи:

1. Інформаційна безпека у сфері прав та свобод людини та громадянина.
2. Інформаційно-психологічна безпека.
3. Інформаційно-технічна безпека. [4]

Нормативно-правове регулювання ІБ становить владну форму правового впливу на інформаційні відносини суспільства, що з метою упорядкування, закріплення, забезпечення здійснюється державою.

Для забезпечення безпеки інформації а АСДО прийнятий ряд законів, що виступає незмінним фундаментом в технічному захисті інформації. Конкретними законами щодо регулювання в сфері АСДО виступають: Закон України *«Про захист інформації в інформаційно-телекомунікаційних*

системах», Закон України *«Про електронні документи та електронний документообіг».*

Також перелік не менш важливих документів щодо захисту інформації в АСДО:

- Закон України *«Про інформацію»*;
- Закон України *«Про захист персональних даних»*;
- Закон України *«Про захист інформації в автоматизованих системах»*;
- Закон України *«Про електронну комерцію»*;
- Закон України *«Про державну таємницю»;*
- Закон України *«Про електронний цифровий підпис»;*
- Закон України *«Про електронні документи та електронний документообіг»;*
- Закон України *«Про Національну програму інформатизації»*;
- Положення про порядок здійснення криптографічного захисту інформації в Україні;
- Перелік постанов Кабінету Міністрів України щодо врегулювання відносин у сфері електронного документообігу та ведення електронної документації.

Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ направлені на нормування АСДО:

- НД ТЗІ 1.4-001-2000 *Типове положення про службу захисту інформації в автоматизованій системі;*
- НД ТЗІ 2.5-005-99 *Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;*
- НД ТЗІ 3.7-001-99 *Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.*

Державну політику у сфері захисту інформації відповідно до закону реалізує Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку України).

Більш детально розглянемо закони що безпосередньо стосуються АСДО.

1.1.1. Закон України «Про інформацію»

Закон висвітлює права особи на володіння інформацією в усіх сферах суспільного та державного життя, регулює сам доступ до інформації встановлюючи законні підстави володіння та захисту інформації та інформаційної системи аналогічно. Встановлює основи права володіння, одержання, зберігання та передачі інформації.

Даний Закон діє на будь-які відносини в сферах життєдіяльності суспільства, окремої особи і держави включно, що ведуть за собою інформаційну взаємодію, будь то одержання, зберігання чи поширення.

Закон виділяє поняття інформації та надає її опис як документованих або оголошених публічно відомостей про явища, події, шо могли відбутися чи відбуваються в державі, суспільстві, навколишньому середовищі.

Надає визначення об’єкту та суб’єкту інформаційних відносин.

«Основними принципами інформаційних відносин закон визначає:

- *гарантованість права на інформацію;*
- *відкритість, доступність інформації та свобода її обміну;*
- *об’єктивність, вірогідність інформації;*
- *повнота і точність інформації;*
- *законність одержання, використання, поширення та зберігання інформації»* [5, с. 2].

1.1.2. Закон України «Про державну таємницю»

Закон виділяє поняття державної таємниці, засекречування, розсекречуванням та суспільні відносини пов’язані з державною таємницею, її охороною задля захисту безпеки України.

Визначає поняття державної таємниці, що являє собою вид такої інформації, яка є таємною та охоплює відомості держбезпеки, оборони,

економіки, науки, техніки та інше, розголошення якої може бути шкідливим національній безпеці України.

Визначає чинних державних експертів з питань таємної інформації.

1.1.3. Закон України «Про електронні документи та електронний документообіг»

Закон запроваджує організаційно-правові поняття електронного документообігу та загалом використання електронних документів. Відповідно даний Закон діє при виникненні відносин передавання, відправлення, зберігання, створення, оброблення та знищення документів в електронній формі. Державну політику електронного документообігу реалізують, враховуючи повноваження визначені законом, органи виконавчої влади та Кабінет Міністрів України.

Державне регулювання у сфері електронного документообігу спрямовано на:

- реалізацію єдиної державної політики електронного документообігу;
- забезпечення прав і законних інтересів суб’єктів електронного документообігу;
- нормативно-правове забезпечення технології оброблення, створення, передавання, одержання, зберігання, використання та знищення електронних документів [6, с. 1-2].

1.1.4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

Даний Закон висвітлює повноваження та відносини сторін при забезпеченні захисту інформації в інформаційно-телекомунікаційних системах та її підрозділи. Також виділяє поняття об’єкта захисту, якою являється інформація що обробляється в системі і ПЗ, яке призначене для її опрацювання.

Розтлумачує та встановлює вимоги щодо захисту інформації, яка є державною власністю або з обмеженим доступом, правомірність її захисту та

сертифікація із застосуванням КСЗІ. Сертифікація КСЗІ відбувається за допомогою державної експертизи в порядку, що встановлений законом.

Встановлює обмеження щодо створення КСЗІ, відповідно для її створення повинні використовуватися тільки сертифіковані або з позитивним експертним висновком державної експертизи технічній сфері або КЗІ.

1.2. Відповідальність, що несе за собою порушення законодавства щодо захисту інформації

1.2.1. Адміністративна відповідальність

За недотримання вимог щодо законодавства із захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах може наступати адміністративна відповідальність керуючись статтею 188-31 Кодексу України про адміністративні правопорушення: «*Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України щодо усунення порушень законодавства про криптографічний та технічний захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, та законодавства у сфері надання послуг електронного цифрового підпису, а також створення інших перешкод для виконання покладених на них обов'язків, – тягнуть за собою накладення штрафу на посадових осіб від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян.*

Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, – тягнуть за собою накладення штрафу на посадових осіб від ста до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян» [7].

Також стаття 212-2 Кодексу України про адміністративні правопорушення за недотримання законодавства про державну таємницю визначає відповідальність: «*Невиконання норм і вимог криптографічного та*

технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності, – тягне за собою накладення штрафу на громадян від одного до трьох неоподатковуваних мінімумів доходів громадян і на посадових осіб – від трьох до десяти неоподатковуваних мінімумів доходів громадян. Повторне протягом року вчинення порушення з числа передбачених частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню, – тягне за собою накладення штрафу на громадян від трьох до восьми неоподатковуваних мінімумів доходів громадян і на посадових осіб – від п'яти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян» [7].

Виходячи з цього адміністративна відповідальність порушеного законодавства про захист персональних даних, що веде за собою незаконний доступ до нихабо порушення прав субєкта особистих даних призведе до накладення штрафу на громадян від ста до п’ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб’єктів підприємницької діяльності - від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

При здійсненні повторного правопорушення протягом року, в даній категорії, тобто за яке особа вже була піддана адміністративному стягненню - тягне за собою накладення штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян.

1.2.2. Кримінальна відповідальність

Кримінальний кодекс України передбачає покарання щодо порушення вимог Закону України *«Про захист інформації в інформаційно-телекомунікаційних системах»* за такими статтями:

- Стаття 111. Державна зрада (у формі шпигунства). - «*Карається позбавленням волі на строк від дванадцяти до п’ятнадцяти років з конфіскацією майна або без такої*»[8].

- Стаття 114. Шпигунство. - «*Карається позбавленням волі на строк від десяти до п'ятнадцяти років з конфіскацією майна або без такої*»[6].

- Стаття 328. Розголошення державної таємниці. – «*Карається позбавленням волі на строк від двох до п'яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого, те саме діяння, якщо воно спричинило тяжкі наслідки, карається позбавленням волі на строк від п'яти до восьми років*»[8].

- Стаття 330. Передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави.

- Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

1.3. Висновки до розділу 1

Законодавча база України розглянута в даному розділі виключно стосується АСДО, ІКС, та забезпечення інформаційної безпеки. Потрібно сказати, що законодавча база України потребує нововведень з боку стрімкого розвитку технологій, введення новітньої термінології та незважаючи на це вона в повній мірі забезпечує законні підстави організації технологій інформаційної структури та їх захисту, встановлює відповідальність за порушення законів.

Нормативні документи щодо технічного захисту інформації дають опору для реалізації захищеного інформаційного простору і подальшого його сертифікації.

Розділ 2. ПРИНЦИПИ РОБОТИ, ПРИЗНАЧЕННЯ, СТРУКТУРА ТА ФУНКЦІЇ АВТОМАТИЗОВАНОХ СИСТЕМИ ДОКУМЕНТООБІГУ. АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ В АСДО.

2.1. Базові поняття документообігу

Документообіг будь-то державна установа чи приватне підприємство являє собою систему процесів збирання, перетворення, зберігання деякої інформації та в той самий час пропонує користувачу розширені можливості процесів управління, а саме підготовку та прийняття рішень, контроль за їх виконанням, розподіл обов'язків.

Відповідно на рівні установи котра використовує можливості документообігу, служби підтримки відповідають за допомогу адміністрації вирішувати управлінські питання, таким чином забезпечуючи повне та коректне функціонування системи, підготовку, доставку та безпосередньо рух документованої інформації до її виконавця або зацікавлених осіб. Такими службами в підприємницькій та управлінській діяльності можуть виступати: юридичний відділ, бухгалтерія, плановий відділ, канцелярія, відділ кадрів та інші.

В розрізі сьогодення, стрімкому прирості технічних досягнень та обсягів інформації, яка опрацьовується в установах для функціонування та управлінської діяльності, її структурна складність та потреба у швидкому доступі, а заразом постійна оновлюваність потребує впровадження інтегрованої системи автоматизації документообігу.

Впровадження технологій АСДО в урядування електронними документами неможливе без налаштування та відповідної роботи технологій електронного цифрового підпису. Виділяючи електронний документ як одиницю роботи системи автоматизованого документообігу, потрібно зазначити, що саме він забезпечує найголовніший технічний елемент системи –

електронний документообіг, в свою чергу який забезпечує циркуляцію документі, що складають основу взаємодії держави – суспільства, підприємства – співробітників та клієнтів. Саме звернення за допомогою документованої форми взаємодіє становить необхідну умову надання послуг [5]. Кожин документ повинен відповідати встановленому законодавством набір реквізитів [9].

Електронний документообіг – процеси як окремо так і їх сукупність: створення, опрацювання, зберігання, знищення, відправлення та отримання ЕК, при тому слідується перевірка цілісності та при необхідності підтвердження факту одержання документа.

Ігнорування або запізніле впровадження АСДО може вести за собою проблеми своєчасної взаємодії з клієнтами або її незручності, що як наслідок може критично відбитися на веденні справ, неконкурентноспроможність та суттєві збитки.

2.1.1. Електронний документ.

Під поняттям «електронний документ» відповідно до закону України “Про електронні документи та електронний документообіг”, потрібно розуміти деякий документ інформація в якому зафіксована у вигляді електронних даних, разом з тим обов’язковими є реквізити цього документа.

Правомірним є виклад щодо електронного документа який зазначає, що створення ЕД або сукупності ЕД представляє доказ взаємодії учасника або їх множини, які його створили та містить інформації про зміст дій та взаємодій. Охарактеризувати електронний документ можна його змістом, структурою та контекстом.

Зміст електронного документу – становлять такі текстові та/або графічні структури, що складають документ. В свою чергу контекстом являється інформація щодо зв’язків даного документа із іншими документами та фізичними або юридичними особами.

Електронний документ має наступну структуру:

- внутрішня – змістовна частина документа;

- зовнішня – саме структура того середовища, де існує ЕД.

Також електронний документ має відповідні метадані , які визначають його. Метадані є частиною документа, які несуть інформацію про розуміння змісту, соціальну визначеність, контексту та структури. Таким чином метадані є обов'язковим елементом зберігання електронного документа і можуть зберігати дані цілісності, причетності до створення або зміни юридичною чи фізичною особою.

Електронний документ є об'єктом архівного зберігання та характеризується такими ознаками:

- зберігається на фізичних носіях інформації;
- може мати посилання, що не контролюються авторами (використання Інтернет-файлів або файлів корпоративних баз даних, які мають короткий діапазон життєвого циклу);
- зміст документа може бути фрагментований;
- може відображати великий спектр інформації (текст, графіка, таблиці, бази даних, різного роду мультимедіа);
- являється програмно-технічним продуктом.

Одним з головних питань є збереження автентичності та цілісності електронного документа, що архівується. Доказом автентичності являється:

- відповідність ЕД зазначеному;
- відповідність зазначеного автора або організації, що надіслала документ;
- відповідність зазначеного часу створення або надсилання ЕД.

В свою чергу доказом цілісності являється те що документ повний за своїм складом та не підлягав неавторизованим змінам.

Можливість реалізації загрози втрати цілісності або автентичності ЕД зумовлена здатністю втручання програмними засобами, збій програм передачі даних або їх збереження. Наступні покоління ПЗ можуть бути несумісними з документованою інформацією, що в свою чергу може повести за собою зміни ЕД, втрату цілісності.

Для збереження відповідних властивосте електронного документу згідно із Законом України «Про електронний цифровий підпис» наявність такого підпису є обов'язковим реквізитом, його правомірність та гарантії забезпечують спеціалізовані сертифіковані центри з відповідними повноваженнями.

Саме накладання ЕЦП і становить завершальний етап створення електронного документу.

Таким чином, електронним документом називається інформація, що представлена у вигляді електронних даних, зберігається на фізичних носіях інформації, володіє деякими реквізитами та є підписаний за допомогою ЕЦП. Рахується одиницею АСДО та обробляючи його, відправляючи і тп., утворює електронний документообіг.

2.1.2. Поняття та проблематика впровадження автоматизованої системи електронного документообігу.

Автоматизована система електронного документообігу – організаційно-технічна система, що забезпечує розповсюдження ЕД у комп'ютерних мережах відповідної компанії та може надавати контроль над потоками документів в ній, також реалізує процеси створення та управління доступом до документів [10].

Проблематика традиційного документообігу:

- втрата відомостей про призначення документів, через їх великий потік;
- легкий доступ сторонніх осіб до інформації;
- загублені документи;
- задача систематизації документів потребує затрати великого ресурсу;
- витрати на копії, підготовку та узгодження документів.

Автоматизація електронного документообігу дозволяє уникнути проблем традиційного діловодства або звести їх до мінімуму.

Таким чином, можна виділити наступні пункти, які повинні бути наявні на підприємства для ефективного і доцільного впровадження та автоматизації системи електронного документообігу:

1. На підприємстві можна спостерігати значний документопотік, а саме вхідна, вихідна та внутрішня документація, при опрацюванні якої сповільнюється робота установи та обслуговування клієнтів.

2. Збільшення кількості обговорень, зустрічей та нарад серед керівних підрозділів різних рівнів.

3. Наявність документованої інформації однакової за змістом але різної за формою структуризації.

4. Періодично виявляються проблеми витоку інформації та потрапляння її до осіб, що не мають доступу.

5. Проблема порушення трудової дисципліни, недостатня швидкість прийняття управлінських рішень.

Ігноруючи перелік наведених проблематичних ситуацій, ведення бізнесу та взагалі діяльності на ринку може ускладнюватися в гіршу сторону та вести за собою великі затрати ресурсів.

Саме алгоритми та засоби створення, ведення документів, їх організації, до того ж ведення електронного архіву, якими володіє автоматизована система документообігу, може забезпечити стабільність роботи та організованість підприємства. Базуючись на програмно-технічних засобах АСДО у більшості випадках виключає вплив людського фактору на документооборот в компанії, доступ до неї та ін.

Основні принципи автоматизованої системи електронного документообігу [11]:

- разова реєстрація деякого документа, в наслідок чого його можна ідентифікувати в буд-якій підсистемі;
- система контролю якості;
- регламентування доступу, управління даними, накопичення інформації;

- контроль руху документів по процесах обробки представлена розгалуженою системою звітності, що контролює статус та атрибути документів;
- ефективне управління на всіх рівнях урядування та прозорість діяльності;
- розширена система пошуку документів;
- забезпечення паралельності роботи та виконання різних операцій для підвищення результативності та оперативності спрацьовування;
- постійний рух документів в системі.

Ставлячи в першочерговість максимальне обмеження осіб, що приймають участь в створенні і подальшому опрацюванні документа АСДО досягає не лише пришвидшення самого руху документів, а і загальної ефективності роботи системи.

Ефективність АСДО описуються наступними факторами [12]:

- за допомогою швидкодіючої електронно технології потрібні документи поступають до одержувача за доволі короткий час;
- заощадження ресурсів на матеріальні копії, реєстрацію, багато-осібну взаємодію при їх передачі;
- єдина система діловодства, встановлення уніфікованих структур документів;
- повний контроль діяльності підприємства, руху документів та збір аналітичних даних установи.

Проблеми ефективності реалізації АСДО

Основу проблеми з автоматизації електронного документообігу на підприємстві чи державній установі становить саме масштабність системи та всі процеси пов’язані з переходом на неї, оскільки це стосується усіх сторін діловодства. Одночасне впровадження системи може сповільнити роботу установи на деякий час, під час привикання та підлаштування системи відповідно до типової роботи та особливостей установи можуть неодноразово

виникати збої системи. Загалом проблеми впровадження можна розділити на такі дві групи: організаційна та технічна.

Збоку технічних проблем можуть виступати різноманітні фактори пов'язані із забезпеченістю організації відповідною технічною структурою в повній мірі всіх відділі, що пов'язані з опрацюванням, створенням, передачею чи знищенням документованої інформації, які потребує АСДО. Для її коректної роботи повинні бути залучені усі структурні елементи організації.

В свою чергу організаційні проблеми напряму стосуються керівництва та кадрового складу організації. Для забезпечення швидкого та легкого переходу на новий вид взаємодії, ведення документації працівники та керівництво має приділяти багато уваги вивченню правил користування, правильності ведення в АСДО, щоб уникнути збоїв, заплутаності та уповільнення системи.

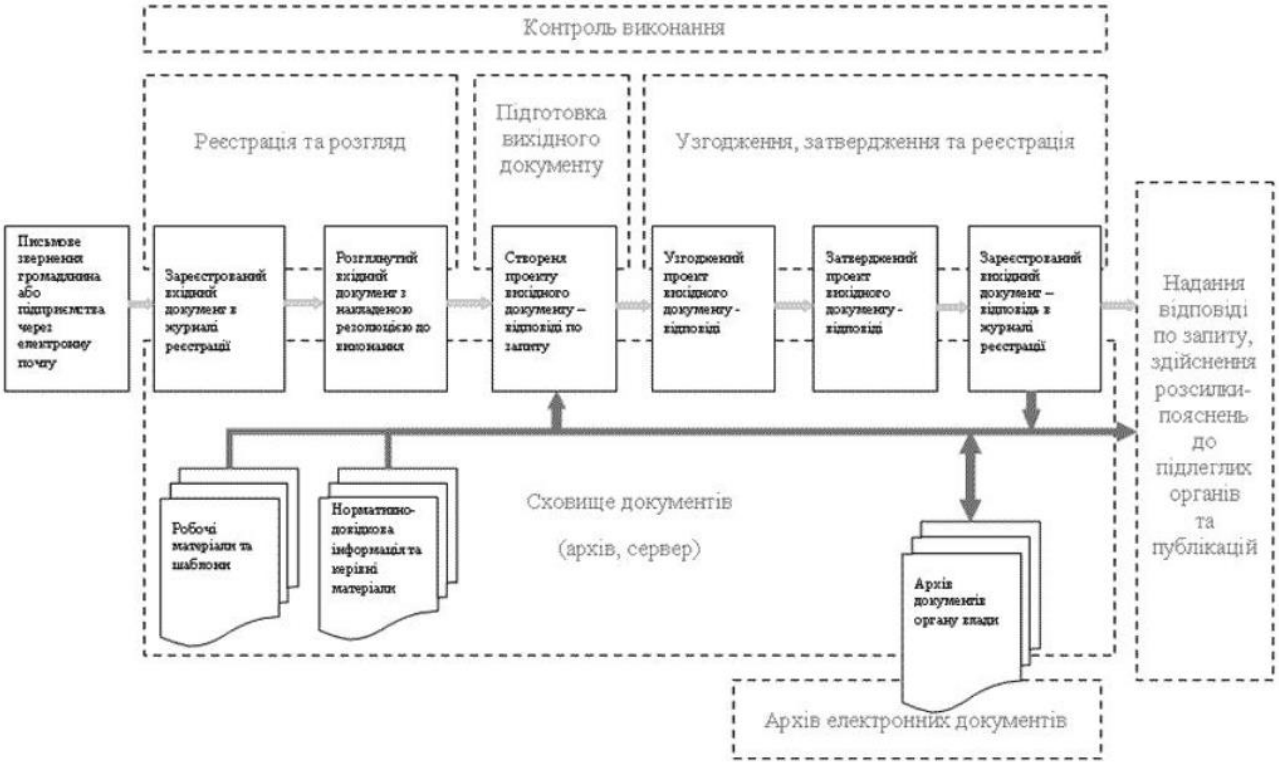
На етапі впровадження з дуже великою вірогідністю може виникнути одна з основних проблем, а саме – консерватизм персоналу, така поведінка є характерною в особливості для державних органів, слабкий кадровий склад підсилює негативну дію даного фактору. Поведінка працівників в такому ключі задається не тільки небажанням освоювати нові навички роботи, а і можливою низькою освіченістю. Впровадження АСДО в організації з дуже консервативною політикою щодо нововведень та роботи над освоєнням нових робочих інструментів зводить нанівець коректну роботу та доцільність переходу на таку систему.

Саме тому запуск АСДО потребує досягнення психологічної готовності працівників насамперед до перенавчання, запровадження нових правил та перебудови бізнес-процесів, потрібно розуміти, що дана процедура займе певний період часу і саме повну ефективність роботи АСДО буде отримано опісля проходження всіх етапів.

Наступною не менш важливою організаційною проблемою може виступати фактор керівництва та його пряме бажання впливати на розвиток системи документообігу. Зумовлена острахом перед наслідками поведінка керівництва може вести за собою в кращому випадку впровадження системи

тільки в деяких підрозділах, що буде виливатися в її неефективності, і в гіршому взагалі ігнорування запровадження такої системи, адже система електронного документообігу показує роботу кожного працівника прозорою та зобов'язує керівництво моніторити процеси обміну та контролювати їх, замість звичної взаємодії з людьми. Також психологічна готовність використання електронних аналогів власних підписів та їх достовірності.

Важливу проблему можу становити постійні структурні зміни в організації, наслідком яких є слабка формалізація бізнес-процесів. Повністю



впроваджену систему здатна спростити дані структурні зміни (рис. 2.1.).

Рис. 2.1. Модель взаємодії систем в автоматизованій системі електронного документообігу

Ще однією проблемою, вже з боку технічної групи полягає у необхідності забезпечення юридичної сили електронних підписів та самих документів [13]. Головним поняттям є що документи в електронній формі можуть супроводжуватися паперовими копіями з «реальним підписом» та «мокрою печаттю», тобто потрібно розуміти – впровадження системи електронного документообігу не має на мені повністю викорінити паперові примірники,

задачею є саме створення середовища ефективного керування, упорядкування та управління організацією. Використовуючи модулі системи в кінцевому результаті буде потрібен тільки один примірник документа, вже з відредагованою і правильно опрацьованою інформацією, що як наслідок знижує обсяг друкованих примірників.

Відсутність або ненадійність організованості паперового діловодства, переростає в проблему інтеграції системи електронного документообігу, так як формування та систематизація нового пристрою функціонування документообороту в організації займає великий проміжок часу та ресурсні затрати. Таким чином для коректного переходу на АСДО заздалегідь потрібно володіти деякою систематизованою структурую діловодства або упорядкувати його перед впровадженням.

З технічної точки зору АСДО вимагає наявність для всіх робочих місць наступних елементів:

- адекватна продуктивність електронно-обчислювальної техніки;
- хороша пропускна здатність між усіма робочими місцями;
- технічні можливості та служби переводу традиційних документів в електронні.

Разом з тим важливу роль становить забезпечення безпеки даних і обмеження доступу при переході на АСДО, наявність експертних висновків та сертифікованості продукції. Даний пункт може становити проблему, яку потрібно відслідковувати при виборі системи електронного документообігу.

Врахування усіх проблематичних зон не дасть гарантій простого переходу на АСДО та фінансових витрат на їх залагодження але надасть поняття можливих затримок та допоможе вирішити їх в найкоротший час.

2.1.3. Стратегічні та тактичні переваги автоматизації документообігу

Призначення та функції забезпечувані АСДО

Існують дві тенденції щодо автоматизації документообігу. Перша тенденція представляє собою документообіг як складову частину діловодства, його автоматизація являється частиною створення інформаційної системи

підприємства і займається простором вже існуючих бізнес-процесів для їх якісної та продуктивної роботи. Тобто автоматизується вже існуюча, налагоджена система процесів підприємства.

Друга ж тенденція представляється використанням вузьконаправлених програм для контролю і управління документами. Такі системи використовують при вже налагодженій моделі документообігу, обробляють великі обсяги документів та вже взаємосумісні з багатьма офісними програмами [14].

Розвиток комп'ютерних технологій на даний момент дозволяють автоматизувати увесь процес роботи з документами, від його створення, реєстрації, відслідковування усіх редакцій, процесу обробки, до переміщення в архівні бази або знищення [15].

Першочерговим і основним етапом роботи з документами АСДО є наступні процеси:

- підготовка, створення і оформлення документів;
- рух документів, передача або прийом;
- курсування документів всередині організації;
- реєстрація, контроль виконання;
- робота з виділення інформаційно-довідкової інформації;
- збереження документів.

Документообіг здійснюється представляється потоками документів, які циркулюють між пунктами обробки інформації, такими як службовці, фахівці або керівники та пунктами технічної обробки, тобто секретарством, копіювальної служби та іншими підрозділами. Саме документообіг охоплює всю послідовність руху документів в апараті управління, в ході якого виконуються операції прийому, підготовки, розгляду, передачі, оформлення та відправки документів. АСДО забезпечує вибір раціонального, найкоротшого шляху документа та використаного часу його опрацювання.

Основними правилами реалізацій автоматизованого процесу документообігу є:

1. Прийом та відправка документів повинна бути централізованою. Всі документи , що надходять в організацію та відправляються з неї, при тому спосіб доставки може бути різним, обробляються централізовано в службі діловодства.

2. Одноразова реєстрація. Документи, що надходять або виходять з організації повинні бути разово зареєстровані з присвоєнням реквізитів для правильного визначення шляху та його пошуку. Така разова реєстрація дозволяє уникнути додаткового введення реєстраційних даних на інших інстанціях.

3. Попередній розгляд документів. Така дія дозволяє заздалегідь виділити відповідність документа до потрібного відділу організації та попередньо розглянути його особливості та дії, що потрібні для його подальшого руху.

4. Виключення зворотного руху без обґрунтування. Передача документі в інстанції які він уже пройшов витрачають зайвий час, що сповільнює роботу системи, тому важливим є визначення та оцінка доцільності його повернення до попередньої точки опрацювання.

5. Можливість делегування права підписання документів. Скорочує час опрацювання готових документів в останній точці де їх скупчення при одноосібній роботі неможливо уникнути.

6. Кваліфіковане розділення операцій обробки вхідних та вихідних документів.

7. Поділ документів, що включені до документообігу на документопотоки.

8. Виділення нереєстрованих документів для їх оперативної реєстрації або скорочення їхнього шляху. Зазвичай це документи, що не потребують опрацювання та своєю присутністю в системі загружають її.

Документопотік визначається як деякий потік документів між пунктами створення та опрацювання інформації і пунктами для їх технічної обробки.

Виділяють наступні документопотоки в організації:

- вхідна документація, потік документів, що надходить в організацію;
- внутрішня документація, потік документів, які опрацьовуються всередині організації та які були створені в ній та не призначені для виходу за її межі;
- вихідна документація, всі документи, які призначаються для відправки.

Також виділяють напрям документопотоку, що забезпечує АСДО, він залежить від змісту конкретного етапу та способу посвідчення документів (Таблиця 2.1).

Таблиця 2.1

<table>
<tr><td colspan="3">Прийом вхідних документів</td></tr>
<tr><td colspan="3">Предогляд</td></tr>
<tr><td colspan="3">Реєстрація</td></tr>
<tr><td colspan="3">Розгляд документів керівництвом</td></tr>
<tr><td colspan="3">Прийняття рішення щодо подальшого руху, обробки документів</td></tr>
<tr><td colspan="3">Контроль виконання</td></tr>
<tr><td colspan="3">Формування документів у справи</td></tr>
<tr><td colspan="3">Довідково-інформаційна робота</td></tr>
<tr><td colspan="3">Зберігання документів, строки та архівні відділи</td></tr>
<tr><td>Передача до архіву</td><td>Подальше опрацювання</td><td>Знищення</td></tr>
</table>

Структурований документопотік який надає АСДО налічує наступні функції та призначення:

1. Оперативність обробки даних. Швидкість занесення інформації, обробки документів та загалом їхнє переміщення по структурах опрацювання збільшується в рази. Документ який щойно був введений в систему стає зразу ж доступний для перегляду та роботи з ним.

2. Оптимізація обліку. Забезпечується автоматизація виявлення копій документів та нереєстрованих документів, що дозволяє уникнути непотрібного дублювання та очищення бази від лишньої маси даних.

3. Гнучке налаштування системи обліку. Можливість розмежування прав доступу.

4. Побудова розподілених систем обліку. Систему можна актуально підлаштувати для обліку документів якщо організація розпределена на філіали.

5. Ведення аналітики та даних по роботі з документами. Аналітичні дані про строки обробки документів, а також обробка та перегляд процесу роботи над документами за будь який час [16].

Підсумовуючи все вищесказане потрібно відмітити, що основним призначенням АСДО є створення упорядкованого, систематично правильно розприділеного документопотоку, який надає організації відповідні функції щодо створення, обробки, контролю якості виконання та подальшого руху документів аж до їх архівного зберігання та знищення. Автоматизація надає винятково простів у використанні та ефективні інструменти взаємодії службовців з документами, що циркулюють в системі, а також повний контроль процесу опрацювання вхідного документу, можливість в кожен момент часу переглядати попередні версії та відповідно редагувати їх.

Структура системи та її модульність

Автоматизовану систему електронного документообігу за структурою можна описати як взаємну організацію двох систем. Першою є апаратно-програмний комплекс, другою ж являється внутрішня система виконуваних функцій.

Апаратно-програмний комплекс складається з наступного напору компонентів: сервери, робочі станції, програмне забезпечення, мережеве обладнання, додаткове обладнання виводу, вводу інформації та її обробки та інші елементи.

Серверна частина даного комплексу реалізує усю бізнес-логіку і здійснює взаємодію клієнтських програм з СУБД. Модулі, що визначають функції

системи, підключаються до сервера додатків. Виходячи з вищесказаного, продукти розрізняються серверними частинами, які містять різні набори модулів.

Автоматизоване робоче місце (АРМ, робоча станція працівника) забезпечує взаємодію працівника з системою. Відповідним набором програмних засобів, які надаються АСДО відкривається можливість прямої взаємодії та доступу до документообороту і самих документів. АРМ користувача є також відправною точкою для отримання, обробки та передачі даних.

Програмне забезпечення виступає посередником між працівникам що взаємодіє з АРМ та інформацією, щодо відповідних документів.

Мережеве обладнання забезпечує функціонування усієї системи як одного цілого організму.

Додаткове обладнання налічує різного розу апаратні та програмні рішення для оцифрування, маршрутизації, виведення, введення інформації.

В свою чергу внутрішня система – це архітектура взаємозвязків програмних модулів та системматизованість циклів проходження документів в АСДО (рис. 2.3.).

На рис. 2.2. представлена загальна модель АСДО із внутрішніми та зовнішніми секторами.

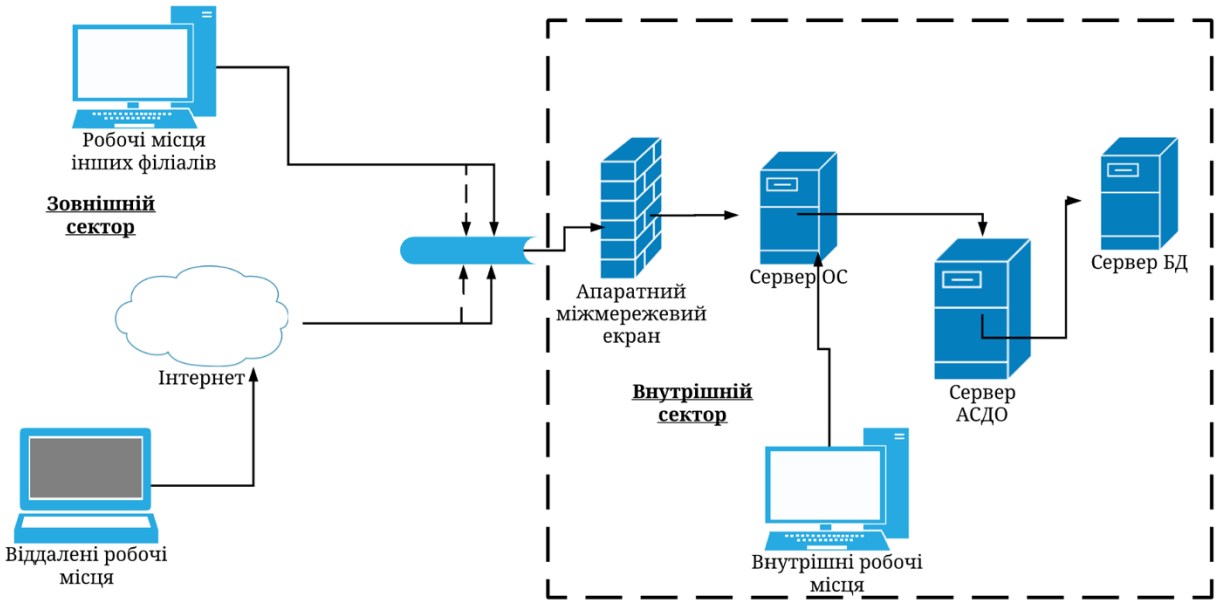


Рис. 2.2. Загальна модель автоматизованої системи документообігу

Структурований електронний документообіг створює в організації деякий єдиний інформаційний простір, в свою чергу інтегруючи усі системи документного упорядкування та роботи з ними в інформаційний вузол. Дана інтеграція здійснюється без втрати якості роботи з документами та збереженням деякого традиційного діловодства [17]. За основу такої системи повинна виступати узагальнене сховище документів, що взаємодіє із загальним документообігом. Таким чином усі оброблювальні документи зберігаються в цьому сховищі та доступні для будь яких підрозділів з відповідним доступом, а також дозволяє забезпечити оптимальний пошук і вибірку потрібної інформації. Загальна схема взаємодії системи електронного документообігу з єдиним сховищем наведена на рис. 2.3.

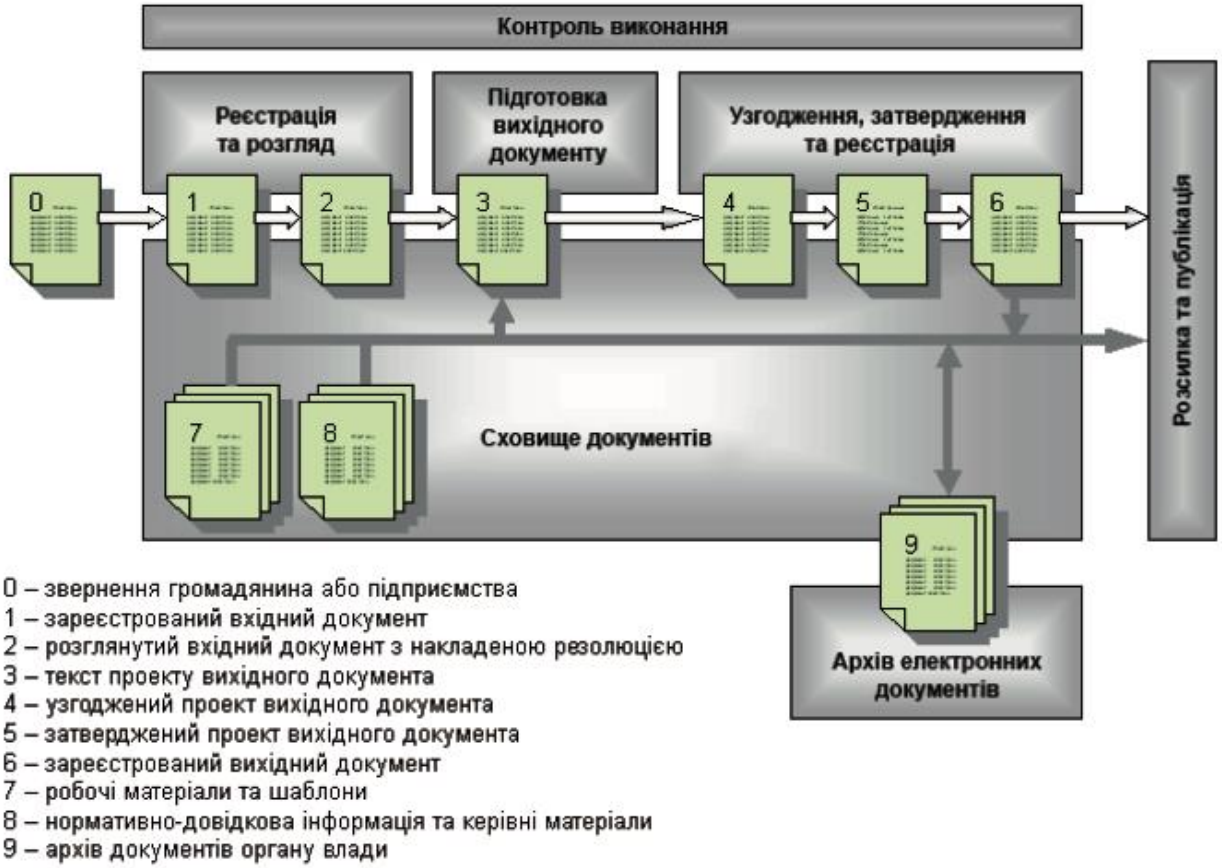


Рис. 2.3. Схема взаємодії системи електронного документообігу з єдиним сховищем документів

Розглянувши загальну модель АСДО та схему взаємодії і курсування документованої інформації по системі, варто також приділити увагу інстанціям, які проходить документ під час свого життєвого циклу в конкретній системі електронного документообігу.

Інстанції взаємодії з документами можна поділити наступним чином:

- канцелярія або інший орган прийняття вхідних документів (реєстрація документів, присвоєння початкових реквізитів);
- виконавець або група виконавців (документ може опрацьовуватися як одним виконавцем так і проходити різні етапи редагування серед послідовності виконавців);
- автор проєкту (документ який було створено всередині організації);
- керівництво (всі оброблювальні документи поступають на завірення);

- архів (документи, які виконали своє функціональне призначення переносяться в архівне зберігання, строки зберігання попередньо визначені установою)(рис 2.4.);

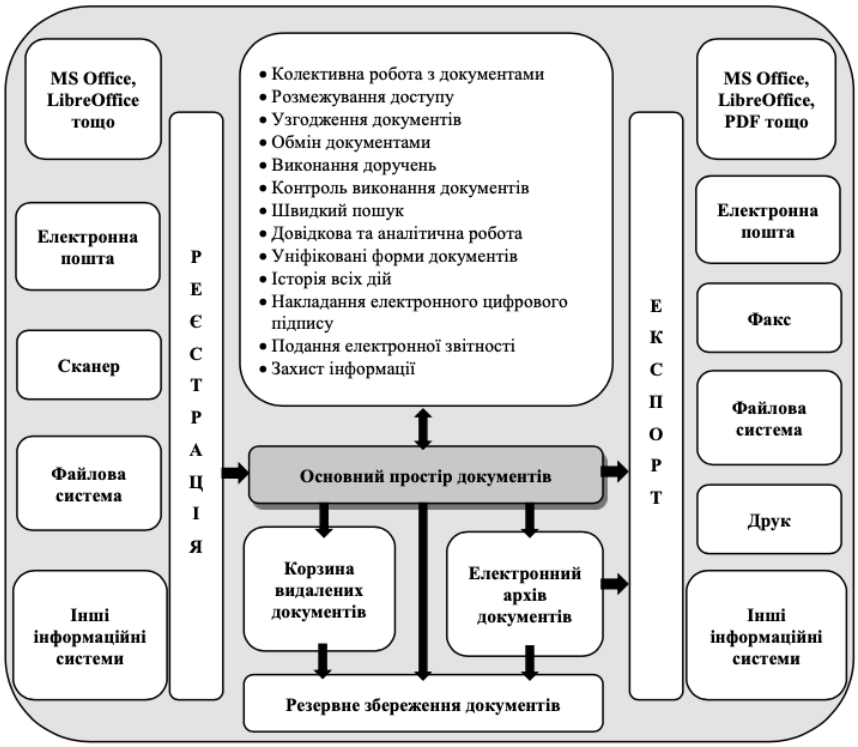


Рис. 2.4. Схема взаємодії інстанцій електронного документообігу

З точки зору виконуваних функцій, структура системи електронного документообігу включає в себе модулі, які реалізують такі дії: введення даних, індексування, обробка документів, управління доступом, маршрутизація документів, системна інтеграція, зберігання.

Модуль введення даних. Використовується для внесення в систему електронного документообігу вихідної інформації. Джерелом документованої інформації можуть бути паперові документів, скани, повідомлення з пошти, online-форми та ін. Даний модуль забезпечує отримання та первісну обробку даних.

Модуль індексування. Реєстрація і систематизація даних, за допомогою яких система електронного документообігу може організувати зберігання і пошук необхідних документів відповідно до потреб користувачів.

Модуль обробки документів. Після введення даних в систему вони повинні бути оброблені і збережені для подальшої роботи. Даний модуль забезпечує розподіл інформації і документів по заданим правилам.

Модуль управління доступом. За рахунок цього модуля забезпечується

розподіл інформації і документів по працівниках. Кожен працівник системи може працювати тільки з тим набором документів, які йому необхідні.

Модуль маршрутизації. У цьому модулі задані правила руху і обробки документів. Для створення маршрутів руху документів попередньо повинні бути визначені процеси документообігу.

Модуль системної інтеграції. Як правило, системи електронного документообігу працюють у взаємозв'язку з іншими системами управління (Наприклад, CRM, ERP, OLAP системами). Модуль системної інтеграції забезпечує передачу даних між такими системами.

Модуль зберігання документів і даних. Цей модуль реалізує функції бази даних документів. За рахунок даного модуля забезпечується зберігання, архівування, відновлення, резервне копіювання документів.

Прямі переваги АСДО над традиційним діловодством

Автоматизована система електронного документообігу виконує безліч функцій, які необхідні для підтримки документообігу та ефективного управління підприємством. Дані отримані після аналізу джерел щодо АСДО, показують ефективність та переваги електронного документообігу над традиційним(Таблиця 2.2. [18],[19],[20]).

Таблиця 2.2.

Традиційне діловодство	**Робота з АСДО**
Безповоротна втрата документів, 15%	Продуктивність праці зростає на 25-50%
Довгий пошук потрібних документів займає близько 30% робочого часу	Обробка одного документа по часу зменшується на 75%
8% часу роботи з документом	Звільнюється 65% часу за рахунок

витрачається на роботу над його змістом	реорганізації операцій введення, сортування, розмноження, маршрутизації документу
Велика кількість копій одного і того ж документу	Час створення одного документу скорочується на 20-30% (завдяки швидкості пошуку і наявності прототипів)
Прямий потік документів, скорочення зворотних переміщень документів в організації	АСДО оптимізує ділові і управлінські процеси, маршрутизація документів за допомогою корпоративних IT систем , одночасна робота декількох учасників над одним документом
Технічні операції та формальні частини обробки зосереджені в діловій службі, змістовні в інших підрозділах	В рамках ділових і управлінських процесах, співробітники являються учасниками електронного документообігу

Систематизуючи переваги АСДО умовно їх можна розділити на такі групи: управління, фінансові, безпеки, контролю, методичні, технічні, інформаційні, технологічні (рис. 2.5).

Велика кількість переваг створює значні можливості для реінжинірингу бізнес-процесів, організаційного розвитку та підвищення ефективності робочого процесу. АСДО сприяє збереженню і раціональному використанні людського ресурсу.

Рис. 2.5. Переваги впровадження АСДО

Таким чином запроваджуючи АСДО в організацію отримується приріст продуктивності роботи та раціональність розподілу ресурсів.

2.3. Види рішень для автоматизації документів та пропоновані вбудовані методи захисту

На даний момент на ринку існує багато рішень щодо запровадження та автоматизації електронного документообігу на підприємстві. Відповідно аналізу підлягає ринок допустимих програмних продуктів, їх сертифікованість та функціональні можливості, що надаються. Не кожне підприємство налічує великий обсяг документованої інформації і потребує не повного списку

пропонованих інструментів, тоді стоїть питання доцільності впровадження та використання коштів на такий перехід, та чи може програмний комплекс АСДО своєю модульністю задовільнити тільки потрібні елементи установи.

2.3.1. Світовий ринок АСДО та України зокрема

З огляду на сучасний розвиток автоматизованих систем документообігу потрібно пильно підійти до вибору саме тої системи, що відповідатиме потребам тої чи іншої установи, підприємства. На даний момент ринок програмного забезпечення в даній сфері пропонує широкий обсях програмних рішень для переходу та впровадження автоматизації електронного діловодства.

Такі системи характеризуються активним прагненням до відмови від паперових носіїв інформації. Широка практика застосування АСДО в Україні, що зазвичай використовуються наступні дві технології, які в подальшому будемо умовно розділяти як «західну» та «східну».

Традиційна «західна» система бізнес-процесів представляє високу виконавчу дисципліну працівників та в основному виділяється означається такими особливостями:

- рух документів характеризується своєю горизонтальною направленістю, такий аспект передбачає надходження документа зразу до виконавця, оминаючи при цьому керівництво;
- в межах установи відсутнє централізований контроль;
- саме виконавці проводять реєстрацію документів.

Система такого типу опирається на відсутність або мінімізацію проміжних планок і орієнтована на колективну роботу та максимальну взаємодію з електронними документами.

В свою чергу традиційна «східна» система процесів володіє наступними особливостями:

- рух документів характеризується горизонтальною прямою, наслідуючи таку схему: керівник – виконавець – керівник;

- система сконцентрована на відслідковуванні усього комплексу робіт (реєстрація усіх відомостей про документ, їх переміщення, звітність та ін.).

Єдиний порядок опрацювання забезпечується утворенням спеціальних служб, що ведуть управління справами (секретаріат, канцелярія).

Автоматизовані системи електронного документообігу, що пропонуються зараз на українському ринку, зазвичай вітчизняних виробників або ж інтеграторів зарубіжних систем.

Однією з інтегрованих під українське діловодство зарубіжною системою є Lotus Notes/Domino від компанії IBM [21].

Серед відомих та доступних АСДО вітчизняних та російських виробників можна назвати наступні:

- DocsVision;
- ДЕЛО;
- БОСС-Референт;
- Парус-Канцелярия;
- Optima-Workflow;
- DIRECTUM;
- DOCUMENTUM;
- LanDocs;
- CompanyMedia;
- FossDoc;
- Атлас ДОК;
- ДОК ПРОФ;
- M.E.Doc;
- Megapolis.Документообіг;
- Comarch EDI;
- АСКОД.

З вищенаведеного списку можна спостерігати, що приріст компаній та їхнього ПЗ значно збільшився, українське діловодство зазвичай наслідує

«східну» систему бізнес-процесів та частково переходить на «західну». Під час вибору ПЗ АСДО потрібно керуватися та виділяти ключові етапи, які будуть визначати успішність впровадження:

- порівняння початкових функціональних можливостей усіх систем;
- пристосування продукту до вимог національного законодавства, сертифікації та відповідності;
- визначення співвідношення ціни та функціоналу, що надаєся ПЗ.

Таким чином, підприємству або державній установі надається широкий спектр вибору ПЗ для впровадження АСДО, правильно вибудувані вимоги щодо потрібного функціоналу та роботи з документами, порівняння ПЗ та співвідношення цін дозволить обрати оптимальне рішення для ефективного переходу та роботи.

2.3.2. Огляд функціоналу пропонованих систем з автоматизації електронного документообігу.

Програмне забезпечення АСДО FossDocs

Автоматизація діловодства на базі системи FossDoc – це програмне забезпечення на платформі FossLook, яке призначене для організації електронного архіву, корпоративного документообіг, а також автоматизації бізнес-процесів. Дане ПЗ дозволяє вирішити велику кількість завдань, що в свою чергу покладаються на різні модулі системи. Реалізація будь-якого роду діяльності та підлаштування з врахуванням специфіки конкретної установи або підприємства.

FossDoc передбачає загальну структуру, що побудована на основі класичної клієнт-серверної архітектури (рис. 2.6).

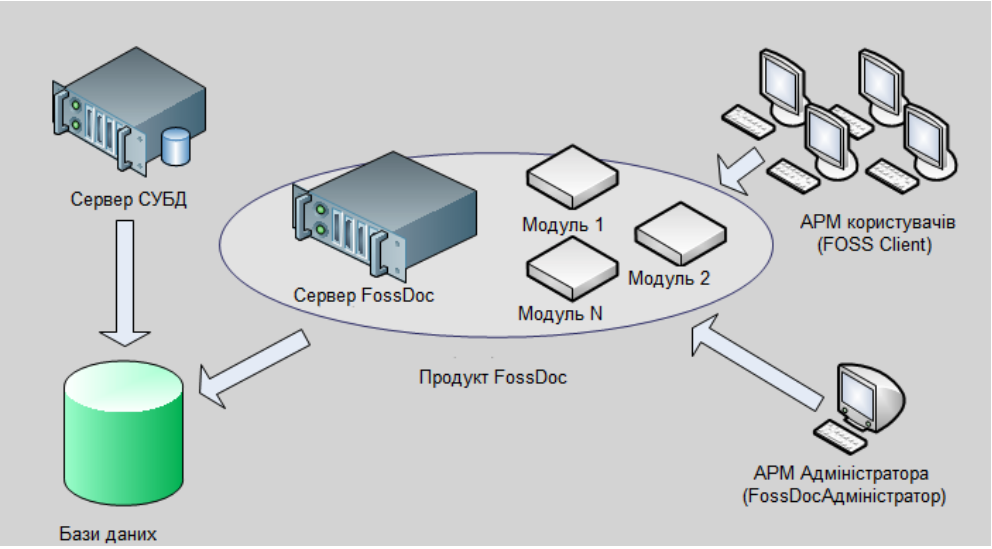


Рис. 2.6. Структура АСДО на базі ПЗ FossDoc

Основними функціями, які забезпечує дане ПЗ є:

1. Автоматизація діловодства – створення реєстраційно контрольних карток, відправка доручення, облік паперових оригіналів, контроль над виконанням, підготовка резолюцій, взаємодія з ЕЦП та звітність (див. Додаток А.1).

2. Підтримка різних типів документів – листи, звернення, службові записки та інше (див. Додаток А.2).

3. Проектування бібліотеки документів – функціональні бібліотеки: додавання, видалення полів, налаштування довідки, шаблони друкарських форм та інше.

4. Гнучка маршрутизація документів (див. Додаток А.3).

5. Підтримка колективної роботи користувачів.

6. Вбудований поштовий сервер.

7. Електронно цифровий підпис [22].

Модульність даного ПЗ дозволяє вдало підібрати потрібні компоненти для автоматизації документообігу як на великих підприємствах з відповідним документопотоком так і на малих. Модулі системи налічують такі пункти: платформа FossLook, сховище, резолюції, проєкти документів, періодичні задачі, службові записка, журнал, історія, Web-сервер, доменна авторизація, контроль документів, звернення громадян, аудит, статистика, інтернет пошта, помічники співробітників, обчислювальні поля, повідомлення маршрутизації,

обговорення документів, Веб-портал, інтеграція СЕВ, розпізнавання, архівний центр, ЕЦП [22].

Доступна також пробна версія в яку входить базовий набір модулів та обмеження можливих підключених АРМ, опісля тестування системи її можна розширити не порушуючи вже налаштованої автоматизації. Також дається можливість повного придбання або ж помісячної оренди та технічна підтримка продукції.

Програмне забезпечення elDoc

elDoc – програмне рішення по впровадженню та забезпеченні автоматизації електронного документообігу рівня Enterprise? Я ке розроблене на сучасних web 2.0 технологіях. Гнучкий інтерфейс дозволяє налаштувати систему документообігу для ефективного забезпечення усіх функцій та виконання належним чином роботи працівників. Вітчизняний виробник, компанія «DMS Solutions» є технологічною продуктовою компанією, розробником інтегрованої платформи для інтелектуальної автоматизації процесів обробки документів (IDP – Intelligent Document Processing & Document Workflow Automation) - «elDoc» [23].

Напрямки діяльності, які пропонує DMS Solutions:

- автоматизація бізнес-процесів, обміну інформацією;
- інтелектуальна обробка документів;
- роботизація бізнес-процесів (на базу RPA рішень);
- консалтинг у сфері автоматизації діловодства.

Впровадження компанією продукції АСДО включає в себе забезпечення наступних підсистем:

- система автоматизації бізнес-процесів;
- автоматизації процесів обміну документами;
- автоматизація робочих місць [23];

Функції що надає elDoc мають широкий спектр застосування при роботі з електронними документами та веденні діловодства загалом. Замовнику

пропонується онлайн демо-версія для ознайомлення з інтерфейсом програмного забезпечення, а також основним його функціоналом (див. Додаток Б.1).

До додаткових можливостей, які пропонує elDoc належать:

- використання штрих-коду;
- пошук, фільтрація документів;
- онлайн редактор;
- CRM;
- виконання обов’язків заступника.

Великою перевагою даного ПЗ є наявні технології кросплатформеності, що дозволяють виконання деяких основних функцій через мобільні додатки. Такий підхід полегшує віддалену роботу працівників, а також роботу у відрядженнях.

Також легкий інтерфейс в сумісності з відкритою системою API, стає хорошим інструментом, що особливо якісно підлаштувати ПЗ під вимоги замовника.

Наявність електронного цифрового підпису.

Програмне забезпечення LanDocs

LanDocs – програмне забезпечення пропоноване компанією «ЛАНИТ» для автоматизації електронного документообігу характеризується високим ступенем готовності базового ПЗ до роботи, гнучкістю контролю виконання та обліку документів, широкими можливостями по інтеграції з корпоративними інформаційними системами. Розробник заявляє про можливість розробки документообігу в системі територіально-розділеної організації [24].

LanDocs налічує велику кількість компонентів, що забезпечують стабільність роботи системи та її багатофункціональність.

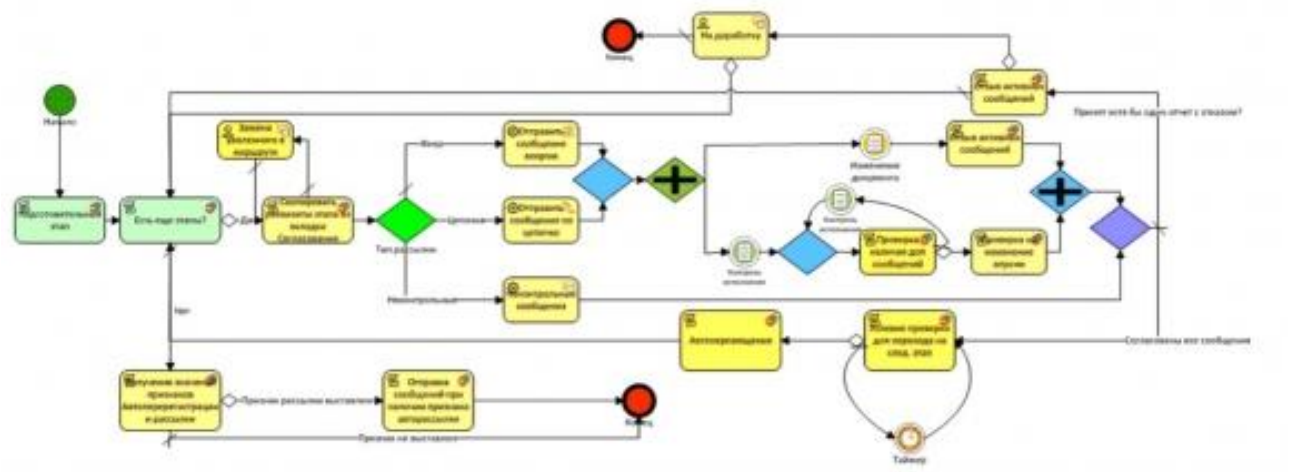
Основні компоненти системи:

1. Сервер контенту – основний сервер додатків забезпечує управління користувацькими сесіями, розмежування прав доступу, реалізує бізнес-логіку обробки даних.

2. Сховище контенту – підтримка двох типів файлового сховища: на мережевому ресурсі або базі даних. Доступ до сховища відбувається через сервер контенту.

3. Управління бізнес-процесами – BPM система, яка дозволяє створювати маршрутні карти (рис. 2.7), що описують бізнес-процеси, і роботи над ними.

4. Центр управління – додаток клієнта який об’єднує всі інструменти налаштування і моніторингу системи. Кожен інструмент реалізований у вигляді окремого функціонального пристрою. Налічується можливість підключення



додаткових модулів (див. Додаток Б.2).

Рис 2.7. Маршрутна карта бізнес-процесу LanDocs

Інструментарій даного ПЗ забезпечує можливість гнучкого налаштування системи. Сертифіковані та партнерські програмні засоби роблять АСДО на базі даного ПЗ стійким до системних та апаратних збоїв, разом з тим вимагають досить високих ресурсів інформаційної системи підприємства-замовника [24].

В комплекс безпеки входить ЕЦК, можливість розмежування доступу та окремий модуль шифрування даних.

2.3.3. Цінова політика на ринку ПЗ АСДО та доцільність вкладень.

Сучасний ринок пропонованого програмного забезпечення з впровадження АСДО на підприємство або державну установу повниться безліччю варіантів відповідно до специфіки організації та її потреб, відповідно

цінова політика такого ПЗ коливається відносно величини організації, функції, що повинні реалізуватися, а також самого продукту, тобто ціни встановленої розробником.

Таким чином, підходячи до цінової політики ПЗ АСДО потрібно проаналізувати ринок пропонованої продукції, їх повнота надання функцій та взагалі доцільності використання того чи іншого продукту.

Першим чинником оцінки АСДО стоїть її модульність, адже саме додаткові модулі надають можливість вдало підібрати потрібний інструментарій елементів системи відповідно до запитів організації.

Другим критерієм є забезпечення технічної підтримки та її собівартість. Саме технічна підтримка надає безпечний бар'єр між виходом з ладу системи документообігу та швидким встановленням її робочої можливості.

Також не менш важливим є врахування кількості АРМ, що може пропонувати базова версія АСДО, та політика цін при розширенні системи документообігу.

В таблиці 2.3. представлені основні дані щодо цінової політики конкуруючих та лідерів в постачанні ПЗ з АСДО [22],[24],[25],[26],[27].

Таблиця 2.3.

Найменування продукту	Вартість основних рішень	Вартість додаткових модулів	Вартість технічної підтримки	Ціна за додаткове АРМ
FossDoc	29554 грн.	2800-8400 грн.	4433 грн (15% від закуплених інструментів)	2850 грн.
ДЕЛО	13020 грн.	3100-31000 грн.	21650 грн/рік	1200 грн.
LanDoc	11750 грн.	500-17500 грн.	18000 грн/рік	2400 грн.
ГранДок	21500 грн.	1200-8500 грн.	14700 грн/рік	2880 грн.
OPTiMA Base	39900 грн.	2200-8800 грн.	10500 грн/рік	1550 грн.

Виходячи з наведених вище цінових рішень можна зазначити, що повний перехід та впровадження АСДО на підприємстві вимагає доволі великих вкладень, що може стримувати малі за обсягом види діяльності. Зважаючи на це потрібно сказати, що кожен розробник пропонує особистий підхід до оцінки та впровадження АСДО, гарантуючи його доцільність та окуповуваність.

2.3.4 Оцінка вбудованих модулів захисту інформації в АСДО

Будь-яка АСДО представляє собою – систему каналами зв'язку якої циркулює документована інформація. Електронні документи, які мають свій життєвий цикл несуть деяку, потенційно важливу для її власника інформацію, втрата якої може нанести як незначні так і великі збитки. Саме тому захист інформації в системах електронного документообігу є важливою складовою системи в цілому. Зациклившись на конкретних задачах автоматизації бізнес-процесів та розробці великого масиву функціоналу, часто розробники забувають включити в їх список потужні модулі захисту інформації.

Відсутність засобів шифрування та захисту каналів зв'язку або часто прості алгоритми, які легко піддаються розшифруванню роблять систему вразливу для реалізації інформаційних загроз.

Відповідно чим більшою є мережа компанії під управлінням АСДО, тим більш важливі документи, корпоративні таємні та інше зберігається і циркулює в системі. Велика мережа також своїм об'ємом відкриває ряд переваг для зловмисника, даючи велику територію для можливих реалізацій загроз, в її масштабах важко прорахувати найменші деталі безпеки, а саме такі «дірки» відкривають двері.

Тому не беручи до уваги розміри підприємства, інформаційну цінність та процеси, першочерговим пунктом вдалого впровадження АСДО є наявність та забезпечення безпеки системи та інформації, що в ній зберігається.

Пропоновані розробником модулі захисту

Проаналізувавши сучасний ринок АСДО можна зазначити, що практично всі системи забезпечуються ЕЦП та розмежуванням доступу. Залежно від розробника дані модулі можуть постачатися як в основному пакеті програмного

забезпечення так і як окремі додаткові функції. В одиничних випадках розробники пропонують захист інформаціями модулями шифрування.

З вищенаведеного в даному розділі невід'ємною частиною електронного документа є електронний цифровий підпис (ЕЦП), що захищає його від підробки.

Дані що передаються, їх цілісність та справжність зазвичай досягається використанням ЕЦП, на базі технологій асиметричного шифрування та односторонніх функцій.

Функції, які забезпечує ЕЦП:

- механізм візування та підпису документа;
- здійснення перевірки цілісності документа;
- перегляд системного протоколу застосування підпису.

Накладання ЕЦП забезпечує ідентифікацію підпису посадової особи та його подальший захист від підробки або використання іншою особою.

ЕЦП вирішує наступний ряд питань електронного документообігу:

- контроль за юридичною достовірністю документа та повноцінна заміна традиційних завірювальних засобів;
- спрощує процедуру обліку документа, гарантуючи його цілісність.

Процедура підписання документа налічує такі етапи (рис. 2.8):

- ПЗ на основі математичної функції формує відбиток документа (message digesst);
- шифрування відбитка та отримання особистого ключа автора;
- накладання відбитку на документ.

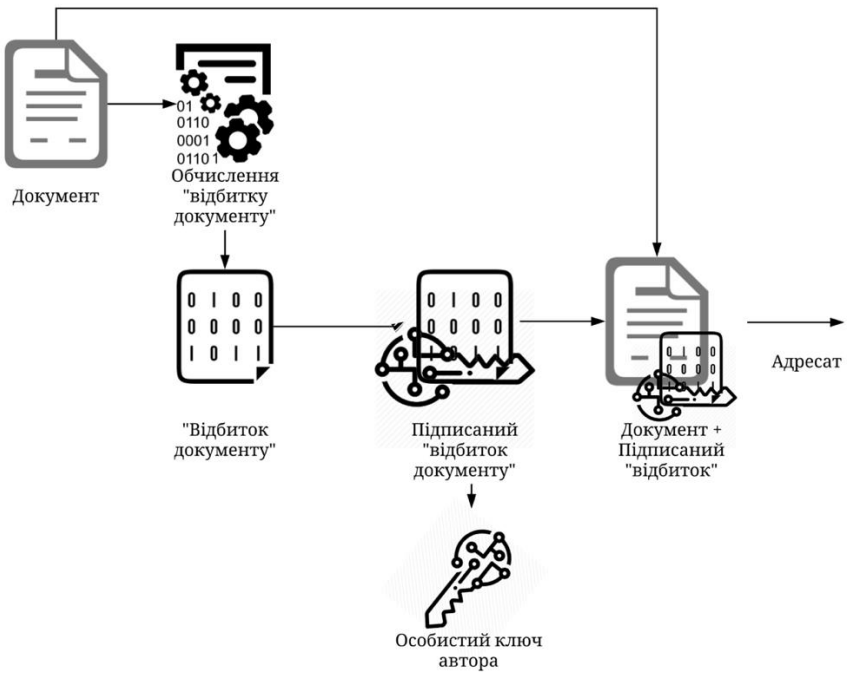


Рис. 2.8. Схема підписання документа за допомогою ЕЦП

Перевірка ЕЦП після одержання в зворотному порядку з використанням ключа автора порівнюючи відбитки початкового і отриманого документів (рис. 2.9).

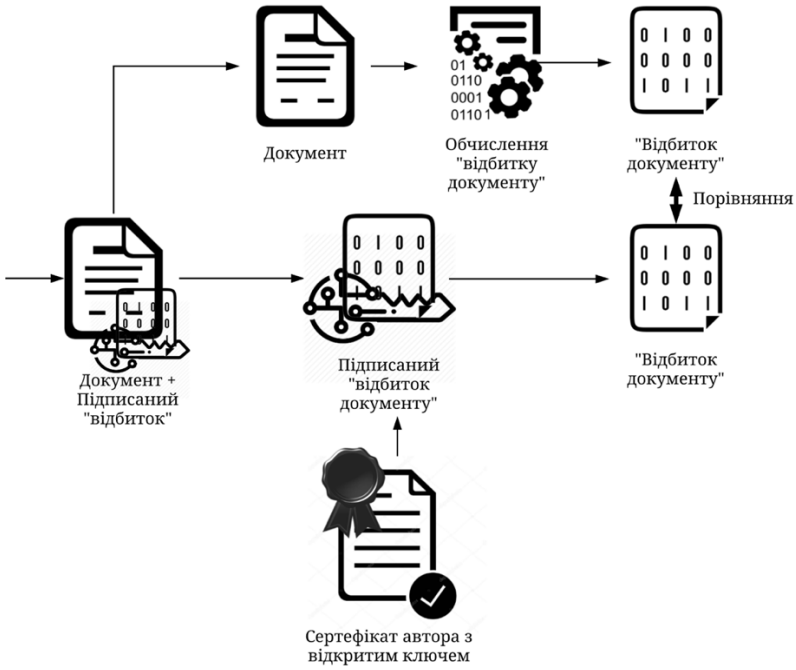


Рис. 2.9. Схема перевірки ЕЦП одержаного документа

Таким чином ЕЦП може забезпечувати достовірність і цілісність документа. Сертифікати відкритого ключа несуть в собі інформацію про автора документа, що дозволяє його ідентифікувати. Опираючись на симетричні або

асиметричні методи шифрування, а також можливе використання хеш-функції, забезпечується досить високий рівень захисту актуальності, цілісності документа [28].

Наступним та не менш важливим засобом захисту інформації в АСДО, що пропонується розробником є розмежування прав доступу.

Існують чотири технології розмежування доступу:

- дискреційна;
- рольова;
- мандатна;
- суб'єктно орієнтована.

Кожна з них налічує декілька моделей розмежування доступу, та може випливати одна з іншої. Найбільш популярними в інформаційних системах є модель *Харрісона-Руззо-Ульмана (HRU)*, *Take-Grant* та *Белла- ЛаПадула*.

Моделі розмежування доступу гарантують виключення доступу осіб в середині організації яким не надані відповідні права, таким чином зберігається конфіденційність даних, що циркулюють в системі.

Узагальнення та оцінка аналізу модулів захисту інформації в АСДО

Для мінімізації можливих реалізацій загроз інформації в АСДО розробники зазвичай пропонують наступні методи захисту:

1. Автентифікація користувачів, кожному АРМ та відповідно його користувачу присвоюються особисті дані автентифікації, зазвичай логін і пароль. Такий первинний метод захисту не гарантовано унеможливить доступ зловмисника до системи але стане першим бар'єром який в подальшому можна удосконалити, допрацювавши метод автентифікації. Додаткові технології, такі як багатофакторна автентифікація або за допомогою біометричних показників, хоч і дорогі в обладнанні але зможуть повністю виключити проникнення з середини.

2. Наступним захисним бар'єром виступає рольове розмежування доступу. Надавши кожному співробітнику відповідні права доступу, зберігається конфіденційність документів всередині системи електронного

доступу. Користувачі з нищим рангом доступу не можуть переглядати, редагувати або видаляти документи, які потребують права доступу вищої категорії;

3. Використання ЕЦП. Саме ЕЦП і становить головну особливість та відмінність електронного документа від традиційного. Застосовуючи таку технологію можна забезпечити цілісність документа, а також повністю замінити традиційні методи завірення документів. Інформація, яку несе в собі ЕЦП не тільки гарантує його справжність, а і дозволяє в разі необхідності визначити автора підписаного документа.

4. Також невелика кількість розробників пропонує модулі шифрування даних, які повинні захищати документи. Цінова політика впровадження таких модулів зачасту виключає їх використання навіть на великих підприємствах.

5. Технічні засоби захисту нараховують мережеві екрани.

Визначивши основні принципи захисту інформації в АСДО можна сказати, що захищеність інформаційних потоків є недостатньою і потребує допрацювання.

2.5. Загрози інформації в АСДО

2.5.1. Загроза конфіденційності

Визначенням загрози конфіденційності інформації є деякі загрози несанкціонованого доступу та ознайомлення з інформацією, що циркулює в АСДО з врахуванням тонких політик безпеки системи.

Загальна схема АСДО налічує такі компоненти: АРМ, серверні частини ОС, АСДО та БД, канали зв’язку. Виділивши їх можна оцінити для кожного з компонентів загрози конфіденційності.

Загроза конфіденційності АРМ полягає у фізичному доступі зловмисника до робочої області системи, безпосередньо володіючи логіном та паролем або

іншим методам автентифікації законного користувача. Такий вид загрози дозволяє отримати доступ до користувацької інформації, а також як наслідок до всіх даних системи та взагалі виведення її з ладу.

Доступ до серверної частини ОС дасть змогу зловмиснику завантажити шкідливі програми в систему, які як наслідок будуть моніторити роботу АСДО, відправляти дані, відкриють можливість «положити систему» або викрадати дані непоміченим.

Порушення конфіденційності інформації, також можливе отриманням доступу до сервера АСДО. Даний сервер забезпечує роботу системи, обробку запиті, маршрутів документів та автоматизації бізнес-процесів. Доступ до нього – прямий доступ до інформації що протікає в системі, а також основного ПЗ.

Сервер БД слугує основним сховищем документів, та конфіденційних даних співробітників і клієнтів. Реалізація загрози доступу до неї надає зловмиснику дістати конфіденційну інформацію.

Канали зв’язку виступають проміжними точками між АРМ та іншими компонентами АСДО. Реалізація загрози дозволить перехоплювати пакети даних між робочими та технічними станціями. Використання шифрованого протоколу HTTPS може значно ускладнити спроби перехоплення пакетів [29].

2.5.2. Загроза цілісності та доступності

При реалізації загроз цілісності інформація втрачає наперед визначену системою вид, повноцінність та якість.

Модифікація електронних документів в системі може нанести за великі збитки організації. Невірно подані дані, підмінені або ж спотворені, їх сприйняття в подальшому може призвести до непорозумінь у внутрішній та зовнішній сферах діяльності організації. Пізнє виявлення порушення цілісності перешкоджає та зупиняє повноцінну роботу організації.

Загрози доступності характеризуються можливістю доступу до електронних документів та потоків даних, що циркулюють в системі в будь-який момент часу. Найчастішими та за своєю збитковою ціною найнебезпечнішими є випадкові помилки штатних працівників, операторів та

системних адміністраторів, що мають доступ до системи та обслуговують її. Частими випадками є саме такі помилки, які і дозволяють реалізувати дану загрозу, створюючи вразливі місця в системі, котрими можуть скористатися зловмисники.

Доступність комунікаційних каналів в зовнішньому секторі АСДО може призвести до перехоплення зловмисником інформаційних пакетів.

2.5.3. Загроза відмови

Така загроза виникає при обставинах коли автор відмовляється від авторства документа, його складання або відправлення. Невдоволення упорядника або керівника може призвести до відмови авторства або розповсюдження неправдивих відомостей щодо документа. Така загроза реалізовується всередині компанії, її співробітниками та може нанести загалом невелику шкоду заплутаності бізнес-процесів та документообороту, що в свою чергу затримує ефективну роботу системи. Проведення внутрішньо-організаційних розслідувань і робіт з співробітниками становить важливу ланку стабільної роботи системи.

2.5.4. Збій у роботі обладнання, встановлення шкідливих програм, стихійні джерела загроз

Збій у роботі обладнання може бути реалізований як працівником організації, служби технічної підтримки, так і самою системою представлені недоліками апаратної або програмної складової. Також до списку дій пов’язаних із неправильною роботою системи можна віднести перепади напруги в електро-забезпечувальних корпусах постачання та загрози природного характеру. На випадок енергетичних перепадів повинні бути передбаченні силові модульні системи стабілізації. Загрози з боку природних катаклізмів за своїм характером непередбачувані та вимагають попередньої готовності та врахування усіх факторів, що можуть нанести шкоду системі.

На перший погляд непомітні збої в АСДО можуть не наносити шкоди загальній роботі системи та періодичне блокування декотрих систем значно сповільнить роботу та ефективність яку пропонує АСДО. Також потрібно

врахувати, під час налагодження роботи та нового запуску модуля, що був виведений зі строю, саме першочергове входження та відновлення зв’язку з іншими компонентами рахується вразливою точкою, даючи змогу підключення стороннього ПЗ та проникнення в системо. Перевірка якості електропостачання є вагомим рішенням, однак потрібно допускати, що її несправність може бути змодельована штучно.

Наслідками збоїв у роботі може бути:

- блокування одного або декількох інформаційних ресурсів;
- втрата даних та неможливість їх відновлення;
- формування нових, раніше невідомих, каналів витоку інформації.

Встановлення шкідливих програм становить не менш важливу загрозу інформаційному простору системи електронного документообігу та самих документів.

Шкідливе ПЗ, що виглядає як корисна програма з функціональної точки зору, називається троянським. Частим випадком є написання такого програмного коду та видавання його довірливому користувачеві за потрібну програму або додавання цього ж коду до вже перевіреного та від відомого виробника комплексу ПЗ, таким чином АРМ заражає всю систему.

Вікно небезпеки для шкідливого програмного забезпечення з’являється з випуском нового різновиду “бомб”, вірусів та/або “хробаків” і перестає існувати з оновленням бази даних антивірусних програм і накладенням інших необхідних латок.

Останніми тенденціями такого виду діяльності зловмисників є інциденти коли використовуючи деяке ПЗ модифікуються дані на комп’ютері-жертві або іншому компоненті системи документообігу, де програмні модулі можуть бути вразливими до такого виду атаки з метою подальшого шантажу і отримання фінансової вигоди. Сценарії роботи таких програм багато в чому повторюють один одного і зводяться або до блокування нормальної роботи комп’ютера, або до блокування доступу до даних.

2.6. Висновки до розділу 2

В даному розділі було детально висвітлені базові поняття автоматизованої системи електронного документообігу, принципи її роботи, а також загальні компоненти інформаційний технологій для її реалізації. АСДО представляє собою комплексну систему взаємо пов’язаних модулів, на базі апаратних технологій, що в своїй сукупності реалізує автоматизацію бізнес-процесів та рух електронних документів.

Означено поняття електронного документа як одиниці автоматизованого документообігу.

Проаналізовано проблематику впровадження такої системи на підприємство чи установу, а також її ефективність та переваги над традиційним діловодством.

Також розглянуто Український ринок постачальників ПЗ із запровадження та переходу на електронне діловодство, врахування цінової політики та доцільності такого переходу. Для загального поняття представлені декотрі лідери в цій області та пропоноване ПЗ.

Таким чином, потрібно сказати, що перехід від традиційного діловодства до електронного є доцільним рішенням для будь якого роду організацій. Своєчасне виконання поставлених задач, швидкий обмін документами, контроль виконання та побудова маршрутів руху робить куди ефективнішим використання людського ресурсу.

Поряд з усіма перевагами такої системи були розглянуті загрози інформаційній безпеці в АСДО. В АСДО можуть бути реалізовані такі загрози як: порушення конфіденційності, цілісності, доступності, відмови, збої системи та природнього характеру.

Недоліками АСДО, якими можуть бути втрата конфіденційної інформації або доступ до них зловмисників, розробники пропонують модулі захисту системи. ЕЦП – замінює традиційні завірювальні методи, а також гарантує

цілісність документа. Також хороша система автентифікації та розмежування доступу можуть забезпечити деяку захищеність системи.

Загалом АСДО не володіє достатньою захищеністю інформаційних потоків від можливих реалізацій загроз та потребує вдосконалення.

Перехід на систему електронного документообігу з автоматизацією процесів, враховуючи усі переваги та недоліки є доцільним в сучасному світі, беручи до уваги безупинний розвиток інформаційних технологій.

Розділ 3. ПРОГРАМНИЙ МОДУЛЬ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПОТОКІВ В АСДО

3.1. Теоретичні засади та опис реалізації програмного модуля

АСДО являє собою заміну традиційного діловодства, автоматизуючи бізнес-процеси та створюючи платформу швидкого обміну і доступу до потрібних документів. Пропонуючи перейти на електронне діловодство, система документообігу пропонує масу можливостей з пристосування до новітніх методів роботи з документами. Таким чином електронний документ стає одиницею ведення діловодства, замінюючи традиційний паперовий примірник. Електронний документообіг не переслідує ціль повністю вилучити паперові примірники, а тільки скоротити їх кількість та кількість копій, що створюються під час обробки даних документів, зменшити трату ресурсів.

У вищенаведених розділах була в повній мірі розглянута структура такої системи, її особливості, переваги та недоліки. Також представлені можливі рішення ПЗ, які пропонує Український та зарубіжний ринок.

Провівши загальну оцінку даного ПЗ, можна сказати, більша частина пропонованих систем є схожою у функціоналі та пропонованих послугах. Кожне ПЗ тим чи іншими можливостями пропонує замовнику АСДО, зазвичай модульну, з можливістю подальшого вдосконалення або розширення потужностей.

Враховуючи те що головною ціллю АСДО є циркуляція документів між різними інстанціями, приходиться стикнутися з такою проблемою як захист цих документів, адже поміж всіх інших налічуються і такі, що несуть конфіденційну інформацію, від реалізації загроз інформаційної безпеки системи. В рахунок цієї теми було проаналізовано можливості захисту

документів, які пропонує розробник. У більшості випадків отримуючи стандартний пакет ПЗ АСДО, розробник пропонує такі модулі захисту як:

- ЕЦП – завірює документ та може гарантувати його цілісність;
- базова автентифікація користувачів (парольна) – може забезпечити безпосередній доступ співробітників з унікальними даниими;
- розмежування доступу – кожен користувач отримує відповідні права доступу до того чи іншого ресурсу.

Декотрими з постачальників АСДО пропонуються також модулі шифрування як додатковий компонент захисту, зазвичай такий продукт пропонуються як окремий і дорогий в цінові політиці. Більшість систем постачаються без модулів шифрування та захисту каналів зв'язку. Виходячи з цього, базова автоматизована система електронного документообігу не володіє достатньою захищеністю, всі пропоновані захисні механізми не гарантують уникнення витоку інформації.

Продукт розробки пропонує автоматизувати процес шифрування даних та їх передачі отримувачу або подальшого зберігання. Шифрування даних, які повинні передаватися по каналу зв'язку системи забезпечить захист та збереження конфіденційності навіть при витоку інформації.

3.1.1. Проблема, яку вирішує продукт

Насамперед слід зауважити що будь-які методи та засоби шифрування не можуть гарантувати повний захист зашифрованих даних, зловмисних, різними маніпуляціями може обійти виконані процеси хоча із труднощами. Зберігання ключів доступу та паролів у відкритому вигляді, а також встановлені шкідливі ПЗ, можуть призвести до реалізації загрози.

У нашому випадку програмний модуль захисту буде керуватися наступною послідовністю дій:

- моніторинг документів на відправку;
- визначення наявності такого документу та його шифрування;
- передача криптографічно-захищеного файлу одержувачу;
- перевірка відповідності даних одержувача;

- звірка криптографічних ключів;
- розшифрування даних на машині одержувача.

Таким чином, під’єднаний паралельно системі даний модуль зможе забезпечити захищеність інформаційних потоків, що курсують по каналах зв’язку.

Програмний модуль розроблений середовищем програмування inteliJ IDEA CE, що пропонує великий набір інструментів та бібліотек, мовою програмування Python. Користуючись розширеними бібліотечними ресурсами код програми було оптимізовано для заощадження використовуваних ресурсів та зведення їх до мінімуму.

Можливості, що реалізує розроблений продукт дають можливість утворення безпечного тунелю передачі даних, в разі витоку інформації дані залишаться недоступними та не представлятимуть цінності для зловмисника. Працюючи в «тихому режимі», не перериває основну роботу системи, цим самим забезпечуючи таку ж продуктивність, що і без неї.

Розроблений модуль захисту інформаційних потоків, з рядом допрацювань може взаємодіяти і з іншими компонентами інформаційних систем.

Метою розробки такого ПЗ є забезпечення інформаційної безпеки документів, що передаються в АСДО.

3.1.2. Обґрунтування вибору середовища розробки

Обране середовище розробки дозволяє правильно та в повну міру використовувати можливості мови програмування для реалізації продукти та його подальшого коректного функціонування. Саме такий функціонал надає inteliJ IDEA CE, підтримуючи основні плагіни роботи для мови програмування Python.

Мова програмування Python є сучасним інструментом для розробки додатків, прикладних програм та web-ресурсів, разом з тим налічує такі переваги:

1. Синтаксис. Легко сприймається та інтуїтивно зрозуміла;

2. Гнучкість. Легко працює та взаємодіє з великою кількістю ОС;

3. Масштабованість. Ефективне масштабування при мінімальних витратах;

Виходячи з вищенаведеного списку саме мова програмування Python найкраще підходить для розробки ефективних додатків, які використовують малий ресурс системи.

3.2. Технічне завдання та вимоги програмного модуля

Мета та призначення програмної надбудови

Надбудова призначена для шифрування конфіденційних даних в АСДО та їх передачі отримувачу з післярозшифруванням. Програмна надбудова автоматизує процес захищеного обміну документів, не впливаючи на швидкодію системи. Дає можливість генерації криптографічних ключів доступу та їх своєчасної зміни.

Характеристики об’єкту розробки

Програмний модуль повинен мати до інформації, процесом налаштування та впровадження повинен займатися працівник технічної підтримки для коректної роботи та розподілу ключів. Технічний працівник забезпечує чітке розмежування доступу до файлів, якими буде керувати надбудова та правильності їх надсилання.

Надбудова повинна мати можливість функціонувати безперервно, двадцять чотири години, сім днів на тиждень.

Експлуатація програмної продукції повинна здійснюватися в умовах, що відповідають експлуатації комп’ютерних інформаційних засобів.

Вимого до структури в цілому

Процес обробки інформації програмним модулем повинен здійснюватися на ресурсах відмовостійкого комплексу апаратних засобів з метою постійного доступу та користування ним користувачами АРМ.

З метою забезпечення комплексного захисту системи програмний модуль повинен бути впровадженим на головний сервер АСДО як надбудова та керуючись його запитами. ПМ повинен забезпечувати автоматизацію процесу передачі конфіденційної інформації в захищеному виді, в тому числі і інформації про відправника, отримувача, їх ключі доступу.

ПЗ повинно мати наступні режими роботи:

- робочий режим;
- режим регламентного обслуговування;
- аварійний режим.

Вимоги до надійності

Апаратно-програмними заходами, а також технічними та організаційними повинна досягатися надійність роботи розроблюваного ПЗ.

Повинна бути реалізована система збереження інформації в разі аварійних ситуацій для уникнення втрати інформації. Такими засобами може бути резервне збереження ключів доступу та дублікатів документів на захищеному сховищі даних.

Вимоги до економіки та технічної естетики

Реалізація графічного інтерфейсу повинна бути примітивно простою та інтуїтивно зрозумілою для швидкого налаштування та коректної роботи, без зайвої інформаційної завантаженості.

3.3. Розробка, алгоритм, постановка експерименту

Алгоритм програмного модуля

Програмний модуль захисту інформаційних потоків складається з наступних елементів: підключення до об’єкту передачі даних, моніторинг стану директорій відправки документів, при отриманні документів на відправку файл шифрується, визначається об’єкт, що приймає дані, дані передаються та дешифруються.

Таким чином, користувач АРМ, перебуваючи в системі електронного документообігу фактично не помічає змін роботи системи, в свою чергу розроблюване ПЗ, що постійно виконується в фоновому режимі та моніторить файли, які призначені на відправлені в тихому режимі, отримавши їх безпечно передає одержувачу. Загальний алгоритм роботи програми приведено на рисунку 3.1., 3.1.

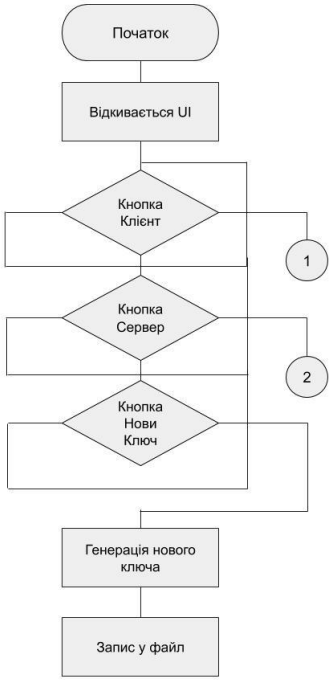


Рис. 3.1. Загальний алгоритм роботи програмного модуля

Рис. 3.2. Загальний алгоритм роботи продовження

При шифруванні даних можна використовувати декілька шифрів, зазвичай обираються симетричні блокові шифри. Причиною такого вибору служить ефективність та універсальність блок-шифрів. Для впровадження були розглянуті наступні варіанти: DES, Blowfish та Rijndael.

Для реалізації шифрування в даному програмному модулі обраний метод AES (Rijndael). Даний метод шифрування є спадкоємцем DES і обраний за критеріями достатньої безпеки, вартості та характеристики алгоритму. Rijndael – метод на основі шифру Square, використовує S-коробки (підміна), XOR для шифрування 128-бітних блоків та перенесення. Також підтримує 128, 192 та 256 бітові ключі.

AES (Rijndael) забезпечує найкраще поєднання безпеки, простої реалізації, ефективності, гнучкості та продуктивності, був розроблений на основі трьох таких критеріїв:

- простота дизайну;
- швидкість та компактність коду на широкому діапазоні платформ;
- завадостійкість всім відомим атакам.

Шифрування або дешифрування здійснюється шляхом ітерації конкретного перетворення. На вхід приймає одновимірні 8-бітові байтові масиви, котрі в свою чергу створюють масиви даних. Таким же і являється ключ, 8-бітовий байтовий масив. З ітераційним блоковим шифром різні перетворення діють послідовно на проміжних результатах шифрів.

Додаткову гнучкість забезпечує можливість роботи алгоритму з різними розмірами ключа 128, 192 та 256 біт. Оскільки алгоритм визначає три розміри клавіш, це означає, що існує приблизно 3,4 x 1038 можливих 128-бітних ключів, 6,2 x 1057 можливих 192- бітних ключів і 1,1 x 1077 можливих 256-бітних ключів.

З основного ключа формуються підключі, для створення розгорнутого ключа ключ шифру розширюється. Довжина раундового ключа дорівнює довжині блоку даних, що множиться на кількість раундів плюс один. Получається, раундові ключі беруться із розгорнутого ключа. Розширкний ключ завжди виводиться з ключа шифру, таким чином гарантується захищеність системи і розширений ключ ніколи не буде вказаний безпосередньо.

Для того щоб блок даних був зашифрований, першочергово виконується крок Add Round Key (XORing підрозділу з блоком) самостійно, після чого регулярні раунди трансформації, і в кінці раунд із кроком змішування стовпця.

Шифр визначається такою послідовністю кроків:

- початкове додавання раундів;
- Nr-1 раунди;
- останній раунд.

Де Nr - кількість раундів, які необхідно виконати. Nr залежить від довжини блоку даних (Nb) та довжини ключа (Nk). Не враховуючи додатковий раунд, виконаний в кінці шифрування, кількість раундів у Rijndael становить: 9, якщо і блок, і ключ мають 128 біт, 11 якщо або блок, або ключ довжиною 192 біта, і жоден з них довше цього і 13, якщо або блок, або ключ, довжина 256 біт.

Раундове перетворення розбивається на шари, які є лінійним змішувальним шаром, який забезпечує високу дифузію протягом декількох раундів. Нелінійний шар, який в основному є додатком S-box Rijndael та ключовий шар додавання, який є просто ексклюзивним або раунловим ключем і проміжним станом. Кожен шар розроблений таким чином, щоб мати свою чітко визначену функцію, яка підвищує стійкість до лінійного та диференціального криптоаналізу [30].

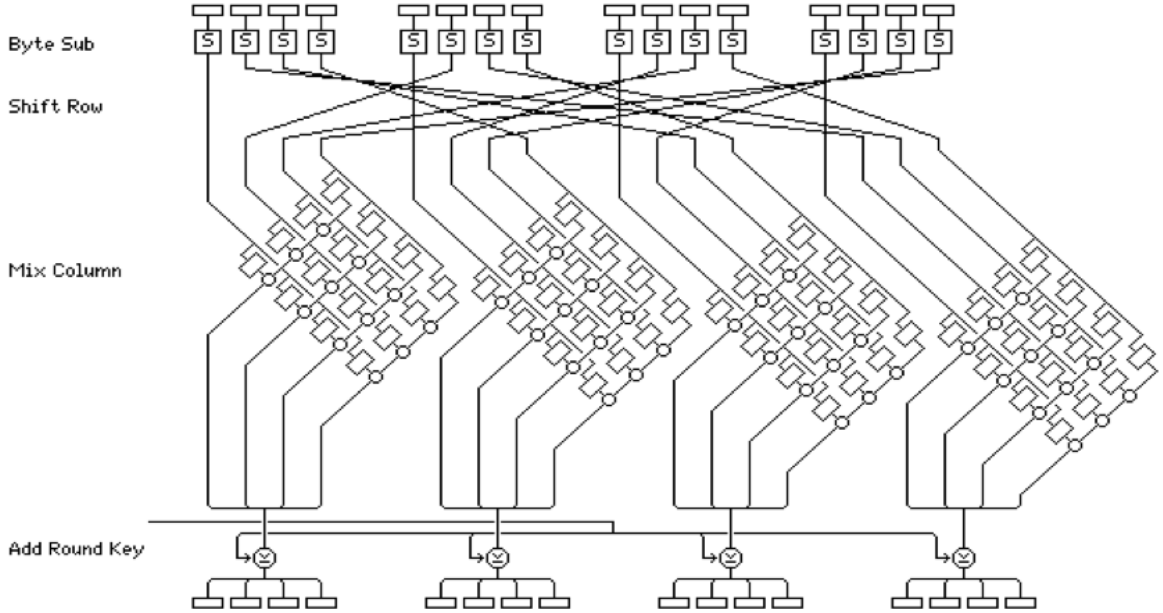


Рис. 3.3 Алгоритм роботи Rijndael

Такі шари утворюються за допомогою чотирьох етапів трансформації. Byte Sub – становить нелінійну підміну байтів. Shift Row – циклічний зсув. Mix Column – стовпці стану як поліноми над кінцевим полем множаться по модулю на фіксований многочлен, після чого виконується Add Round Key (рис. 3.3)

Виходячи з цього ми отримуємо достатньо захищений алгоритм шифрування, що дозволяє реалізувати програмний модуль захисту інформаційних потоків в АСДО.

Постановка експерименту

Першочергово запускаємо сервер АСДО та налаштовуємо всі можливі методи захисту. Додаємо користувачі, задаючи їм логін та пароль, а також роль у відповідному полі (рис. 3.4). Наступним кроком вибираємо провайдера ЕЦП таким чином тепер можемо підписувати документи (рис. 3.5).

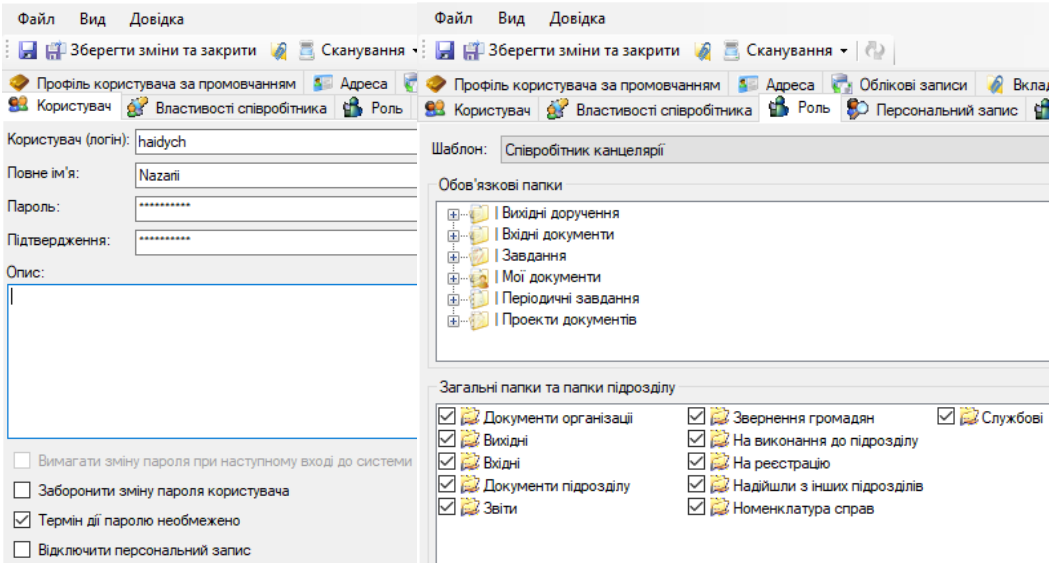


Рис. 3.4. Дані автентифікації користувачів та роль

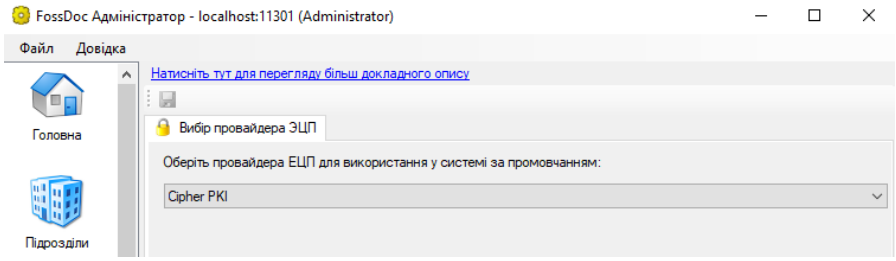


Рис. 3.5. Встановлення провайдера ЕЦП

Наступним кроком запускаємо клієнтську програму, а також розроблений програмний модуль шифрування даних. В початковому вікні програма налічує кнопки вибору відповідності до запущеного ПЗ АСДО, а також генерацію нового ключа. Запускаємо «Клієнт» (рис. 3.6). Для наочності проведення експерименту відправки та шифрування даних, процес виведено в консольному вікні (рис. 3.7). При старті розробленого ПЗ, вичислюються IP адреси користувачів яким можна надіслати документ, а також підключення до відповідних дерикторій. Програмний код наведено в додатках (див. Додаток В).

Рис. 3.6. Вікно програмного модуля

Рис. 3.7. Консольне вікно програмного модуля клієнта

Далі з клієнтської програми АСДО формуємо повідомлення для відправлення. Обираємо отримувача та прикріплюємо файл для відправки (рис. 3.8).

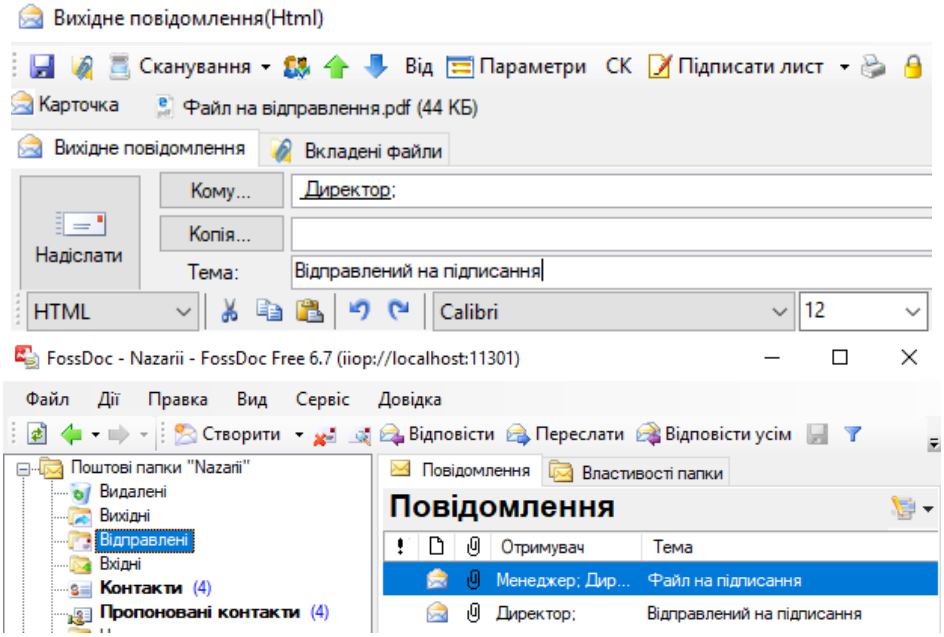


Рис. 3.8. Формування та відправлення повідомлення

Відповідно у консольному вікні програмного модуля можемо спостерігати процес шифрування даних методом Rijndael, раундове почергове перетворення (рис. 3.9). Як видно з рисунка ПЗ продовжує моніторити файли на відправлення. Також зі сторони отримувача повідомлення про успішну передачу даних та розшифрований файл (рис. 3.10.,3.11).

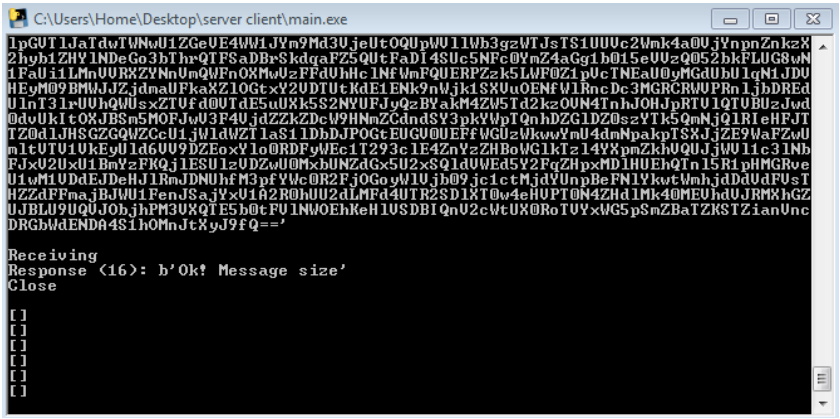


Рис. 3.9. Шифрування даних методом Rijndael

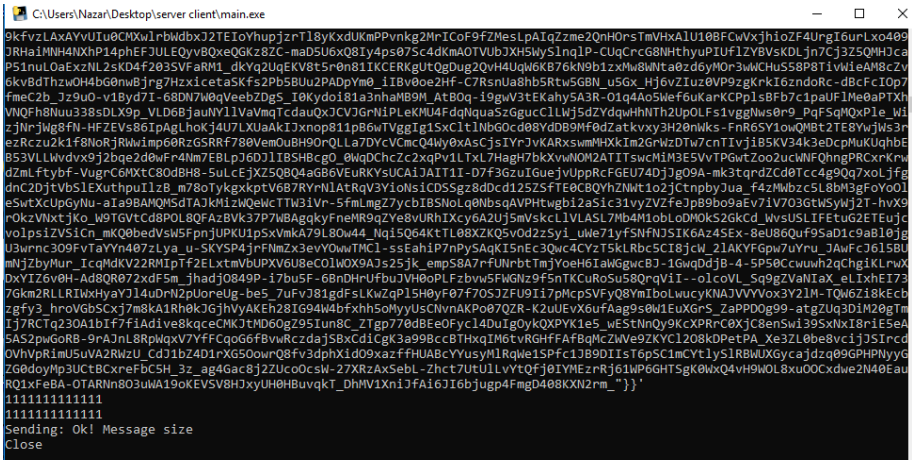


Рис. 3.10. Успішна передача даних та їх дешифрування

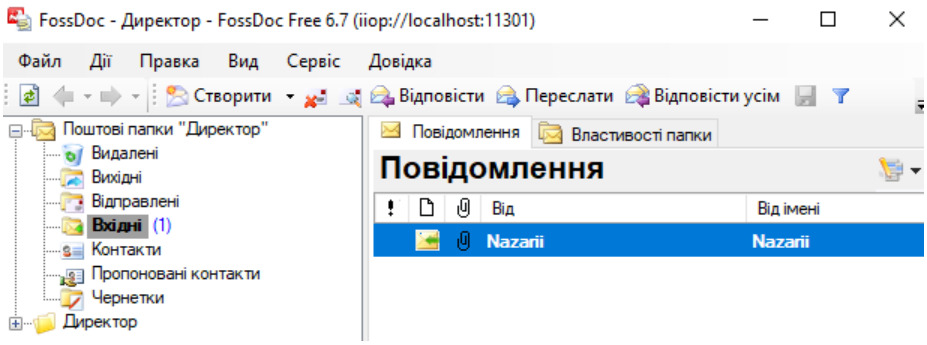


Рис. 3.11. Отримання вхідного файлу в АСДО

Узагальнення успішності експерименту, недоліки та проблематика ПЗ

При проведенні експерименту було досягнуто цілі, електронні документи відправлені в АСДО підлягали попередньому шифруванню та після отримання дешифруванню, таким чином забезпечуючи їхню захищеність під час передавання по каналу зв’язку. Програмний модуль виконуючи відповідні вимоги працював стабільно впродовж ряду виконаних експериментальних прогонів системи. В більшій частині постановок проблем виявлено не було. Також потрібно згадати, що в ряді випадків при втраті з’єднання відслідковувалася некоректна робота механізму встановлення даних, це свідчить про те що даний модуль хоч і проявив свою стабільність роботи але все ж потребує деякого доопрацювання.

Вибраний метод шифрування забезпечує достатню захищеність системи, а тому експериментальної мети було досягнуто.

3.4. Висновки до розділу 3

В даному розділі висвітливши теоретичний опис програмного модуля захисту інформаційних потоків в автоматизованій системі документообігу проаналізовано основні компонентні складові розроблюваного ПЗ. Розглянуто проблеми, які повинен вирішувати даний продукт, а також описаний основний алгоритм роботи ПЗ.

Також детальний опис алгоритму роботи методу шифрування, який використовується в програмному модулі для забезпечення безпеки інформації, надав поняття основних процесів, які відбуваються при шифруванні даних.

Неодноразовою постановкою експерименту було досліджено ефективність роботи програмного модуля захисту, його надійності та виконання в повній мірі свого призначення. Виявлені мінімальні недоліки розроблюваного ПЗ та в цілому роботу можна рахувати більш ніж задовільною. Свої функції та вимоги програмний модуль захисту виконує.

ВИСНОВОК

Автоматизована система документообігу представляє собою комплексне рішення для переходу від традиційного діловодства до використання електронних документів, а також автоматизації бізнес-процесів. Несе ряд функціональних переваг та є невід’ємною частиною ведення бізнесу в сучасному світі. Дає можливість ефективно розподіляти людські ресурси та

ресурси інформаційних технологій, від контролю виконання поставлених задач до миттєвої передачі даних. Така система володіє великою кількістю переваг та на ряду з ними недоліками. Основними недоліками АСДО є наявність можливого витоку або реалізації загроз інформації, що несе особливу цінність його власнику.

У зв’язку з цим необхідно забезпечити систему електронного документообігу відповідними засобами захисту використовуючи методи криптографічного захисту для виключення або зниження до мінімального ризику реалізації загрози.

Основні результати проведеної роботи полягають в наступному:

1. Проаналізована нормативно-правова в сфері інформаційного захисту.

2. Визначені базові поняття АСДО, проблематика її впровадження, а також основні переваги та недоліки експлуатації.

3. Досліджено структуру АСДО, взаємодію компонентів та вимоги щодо апаратних можливостей.

4. Представлено світовий та зокрема Український ринок програмного забезпечення АСДО та їх цінова політика.

5. Проаналізовано пропоновані розробником методи захисту, їх переваги та недоліки.

6. Розроблено власний компонент захисту АСДО та експериментально досліджено ефективність його роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України [Текст] / Одеська національна юридична академія. – О.: Юридична література, 2003. – 471 с.

2. Кормич Б. А. Інформаційне право [Текст] / Б. А. Кормич. – Х.: БУРУН і К, 2011. – 334 с.

3. Ліпкан В. А. Правові засади розвитку інформаційного суспільства в Україні: [монографія] / В. А. Ліпкан, І. М. Сопілко, В. О. Кір'ян / за заг. ред. В. А. Ліпкана. – К. : ФОП О. С. Ліпкан, 2015. – 664 с.

4. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: Дис. ... канд. юрид. наук. – К., 2007.

5. Закон України «Про інформацію» // ВВР. – 1992. – № 48. – Ст. 650. Вводиться в дію Постановою ВР від 02.10.92 №2658-12 // ВВР. – 1992. – №48. – Ст. 651. Із змінами, внесеними згідно із Законами: № 1642-III від 06.04.2000, ВВР, 2000, № 27, ст.213 // № 3047-III від 07.02.2002, ВВР, 2002, № 29, ст.194 // № 2724-VI від 30.11.2010, ВВР, 2011, № 12, ст.86 // № 2756-VI від 02.12.2010, ВВР, 2011, № 23, ст.160 // № 317-VIII від 09.04.2015, ВВР, 2015, № 26, ст.219 // № 1405-VIII від 02.06.2016, ВВР, 2016, № 28, ст.533 // № 1774-VIII від 06.12.2016, ВВР, 2017, № 2, ст.25

6. Закон України «Про електронні документи та електронний документообіг» //ВВР. – 2003. – № 36. – Ст. 275. Із змінами, внесеними згідно із Законами № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст.349 // № 1170-VII від 27.03.2014, ВВР, 2014, № 22, ст.816 // № 1206-VII від 15.04.2014, ВВР, 2014, № 24, ст.885 // № 675-VIII від 03.09.2015, ВВР, 2015, № 45, ст.410 //№ 2155-VIII від 05.10.2017, ВВР, 2017, № 45, ст.400

7. Кодекс України про адміністративні правопорушення // Вводиться в дію Постановою Верховної Ради Української РСР № 8074-10 від 07.12.84.

8. Кримінальний кодекс України // Відомості Верховної Ради України (ВВР), 2001, № 25-26.

9. Державна уніфікована система документації. Основні положення: ДСТУ 3843-99. – К.: Держстандарт України, 2000. – 8 с.

10. Прилипко Н.О. Вдосконалення системи електронного документообігу в органах державної влади / Н.О. Прилипко // Збірник наукових праць Донецького державного університету управління. Серія : Державне управління. – 2014. – Т. 15, Вип. 286. – С. 155-164.

11. Кадан А.М. Возможности системы электронного документооборота Alfresco для организации делопроизводства кафедры / А.М. Кадан, Р.В. Кизер // Технологии информатизации и управления : сб. науч. ст. – Минск : БГУ, 2011. – Вып. 2. – С. 388-392.

12. Автоматизація паперового документообігу та діловодства [Електронний ресурс]. – Режим доступу : https://www.microsoft.com. – Назва з екрану.

13. Про електронний цифровий підпис: Закон від 22 травня 2003 року No 852-IV України (зі змінами та доповненнями)// Вісник Державного комітету архівів України. – 2003. – Вип. 2(14). –С. 23-32.

14. Новицький А. М. Інформаційне законодавство України: окремі питання систематизації / А.М. Новицький, Т.С. Касянюк //Правова інформатика. – 2009. – №2. – С. 17-23.

15. Новак В. О. Інформаційні системи в менеджменті: Навчальний посібник / В.О. Новак, Л.Г. Макаренко, М.Г. Луцький. – Київ: Кондор, 2008. – 462 с.

16. Котлієва Я. І. Документообіг: організація та ведення. 3-тє вид., перероб. і доп. / Я.І. Котлієва. – Харків: Фактді, 2002. – 63 ст.

17. Електронний документообіг та діловодство. Рішення Microsoft в сфері документообігу для російських органів державної влади та місцевого самоврядування [Електронний ресурс]: інформ. бюл. Microsoft. – М. , 2003. – Лютий. – 78 с. – Режим доступу: www. URL:http://www. microsoft. com/Ukraine/Government/ Newsletters/ DocFlow/Default. mspx. – Назва з екрану.

18. Фролов М.Ю. Обзор и анализ основных систем автоматизации документооборота / М.Ю. Фролов // Системи обробки інформації. – 2009. – Вип. 3. – С. 131-134.

19. Основные принципы СЭД [Электронный ресурс]. – Режим доступа : http://www.baikaldoc.ru. – Название с экрана.

20. Пахтанова О. Российские системы автоматизации документооборота [Электронный ресурс] / О.Пахтанова, А. Прохоров. – Режим доступа : http://compress.ru. – Название с экрана.

21. Вибір системи електронного документообігу [Електронний ресурс]. – Режим доступу : https://lotusnotes.com. – Назва з екрану.

22. Вибір системи електронного документообігу [Електронний ресурс]. – Режим доступу : https://fossdoc.com. – Назва з екрану.

23. Вибір системи електронного документообігу [Електронний ресурс]. – Режим доступу : https://dms-solutions.com. – Назва з екрану.

24. Вибір системи електронного документообігу [Електронний ресурс]. – Режим доступу : https://landocs.ru. – Назва з екрану.

25. Вибір системи електронного документообігу [Електронний ресурс]. – Режим доступу : https://eos.com.ua. – Назва з екрану.

26. Вибір системи електронного документообігу [Електронний ресурс]. – Режим доступу : https://grandoc.ru. – Назва з екрану.

27. Вибір системи електронного документообігу [Електронний ресурс]. – Режим доступу : https://optima-ukraine.com.ua. – Назва з екрану.

28. Чугунков И.В., Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2012. – 400 с.: ил.

29. Почепцов Г. Г., Чукут С. А. Інформаційна політика. – К.: Вид-во «Знання», 2008. – 665с.

30. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп’ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.