ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:
«Захист інформації в системах електронного документообігу»

на здобуття освітнього ступеня магістра
зі спеціальності __125 Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____Назар НІКОЛАЄВ

Виконав: здобувач вищої освіти групи СЗДМ 61
_____Назар НІКОЛАЄВ_____

Керівник:_____Андрій КОТЕНКО_____
к.т.н., доцент

Рецензент:_____

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___технічних системкіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСК
_____Олександр Туровський

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

_____Ніколаєву Назару Миколайовичу_____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Захист інформації в системах елекитронного документообігу»
керівник кваліфікаційної роботи КОТЕНКО Андрій к.т.н., доцент
(ПРІЗВИЩЕІм'я,науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 30 » жовтня 2025р. № 467

2. Строк подання кваліфікаційної роботи 20.12.2025

3. Вихідні дані до кваліфікаційної роботи:
__Система електронного документообігу
__Загрози інформації в системах електронного документообігу
__Електронний цифровий підпис.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.__Склад, призначення СЕД_____
2.__Аналіз загроз інформації в СЕД
3.__Використання електронного цифрового підпису для захисту інформації у для захисту інформації у СЕД

5. Перелік графічного матеріалу: ___Презентаційний матеріал на 13 слайдах_____

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ _Назар НІКОЛАЄВ___
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ __Андрій КОТЕНККО_
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: 80стор., 9 рис., 1табл., 20 джерел.

Об'єкт дослідження – процес захисту інформації в системах електронного документообігу

Предмет дослідження – захист систем електронного документообігу

Мета роботи– Обґрунтувати доцільність використання електронного цифрового підпису для захисту інформації у СЕД.

Методи дослідження – системний аналіз, чисельні методи, опрацювання літератури за даною темою.

У роботі проаналізовано загрози інформації у СЕД. Розглянуто доцільність використання електронного цифрового підпису для захисту інформації

Для виконання поставленої мети, у дипломній роботі зроблено аналіз особливостей забезпечення захисту інформації у системах електронного документообігу. Зроблено дослідження системи захисту електронного документообігу на основі застосування електронного цифрового підпису

Галузь використання –захист інформації у системах едектронного документообігу.

Апробація:

А.М. Котенко, Н.М. Ніколаєв, ЗАХИСТ ІНФОРМАЦІЇ У СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.14-16. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ, КЛЮЧ, ЗАХИСТ ІНФОРМАЦІЇ, ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС, КОНФІДЕНЦІЙНІСТЬ, ЦІЛІСНІСТЬ, ІДЕНТИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ.

ABSTRACT

The text part of the bachelor's (master's) qualification work:80 pages, 9 figures, 1tables, 20sources.

*The object of the study:*is the process of information protection in electronic document management systems.

*The subject of the study:*is the protection of electronic document management systems.

*The purpose of the work:*is to substantiate the feasibility of using an electronic digital signature to protect information in the EDS.

*The methods of the study:*are system analysis, numerical methods, and literature review on this topic.

The paper analyzes the threats to information in the EDS. The feasibility of using an electronic digital signature to protect information is considered.

To achieve the goal, the thesis analyzes the features of ensuring information protection in electronic document management systems. The study of the electronic document management protection system based on the use of an electronic digital signature is carried out

The field of use is the protection of information at the object of information activity.

ELECTRONIC DOCUMENT CIRCULATION, KEY, INFORMATION PROTECTION, ELECTRONIC DIGITAL SIGNATURE, CONFIDENTIALITY, INTEGRITY, IDENTIFICATION, AUTHENTICATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРМ	–	Автоматизоване робоче місце
АЦСК	–	Акредитований центр сертифікації ключів
ЕЦП	–	Електронний цифровий підпис
ІБ	–	Інформаційна безпека
КЗІ	–	Криптографічний захист інформації
КЗЗ	–	Комплекс засобів захисту
МЕ	-	Міжмережевий екран
НСД	–	Несанкціонований доступ
ОС	–	Операційна система
ПБ	–	Політика безпеки
СЕД	–	Система електронного документообігу
ТЗІ	–	Технічний захист інформації
ЦСК	–	Центр сертифікації ключів
DLP	–	Data Lost Protection/Data Leak Prevention
ISO/IEC	–	International Organization for Standardization/ International Electrotechnical Commission

ВСТУП

Актуальність дослідження. Загальновизнаною тенденцією сучасності є трансформація індустріального суспільства в постіндустріальне, що відбувається в умовах посилення процесів глобалізації, зростання нематеріального виробництва та ринків послуг на основі досягнень науково-технічного прогресу, зокрема, завдяки масштабному, глибинному та динамічному втіленню інформаційно-комунікаційних технологій в усі сфери життєдіяльності особи, суспільства, та держави [1].

Однією із ефективних форм створення, накопичення і обміну інформацією та її використання у процесі управлінської діяльності є технологія електронного документообігу. Тому актуальним завданням в Україні є розвиток інфраструктури електронного документообігу та взаємодії суб'єктів інформаційних відносин.

Втім, ступінь розбудови системи інформаційної та кібернетичної безпеки, зокрема, на рівні окремих підприємств, установ та організацій є недостатньою і не відповідає потенціалу та можливостям України.

Постає необхідність невідкладного удосконалення захисту не тільки окремих елементів електронного документообігу а його системи у цілому з урахуванням зростання кількості та небезпеки кібернетичних атак.

Наведене зумовлює актуальність проблематики, необхідність додаткового дослідження вказаних питань, а відтак вибір теми.

Об'єкт дослідження – процес захисту інформації в системах електронного документообігу

Предмет дослідження – захист систем електронного документообігу

Мета роботи– Обґрунтувати доцільність використання електронного цифрового підпису для захисту інформації у СЕД.

Методи дослідження – системний аналіз, чисельні методи, опрацювання літератури за даною темою.

Методи дослідження – системний аналіз, чисельні методи, опрацювання літератури за даною темою.

Практичне значення одержаних результатів полягає у обґрунтуванні доцільності використання ЕЦП для захисту інформації у СЕД.

1 СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕТООБІГУ

1.1 Сутність системи електронного документообігу

СЕД дає виконавцю інструмент, що дозволяє в реальному часі відстежувати виконання покладених на нього доручень, переводячи документаційне забезпечення управління організації на якісно новий рівень.

Особливістю СЕД є робота з неструктурованої документацією. Вони можуть передаватися між співробітниками в електронному вигляді, скорочуючи витрати на переміщення чи пересилання паперових копій, і разом з тим візуватися за допомогою електронного підпису, дозволяючи користувачам отримувати і видавати завдання певним співробітникам і навіть цілим відділом або масштабним підрозділам[1].

Незважаючи на зовнішню схожість віконець, діалогів, форм і запитів, які формують в процесі роботи СЕД, вони істотно відрізняються. Їх можна класифікувати по ряду ознак, у тому числі вартості впровадження, обслуговування та іншим параметрам, однак, не для кожного підприємства ці характеристики є суттєвими. Набагатоважливіше в СЕД йогофункціонал, адженавіть укомплектована всімасучаснимиінструментами система не дасть позитивного результату, якщо не буде відповідатизапитамспоживача, а самефункціями, які вона повинна автоматизувати (рис. 1.1).

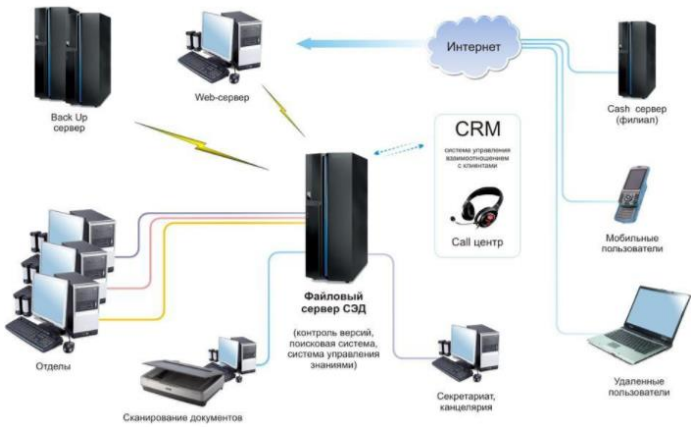


Рис.1.1 Склад системи електронного документообігу

Таким чином, головний критерій оцінювання подібних систем на початковому етапі їх впровадження – це функціональне наповнення. Та умовно можна виділити такі підвиди систем документообігу:

- автоматизатори діловодства;
- архіви електронної документації;
- системи типу workflow;
- комплексні багатофункціональні системи.

Причому якщо перший варіант у списку автоматизує лише базовий набір функцій, то останній, відповідно, дає практично повністю автоматизований процес обміну документами і є найсучаснішим рішенням.

Існуєчимало систем документообігу з різнимфункціональнимнаповненням, в тому числі не завждивдалим, тому для відповідальної особи знайти комплекс з оптимальнимнаповненнямможнавважатинадскладнимзавданням. Приміром, доситьпопулярними і ефективними є: DocLogix; E1 Євфрат; Verdox; WSSDocs; БОС-Референт; СПРАВА; МОТИВ; ТЕЗУ.

Для прикладу у роботі розглянуто систему OptimaWorkFlow, яка має чимало плюсів. Вона легко підлаштовується під потреби оператора, в тому числі її рубрикатори, журнали, елементи управління і навіть картки доручення. Система досить гнучка і підтримує як додавання надбудов, так і вбудовування в IBM WebSphere MQ. OptimaWorkFlow підтримує ведення архіву та має широкі можливості пошуку об'єктів з опціями фільтрації. Унікальна особливість – робота в одному вікні з документом, його зв'язками і рухом. Вона доповнюється зручною роботою з картками, зокрема, їх проектуванням при створенні завдань, а також спеціальним дизайнером для них. Варто виділити наочну ОШС навіть для кількох фірм, реалізовану функцію заміщення, сортування об'єктів і інтуїтивну роботу з довідниками. Що стосується управління БП, є спеціальний дизайнер на безе скриптів API і майстер CrystalReports 11.0. Система безпеки заснована на використанні базових функцій, але і використовує дискретну та рольову моделі управління. Додатковий захист створює ЕЦП. Що стосується недоліків, то їх у OptimaWorkFlow теж чимало. В ній користувачам забороняється створювати свої

папки, журнали і копіювати посилання, настройки не зберігаються. Крім того, реквізити не локалізуються, функціонал заміщення неповноцінний, а для окремих документів неможливо призначити права доступу, а містить лише їх об'єктів. Не варто розглядати систему як основний інструмент для моделювання БП, оскільки її механізми незручні, є проблеми з налаштуванням і СЕД доводиться допрацьовувати за рахунок скриптів.

1.2 Загрозиінформації у системах електронногодокументообігу

Загрози СЕД можназгрупувати по порушеннямвластивостейбезпеки, до яких належать:

- загрозаконфіденційності;
- загрозацілісності;
- загрозадоступності.

Загрозиконфіденційності - цезагрозинесанкціонованого доступу та ознайомлення з урахуванням тонких політикбезпеки СЕД. За вищеописаноїмоделіможнаскласти список загрознесанкціонованого доступу до СЕД, метою яких є порушенняконфіденційностіінформації, щозберігається. До данихпорушеньвідносяться:[2]

1. Погрозаробочиммісцям (внутрішнім, віддаленим і філій) - цебезпосередньофізичний доступ до ЕОМ, коли порушниквжемаєданіідентифікації (логін і пароль, сертифікатзахищеного протоколу HTTPS) законно зареєстрованогокористувачаабоадміністратора СЕД. Даний вид загрозидозволяєотримати доступ до документівкористувача, у якогобуливикраденіданіідентифікації. У разірозкраданняданихідентифікаціїадміністратора СЕД можливоотриманнязловмисником доступу до всіхдокументів СЕД.

2. Загроза серверу ОС - отримання доступу до сервера операційноїсистеми (ОС) дозволить завантажувати в пам'ять сервера шкідливіпрограми (віруси, програми-шпигуни), якіможутьістотнополегшитизламування СЕД. При

отриманнізловмисником доступу до сервера ОС вінможестворитиновенезаконнеробочемісце СЕД, підмінитизаконнеробочемісце на незаконне, імітуватизаконнеробочемісце, отримати доступ до базиданих (БД) СЕД, отриматичастковийабоповний контроль над сервером СЕД.

3. Загроза серверу автоматизованої СЕД (АСЕД) - отримання доступу до сервера автоматизованої СЕД можедозволитизловмисникупідключитисябезпосередньо до СЕД, минаючи сервер ОС і тим самим минаючиосновну систему безпеки, яку і забезпечує сервер ОС. При підключеннізловмисникомсвогоробочогомісцянаслідкианалогічнінаслідкамзагроз иробочихмісць.

4. Загроза серверу баз даних - отримання доступу до сервера БД дозволить зловмисникуотриматичастковийабоповний контроль над СЕД, а також до зберігаємихдокументів. Даний вид загрозинайбільшнебезпечний, тому що в БД зберігаютьсявсідокументи, якіскладаютьосновнуцінність як для власника СЕД, так і для зацікавленогозловмисника.

5. Загроза каналам зв'язкуміж компонентами системиможедозволитизловмисникуперехоплюватипакетиміжробочимимісцями і основними серверами системи шляхом підключення до канала зв'язку. Використанняшифрованого протоколу HTTPS можезначноускладнитиспробиперехопленняпакетів.

Загрозицілісності - загрози, при реалізаціїякихінформаціявтрачаєзаздалегідьвстановлені системою вид і якість. На рис. 1.4.зображена схема ступенівцінностікомпонентів СЕД з точки зорузабезпеченняцілісностіінформації, щозберігається.

У СЕД об'єктамиданоїзагрозиможуть бути всікомпонентиописаноївищезагальноїмоделі СЕД.

Документи - дані, щозберігаються на сервері БД, резервнікопіїдокументів. Ця ланка є самим важливим і цінним, тому щосамесамідокументимістятьконфіденційнуінформацію, для

безпекиякоїорганізована вся система політикибезпекиавтоматизованої СЕД (рис. 2.1).

Рис.1.2Ступеніцінностікомпонентів СЕД

Ступіньцінностіданого компонента охоплена сектором, зазначеним номером 1.Сервер БД - середовищезберіганняелектроннихдокументів. Цілісність сервера БД є другою за значимістюпісляцілісностідокументів - сектор 2.Сервер ОС і автоматизованої СЕД - операційна система і інтерфейсначастина (оболонка) СЕД, встановлені на серверах і робочихстанціях, включаючиклієнтів СУБД; протоколипередачіданих; криптографічніметодизабезпеченнябезпеки. Безпекаданихкомпонентів не настільки критична, тому що при їхвиході з ладу цілісністьінформації, щозберігається (документів) не буде порушена. Слідтакожврахувати, що при позаштатнихситуаціях в рамках цихкомпонентівчастковоабоповністюможуть бути порушенітранзакціїіінформаціївсередині СЕД. Компонентивіднесенідо секторупід номером 3.

Апаратна система - канали зв'язкуміж компонентами, апаратнийміжмережевийекран - сектор з номером 4. Вихід з ладу апаратнихкомплектуючих і комунікаційнихпроводів не призведе до руйнуваннязбереженихдокументів, а несправнікомплектуючі й проведенняможназамінити на нові.

Загрозидоступності - характеризуютьможливість доступу до інформації, щозберігається і оброблюваної в СЕД інформації будь-якоймиті. Найчастішими і найнебезпечнішими (з точки зорурозмірузбитку) є ненавмисніпомилкиштатнихкористувачів, операторів, системнихадміністраторів та іншихосіб, якіобслуговуютькомпоненти СЕД.

Іноді такіпомилки і є власнепогрозами (неправильно введеніданіабопомилка в програмі, яка викликала крах системи), іноді вони створюютьвразливімісця, якимиможутьскористатисязловмисники (такізазвичайпомилкиадміністрування).

Використовуючихалатнеставлення при роботівіддаленогокористувача, зловмисникможереалізуватинесанкціонований доступ. Доступність же комунікаційнихканалів в зовнішньомусекторі СЕД можепризвести до перехопленнязловмисникомінформаційнихпакетів.

Післявизначеннязагроз СЕД, можнавиділитивісімкатегорійпорушника:

- хакери, конкуренти, злочинніорганізації - N1;
- колишніспівробітники - N2;
- технічний персонал без доступу до СЕД; клієнти і партнери - N3;
- користувачкорпоративноїінформаційноїсистеми (ІС) - N4;
- користувач СЕД - N5;
- ІТ-адміністратор ІС - N6;
- дміністратор СЕД - N7;
- адміністраторінформаційноїбезпеки - N8.

Данінорушникивідрізняютьсярівнемобізнаності, рівнемпідготовки, технічноюоснащеністю, а такожрівнем, на якому вони можуть провести атаку.

З вищесказаноговипливає, щоорганізаціясистемикомплексноїзахистуелектронногодокументообігу (КСЗЕД) є актуальною на сьогоднішній день завданням.

КСЗЕД повинна задовольнятидодатковимвимогам, щовідповідаютьактуальнимумовамфункціонування СЕД підприємства і щодозволяєпідвищитиефективністьїїзахисту.

Для зовнішнього ЕД додатковимивимогами до комплексноїсистемизахисту є:

- обов'язкованаявністьзасобівантивірусногозахисту з автоматично оновлюємим списком шкідливихпрограм;

- наявністьзасобівідентифікації атак з реалізованим алгоритмом дій у відповідь на атаки;

- наявністьмеханізму контролю коректностізавантажених в пам'ятькомп'ютераданих;

- наявністьмеханізмузапобіганняперевантаження СЕД відмножиннихзапитів;

- наявністьзасобівзапобіганнязовнішньогосканування СЕД;

- наявністьзасобівзапобіганнярозкриттяінформації, щоміститкомерційнутаємницю та переданої в електронних документах зовнішнімкореспондентам.

З додатковихвимог до захистувнутрішнього ЕД можнавиділитинаступні:

- наявністьмеханізмуперевіркиправильностізаданняпаролів для доступу до ресурсів, щозахищаються;

- наявністьмеханізмуідентифікації атак на засобиаутентифікації, з реалізованим алгоритмом дій у відповідь;

- наявністьмеханізму контролю цілісностівикористовуваного ПЗ;

- наявністьмеханізму автоматичного оновлення ПЗ;

- наявністьзасобів, керуючих правами доступу до різноманітнихпослуг та сервісів;

-наявністьзасобівзапобіганнявнутрішньогосканування СЕД.

Таким чином, зміненаархітектура КСЗЕД підприємства дозволить забезпечитиінформаційнусумісністьвсіхїїскладовихелементів, автоматизованеуправлінняпроцесами, системнувзаємодію служб підприємства, щозалучаються для забезпеченнязахистуінформації, а такожможливістьнайбільшефективногозахисту СЕД підприємства.

Впровадження системи електронного документообігу (СЕД) має свої переваги і недоліки, так звані «плюси» і «мінуси» при використанні у виробничій практиці.

Зважити «все за і проти» впровадження СЕД підприємств, це дуже важлива частина при плануванні структури підприємства і типу її документообігу. Хоча багато керівників не приділяють достатньої уваги питанню автоматизації документообігу і бізнес-процесів в цілому, не інформовані про переваги електронного документообігу.

Основні переваги електронного документообігу проявляються в тому, що при його використанні усі підрозділи і структури підприємства будуть працювати в єдиному інформаційному просторі. У зв'язку з цим, дуже сильно зростає швидкість обробки документів всередині підприємства. Також, важливим фактором, що ставить електронний документообіг на порядок вище звичайного, є збереження і безпеку документів. У сучасних системах використовується шифрування даних, яке допомагає при припинення спроби створення каналів витоку інформації. При використань такого типу документообігу зростає продуктивність співробітників і знижується ймовірність помилок в обробці документів, яка залежить від кваліфікації працівника. Впровадження системи електронного документообігу дає значний економічний ефект, проте кількісна його оцінка є складним процесом, тому що доводиться враховувати безліч чинників.

Прямий ефект від впровадження системи дозволяє економити фінансові кошти, що витрачаються на витратні матеріали, оплату служб поштової та кур'єрської доставки, копіювання матеріалів, зменшує трудовитрати. Непрямим ефектом є переваги управління, які значимі для функціонування організацій: прозорість управління, контроль виконавської дисципліни, можливість протоколювання дій і інші. Впровадження систем електронного документообігу забезпечує[3]:

Одноразову реєстрацію документу, що дозволяє однозначно ідентифікувати документ.

Можливість паралельного виконання операцій, що скорочує час руху документів і підвищення оперативності їх виконання.

Безперервність руху документа, що дозволяє ідентифікувати відповідального за виконання документа (завдання) кожной миті часу життя документа (процесу).

Єдина (або узгоджена розподілена) базу документної інформації, що дозволяє виключити дублювання документів.

Ефективно організовану система пошуку документа, що дозволяє знаходити документ, володіючи мінімальною інформацією про нього.Розвинену систему звітності по різним статусам і атрибутам документів, що дозволяє контролювати рух документів по процесах документообігу і приймати управлінські рішення, ґрунтуючись на даних зі звітів.

Можливість роботи організацій з віддаленими користувачами і групами користувачів.

Збереження історії роботи з документами (облік часу і авторів, всіх дій з документом, збереження робочих коментарів, підтримка версійності приєднаних файлів).

Підтримка змішаного документообігу (підготовка паперових документів і звітів за шаблонами, висновок на друк реєстраційної картки документа, облік місця зберігання оригіналів документів).

Забезпечення інформаційної безпеки (підтримка електронно-цифрового підпису, шифрування даних, протоколювання, розмежування прав доступу і системи ролей, наявність вбудованих засобів контролю цілісності даних і автоматичного резервного копіювання).

Але при всіх перевагах системи електронного документообігу, вона має свої недоліки, які теж варто брати до уваги при прийнятті рішень про впровадження СЕД. Якщо підприємство впроваджує СЕД з самого свого заснування, то труднощів у співробітників воно не викличе. Але якщо рішення приймає керівник підприємства, у якому вже досить тривалий час діє звичайний документообіг, то потрібно брати до уваги те, що реформування системи може

викликати ряд труднощів у співробітників. Потрібно взяти до уваги той факт, що підприємства може понести витрати на придбання програм і систем документообігу, а також на їх впровадження та подальше обслуговування.

Впровадження електронного документообігу включає в себе кілька етапів. На самому початку процесу має бути автоматизовано роботу відділів, що мають справу з максимальною кількістю документів, що диктує необхідність суворого контролю за документацією.

Етапи впровадження СЕД[4]:

Етап 1, або підготовчий. Його метою є розуміння цілей замовника. Для цього проводиться аналіз і класифікація проблем.

Етап2. Обстеження документообігу та його оптимізація. Проводиться для уточнення використовуваної схеми і особливостей документообігу: маршруту, правил реєстрації, секретності і т.д.

Етап 3. Підготовка технічного завдання. Враховуються вимоги щодо функціональності системи, її налаштування, організаційної структури, технічних характеристик, забезпечення надійності і т.д. Приклад технічного завдання для підприємства, складений на базі попередніх етапів наведено у Додатку А.

Етап 4. Укладення договору. Проводиться для зведення до мінімуму можливих непорозумінь, затвердження графіка робіт, їх обсягу, вартості.

Етап 5. Підготовка інфраструктури. Інфраструктура замовника приводиться у відповідність до вимог ТЗ.

Етап 6. Приведення технічної інфраструктури замовника у відповідність до вимог технічного завдання.

Етап 7. Інсталяція системи. Включає в себе:

- установку серверного ПЗ;

- підготовку призначених для користувачів місць;

- тестування роботи системи;

- її налаштування для відповідності особливостям організаційної структури підприємства.

Eman 8. Навчання. Має включати повні курси навчання адміністратора системи. Навчання в групі проводиться за допомогою презентацій.

Eman 9. Дослідна експлуатація. Її суть полягає в роботі співробітників з налагодженою функціонуючою системою.

Eman 10. Коригування. Проводиться на основі отриманих при дослідної експлуатації результатів.

Eman 11. Введення СЕД в промислову експлуатацію.

Також існують недоліки і в інформаційній безпеці. Несумлінному конкуренту отримати інформацію, розміщену на паперових носіях, складніше: документи можуть зберігатися в різних приміщеннях, шафах (столах, сейфах), розрізнених папках. З електронними базами даних інакше. Сучасні зловмисники за допомогою віддаленого доступу зламують дорогі програми з високим ступенем захисту.

Наступний недолік - це різке збільшення потоку документообігу. Як результат – можливостей серверів не вистачає , падає продуктивність праці. При наявності паперового документообігу такий різкий ривок неможливий.

І ще один недолік - це збільшення трудовитрат як наслідок збільшення документообігу. Роботодавець не встигає адекватно реагувати на подібні скачки в прийнятті рішень з кадрових питань. Обсяги зростають, тоді, як штатний склад залишається тим самим.

Після розгляду системи електронного документообігу можна зробити висновок, що воно має свої переваги і недоліки і впровадження її всередині підприємств залежить від керівника.

1.3Напрямизахистуінформації у системах електронногодокументообігу

Побудова системи електронного документообігу, як документно-орієнтованої інформаційної системи, здійснюється на мережевій платформі: як у вигляді локальної, так і у вигляді розподіленої обчислювальної мережі (LAN і POM, відповідно).

Захищена СЕД повинна забезпечувати збереження і справжність документів, безпечний доступ і протоколювання дій користувачів в умовах потенційних загроз інформаційній безпеці.

Збереження документів повинна забезпечуватися в період усього часу життєвого циклу документа, а в разі його непередбаченої втрати або псування, СЕД повинна мати можливість його швидкого відновлення[5].

Основним і практично єдиним рішенням забезпечення достовірності документа в даний час є електронно-цифровий підпис. СЕД підтримує два види ЕЦП: візи і затвердження. Віза свідчить про те, що підписант документу ознайомився з ним (завізував його). Затвердження може бути поставлено обмеженим колом осіб в рамках заданих повноважень і свідчить про остаточне затвердження документа. Підпис будь-якого виду, поставлена на версії документа, захищає її від змін.

Безпечний доступ до даних СЕД забезпечується аутентифікацією і розмежуванням прав користувачів. Контроль та налаштування прав доступу до інформації СЕД, (повний доступ, зміну, перегляд, повна відсутність доступу), забезпечує захист від несанкціонованого доступу.

Протоколювання всіх дій користувачів, дозволяє швидко відновити історію роботи з документом і проконтролювати такі дії над документом, як перегляд, зміна, експорт копії документа і інші.

Таким чином, об'єктами захисту інформації в СЕД є:

Апаратне забезпечення - СВТ, сервери, елементи LAN та мережеве обладнання.

Системні файли, файли бази даних при їх обробці.

Електронні документи.

До механізмів захисту інформації в СЕД пред'являються наступні основні функціональні вимоги: висока надійність, підтримка основних комунікаційних стандартів і протоколів, масштабованість, сумісність з усіма підсистемами СЕД, можливість зміни логічної конфігурації СЕД без зміни фізичної, керованість.

СЕД, реалізована на платформі РОМ, як правило, об'єднує офіси, філії та інші структури організації, що знаходяться на відстані один від одного. При цьому вузли РОМ можуть розташовуватися в різних містах країни. Принципи, за якими будується така мережа, відрізняються від тих, що використовуються при створенні LAN[6].

Основна відмінність полягає в тому, що РОМ використовують орендовані лінії зв'язку, орендна плата за використання яких становить значну частину в собівартості всієї мережі і зростає зі збільшенням якості і швидкості передачі даних. Тому організація каналів зв'язку є основним завданням, яке необхідно вирішувати при створенні СЕД на платформі РОМ. Якщо в межах одного міста можлива оренда виділених ліній, в тому числі високошвидкісних, то при переході до географічно віддалених вузлів вартість оренди каналів стає значною, а їх якість і надійність при цьому можуть бути невисокими. При цьому істотно збільшується рівень вразливості СЕД до впливу загроз інформаційної безпеки[7].

Можливим вирішенням завдання організації каналів зв'язку між віддаленими вузлами РОМ СЕД є використання вже існуючих глобальних приватних мереж. В цьому випадку необхідно забезпечити канали від філій організації до найближчих вузлів глобальної приватної мережі. Приватні мережі можуть містити канали зв'язку різних типів: кабельні оптичні та електричні, в тому числі телефонні, бездротові радіо- і супутникові канали, що мають різні пропускні спроможності.

При підключенні філій організації через глобальні приватні мережі віддалені користувачі не відчувають себе ізольованими від інформаційних систем, до яких вони здійснюють доступ, віддалені місця розташування організації можуть здійснювати обмін інформацією негайно, і вся передана інформація залишається в секреті. Однак організація каналів зв'язку через глобальні приватні мережі також може бути дорогою.

Забезпечити багато переваг приватних мереж за меншу вартість дозволяє технологія віртуальних приватних мереж (VPN, VirtualPrivateNetwork). VPN - це логічна приватна мережа, організована поверх публічної мережі, як правило,

мережі Інтернет. Слідуючи тим же функціональним принципам, що і виділені лінії, VPN дозволяє встановити захищене цифрове з'єднання між двома віддаленими місцями розташування (або LAN). При використанні в архітектурі РОМ СЕД публічних мереж, інформаційний обмін між її сегментами здійснюються за допомогою небезпечних протоколів, але за рахунок шифрування створюються закриті інформаційні канали, що забезпечують безпеку переданих даних. У СЕД, реалізовані на платформі РОМ вбудовується підсистема захисту інформації з інтегрованими засобами криптографічного захисту інформації.

Віртуальні приватні мережі дозволяють об'єднати географічно розподілені філії організації в єдину мережу і таким чином забезпечити єдиний адресний простір СЕД, єдину нумерацію телефонного зв'язку, загальну базу даних і т.д. Іншими словами, організовується єдина мережева інфраструктура та інформаційний простір організації, доступ до якого однаково можливий з будь-якої точки РОМ.

СЕД, побудована на основі технології VPN, є фундаментом для впровадження всіх наступних додаткових сервісів, таких як передача голосу по IP, відеоконференц-зв'язок, технічні додатки та сервіси, а також для організації оперативного та конфіденційного зв'язку з усіма філіями організації та значного зменшення обсягу міжміського і міжнародного трафіку за рахунок передачі телефонних дзвінків по каналах РОМ.

Як зазначено вище, апаратну основу будь-якої СЕД становить обчислювальна мережа, що володіє можливостями автономного функціонування або з виходом у зовнішнє інформаційне середовище. У першому випадку в якості такої основи може використовуватися мережа Intranet - обчислювальна мережа з відповідним програмним забезпеченням, що дозволяє користувачам однієї організації обмінюватися інформацією, електронною поштою, документами і спільно їх використовувати.

Мережа Intranet об'єднує в єдину захищену мережу кілька розподілених філій однієї організації і застосовується для побудови СЕД в автономному варіанті. Intranet заснована на додатку технологій Internet для приватних

локальних і глобальних мереж організацій. Сучасне програмне забезпечення для мереж Intranet включає в себе модулі координації спільної роботи і управління документами.

Одночасно, з системами закритого типу, користуватися якими можуть тільки співробітники однієї організації, стали з'являтися мережі Extranet. Extranet призначена для мереж, до яких підключаються користувачі зовнішніх організацій, рівень довіри до яких нижче, ніж до основних користувачам мережі, але взаємодія між організаціями здійснюється в рамках загальної РОМ.

Extranet дозволяє організації користуватися інформацією спільно зі своїми партнерами безпосередньо по самій мережі Internet, що розширює можливості взаємодіючих організацій. Основними функціями Internet залишаються електронна пошта і обмін інформацією між розподіленими документно-орієнтованими системами. Internet служить сполучною ланкою між окремими сегментами РОМ.

СЕД на платформі РОМ забезпечує автоматизацію формування та обробки транзитних електронних документів, які направляються від відправника до одержувача через головний сервер РОМ в «закритому конверті».

Для забезпечення технологічних процесів, пов'язаних з управлінням сертифікатами ключів електронного підпису, в СЕД функціонує Центр управління сертифікатами (ЦУС), який складається з Центру сертифікації (ЦС) і Центру реєстрації. Центр сертифікації забезпечує: формування сертифікатів ключів електронного підпису, формування списку відкликаних сертифікатів (СОС), а також ведення реєстру сертифікатів ключів електронного підпису. Крім сертифікатів ЦС формує і публікує список відкликаних сертифікатів з періодичністю, визначеною регламентом СЕД. При цьому ЦС відповідає за формування політики використання сертифікатів для підлеглих йому центрів.

Центр реєстрації забезпечує взаємодію в СЕД в процесі формування криптографічних ключів і сертифікатів ключів електронного підпису; проводить планову зміну, а при необхідності і заміну криптографічних ключів СЕД; і публікацію сертифікатів ключів електронного підпису, а також СОС в мережевих

довідниках сертифікатів ключів електронного підпису. Для забезпечення функціонування ЦУС в СЕД створюється необхідна технічна інфраструктура, яка дозволяє забезпечити цілодобовий доступ до мережевих довідників сертифікатів.

Таким чином, у захищених СЕД, реалізованих на мережевій технологічній платформі забезпечується як високоефективна інформаційна взаємодія всіх сегментів СЕД, так і високий рівень інформаційної безпеки при роботі з електронними документами.

Існуючі методи і засоби захисту інформації систем електронного документообігу можна розділити на чотири основні групи:

- методи і засоби організаційно-правового захисту інформації;
- методи і засоби інженерно-технічного захисту інформації;
- криптографічні методи і засоби захисту інформації;
- програмно-апаратні методи та засоби захисту інформації.

Методи і засоби організаційно-правового захисту інформації

До методів і засобів організаційної захисту інформації відносяться організаційно-технічні та організаційно-правові заходи, що проводяться в процесі створення і експлуатації СЕД для забезпечення захисту інформації. Ці заходи повинні проводитися при будівництві або ремонті приміщень, в яких буде розміщуватися сервер СЕД; проектуванні системи, монтажі та налагодження її технічних і програмних засобів; випробуваннях і перевірці працездатності СЕД.

На цьому рівні захисту інформації розглядаються міжнародні договори, підзаконні акти держави, державні стандарти і локальні нормативні акти конкретної організації.

Методи і засоби інженерно-технічного захисту.

Під інженерно-технічними засобами захисту інформації розуміють фізичні об'єкти, механічні, електричні та електронні пристрої, елементи конструкції будівель, засоби пожежогасіння та інші засоби, що забезпечують[8]:

- захист території і приміщень, де стоїть СЕД, від проникнення порушників;

- захист апаратних засобів електронногодокументообігута носіїв інформації від розкрадання;

- запобігання можливості віддаленого (з-за меж території, що охороняється) відеоспостереження (підслуховування) за роботою персоналу і функціонуванням технічних засобів електронний документообіг;

- запобігання можливості перехоплення ПЕМВН (побічних електромагнітних випромінювань і наведень), викликаних працюючими технічними засобами комп'ютерної системи і лініями передачі даних;

- контроль над режимом роботи персоналу, який забезпечує роботу СЕД;

- протипожежний захист приміщень СЕД;

- мінімізацію матеріальних збитків від втрат інформації, що виникли в результаті стихійних лих і техногенних аварій.

Криптографічні методи захисту і шифрування

Шифрування є основним засобом забезпечення конфіденційності. Так, у разізабезпеченняконфіденційностіданих на локальному комп'ютерізастосовуютьшифруванняцихданих, а в разімережевоївзаємодії - шифровані канали передачіданих.

Криптографіязастосовується:

- для захистуконфіденційностіінформації, щопередається по відкритих каналах зв'язку;

- для аутентифікації (підтвердженняаутентичності) переданоїінформації;

- для захистуконфіденційноїінформації при їїзберіганні на відкритихносіях;

- для забезпеченняцілісностіінформації (захистінформаціївідвнесеннянесанкціонованихзмін) при їїпередачі по відкритих каналах зв'язкуабо при зберіганні на відкритихносіях;

- для забезпечення незаперечностіпереданої по мережіінформації (запобіганняможливогозаперечення факту відправкиповідомлення);

- для захиступрограмногозабезпечення та іншихінформаційнихресурсіввіднесанкціонованоговикористання і копіювання.

Програмні і програмно-апаратніметоди та засобизабезпеченняінформаційноїбезпеки[9].

До апаратнихзасобівзахистуінформаціїналежатьелектронні та електронно-механічніпристрої, щовключаютьсядо складутехнічнихзасобів СЕД і виконують (самостійноабо в єдиномукомплексі з програмнимизасобами) деякіфункціїзабезпеченняінформаційноїбезпеки. Критеріємвіднесення пристрою до апаратних, а не до інженерно-технічнихзасобівзахисту є обов'язковевключеннядо складутехнічнихзасобів СЕД.

Підпрограмнимизасобамизахистуінформаціїрозуміютьспеціальніпрограми, щовключаютьсядо складупрограмногозабезпечення СЕД виключно для виконаннязахиснихфункцій. До основнихпрограмнихзасобівзахистуінформаціївідносяться:

програмиідентифікації і аутентифікаціїкористувачів СЕД;

програмирозмежування доступу користувачів до ресурсів СЕД;

програмишифруванняінформації;

програмизахистуінформаційнихресурсів (системного і прикладного програмногозабезпечення, баз даних, комп'ютернихзасобівнавчання і т. п.) віднесанкціонованогозміни, використання і копіювання.

Методиідентифікації і аутентифікації

Підідентифікацією, стосовнозабезпеченняінформаційноїбезпеки СЕД, розуміютьоднозначнерозпізнаванняунікальногоіменісуб'єкта СЕД. Аутентифікаціяозначаєпідтвердження того, щопред'явленеім'явідповідаєданомусуб'єкту (підтвердженняавтентичностісуб'єкта).

Системиідентифікації і аутентифікаціїможнаподілитинаступним чином(рис. 1.3).

Останнім часом з'явилася така управлінська функція як бенчмаркінг. Бенчмаркінг є мистецтвом знаходження або виявлення ноу-хау, того, що інші роблять краще за всіх, з подальшим вивченням, удосконаленням і застосуванням

чужих методів роботи. Дослідники та експерти вважають, що бенчмаркінг є необхідною складовою успіху будь-якого підприємства в сучасному світі.

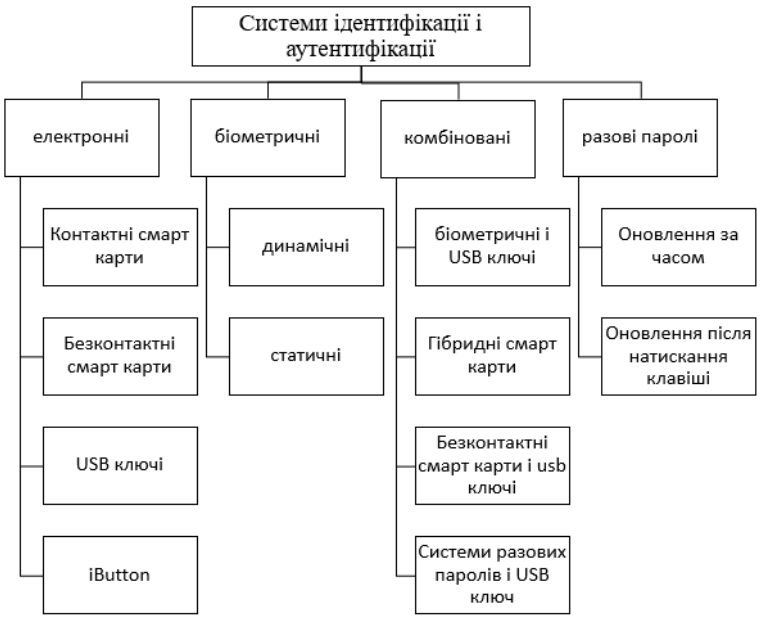


Рис. 1.3Системиідентифікації і аутентифікації

Аутентифікація на основіключів ЕЦП

Аутентифікаціякористувача повинна проводитися при йогодоступі в СЕД на основійогологіна і пароля, а також секретного ключа ЕЦП користувача.

При перевірці ЕЦП користувача СЕД, щопред'являється для йогоаутентифікації, повинніперевірятися:

- відповідністьвідкритого ключа закритому ключу ЕЦП користувача;

- дійсністьсертифікатавідкритого ключа ЕЦП на момент аутентифікації;

- перевірка статусу сертифікатавідкритого ключа ЕЦП в Центріреєстраціїключів ЕЦП.

У разізакінченнятермінудіїсертифікатавідкритого ключа ЕЦП, призупиненняйогодіїабоанулювання в Центріреєстраціїключів ЕЦП, доступ до системикористувача повинен автоматично стати неможливим.

Посиленааутентифікація

Посиленааутентифікація є аутентифікацію з використаннямдодатковихапаратнихзасобів - USB-пристроїв і смарт-карт. Вони являють собою коштипосиленоюдвофакторноїаутентифікації на основіцифровихсертифікатів стандарту X.509. Такі засобизабезпечуютьєдинуреєстраціюкористувача і усуваютьнеобхідністьдодаткової їреєстрації в кожному з використовуванихдодатків.

1.4Шляхи удосконаленняпроцесузахистуінформаціїу системахелектронногодокументообігу

Широкомасштабневикористанняінформаційнихтехнологій в діловодствіпризвело до розробкивідповіднихстандартів на міжнародномурівні. Вимоги до систем управлінняелектронними документами розробляються в основному в інтересахдержавнихорганів, щобвизначитиєдинийпідхід до обміну документами на міжвідомчомурівні.Але в той же час цимивимогамикористуютьсяіншіорганізації, для проведеннясвоїхзакупівель, вибираючи з них потрібніїмположення.

Можнасказати, що в 2007-2008 рр. стали з'являтисявимоги до СЕД третьогопоколінняпочинаючи з третьоїредакціїамериканського стандарту DoD 5015.2. Найбільшпомітноюподією став вихід у світ в лютому 2008 року європейськихвимог MoReq2 (ModelRequirementsforthemanagementofelectronicrecords), розроблених на замовленняЄврокомісії (уряду Євросоюзу).

Новою тенденцією стала появавимог до мінімального набору функціональнихможливостей для управління документами, необхідного для ділових систем (облікових, управління ресурсами і бізнес-процесами і т.п.) - на відмінувідвимог до повномасштабнихспеціалізованим системам для управління документами.

Стандарт DoD 5015.2-STD з'явився в Міністерстві оборони США в 1996 році і був першим в ційгрупістандартів. Йогоуспіх став серйозним стимулом для розробкианалогічних норм в іншихкраїнахсвіту, особливо в Європі.

У 2007 р. з'явиласятретяверсія стандарту. Стандарт доповненийдвомарозділами, присвяченимивимогам до тих функціональнимиможливостями систем управління документами, якінеобхідні для виконаннядержавнимиорганами положеньзаконів про захистперсональнихданих і доступу до державноїінформації. Це, в першучергу, дало наступнеможливості:

- виділятидокументи, щомістятьперсональнідані і абопідлягаютьрозкриттюзгідноіз законом про свободу доступу до державноїінформації;
- реєструватизапитигромадянщодосвоїхперсональнихданих, а такожзапитигромадян і організацій про доступ до державноїінформації; формувативідповідніелектроннідосьє, щомістятьдокументи, створювані в ходівідпрацюванняцихзапитів;
- управлятидокументацією з питаньрозкриттяперсональної та державноїінформації;
- збиратинеобхідністатистичнідані та формувативідповіднізвіти;
- підтримуватистворенняцензурованихверсійрозкриваютьсядокументів та їхзберігання в зв'язці з оригінальними документами.

Стандарт, крім того, включаєтеперрозділ з вимогамищодозабезпеченнявзаємодіїміж СЕД при передачіелектроннихдокументів з однієїсистеми в іншу. Суттєводоопрацьовано і доповненорозділ про управлінняелектроннимисекретними документами, а такожінформацією, щомістить відомості, віднесені до державноїтаємниці.

Специфікації MoReq2.

MoReq2 - це друга версіяТиповихвимог (ModelRequirements, MoReq), яка є європейським стандартом для систем, керуючихелектронними документами.

MoReq2 вже зараз вельми впливовий в областіуправлінняелектронними документами, і цейвплив, як очікується, в майбутньому буде тількизростати. Причини цьогокриються в наступному:

- вінпризначений для всіхсекторів, а не тільки для державнихорганів;

- цеміжнародний стандарт, використовуваний у всійЄвропі, а також в Азії, ПівнічнійіПівденнійАмериці;

- віноописуєфункціональніможливості, щовиходять далеко за межівласнеуправління документами;

- в ходійогорозробкибулоорганізовановеличезна за масштабами міжнароднеобговорення проекту фахівцями з багатьохкраїнсвіту.

У стандартіпереробленіі доповненітірозділи, якіостаннім часом набулинайбільшогозначення.
Доданічіткосформульованівимогищодоновихважливихаспектіврозробки і застосування СЕД. Вимогирозділені на модулі, з тим, щобполегшитивикористаннястандартів. Забезпеченопроверяемостьвимог, розробленінеобхіднідокументи і матеріали, щодозволяютьпроводититестування систем управління документами на відповідністьвимогам MoReq2.

NOARK-5

НаціональнівимогиНорвегії до управліннєлектронними документами і їхархівації. Незважаючи на успіхєвропейського стандарту MoReq / MoReq2 ряд європейськихкраїнрозробляєсвоїнаціональнівимоги до СЕД і регулярно їхоновлює. Найчастішецепов'язано з тим, що в данихкраїнах є особливості в галузіуправління документами, якінеобхідноврахувати при розробці СЕД. Прикладом є Норвегія, яка продовжуєрозвивативласний стандарт NOARK.

У 2008 р НаціональніАрхівиНорвегіїопублікувалиновуредакціювимог до управління і архівації їелектроннихдокументів NOARK-5, яка замінитьзастосовувавсяраніше стандарт NOARK-4.

NOARK-5 повинен використовуватися у всіхархівних органах, незалежновідїх типу і використовуваноготехнологічногорішення. Рішення, щозабезпечуєформуванняархівів, маєохоплюативсівидидіяльності, в

ходіякихстворюютьсядокументи, якінеобхіднозберегти в автентичномувигляді. Вимоги NOARK-5 не залежатьвід того, відноситьсяорганізація до державного або приватного сектору, обробляютьсячидокументитрадиційним чином, якийїхнійтермінзберігання і чибудуть вони передаватися на архівнезберігання.

Комплект документів (в норвезькійверсії) включає:

Власневимоги NOARK-5: Стандарт електронноїархівації, версія 1.2 від 17 жовтня 2008 року (Standardforelektroniskarkiv);

Додаток 1: Каталог метаданих;

Додаток 2: Метадані, згруповані за їхпризначенням;

Додаток 3: XML-схема для використання при передачідокументів.

Стандарт розроблений з позиційцілісногопідходу до архівногозберіганнядокументів в електронномусередовищі. Основнаувагабулаприділенарозробцівимог, націлених на те, щобстворюванірішеннязабезпечувалиналежнеуправлінняелектронними документами і архівами[10].

У NOARK-5 передбачені три рівнявимог: ключовівимоги(«ядро»), розширення «ядра» і вимоги до повномасштабнихреалізацій NOARK-5. Рішення, засновані на «ядрі» NOARK-5, використовуються для забезпеченняналежноїреєстраціїдокументів, і вони можутьтакожвикористовуватися для управлінняелектронними документами в організаціях приватного сектора Норвегії. NOARK-5 замінює 4-ю версіюстандартів, при цьомупередбачена «зворотнасумісність» з NOARK-4, тобтоможливаміграціядокументів з систем, заснованих на ранішедіючомустандарті, в новісистеми. Цевраховано при розробці як структуриелектронногоархіву, так і метаданих. Системи, яківикористовуються для прийомудержавнихдокументів в електронномувигляді, повиннівідповідативідповіднимвимогам NOARK-5 і повинні бути схвалені для цієї мети керівникомархівноїслужбикраїни.

Висновок до першого розділу

В результатідослідженнярозглянуто нормативно-правовіпідставиведенняділоводства та електронногодокументообігу в Україні. В ходідослідженнявизначилося, що нормативно-правове база по данійгалузірозвиваєтьсяпоетапно. Були проаналізованіпереваги і недоліки систем електронногодокументообігу. Вивченозагрозиінформації в системах електронногодокументообігу.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ У СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

2.1 Політика безпеки інформації у системах електронного документообігу

Загальнийпідхід до побудовиполітикибезпекисистемиелектронногодокументообігуможнасформулювативиходячи з вимог стандарту ISO/IEC 17799 [11].

Для захистуелектронногодокументообігувартозастосовувати (за необхідностю) спеціальнізасобиуправліннябезпекою, оскільки ЕДО з партнерами уразливийстосовнонесанкціонованогоперехоплення й модифікаціїінформації. Крім того можливо буде потрібнопідтвердженняпередачіабоодержанняданих. Необхіднотакожподбати про захистпідключених до мережікомп'ютерних систем відзагроз, яківиходятьвіделектронногопідключення.

Засобиуправліннябезпекоюоперацій по ЕДО повинні бути погоджені з партнерами й постачальникамидодатковихмережнихпослуг. Для забезпеченнясумісностіізпромисловими стандартами, необхіднопроконсультуватися з фахівцями з відповідноїасоціації з ЕОД.

Для забезпеченняконфіденційностіданих, щопотребують особливого захисту, необхіднорозглянутиможливістьїхньогошифрування. *Шифрування* - цепроцесперетворенняінформації в зашифрований текст для забезпеченняїїконфіденційності й цілісностіпід час передачіабо при зберіганні. У цьомупроцесівикористовується алгоритм шифрування й інформація про секретний ключ, щовідоматількизареєстрованимкористувачам. Рівеньзахищеності, забезпечуванийпроцесомшифрування, залежитьвідякості алгоритму й таємності ключа.

Шифруванняможезнадобитися для захистуконфіденційноїінформації, щоуразливастосовнонесанкціонованого доступу, як під час їїпередачі, так і при зберіганні. Для визначеннянеобхідностішифруванняданих і

необхідногорівнязахищеностінеобхідно провести оцінкуризикупорушення режиму безпеки. Щобвибратипідходящіпрограмніпродукти з належнимрівнемзахисту й розробитинадійну систему управління ключами, вартозвернутися за порадою до фахівців.

Прикладом пристрій «Оникс 200» зображено на рис.2.1 призначендля шифруванняданих, переданих повідкритих каналах зв'язкумережзагальногокористуванняміжлокальнимифрагментамикорпоративноїIP-мережі.

Апаратвключаєтьсяврозривзіз'єднаннямультиплексногообладнаннялокальноїі глобальноїмереж. В якостіглобальноїмережіможевиступатимережу Інтернет.

Реалізаціякриптографічного алгоритму- відповідно доДСТУГОСТ28147:2009врежимігамуванняіззворотнимзв'язком. Максимальнийгрифзахищаєтьсяінформації-«для службовогокористування».Ключова система - «симетричного» типу

Довжинадовготривалогоключовогоелемента -512біт.

Довжина сеансового ключа - 256 біт.

Пропускна здатність - до 94 Мбіт/с.

Мережевий інтерфейс - LAN - Ethernet 100 Base-FX типу SC;

WAN - Ethernet 10/100 Base-TX типу RG-45.

Введення в пристрій ключової інформації здійснюється за допомогою модуля ключових даних (МКД). Доставка МКД здійснюється фізично, що з точки зору збереження ключової інформації безпечніше. Максимальний період фізичної доставки ключових даних становить 1 рік.

Структура шифратора забезпечує 96% дублювання функцій шифрування і контролю. При включенні «Онікс-200» виконує систему тестів(рис.2.1). У процесі роботи проводиться тестування трактів зашифрування розшифрування. Вжиті всі заходи для виключення неправильної роботи шифраторів. Безпека підтримується системою контролю і знищення критичної інформації, як по команді оператора, так і при виявленні несанкціонованого доступу до виробу.

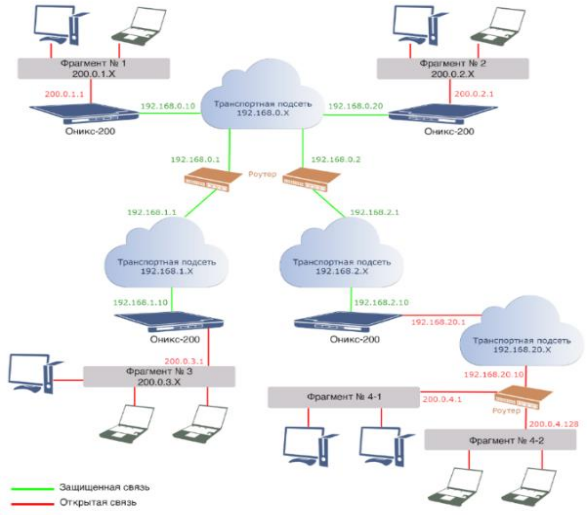


Рис 2.1 Приклад використання СЕД«Онікс-200»

Автентифікаціяповідомлень - це метод, використовуваний для виявленнянесанкціонованихзмін, внесених у переданіелектронніповідомлення, абоїхньогоушкодження. Йогоможнареалізувати на апаратномуабопрограмномурівні за допомогоюфізичного пристрою автентифікаціїповідомленьабопрограмного алгоритму.

Можливістьавтентифікаціїповідомленьварторозглянути для тих додатків, для якихжиттєвоважливимєзабезпеченняцілісностіповідомлень, наприклад, електронніпередачіінформації про коштиабоіншіелектронніобміниданими. Для визначеннянеобхідностіавтентифікаціїповідомлень і виборунайбільшприйнятого методу їїреалізаціїнеобхідно провести оцінкуризикупорушення режиму безпеки.

Автентифікаціяповідомлень не призначена для захистузміступовідомленьвідперехоплення. Для цихцілейпідходитьшифруванняданих, якихможнатакожвикористати для автентифікаціїповідомлень.

Електроннийпідпис - цеспеціальний вид автентифікаціїповідомлень, звичайнозаснований на методах шифрування з відкритимключем, щозабезпечуєавтентифікаціювідправника, а такожгарантуєцілісністьумісту повідомлення.

Модель забезпечення цілісності Кларка-Вільсона, як основа політики безпеки електронного документообігу

Модель Кларка-Вільсона з'явилася у результаті проведеного авторами аналізу практичних методів забезпечення цілісності документообігу в комерційних компаніях [3]. На відміну від моделей Байба та Белла-Ла Падули, вона орієнтована на потреби комерційних замовників, і, за думкою авторів, є більш адекватною до їх вимог, ніж комерційна модель цілісності на основі решіток. Суть даної моделі — це коректність транзакцій та розмежування функціональних обов'язків. Модель задає правила функціонування комп'ютерної системи та визначає дві категорії об'єктів даних та два класи операцій над ними.

Усі дані, що містяться у системі, поділяються на контрольовані та неконтрольовані елементи даних (constraineddataitemsCDI і unconstraineddataitems — UDI відповідно). Останні містять інформацію, цілісність якої в рамках даної моделі не контролюється (цим і визначається вибір технології).

У подальшому модель вводить два класи операцій над елементами даних: процедури контролю цілісності (integrityverificationprocedures — IVP) і процедури перетворення (transformationprocedures — TP). Перші з них забезпечують перевірку цілісності контрольованих елементів даних (CDI), інші змінюють склад множини усіх CDI (наприклад, перетворюючи елементи UDI в CDI).

Нарешті, модель містить дев'ять правил, що визначають взаємодії елементів даних та процедур у процесі функціонування системи.

Правило C1. Множина усіх процедур контролю цілісності (IVP) повинна містити процедури контролю цілісності будь-якого елемента даних з множини усіх CDI.

Правило C2. Усі процедури перетворення (TP) повинні бути реалізованими коректно у тому сенсі, що не повинні порушувати цілісності CDI, що оброблюється ними. Крім того, с кожною процедурою перетворення повинен бути зв'язаний список елементів CDI, які допустимо оброблювати даною процедурою. Такий зв'язок установлюється адміністратором безпеки.

Правило E1 .Система повинна контролювати допустимість застосування ТР до елементів CDI відповідно до списків, що вказані у правилі С2.

Правило E2. Система повинна підтримувати список процедур перетворення, дозволених конкретним користувачам, із зазначенням допустимого для кожного ТР і даного користувача набору елементів CDI, що підлягають обробці.

*Правило C3.*Список, визначений правилом С2, повинен від повідати вимозі розмежування функціональних обов'язків.

*Правило E3.*Система повинна автентифікувати усіх користувачів, що пробують виконати будь-яку процедуру перетворення.

Правило C4. Кожна ТР повинна записувати в журнал реєстрації інформацію, достатню для відновлення повної картини кожного застосування цієї ТР. Журнал реєстрації — це спеціальний елемент CDI, призначений для додавання до нього інформації.

Правило C5. Будь-яка ТР, що обробляє елемент UDI, повинна виконувати тільки коректні перетворення цього елементу, у результаті яких UDI перетворюється в CDI.

Правило E4. Тільки спеціальна уповноважена особа може змінити списки, визначені у правила С2 і Е2. Ця особа не має права виконувати будь-які дії, якщо вона уповноважена змінювати списки, що регламентують ці дії.

Роль кожного з дев'яти правил моделі Кларка-Вільсона у забезпеченні цілісності інформації можна пояснити, якщо показати яким з теоретичних принципів політики контролю цілісності відповідає дане правило.

Звичайно для моделі Кларка-Вільсона вибирають перші шість з дев'яти абстрактних теоретичних принципів [3]:

коректність транзакцій;

автентифікація користувачів;

мінімізація привілеїв;

розмежування функціональних обов'язків;

аудит подій, що відбулися;

об'єктивний контроль;

управління передачею привілеїв;

забезпечення неперервної працездатності;

простота використання захисних механізмів.

Для кращого розуміння правил моделі розкрию дані принципи.

Поняття *коректності транзакцій* звичайно визначається наступним чином. Користувач не повинен модифікувати дані довільно, а тільки визначеними способами, так, щоб зберігалася цілісність даних. Іншими словами, дані можна змінювати тільки шляхом коректних транзакцій і не можна довільними засобами. Крім того, передбачається, "коректність" (у звичайному сенсі) кожної з таких транзакцій може бути певним чином доведеною. Принцип коректних транзакцій за своєю суттю відбиває основну ідею визначення цілісності даних, що ні одному користувачеві системи, у тому числі авторизованому, не повинні бути дозволеними такі зміни даних, які спричинять їх руйнування або втрату.

Другий принцип говорить, що зміни даних може здійснювати користувач, якого спеціально автентифіковують для цього. Цей принцип працює разом з наступними чотирма, з якими тісно зв'язана його роль у загальній схемі забезпечення цілісності.

Ідея мінімізації *привілеїв* з'явилася ще на ранніх етапах розвитку напрямку комп'ютерної безпеки у формі обмеження, що накладаються на можливості процесів, що виконуються в системі і припускають, що процеси повинні бути наділеними тими і тільки тими привілеями для виконання процесів. Практикам адміністрування операційної системи UNIX це положення знайоме на прикладі використання облікового запису, що має необмежені повноваження. Принцип, відповідно до якого слід мінімізувати привілеї, що призначаються, у суворій відповідності із змістом завдання, що виконується, розповсюджується в рівній мірі як на процеси (працюючі в системі програми), так і на користувачів системи.

*Розмежування функціональних обов'язків*припускає організацію роботи з даними таким чином, що у кожній з ключових стадій, які складають єдиний критично важливий з точки зору цілісності процес, необхідна участь

різноманітних користувачів. Цим гарантується, що один користувач не може виконувати весь процес цілком (або навіть дві його стадії) з тим, щоб порушити цілісність даних. У звичайному випадку прикладом втілення даного принципу служить передача однієї половини паролю для доступу до програми управління ядерним реактором першому системному адміністратору, а другий — другому.

Як відзначалося вище, принцип мінімізації привілеїв розповсюджується і на програми, і на користувачів. Проте, на практиці важко визначити "теоретично досяжний" мінімальний рівень привілеїв за двома причинами. По-перше, користувачі виконують різноманітні завдання, які потребують різних привілеїв. По-друге, якщо суворе дотримання принципу мінімізації у відношенні процесів зв'язане з міркуваннями щодо вартості та продуктивності, то у відношенні користувачів воно скоріше, зачіпає питання етики та моралі, а також зручності та ефективності роботи — це фактори, які не піддаються точній кількісній оцінці. Тому користувачі будуть, як правило, мати дещо більше привілеїв, ніж їх необхідно для виконання конкретної дії на даний момент часу. А це відкриває можливості для зловживань.

Принцип об'єктивного контролю також є одним з каменів політики контролю цілісності. Суть даного принципу полягає утому, що контроль цілісності даних має сенс лише тоді, коли ці дані відображають реальне положення речей. Очевидно, що нема сенсу турбуватися про цілісних даних, з розташуванням бойового арсеналу, який уже відправлений на переплавку. У зв'язку з цим Кларк та Вільсон указують на необхідність регулярних перевірок, метою яких є виявлення можливих невідповідностей між даними, що захищаються, та об'єктивною реальністю, яку вони відображають.

Управління передачею привілеїв необхідне для ефективної роботи усієї політики безпеки. Якщо схема призначення привілеїв неадекватно відображає організаційну структуру підприємства або не дозволяє адміністраторам гнучко маніпулювати нею для забезпечення ефективності виробничої діяльності, захист стає важким тягарем та провокує спроби обійти її там, де вона заважає "нормальній" роботі.

З деякими застереженнями іноді в основу контролю цілісності закладається принцип забезпечення безперервної роботи (включаючи захист від збоїв, стихійних лих та інших форс мажорних обставин), який у класичній теорії комп'ютерної безпеки відноситься, скоріше, до проблеми доступності даних.

В основу дев'ятого принципу контролю цілісності — простота використання захисних механізмів — закладений ряд ідей, призваних забезпечити ефективне застосування наявних механізмів забезпечення цілісності. На практиці часто виявляється, що передбачені в системі механізми безпеки некоректно використовуються або повністю ігноруються системними адміністраторами за наступних причин:

- неправильно вибрані виробниками конфігураційні параметри за умовчанням забезпечують слабкий захист;

- погано розроблені інтерфейси управління захистом ускладнюють використання навіть простих засобів захисту;

- наявні засоби безпеки не забезпечують адекватний рівень контролю за системою;

- реалізація механізмів безпеки погано відповідає їх інтуїтивному розумінню, що склалося у адміністраторів;

- окремі засоби захисту погано інтегровані в загальну схему безпеки;

- адміністратори недостатньо поінформовані про важливість застосування конкретних механізмів захисту та їх особливостях.

Простота використання механізмів захисту припускає, що найбільш безпечний шлях експлуатації системи буде також найбільш простим, і навпаки, найбільш простий — найбільш захищеним.

Відповідність правил моделі Кларка-Вільсона до перелічених принципів показані у таблиці 2.1. Як видно із таблиці принципи 1 (коректність транзакцій) і 4 (розмежування функціональних обов'язків) реалізуються більшістю правил, що відповідають основній ідеї моделі.

Публікація опису моделі Кларка-Вільсона викликала широкий відгук серед дослідників, що займаються проблемою контролю цілісності. У ряді робіт

розглядаються практичні аспекти застосування моделі, запропоновані деякі її розширення та способи інтеграції з іншими моделями безпеки.

Таблиця 2.1

Відповідність правил моделі Кларка-Вільсона до принципів політики контролю цілісності

Правило моделі Кларка-Вільсона	Принципи політики контролю цілісності, що реалізуються правилом
Правило C1	Коректність транзакцій
	Об'єктивний контроль
Правило C2	Коректність транзакцій
Правило E1	Мінімізація привілеїв
	Розмежування функціональних обов'язків
Правило E2	Коректність транзакцій
	Автентифікація користувачів
	Мінімізація привілеїв
	Розмежування функціональних обов'язків
Правило C3	Розмежування функціональних обов'язків
Правило E3	Автентифікація користувачів
Правило C4	Аудит подій, що відбулися
Правило C5	Коректність транзакцій
Правило E4	Розмежування функціональних обов'язків

Менеджер безпеки повинен управляти списками контролю доступу до сховища, папкам з файлами, документам, їхнім версіям, системним даним, внесеним на згадку критеріям пошуку, варіантам дизайну, а також до протоколів роботи користувачів, їхніх груп і системи клієнт/сервер [12]. Він також контролює створення, та каталогізацію звітів по протоколах безпеки роботи користувачів й серверної платформ.

Процеси управління списками контролю доступу

Процеси управління списками контролю доступу виконують функції по забезпеченню безпеки роботи додатків СЕД. Безпека всіх об'єктів, якими управляє система, контролюється за допомогою цих функцій. На рис. 2.2. наведена схема, що ілюструє процеси управління списками контролю доступу.

Забезпечення безпеки сховища. Процес забезпечення безпеки сховища запускає системний адміністратор. У ході процесу ведеться загальний контроль доступу окремих користувачів й їхніх груп до сховища[12].

Забезпечення безпеки папок з файлами. Адміністратор записів запускає процес забезпечення безпеки папок з файлами для здійснення загального контролю доступу до них користувачів і груп. Користувацький доступ може бути встановлений на рівні *Дозволене читання* або *Доступ заборонений*, у той час як для адміністратора записів можуть установлюватися значення *Дозволене читання, Дозволена запис, Дозволене редагування* або *Доступ заборонений*. У питаннях допуску діє принцип наслідування. Наприклад, якщо доступ до папки дозволений тільки певній групі користувачів, то й доступ до всіх документів, розміщеним у цій папці, мають тільки користувачі із зазначеної групи, якщо інше не обговорено на рівні захисту конкретного документа.

Адміністратор записів запускає процес забезпечення безпеки документа для здійсненнязагального контролю доступу до нього користувачів і груп. Користувацький або груповий доступ може бути встановлений на рівні Дозволене читання, Дозволений запис, Дозволене редагування або Доступ заборонений. У цьому випадку принцип спадкування не має зворотної дії. Наприклад, користувачеві може бути дозволений доступ до документа, але не до папки, що містить цей документ. Таку можливість важливо передбачити на той випадок, якщо користувачеві буде потрібно той або інший документ, і при цьому його не буде цікавити місце розташування цього документа в системі класифікації файлів.

Забезпечення безпеки документа.

Забезпечення безпеки версії документа. Кінцевий користувач або адміністратор записів запускає процес забезпечення безпеки версії документа для здійснення загального контролю доступу до неї користувачів і груп.

Користувацький або груповий доступ може бути встановлений на рівні Д*озволене читання, Дозволений запис,* Д*озволені редагування* або *Доступ заборонений*. Певним користувачам може бути наданий доступ до всім розміщеним у комп'ютерній мережі версіям на рівні *Дозволене читання, запис і редагування*(наприклад, фахівці з аналізу політики фірми мають допуск до всіх версій відповідних документів), а інші мають допуск тільки до останніх версій документів на рівні *Дозволене тільки читання*.

*Забезпечення безпеки системної інформації.*Кінцевий користувач або адміністратор записів запускає процес забезпечення безпеки системної інформації для здійснення загального контролю доступу до неї користувачів і груп. Користуцький або груповий доступ може бути встановлений на рівні *Дозволене читання, Дозволений запис, Дозволене редагування* або *Доступ заборонений*. Таку можливість важливо передбачити в організаціях, що працюють за принципом “знання по необхідності”, відповідно до якого користувачі можуть упевнитися в існуванні певного документа, виходячи із системних відомостей про нього, але для того, щоб побачити сам документ, вони повинні одержати відповідний дозвіл від автора.

Забезпечення безпеки індивідуальних параметрів пошуку. Кінцевий користувач або адміністратор записів запускає процес забезпечення безпеки індивідуальних параметрів пошуку для здійснення загального контролю доступу користувачів і груп до внесеного на згадку системи для повторного використання критеріям пошуку. Доступ користувача або груповий доступ може бути встановлений на рівні *Дозволене читання*, *Дозволений запис, Дозволене редагування* або *Доступ заборонений*. Таку можливість варто передбачити в системах, що дозволяють користувачам створювати й запам'ятовувати власні шаблони пошуку, а також передбачають можливість багаторазового використання загальних шаблонів поруч користувачів.Крім того, таким чином, забезпечується контроль за повноваженнями редагувати або видаляти індивідуальні параметри пошуку.

*Забезпечення безпеки варіанта дизайну.*Кінцевий користувач або адміністратор записів запускає процес забезпечення безпеки варіанта дизайну для здійснення загального контролю доступу користувачів і груп до розташування

системної інформації. Доступ користувача або груповий доступ до версії дизайну може бути встановлений на рівні *Дозволене читання, Дозволений запис, Дозволене редагування* або *Доступ заборонений*. Таку можливість варто передбачити в системах, що дозволяють користувачам створювати й запам'ятовувати власні варіанти дизайну, а також передбачають можливість допуску користувачів до загальних версій подання.Крім того, у такий спосіб забезпечується контроль за повноваженнями редагувати або видаляти варіанти дизайну.

*Забезпечення безпеки на рівні груп.*Системний адміністратор запускає процес забезпечення безпеки на рівні груп, щоб ідентифікувати певних членів групи. Члени групи — це користувачі з однаковими обмеженнями на рівень доступу до функцій пошуку документів, системних даних, варіантів дизайну й так далі. Всім членам групи привласнюється найвищий рівень допуску, установлений для групи. Наприклад, якщо користувач Петренко має доступ до документа на рівні *Дозволено тільки читання*, і при цьому він входить до складу групи, який *Дозволене читання й запис*, то Петренку також буде привласнене право *Запису*, як члену відповідної групи.

Забезпечення безпеки на рівні користувача.Системний адміністратор запускає процес забезпечення безпеки на рівні користувача, щоб установити атрибути рівня доступу для конкретного користувача або адміністратора. У цьому випадку доступ користувача до документів, системним даних, варіантам дизайну й так далі контролюється в індивідуальному порядку. Змінна контролю доступу може, як правило, приймати наступні значення: *Доступ заборонений, Дозволене читання, читання/запис, запис, редагування й видалення*.

*Складання звіту про безпеку об'єктів.*Системний адміністратор запускає процес складання звіту про безпеку об'єктів, щоб підсумувати й скласти загальний огляд списків контролю доступу й станів об'єктів СЕД. У число об'єктів входять: сховища, папки з файлами, документи, їхні версії, системна інформація, шаблони пошуку, варіанти дизайну й безпека на рівні груп й окремих користувачів. Як правило, для виконання цієї функції в системі передбачений убудований генератор звітів. У противному випадку

можна здійснити запит бази даних, де зберігається інформація, за допомогою окремої програми.

Процеси забезпечення безпеки протоколів роботи

Процеси забезпечення безпеки протоколів роботи (див. рис. 2.3) відповідають за протоколювання подій, що відбуваються в користувацькому або серверному середовищі. Ця функція може бути успадкована від компонентів середовища СЕД. У противному випадку, “поверх” відповідних додатків може бути встановлена окрема програма, наприклад, монітор контролю взаємодії, що буде протоколювати всі здійснювані в рамках системи дії й відправляти їх у базу даних, де їх зможуть переглянути співробітники групи безпеки.

Забезпечення безпеки протоколу роботи користувача. Системний адміністратор запускає процес забезпечення безпеки протоколу роботи користувача, щоб обмежити доступ до протоколу дій, що виконувалися в середовищі користувача. Протоколи роботи користувача повинні записуватися у форматі, відмінному від ASCII. І необхідно виключити можливість перегляду протоколів для кінцевих користувачів, щоб звести до мінімуму кількість людей, обізнаних про дії й події, інформацію про які можна несумлінно використати.

Складання звіту про безпеку протоколу роботи користувача. Системний адміністратор запускає процес складання звіту про безпеку протоколу роботи користувача, щоб підсумувати й скласти загальний огляд протоколів дій, що здійснювалися в користувацькому середовищі. Для перегляду інформації має бути досить монітора контролю взаємодії або вбудованого генератора звітів. Проте, іноді виникають ситуації, коли групі забезпечення безпеки може знадобитися переглянути повний список операцій, що виконувалися, щоб у точності відтворити послідовність екранів програми або дій, що виконувалися на комп'ютері кінцевого користувача.

Забезпечення безпеки протоколу роботи сервера. Системний адміністратор запускає процес забезпечення безпеки протоколу роботи сервера, щоб обмежити доступ до протоколу дій, що виконувалися в серверному

середовищі. Така можливість повинна бути надана тільки дуже обмеженій групі адміністраторів систем безпеки.

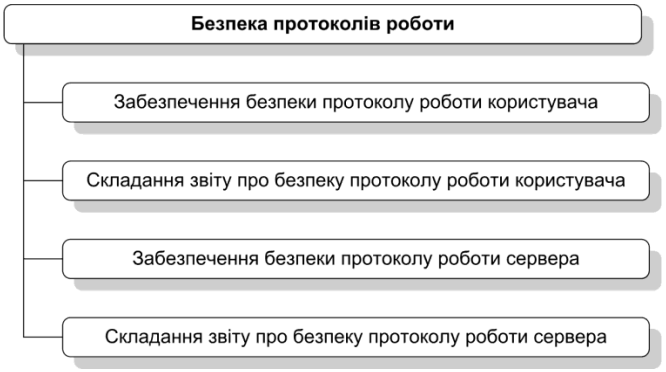


Рис. 2.2 Процеси забезпечення безпеки протоколів роботи.

Складання звіту про безпеку протоколу роботи сервера. Системний адміністратор запускає процес складання звіту про безпеку протоколу роботи сервера, щоб підсумувати й скласти загальний огляд протоколів дій, що здійснювалися в серверному середовищі. Як й у випадку з протоколами, користувачів для перегляду інформації повинне бути досить монітора контролю взаємодії або вбудованого генератора звітів.

Основні правила безпеки системи електронного документообігу

СЕД повинна бути захищена від зловживань і від проникнення в систему не авторизованих користувачів, і при цьому міри безпеки не повинні перешкоджати виконанню користувачами своїх обов'язків. У деяких системах процедура підключення клієнта до мережі дуже поверхнева, і кінцевий користувач може легко змінити параметри цієї процедури.З погляду забезпечення безпеки такі системи не представляються досить потужними. У деяких випадках на серверах спостерігається прямо протилежна ситуація - міри безпеки настільки строгі, що в результаті утворюються затори в роботі. Раціонально організована процедура входу в систему й складання звітності (або, принаймні, використання програмних “гачків” за допомогою інтерфейсу API) дозволить підприємству запустити різні стандартні програми, що задовольняють потреби даної конкретної фірми.

У СЕД повинна бути передбачена можливість простежування історії будь-якого документа. Кожен компонент сховища СЕД, у якому розміщаються інші об'єкти, повинен мати протокол у якому вказується, хто саме одержував доступ

до об'єктів і редагував їх. Така система забезпечує можливість проконтролювати кожен об'єкт і визначити співробітника, що останнім переглядав і редагував документ.

Контроль доступу - це першочергове завдання систем управління документацією. За нею треба ще один важливий момент - організація системи перевірки повноважень осіб, що володіють певними правами. Необхідно контролювати доступ до всіх баз - баз документів, баз даних і текстових баз. Всі вони повинні підпорядковуватися єдиному механізму контролю доступу; у противному випадку співробітник, що має доступ тільки до комп'ютерної мережі, може би обійти системи захисту додатків і без обмежень скористатися пошуковим механізмом бази даних. Таким чином, з'явилася б можливість визначити, чи існує документ і скориставшись його ідентифікатором, одержати його з якої-небудь іншої області комп'ютерної мережі.

Можливості контролю доступу зростають, якщо самі документи зберігаються в системі окремо від бази даних їхніх системних описів. Такий варіант поділу системних функцій представляється дуже зручним, оскільки в деяких випадках організація надає користувачеві право запитувати базу даних за системною інформацією, але не відкриває доступу до самих документів. Якщо документи й системні описи зберігаються в одній базі даних, зростає ймовірність порушення встановлених правил. Якщо людина вийшла на базу даних, то, най імовірніше, вона зуміє добратися й до документів.

Система контролю доступу на рівні приміщень (ієрархічних щаблів, що відповідають кімнаті, шафі, ящику, папці й документу) установлює обмеження на список осіб, що мають право переглядати документ, вносити в нього зміни або видаляти його. Контроль доступу певних співробітників або їхніх груп повинен бути обмежений за допомогою визначення прав групи на перегляд і створення документів. Необхідно знайти спосіб звіряти паролі при вході користувача в систему. У загальному випадку існує два способи здійснити таку перевірку: перший - задати окремий пароль для додатка, другий - дозволити доступ до додатка

всім користувачам, які вже підключилися до мережі, не змушуючи їх одержувати для цього авторизацію другий раз.

Можна також установити систему контролю доступу до окремих функцій програмного забезпечення (таким як перегляд, друк, копіювання, встановлення й зняття обмежень на доступ, видалення й так далі). Різним користувачам можна надати різний рівень доступу.

Система моніторингу відповідає не тільки за контроль доступу; вона також може стежити за повсякденними операціями в рамках СЕД, щоб запобігти несанкціонованим діям. Система може контролювати важливі зміни, які вносяться в процесі експлуатації СЕД користувачем або адміністратором, і вчасно попередити групу забезпечення безпеки, якщо нормальний плин тієї або іншої процедури було порушено. Наприклад, якщо документи в системі видаляються після певної кількості переглядів, співробітник може забрати зі сховища й повернути назад документ 40 разів, щоб одержати можливість знищити оригінал документа, у якому втримується інформація про неправомірні дії цієї людини - і в результаті первісний документ разом зі свідченнями, що втримувалися в ньому, зникне.

Останній елемент, що обов'язково повинен бути присутнім у системі безпеки - функція перевірки вірогідності електронного підпису співробітника на документі й незмінності цього підпису з моменту створення оригіналу документа. Як правило, це робиться за допомогою установки взаємозв'язку електронного підпису з оригіналом документа з використанням певних математичних методів. Якщо відбувається розрив зв'язку, автоматично встановлюється попереджуючий знак, що говорить про те, що документ підроблений.

2.2Засобизахистусистемиелектронногодокументообігу

Для захисту СЕД використаються традиційні засоби:

- ідентифікація, автентифікація й авторизація об'єктів і суб'єктів (так, до питань авторизації в СЕД ставляться механізми розмежування доступу до

даних і функцій системи — це, наприклад, наявність можливості в керівника відділу переглядати всі документи, над якими працюють співробітники відділу, у той час як кожен співробітник бачить лише свою частину роботи й не бачить документи, над якими працюють інші; кожний з документів може мати встановлені для нього права доступу на читання, зміну, видалення; корисно виділяти групи користувачів і делегувати права їхнього доступу до документів);

- управління доступом (дозволяє визначати для кожного документа й для кожної ПП правочинних користувачів й їхнього права);

- засоби контролю імпортованих програм;

- криптографія;

- електронний цифровий підпис.

Розглянемо ці засоби стосовно до захисту від різних загроз.

Захист ЕДО від загроз конфіденційності здійснюється за допомогою стеганографії й криптографії. Стеганографія займається проблемою приховання від зловмисника самого факту передачі повідомлення. Найчастіше це досягається за рахунок введення в повідомлення додаткових бітів, що не псує якості зображення. Виявити заховане в такий спосіб повідомлення малого обсягу увеликому обсязі інформації, не знаючи методу приховання й не маючи “чистого” варіанта файлу, досить складно. Загальний недолік стеганографічних методів захисту інформації — проблема збереження втаємниці самого методу приховування.

Криптографія має на меті приховання тексту повідомлення, роблячи його недоступнім для неавторизованих користувачів. При цьому допускається, що зловмисник знає не тільки сам факт передачі повідомлення, але й саме повідомлення, можливо, його приблизний чи навіть точний текст. Допускається знання супротивником методу шифрування. У таємниці від зловмисника повинен залишатися тільки секретний параметр шифрування — ключ.

Для СЕД найчастіше застосовується два підходи[12].

Абонентське шифрування конфіденційної інформації — шифрування переданих між абонентами ІТС електронних документів. Використовується схема

абонентського шифрування із закритим розподілом ключів шифрування між абонентами, на базі повної матриці ключів (кожній парі абонентів системи відповідає свій секретний ключ для передачі шифрованих документів між ними). Достоїнство цього методу в тім, що алгоритм шифрування забезпечує доступ до переданої інформації тільки тим особам, для яких дана інформація призначена.

Пристрої для абонентського шифрування: IP-шифратори Канал-201, Канал-301 та Канал-401 використовуються для побудови ІТС, які призначені для обробки Інформації з Обмеженим Доступом. Виконують такі функції: шифрування та контроль цілісності IP-пакетів, їх інкапсуляцію та маршрутизацію між мережевими інтерфейсами; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами.

Швидкістьшифрування: Канал-201 – 100 Мбіт/с, Канал-301 – 250 Мбіт/с, Канал-401 – 350 Мбіт/с. Всіпристроївиконані у виглядіокремогомережевоговузла. Конструктивно IP-шифратори Канал-201 та Канал-301 є системними платформами у металевомукорпусі, щоможутьвстановлюватись в 19-ти дюймовустійку, має 2 мережевихінтерфейсиEthernet 10/100/1000, а Канал-401 і має 2×2 (дубльованих) мережевихінтерфейсиEthernet 10/100/1000 (2 електричних та 2 оптичних – LC).

Комплексний захист конфіденційності переданих між абонентами ІТС електронних документів з одночасним стисненням (архівуванням) документів, забезпеченням їхньої цілісності й автентифікація автора за допомогою ЕЦП. Обробка документів виробляється безпосередньо перед передачею або після прийому їхніми звичайними засобами електронної пошти.

Захист цілісності ЕДО ділиться на підзавдання захисту від несанкціонованої зміни, підробки й пропажі. Рішення перших двох проблем здійснюється застосуванням ЕЦП, заснованої на криптографії з відкритим ключем. Рішення проблеми пропажі документа лежить поза криптографією — тут потрібне створення резервних копій з носіїв інформації, їхнє дублювання й строгий облік документів. При передачі документа по каналах зв'язку потрібні захищені протоколи передачі даних (типу SSL, TLS або інших), що надають

можливості одержання підтвердження про доставку, що здійснюють передачу даних різними маршрутами, і т.ін.

Захист ЕДО від загроз доступності, або від атак типу “відмова в обслуговуванні”, реалізується на рівні операційної системи, програмного й апаратного забезпечення установкою відповідних “латок”. Загроза полягає у відмові легальному (санкціонованому) користувачеві одержати доступ до інформації з боку системи. Способів створити ситуацію відмови в обслуговуванні, як буде описано далі, багато, починаючи від примітивних багаторазових спроб входу в систему від імені користувача до блокування його облікового запису й закінчуючи застосуванням хакерських атак на сервер типу “затоплення” повторюваними пакетами.

Підкреслю, що захист СЕД досягається не окремими рішеннями, а системою добре продуманих заходів, включаючи комплекс адміністративних процедур. Також має місце створення системи захисту СЕД як єдиного цілого або розробка підсистем безпеки для окремих інформаційних комплексів СЕД. Незалежно від цього СЕД повинні мати рішення по забезпеченню ІБ у таких важливих областях застосування, як, наприклад, планування відновлення після НСД, розподілене зберігання даних, управління пристроями й сховищами даних, резервне копіювання й архівування.

Особливості використання електронного цифрового підпису в системах електронного документообігу.

Для забезпечення захисту електронних документів і створення захищеної автоматизованої системи в першу чергу використовують криптографічні методи захисту інформації, які дозволяють забезпечити надійний захист цілісності, авторства й конфіденційності електронної інформації й реалізувати їх у вигляді програмних або апаратних засобів, що вбудовують в інформаційно-телекомунікаційну систему.

Незважаючи на безсумнівні переваги, широке впровадження систем електронного документообігу на першому етапі гальмувалося відсутністю ефективних засобів підтвердження авторства й дійсності. Для рішення цієї

проблеми на основі результатів, отриманих класичною й сучасною алгеброю, були запропоновані криптосистеми з відкритим ключем.

Для реалізації криптосистеми з відкритим ключем кожним адресатом інформаційної системи генеруються два ключі, зв'язані між собою за певним правилом. Один ключ оголошується відкритим, а інших закритим. Відкритий ключ публікується й доступний кожному, хто бажає послати повідомлення кореспондентові. Секретний ключ зберігається в таємниці.

Вихідний текст шифрується, підписується відкритим ключем кореспондента й передається йому. Зашифрований текст, не може бути розшифрований тим же відкритим ключем. Розшифровування повідомлення можливо тільки з використанням закритого ключа, що відомий тільки самому кореспондентові.

Надійність технології з відкритим ключем заснована на математично доведеному факті практичної неможливості обчислення секретного ключа з використанням сучасних обчислювальних засобів за доступний для огляду інтервал часу.

Пропоновані сьогодні криптосистеми з відкритим ключем опираються на один з наступних типів необоротних перетворень:

- Розкладання великих чисел на прості множники.
- Обчислення логарифма в кінцевому полі.
- Обчислення коренів алгебраїчних рівнянь.

Електронний цифровий підпис (ЕЦП) – реквізит електронного документа, призначений для захисту даного електронного документа від підробки, отриманий у результаті криптографічного перетворення інформації з використанням закритого ключа електронного цифрового підпису, який дозволяє ідентифікувати власника сертифіката ключа підпису, а також установити відсутність перекручування інформації в електронному документі [6].

ЕЦП дає можливість замінити при електронному документообігу традиційні печатку й підпис. Обчислення цифрового підпису складається із двох етапів.

На першому етапі поспеціальних алгоритмах (геш-функція) обчислюється деяке значення (геш-значення), що відповідає даному документу. Спрямована геш-функція одержує на вході повідомлення (електронний документ) довільної довжини й перетворює його в геш-значення фіксованої довжини. Значення геш-функції певним чином залежить від змісту документа, але не дозволяє відновити сам документ. Геш-функція чутлива до всіляких змін у тексті. Крім того, для даної геш-функції практично не можна підібрати два вихідних повідомлення, які можуть мати те саме геш-значення, або той же цифровий підпис. На другому етапі здійснюється зашифровування отриманого значення на секретному ключі ЕЦП, у результаті якого й виходить властиво цифровий підпис електронного документа. Таким чином, при відомій функції гешування, тільки збереження користувачем у таємниці свого секретного ключа гарантує неможливість підробки зловмисником документа й цифрового підпису від імені що завіряє.

Для перевірки ЕЦП одержувач повинен мати у своєму розпорядженні відкритий ключ відправника, що поставив підпис, і в жодному разі не сумніватися в дійсності відкритого ключа (а саме в тім, що наявний у нього відкритий ключ відповідає відкритому ключу конкретного користувача). Відкритий ключ підпису обчислюється як значення деякої функції від секретного ключа, але знання відкритого ключа не дає можливості визначити секретний. Відкритий ключ може бути опублікований і використовується для перевірки дійсності підписаного документа, а також для попередження шахрайства з боку сторони, що його завіряє, у вигляді відмови від підпису документа. Спочатку одержувач обчислює геш-значення від вхідного документа, яке потім порівнює з отриманим і розшифрованим на відкритому ключі ЕЦП значенням геш-значенням. Якщо знову обчислене значення геш-функції й отримане, а потім розшифроване збіглися, то одержувач робить висновок: “ЕЦП вірна”. У протилежному випадку (значення геш-функції не збігаються), він робить висновок: “ЕЦП не вірна”. Практична неможливість підробки електронного цифрового підпису опирається на дуже великий об'єм певних математичних обчислень[13].

Процедура формування й перевірки ЕЦП показана на рис. 2.3.

В сучасних інформаційно-комунікаційних системах на ЕЦП з відкритим ключем покладається виконання наступних функцій:

Невідмовність від передачі електронного документа. Забезпечується використанням функцій ЕЦП (підпис документа відправником) і зберіганням документа з ЕЦП протягом установленого строку прийомною стороною.

Невідмовність від прийому електронного документа. Відправник не може відмовитися від зробленої дії. Якщо порівнювати з паперовою технологією, то це аналогічно пред'явленню відправником паспорта перед виконанням дії. Забезпечується використанням функцій ЕЦП і квитуванням прийому документа (підпис квитанції одержувачем), зберіганням документа й квитанції з ЕЦП протягом установленого строку стороною, що відправляє.

Захист від переповторів. Забезпечується використанням криптографічних функцій ЕЦП, шифрування або імітозахисту з додаванням унікального ідентифікатора мережної сесії (електронного документа) з наступною їхньою перевіркою приймаючею стороною або розробкою спеціалізованого протоколу автентифікації (обміну електронними документами).

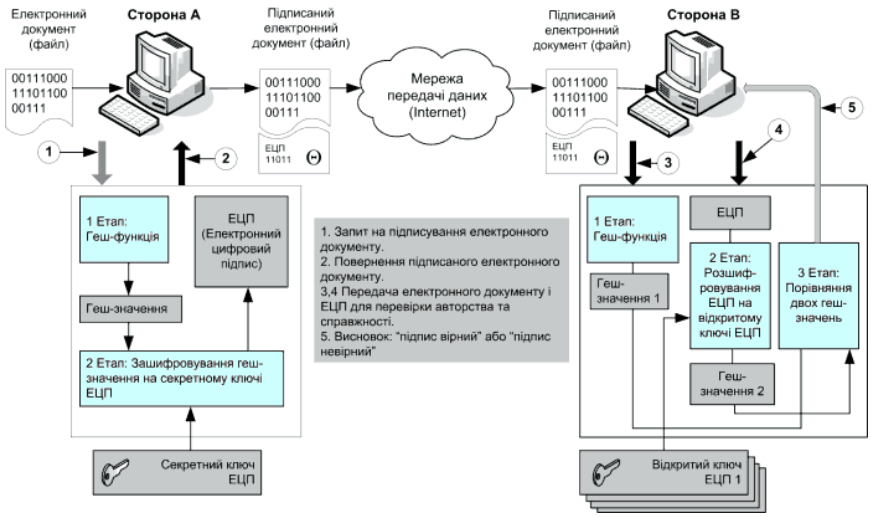


Рис. 2.3 Порядок використання ключів при формуванні та перевірці ЕЦП в криптосистемі з відкритим ключем.

Захист від нав'язування інформації. Захист від порушника з метою нав'язування прийомній стороні власної інформації, переданої нібито від імені санкціонованого користувача (порушення авторства інформації). Забезпечується використанням функцій ЕЦП із перевіркою атрибутів електронного документа й відкритого ключа відправника. У випадку нав'язування інформації про компрометацію ключа забезпечується організаційно-технічними заходами. Наприклад, створенням системи централізованого управління ключовою інформацією (оповіщенням абонентів) або спеціалізованих протоколів електронного документообігу.

Захист від закладок, вірусів, модифікації системного й прикладного ПЗ. Забезпечується спільним використанням криптографічних засобів, антивірусів і організаційних заходів[14].

ЕЦП забезпечує надійний захист даних. Однак необхідно розуміти, що її застосування – це аж ніяк не абсолютне рішення всіх проблем захисту інформації. Для ефективного рішення проблеми захисту інформації потрібен цілий комплекс дій, що містить у собі відповідні організаційно-технічні й адміністративні заходи, пов'язані із забезпеченням правильності функціонування технічних засобів обробки й передачі інформації, а також установлення певних правил для обслуговуючого персоналу, допущеного до роботи з конфіденційною інформацією.

При використанні криптографії з відкритим ключем необхідно вирішити проблему поширення відкритих ключів серед абонентів мережі (учасників електронного документообігу). Справа у тому, що безпосереднє використання відкритих ключів вимагає додаткового їхнього захисту й ідентифікації для визначення зв'язку із секретним ключем. Без такого додаткового захисту зловмисник може представити себе як відправником підписаних даних, так і одержувачем зашифрованих даних, замінивши значення відкритого ключа або порушивши його ідентифікацію. У цьому випадку кожний може видати себе кожного з учасників електронного документообігу. Це приводить до необхідності

верифікації відкритого ключа. На практиці для цих цілей використають два способи:

Перший спосіб: формування для кожного відкритого ключа, що функціонує в системі спеціального документа, що називається “Реєстраційна картка відкритого ключа ЕЦП” або “Реєстраційна картка відкритого ключа шифрування”[15]. Цей документ містить наступну інформацію:

- найменування системи, для якої виготовлений відкритий ключ;
- тип відкритого ключа і його номер у системі;
- інформація про власника відкритого ключа;
- дата виготовлення;
- термін дії;
- запис відкритого ключа в шістнадцятеричній формі;
- кеш-значення, отримане для всіх значимих полів реєстраційної картки.

Реєстраційна картка відкритого ключа – двосторонній документ для кожної пари учасників електронного документообігу, що оформляється у двох екземплярах, підписується керівниками сторін і засвідчується печатками. Разом із двостороннім договором про обмін електронними документами цей документ забезпечує юридичну значимість електронного документообігу в умовах діючого законодавства. Схема організації електронного документообігу між двома юридичними особами показаний на рис. 2.4.

Якщо в мережі конфіденційного зв'язку на основі криптосистеми з відкритим ключем 10 учасників, то для нормального обміну електронними документами кожний з них зобов'язаний підписати пакет документів з 9 іншими учасниками. Таким чином, зі збільшенням числа учасників мережі загальне число необхідних до підписання пакетів документів росте хвиле подібно.

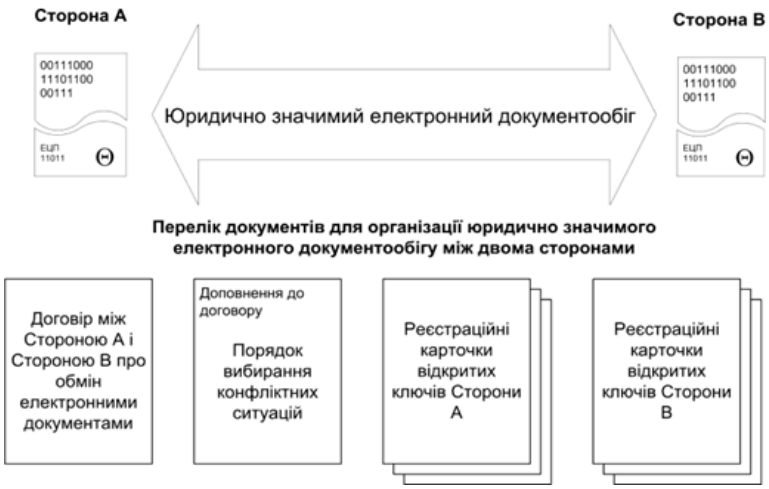


Рис. 2.4Приклад електронного документообігу між двома юридичними особами

Подібний спосіб застосуємо тільки для схем організації електронного документообігу типу “зірка”, у яких учасники системи обмінюються документами тільки з одним центром – організатором системи. Як приклад можна привести системи “банк-клієнт”, біржові системи, депозитарні системи.

Другий спосіб: використання інфраструктури відкритих ключів – невід'ємного сервісу для управління електронними сертифікатами й ключами користувачів, прикладного забезпечення й систем.

2.3 Критерії захищеності інформації у системах електронного документообігу

Згідно з нормативними документами системи ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) за результатом впливу на інформацію та систему її обробки загрози підрозділяються на чотири класи:

порушення конфіденційності інформації (отримання інформації користувачами або процесами всупереч встановленим правилам доступу);

порушення цілісності інформації (повне або часткове знищення, викривлення, модифікація, нав’язування хибної інформації);

порушення доступності інформації (втрата часткова або повна працездатності системи, блокування доступу до інформації;

втрата спостереженності або керованості системи обробки (порушення процедур ідентифікації та автентифікації користувачів та процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).[3]

Для забезпечення конфіденційності, цілісності і доступності інформації, а також керованості системою (спостереженості) необхідно захищати інформацію не тільки від витоку технічними каналами та несанкціонованого доступу, але і виключати можливість негативного впливу на інформацію, втручання у процес її обробки, порушення працездатності системи. Таким чином, захищати необхідно всі компоненти ЛОМ: апаратуру та обладнання, програми, дані, персонал[18].

Джерела виникнення загрози:

- які суб’єкти АС або суб’єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу.
- Можливі способи здійснення загрози:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;
- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
- несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Перші два способи за принципом відносяться до технічного доступу, останній – до логічного доступу.

Коротко розглянемо основні критерії загроз.

КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна

конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

а) Довірча конфіденційність (КД-1...4) - ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

- Мінімальна довірча конфіденційність (КД-1)
- Базова довірча конфіденційність (КД-2)
- Повна довірча конфіденційність (КД-3)
- Абсолютна довірча конфіденційність (КД-4)

б) Адміністративна конфіденційність (КА-1...4) - ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

- Мінімальна адміністративна конфіденційність (КА-1)
- Базова адміністративна конфіденційність (КА-2)
- Повна адміністративна конфіденційність (КА-3)
- Абсолютна адміністративна конфіденційність (КА-4)

в) Повторне використання об'єктів (КО-1) - ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

г) Аналіз прихованих каналів (КК-1…3)

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

- Виявлення прихованих каналів (КК-1)
- Контроль прихованих каналів (КК-2)

- Перекриття прихованих каналів (КК-3)

д) Конфіденційність при обміні (КВ-1…4) - ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

- Мінімальна конфіденційність при обміні (КВ-1)
- Базова конфіденційність при обміні (КВ-2)
- Повна конфіденційність при обміні (КВ-3)
- Абсолютна конфіденційність при обміні (КВ-4)

КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

а) Довірча цілісність (ЦД-1...4) - ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

- Мінімальна довірча цілісність (ЦД-1)
- Базова довірча цілісність (ЦД-2)
- Повна довірча цілісність (ЦД-3)
- Абсолютна довірча цілісність (ЦД-4)

б) Адміністративна цілісність (ЦА-1...4) - ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

- Мінімальна адміністративна цілісність (ЦА-1)
- Базова адміністративна цілісність (ЦА-2)
- Повна адміністративна цілісність (ЦА-3)

- Абсолютна адміністративна цілісність (ЦА-4)

в) Відкат (ЦО-1...2) - ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

- Обмежений відкат (ЦО-1)
- Повний відкат (ЦО-2)

г) Цілісність при обміні (ЦВ-1…4) - ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна цілісність при обміні (ЦВ-1)

Базова цілісність при обміні (ЦВ-2)

Повна цілісність при обміні (ЦВ-3).

КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв:

а) Використання ресурсів (ДР-1...3) - ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

- Квоти (ДР-1)
- Недопущення захоплення ресурсів (ДР-2)
- Пріоритетність використання ресурсів (ДР-3)

б) Стійкість до відмов (ДС-1...3)

Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити

можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови.

- Стійкість при обмежених відмовах (ДС-1)
- Стійкість з погіршенням характеристик обслуговування (ДС2)
- Стійкість без погіршення характеристик обслуговування (ДС-3)

в) Гаряча заміна (ДЗ-1…3)

Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти реалізації.

- Модернізація (ДЗ-1)
- Обмежена гаряча заміна (ДЗ-2)
- Гаряча заміна будь-якого компонента (ДЗ-3)

г) Відновлення після збоїв (ДВ-1…3) - ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

- Ручне відновлення (ДВ-1)
- Автоматизоване відновлення (ДВ-2)
- Вибіркове відновлення (ДВ-3)

КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

а) Реєстрація (НР-1...5)

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності

засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

- Зовнішній аналіз (НР-1)
- Захищений журнал (НР-2)
- Сигналізація про небезпеку (НР-3)
- Детальна реєстрація (НР-4)
- Аналіз в реальному часі (НР-5)

б) Ідентифікація й автентифікація (НИ-1...3)

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

- Зовнішня ідентифікація і автентифікація (НИ-1)
- Одиночна ідентифікація і автентифікація (НИ-2)
- Множинна ідентифікація і автентифікація (НИ-3)

в) Достовірний канал (НК-1...2) - ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

- Однонаправлений достовірний канал (НК-1);
- Двонаправлений достовірний канал (НК-2);

г) Розподіл обов'язків (НО-1...3) - ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів

- Виділення адміністратора (НО-1)
- Розподіл обов'язків адміністраторів (НО-2)
- Розподіл обов'язків на підставі привілеїв (НО-3)

д) Цілісність комплексу засобів захисту (НЦ-1...3) - ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

- КЗЗ з контролем цілісності (НЦ-1)
- КЗЗ з гарантованою цілісністю (НЦ-2)
- КЗЗ з функціями диспетчера доступу (НЦ-3)

ж) Самотестування (НТ-1...3)

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

- Самотестування за запитом (НТ-1)
- Самотестування при старті (НТ-2)
- Самотестування в реальному часі (НТ-3)

з) Ідентифікація й автентифікація при обміні (НВ-1...3)

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

- Автентифікація вузла (НВ-1)
- Автентифікація джерела даних (НВ-2)
- Автентифікація з підтвердженням (НВ-3)

к) Автентифікація відправника (НА-1…2)

Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

- Базова автентифікація відправника (НА-1)

- Автентифікація відправника з підтвердженням (НА-2)

м) Автентифікація отримувача (НП-1…2) - ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

- Базова автентифікація отримувача (НП-1)
- Автентифікація отримувача з підтвердженням (НП-2)

Висновок до другого розділу

Розроблено вимоги до безпеки систем електронного документообігу, а також додаткові вимоги до захищених систем такого типу. Розглянуто можливості забезпечення інформаційної безпеки в мережі. Визначено існуючі проблеми безпеки організації безпечного з'єднання.

3 ТЕХНОЛОГІЇ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ У СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

3.1 Особливості систем криптографічного захисту інформації

Основною метою при розробці технологій електронного документообігу було досягнення максимальної наступності правил і прийомів паперового документообігу і журнально-картотечного діловодства, що дозволяє забезпечити безболісний перехід від традиційних технологій до сучасних.

Технологію електронного документообігу підтримують наступні функціональні можливості системи [10, 11]:

- реєстрація в автоматизованому режимі переданих електронною поштою або через Інтернет-портал вхідних документів, у тому числі таких, що мають електронний цифровий підпис (ЕЦП) і криптозахист;

- сканування і розпізнавання паперових документів;

- прикріплення до реєстраційної картки (РК) електронного образу документу у вигляді файлу (файлів) будь-якого формату;

- розмежування прав доступу до прикріплених файлів електронного образу документу;

- надання кожній посадовій особі — учаснику діловодного процесу — свого особистого віртуального кабінету, чим досягається доступ посадової особи тільки до документів, що відноситься до її компетенції;

- розсилання електронних документів і доручень по них по мережі (по кабінетах посадових осіб);

- забезпечення процесу узгодження (візування) проектів документів;

- повнотекстовий і атрибутивний пошук електронних документів, включаючи віддалений повнотекстовий пошук;

- відправлення електронною поштою або публікація на Інтернет-порталі органу влади електронних вихідних документів (з використанням будь-якої

електронної пошти, що підтримує MAPI), захищених ЕЦП і шифруванням за допомогою сертифікованих засобів;

- формування і оформлення справ, тобто групування виконаних документів у справи відповідно до номенклатури справ і систематизацією документів всередині справи;

- архівне збереження електронних документів, справ органу влади [13].

Програма електронного документообігу з використанням ЕЦП на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕЦП і розвиток електронного документообігу в Україні.

Електронний цифровий підпис функціонально аналогічний звичайному рукописному підпису на папері і володіє всіма його основними перевагами:

- засвідчує, що підписаний документ надходить від особи, що його підписала;

- гарантує цілісність підписаного документа (захист від модифікацій);

- не дає можливості особі, що підписала документ, відмовитися від зобов'язань, пов'язаних з підписаним документом [14].

Безпека використання ЕЦП забезпечується тим, що засоби, які використовуються для роботи з ЕЦП, проходять експертизу та сертифікацію в Департаменті спеціальних телекомунікаційних систем СБУ, що гарантує неможливість злому і підробки ЕЦП.

Система захисту у складі користувач-сервер призначена для:

- автентифікації користувачів системи при підключенні до сервера та забезпечення конфіденційності і цілісності даних, які передаються між користувачами та сервером;

- забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, з використанням електронного цифрового підпису.

Зазначені функції система виконує шляхом застосування механізмів криптографічного захисту інформації, яка обробляється у системі.

Автентифікація користувачів системи на сервері здійснюється під час підключення користувачів до сервера (встановлення з’єднання з сервером) шляхом реалізації протоколу взаємної автентифікації сторін. Забезпечення конфіденційності та цілісності інформації, яка передається між користувачем та сервером системи під час їх взаємодії, реалізується шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум.

Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, реалізуються шляхом формування та перевіряння електронного цифрового підпису від даних та документів, як на стороні користувача системи так і на стороні сервера.

Система в цілому відноситься до типу апаратно-програмних комплексів КЗІ виду «Б», категорії «Ш», «П» та «Р2, класу Б2. Окремі засоби, що входять до його складу, відносяться до типів апаратно-програмних та програмних засобів КЗІ видів «Б» та «В», категорії «Ш», «П» та «Р» класу Б2.

Найвищий гриф обмеження доступу інформації, яка може захищатися засобами системи – конфіденційна, що не є власністю держави.

Для організації ключової системи (управління ключовими даними) засобів системи використовується центр сертифікації ключів.

Структурна схема комплексу захисту наведена на рис. 3.1.

До складу комплексу входять:

- програмні засоби (бібліотеки) КЗІ (користувача ЦСК);

- апаратні засоби КЗІ.

Програмні засоби КЗІ реалізують логіку роботи комплексу та інтегровані безпосередньо у користувальницьку та серверну частини системи (користувача та сервер), через визначені інтерфейси.

Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо.

До складу апаратних засобів комплексу можуть входити:

- електронний ключ;

- мережний криптомодуль

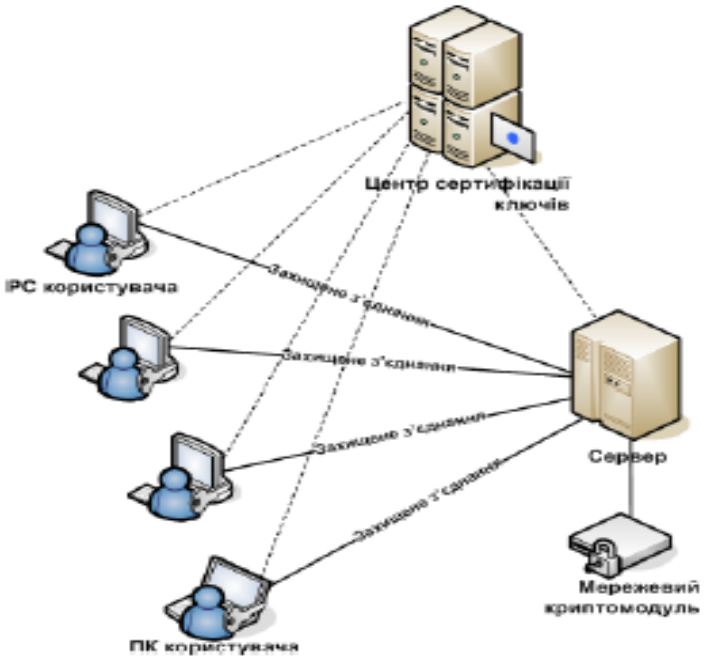


Рис. 3.1Схема комплексу у складі системи

До складу комплексу входять[19]:

- програмнізасоби (бібліотеки) КЗІ (користувача ЦСК);

- апаратнізасоби КЗІ.

Програмнізасоби КЗІ реалізуютьлогікуроботи комплексу та інтегрованібезпосередньо у користувальницьку та сервернучастинисистеми (користувача та сервер), через визначеніінтерфейси.

Програмнізасоби КЗІ комплексу можутьвикористовуватизовнішніапаратнізасоби КЗІ, такі як електронніключі, мережнікриптомодулітощо.

Бібліотекикористувача центру сертифікаціїключів (ЦСК) призначені для використання в якостібазовихзасобів КЗІ та виконуютьнаступніфункції у їхскладі:

- роботу з носіями ключової інформації (зчитування особистих ключів з носіїв);

- роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС), що включає: зчитування сертифікатів та списків відкликаних

сертифікатів із файлового сховища; визначення статусу сертифіката за допомогою списків відкликаних сертифікатів; завантаження списків відкликаних сертифікатів з веб-сторінки ЦСК (з веб-серверу ЦСК);

- зашифрування та розшифрування даних;

- формування та перевірку ЕЦП від даних;

- захист сеансів передачі даних (захист з'єднань), що включає: реалізацію протоколу взаємної автентифікації сторін під час встановлення сеансу захищеної передачі даних (захищеного з'єднання); захист (шифрування та контроль цілісності) сегментів захищеної передачі даних (даних захищеного з'єднання);

- інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК);

- пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК);

- отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Бібліотеки користувача ЦСК інтегруються зазначену у систему (та інші прикладні системи) через визначені інтерфейси та реалізовані для ОС Microsoft Windows 98/2000/XP/2003 Server/2008 Server/7, ОС Microsoft Windows Mobile 5/6/6.5, Linux (SUSE/RedHat/Slackware та ін.), UNIX (AIX/Solaris/BSD та ін.) у вигляді бібліотек підключення (DLL/COM, SO) або у вигляді java-аплетів (J2SE/J2ME).

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів користувача системи.

Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі сервера системи.

На сервері системи встановлюються та використовуються наступні складові частини комплексу:

- програмний комплекс захисту сервера, який включає бібліотеки користувача ЦСК (для відповідної серверної ОС);

- апаратний засіб КЗІ – криптомодуль мережі .

На засобах користувачів системи (робочих станціях чи портативних комп’ютерах – РС та ПК) встановлюються та використовуються наступні складові частини комплексу:

- програмний комплекс захисту користувача, який включає бібліотеки користувача ЦСК (для відповідної ОС);

- апаратний засіб КЗІ – електронний ключ.

Інсталяційні пакети програмних засобів комплексу

Програмні засоби комплексу передаються на об’єкт впровадження у вигляді інсталяційних пакетів на оптичному компакт-диску. Формат інсталяційного пакету залежить від цільової ОС.

До складу інсталяційних пакетів входять:

- інсталяційний пакет з програмним комплексом захисту сервера;

- інсталяційний пакет з програмним комплексом захисту користувача.

До складу кожного з інсталяційних пакетів входить комплект експлуатаційних документів на відповідні програмні комплекси.

Опис апаратних засобів

Електронний ключ призначений для:

- автентифікації користувача системи перед початком роботи;

- зберігання та захисту особистого ключа користувача;

- апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача.

Електронний ключ має електричний USB-інтерфейс для підключення до ПЕОМ.

Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку ПЕОМ користувача.

Мережевий криптомодуль призначений для:

- автентифікації сервера системи перед початком роботи;

- зберігання та захисту особистого ключа сервера;

- апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/1000 для підключення до сервера системи безпосередньо або через комутатори локальної обчислювальної мережі.

Апаратна реалізація мережевого криптомодуля забезпечує захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливлює доступ до особистих ключів сервера з боку ЕОМ сервера системи.

3.2 Практичні рішення систем криптографічного захисту інформації

У засобах системи використовуються такі криптографічні алгоритми та протоколи[20]:

- алгоритм шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни, режим гамування та режим вироблення імітовставки);

- алгоритм ЕЦП за ДСТУ 4145-2002;

- алгоритм гешування за ГОСТ 34.311-95;

- протокол розподілу ключових даних Діффі-Хелмана в групі точок еліптичної кривої (направлене шифрування).

Протокол розподілу ключових даних реалізований згідно методики розподілу ключових даних на основі протоколу Діффі-Хелмана в групі точок еліптичної кривої, яка погоджена з Державною службою спеціального зв’язку та захисту інформації України і відповідає вимогам ДСТУ ISO/IEC 15946-3. Генерація ключових даних виконується згідно методики генерації ключових даних, яка погоджена з Державною службою спеціального зв’язку та захисту інформації України.

Протокол встановлення захищеного сеансу передачі даних реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3. Протокол взаємної автентифікації включає:

- формування користувачем та передачу даних автентифікації (запиту) на сервер, при цьому користувач виконує наступні дії: генерує випадкове число; підписує випадкове число та власний сертифікат (за необхідності) власним особистим ключем ЕЦП;

- передає сформовані дані автентифікації (запит) на сервер;

- обробку запиту від користувача сервером, при цьому сервер виконує наступні дії: отримує дані автентифікації від користувача;

- здійснює пошук (за відсутності сертифіката у запиті) та перевірку чинності сертифіката користувача; перевіряє ЕЦП на даних; у разі успішної обробки отриманих даних автентифікації – генерує сеансові ключі шифрування та вектори початкової ініціалізації; підписує отримане випадкове число та сеансові ключі з векторами початкової ініціалізації власним особистим ключем ЕЦП; зашифровує сформовані дані разом з ЕЦП спрямовано на користувача; передає підписані та зашифровані дані автентифікації (відповідь) користувачу;

- прийом та обробку відповіді користувача від сервера, при цьому користувач виконує наступні дії: отримує відправлені дані автентифікації (відповідь) від сервера; здійснює пошук та перевірку чинності сертифіката сервера; розшифровує дані автентифікації; перевіряє ЕЦП на даних;

- перевіряє відповідність випадкового числа у отриманих даних; у разі успішної обробки отриманих даних автентифікації (відповіді) завершує роботу протоколу.

Структурно-функціональна схема взаємодії користувача та сервера наведена на рис. 3.2. За результатом роботи протоколу на сервері та користувачеві встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування даних у захищеному з’єднанні у дуплексному режимі. Шифрування даних у захищеному з’єднанні здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі гамування. В якості криптографічної контрольної суми для контролю цілісності даних у захищеному з’єднанні використовуються імітовставки, які обчислюються за

алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі вироблення імітовставки.

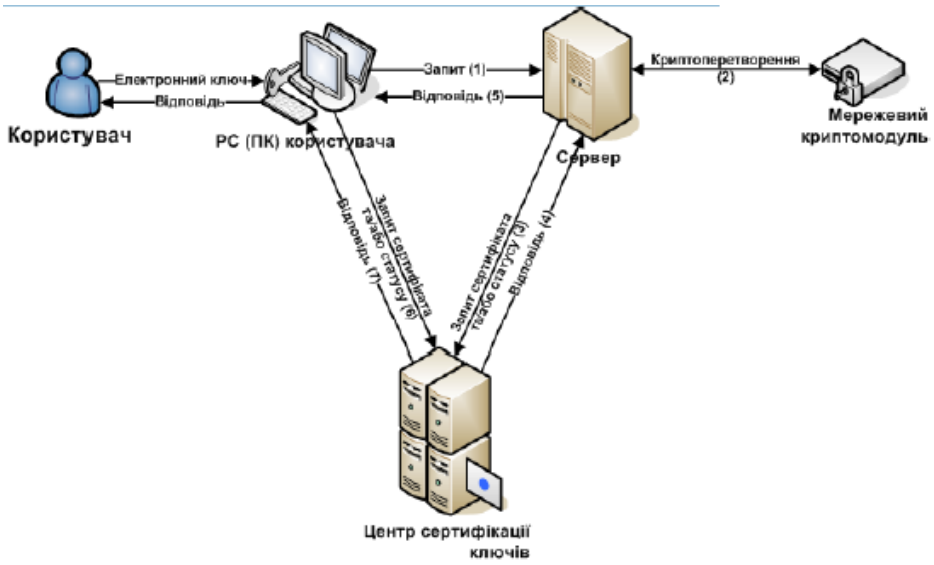


Рис. 3.2 Схема взаємодії користувача та сервера СЕД

Шифрування даних та обчислення імітовставок у захищеному з'єднанні здійснюється на основі сеансових ключів та векторів початкової ініціалізації (синхромаркерів), які розподіляються між користувачем та сервером у результаті виконання протоколу взаємної автентифікації.

3.3. Засоби формування та перевірки електронного цифрового підпису

Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК).

У комплексі використовуються дві підгрупи ключових даних:

- ключові дані ЦСК;

- ключові дані користувачів та сервера системи.

До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних користувачів та сервера системи відносяться особисті ключі та сертифікати відповідно користувачів та сервера.

Параметри еліптичних кривих для алгоритму ЕЦП ДСТУ 4145-2002, та довгострокові ключові елементи (ДКЕ) для алгоритму шифрування ДСТУ ГОСТ 28147:2009, постачаються відповідно до вимог Держспецзв'язку України [21].

Окрім електронних ключів, в якості носіїв ключової інформації для особистих ключів користувачів можуть використовуватися:

- гнучкі диски 3,5" (дискети);

- електронні диски (flash-диски);

- компакт-диски (CD-R, CD-RW, DVD-R або DVD-RW);

- інші електронні ключі: ТехнотрейдuaToken; AladdineToken R2, PRO; Актив ruToken; Автор SecureToken; CIC Almaz; смарт-карти Aladdin, Автор, Криптомаш, та інші модулі з бібліотеками підтримки.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів, а саме:

- формати сертифікатів та списків відкликаних сертифікатів згідно технічних специфікацій форматів представлення базових об'єктів національної системи ЕЦП (затверджені спільним наказом ДСТСЗІ СБ України і Держзв'язку України від 11.09.2006 р. за № 99/166);

- формати захищених даних (даних з ЕЦП та зашифрованих даних) – згідно міжнародних технічних рекомендацій RFC 3630 (PKCS#7) та проекту технічних специфікацій національної системи ЕЦП;

- формати запитів на отримання інформації про статус сертифіката та інформації про статус – згідно міжнародних технічних рекомендацій RFC 2560 та проекту технічних специфікацій національної системи ЕЦП;

- формати запитів на формування позначок часу та самих позначок часу – згідно міжнародних технічних рекомендацій RFC 3161 та проекту технічних специфікацій національної системи ЕЦП.

Опис взаємодії з центром сертифікації ключів

ЦСК призначений для обслуговування сертифікатів відкритих ключів користувачів та сервера системи, надання послуг фіксування часу, а також надання (за необхідності) користувачам системи засобів генерації особистих та відкритих ключів.

ЦСК забезпечує:

- обслуговування сертифікатів користувачів та сервера системи, що включає: реєстрацію користувачів та сервера; сертифікацію відкритих ключів користувачів та сервера; розповсюдження сертифікатів; управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів;

- надання послуг фіксування часу;

- надання користувачам системи (за необхідності) засобів генерації особистих та відкритих ключів

Для взаємодії з центром сертифікації ключів (використання його інтерактивних служб) користувачі та сервери системи повинні мати можливість мережевого підключення до ЦСК. Усі механізми взаємодії з ЦСК виконують бібліотеки користувача ЦСК.

Зміна статусу сертифікатів (блокування, поновлення або скасування) та знищення особистих ключів користувачів та сервера системи здійснюється у відповідності до порядку, який визначений ЦСК (згідно регламенту ЦСК).

Висновки до третього розділу

Досліджено систему забезпечення захисту електронного документообігу на базі LotusNotes; досліджена структура та функціональні особливості системи електронного документообігу; реалізовано систему забезпечення захисту електронного документообігу на базі LotusNotes.

Практична цінність роботи полягає у тому, що запропонована удосконалена СЕД на базі LOTUS DOMINO/NOTES, що може бути використаною у діяльності реального підприємства для підвищення ефективності його роботи.

ВИСНОВКИ

Однією із ефективних форм створення, накопичення і обміну інформацією та її використання у процесі управлінської діяльності є технологія електронного документообігу.

Встановлено, що під захищеним документообігом розуміється контрольований рух конфіденційної документованої інформації з регламентованих пунктів прийому, обробки, розгляду, виконання, використання і збереження в жорстких умовах організаційного забезпечення безпеки як носія інформації, так і самої інформації.

Розглянуто нормативно-правовіпідставиведенняділоводства та електронного документообігу в Україні. Проаналізовано переваги і недоліки систем електронного документообігу. Встановлено, що загрозами інформації в системах електронного документообігу є загрози конфіленційності, доступності, цілісності інформації.

Описано вимоги до безпеки систем електронного документообігу, а також додаткові вимоги до захищених систем такого типу. Досліджено систему забезпечення захисту електронного документообігу на базі LotusNotes.

З технологічної точки зору система електронного документообігу являє собою інтеграційну систему, що охоплює діловодство і підготовку документів і поєднує їх із зовнішнім середовищем електронного обміну.

Практична цінність роботи полягає у тому, що модель СЕД може бути використаною у діяльності реального підприємства для підвищення ефективності його роботи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Мельник Т. Електронний документообіг та електронний підпис //Бухгалтерський облік і аудит. - 2008. - № 7. - С. 47-53.
2. Про електронні документи та електронний документообіг : Закон України від 22.05.03 р. № 851-IV.
3. Янчева Л. Електронна комерція: організація та облік: навч.посіб. / Харківський держ. ун-т харчування та торгівлі. — Х. : ХДУХТ, 2008. — 231с
4. Брижко В.Електронна комерція: правові заходи та заходи удосконалення: монографія / Брижко В., Новицький А., Цимбалюк В., Швець М. / Науково-дослідний центр правової інформатики Академії правових наук України. — К. : НДЦПІ АПрНУ, 2008. — 149с.
5. Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу : Постанова Кабінету Міністрів України від26.05.04 р. № 680.
6. Голубенко О.Л. Політика інформаційної безпеки: підручник/ Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є.,– Луганськ: вид-во СНУ ім.. В.Даля, 2009, - 300с.
7. Гулак Г.М., Методологія захисту інформації: навчально-методичний посібник. / Довгань О.Д., Гулак Г.М., Гринь А.К., Мельник С.В.–К.: Наук.-ви. Центр НА СБ України, 2012. – 184 с.
8. Шорошев В.В. Основи формування політики безпеки комп’ютерних систем, -К, Бизнес и безопасность, 2006, 141с., іл.
9. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.98 р. № 505/98.
10. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації : наказ Державної служби спеціального зв’язку та захисту інформації України від 20.07.07 р. № 141. – (Зареєстрований Міністерством юстиціїУкраїни від 30.07.07 р. № 862/14129).

11. Гулак Г.М. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук, Вінниц. нац. техн. ун-т.– Вінниця : ВНТУ, 2011.– 198 с.
12. Про систему електронних підписів, що застосовується в межах Співтовариства: Директива 1999/93/ЄС Європейського парламенту та Ради від 13.12.99 р.
13. Щодо стану роботи з адаптації законодавства України до законодавства Європейського Союзу: Рішення шостого засідання Міжвідомчої координаційної ради з адаптації законодавстваУкраїни до законодавства ЄС від 28.09.01 р.
14. Про електронний цифровий підпис : Закон України від 22.05.03 р. № 852-IV.
15. Про затвердження Положення про центральний засвідчувальний орган : ПостановаКабінету Міністрів України від 28.10.04 р. № 1451.
16. Про затвердження Порядку акредитації центру сертифікації ключів : ПостановаКабінету Міністрів України від 13.07.04 р. № 903.
17. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності : Постанова Кабінету Міністрів України від 28.10.04 р. № 1452.
18. Про затвердження Правил проведення робіт із сертифікації засобів захисту інформації: наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України, Державного комітету України з питань технічного регулювання та споживчої політики від 25.04.007 р. № 75/91. – (Зареєстрований Міністерством юстиції України від 14.05.07 р. № 498/13765).
19. Про затвердження Положення про державну експертизу у сфері криптографічного захисту інформації : наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 23.06.08 р. № 100. – (Зареєстрований Міністерством юстиції України від 16.07.2008 р. № 651/15342).
20. Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису : наказ Міністерства юстиції України та Державної служби спеціального зв’язку та захисту інформації України

від 20.08.12 р.№ 1236/5/453. – (Зареєстрований Міністерством юстиції України від 20.08.12 р. № 1398/21710).

21. Шорошев В.В. Основи формування політики безпеки комп'ютерних систем, -К, Бизнес и безопасность, 2006, 141с., іл.
22. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.98 р. № 505/98.
23. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації : наказ Державної служби спеціального зв'язку та захисту інформації України від 20.07.07 р. № 141. – (Зареєстрований Міністерством юстиціїУкраїни від 30.07.07 р. № 862/14129).
24. Гулак Г.М. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук, Вінниц. нац. техн. ун-т.– Вінниця : ВНТУ, 2011.– 198 с.
25. Про Національну систему конфіденційного зв'язку : *Закон України* від 10.01.2002 № 2919-III.

ДИПЛОМНА РОБОТА
освітньо-кваліфікаційного рівня “магістр”
НА ТЕМУ:

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

СТУДЕНТ Ніколаєв Н.М.
КЕРІВНИК Котенко А.М.

МЕТА ТА ЗАВДАННЯ 2

ОБ’ЄКТ ДОСЛІДЖЕННЯ – процес захисту інформації в системах електронного документообігу

ПРЕДМЕТ ДОСЛІДЖЕННЯ – захист систем електронного документообігу

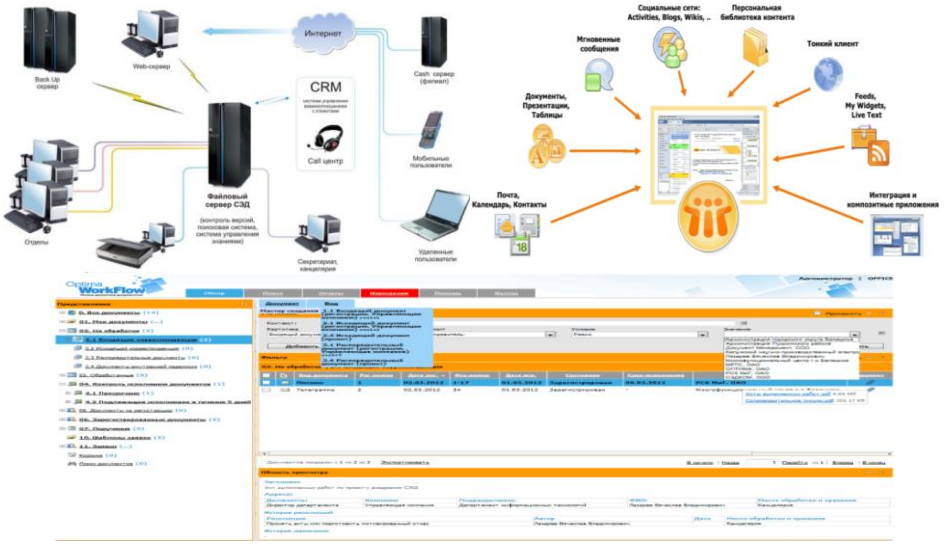
МЕТА РОБОТИ – розробка рекомендацій по захисту інформації в системах електронного документообігу.

Завдання дипломної роботи

1. Проаналізувати загрози інформації в системах електронного документообігу
2. Проаналізувати методи та засоби захисту систем електронного документообігу
3. Розробити рекомендації по захисту інформації в системах електронного документообігу

ВИКОРИСТАННЯ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ 3

Потреба в ефективному управлінні електронними документами призвела до створення систем електронного документообігу під якими розуміють організаційно-технічні системи, що полегшують процес створення, управління доступом і поширення електронних документів в комп'ютерних мережах



ЗАГРОЗИ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ 4

Загрози систем електронного документообігу:

1. ***Загроза конфіденційності*** *- це загрози несанкціонованого доступу та ознайомлення з урахуванням тонких політик безпеки систем електронного документообігу*

2. ***Загроза цілісності*** *- загрози, при реалізації яких інформація втрачає заздалегідь встановлені системою вид і якість.*

3. ***Загроза доступності*** *- характеризують можливість доступу до інформації, що зберігається і оброблюваної в СЕД інформації будь-якої миті.*

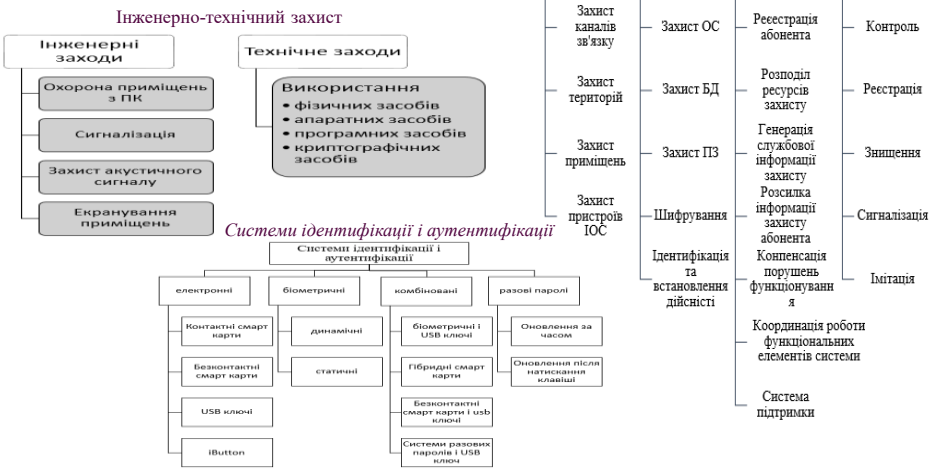
Компоненти систем електронного документообігу:

1. Сервери.
2. Робочі місця.
3. Канали зв'язку.

Ступені цінності комонентів СЕД

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕД 5

Групи методів та засобів захисту інформації в СЕД
- методи і засоби організаційно-правового захисту інформації;
- методи і засоби інженерно-технічного захисту інформації;
- криптографічні методи і засоби захисту інформації;
- програмно-апаратні методи та засоби захисту інформації.



АНАЛІЗ ЗАКОРДОННИХ СТАНДАРТІВ СЕД 6

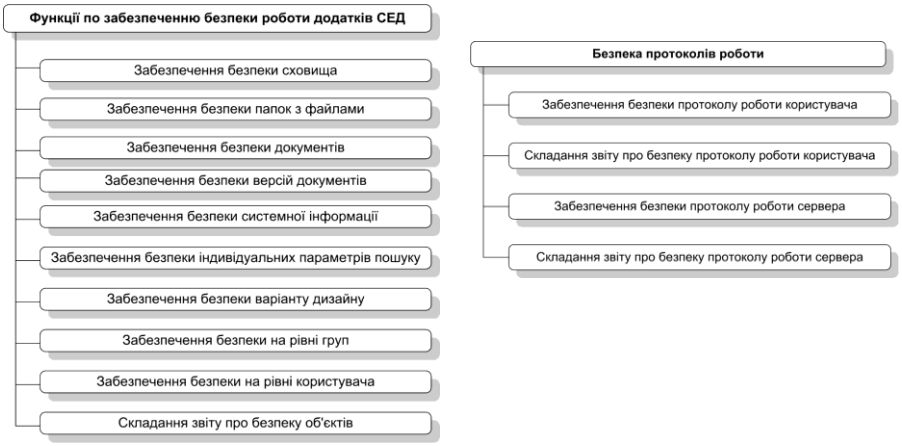
Широкомасштабне використання інформаційних технологій в діловодстві призвело до розробки відповідних стандартів на міжнародному рівні. Вимоги до систем управління електронними документами розробляються в основному в інтересах державних органів, щоб визначити єдиний підхід до обміну документами на міжвідомчому рівні.

Табл. Основні національні стандарти СЕД

Стандарт	Країна	Сфера регулювання
DoD 5015.2-STD версія 3	США	Стандарт вимог до розробки програмних додатків для управління електронними документами; необхідність закупівлі тільки сертифікованих продуктів; розподіл повноважень і відповідальності в СЕД
MoReq2	країни ЄС	Типові вимоги до автоматизованих систем електронного документообігу
NoARK-5	Норвегія	Національні вимоги Норвегії до управління електронними документами і їх архівації
PROS 99/007 версія 2 (VERS)	Австралія	Управління електронними документами; містить вимоги до сховищ документів
Концепція електронного уряду (DOMEA)	Німеччина	Ідея являє собою концепцію управління документами і електронного архівування в сфері державного управління.
концепція ELAK	Австрія	" Електронне справа" містить повномасштабний набір вимог до електронного керування документами (більше 800 вимог, які охоплюють сфери управління інформацією і документами, управління робочими процесами - workflow, а також архівування)

ПРОЦЕСИ УПРАВЛІННЯ КОНТРОЛЮ ДОСТУПУ 7

Процеси управління списками контролю доступу виконують функції по забезпеченню безпеки роботи додатків СЕД. Безпека всіх об'єктів, якими управляє система, контролюється за допомогою цих функцій.



КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ СЕД 8

Засоби захисту СЕД:

1. Ідентифікація, автентифікація й авторизація об'єктів і суб'єктів

Наявність можливості в керівника відділу переглядати всі документи, над якими працюють співробітники відділу, у той час як кожен співробітник бачить лише свою частину роботи й не бачить документи, над якими працюють інші; кожний з документів може мати встановлені для нього права доступу на читання, зміну

2. Управління доступом

Дозволяє визначати для кожного документа й для кожної ПП правочинних користувачів й їхнього права

3. Засоби контролю імпортованих програм

Ліцензія, програми тестування та аналізу ефективності

4. Криптографія

Має на меті приховання тексту повідомлення, роблячи його недоступнім для неавторизованих користувачів

5. Електронний цифровий підпис

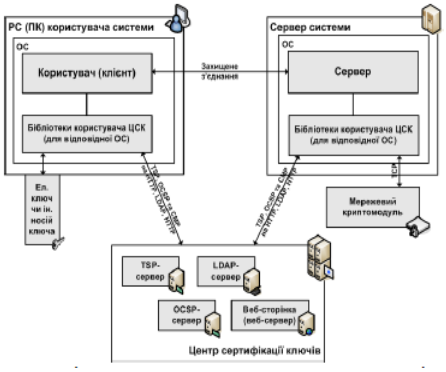
Дозволяє ідентифікувати власника сертифіката ключа підпису, а також установити відсутність перекручування інформації в електронному документі)

ЗАСТОСУВАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ 9

Електронний цифровий підпис функціонально аналогічний звичайному рукописному підпису на папері і володіє всіма його основними перевагами:

- засвідчує, що підписаний документ надходить від особи, що його підписала;
- гарантує цілісність підписаного документа (захист від модифікацій);
- не дає можливості особі, що підписала документ, відмовитися від зобов'язань, пов'язаних з підписаним

Структурна схема комплексу у складі системи



Функціональна схема комплексу у складі системи

РІШЕННЯ ЩОДО КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ 10

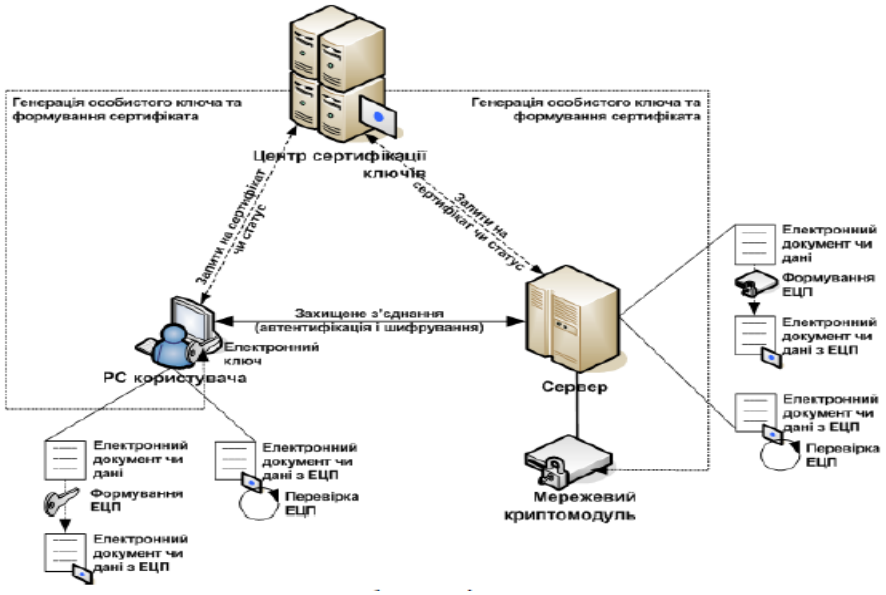
Структурно-функціональна схема взаємодії користувача та сервера

Криптографічні алгоритми та протоколи:

- *алгоритм шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни, режим гамування та режим вироблення імітовставки);*
- *алгоритм ЕЦП за ДСТУ 4145-2002;*
- *алгоритм гешування за ГОСТ 34.311-95;*
- *протокол розподілу ключових даних Діффі-Хелмана в групі точок еліптичної кривої (направлене шифрування).*

Шифрування даних та обчислення імітовставок у захищеному з'єднанні здійснюється на основі сеансових ключів та векторів початкової ініціалізації (синхромаркерів), які розподіляються між користувачем та сервером у результаті виконання протоколу взаємної автентифікації.

ВЗАЄМОДІЯ ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ 11



ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ СЕД 12

Порівняльний аналіз сучасних захищених СЕД вітчизняного виробництва

Функціональні профілі безпеки						
Критерії безпеки	**Системи ЕДО**					**Краща СЕД за критерієм**
	1.АСКОД-К	**2.АСКОД WEB**	**3.eDocs**	**4.Мегаполіс. Документообіг-ДСК**	**5.Megapolis.DocNet**	
Критерії конфіденційності						
Довірча конфіденційність	(-)*	(-)	(-)	КД-2	(-)*	
Адміністративна конфіденційність	КА-2	КА-2	КА-2	КА-2	КА-2	(=)**
Повторне використання об'єктів	КО-1	КО-1	КО-1	КО-1	КО-1	(=)
Конфіденційність при обміні	(-)	(-)	(-)	(-)	КВ-1	[5]
Критерії цілісності						
Довірча цілісність	(-)	(-)	(-)	ЦД-1	(-)	[4]
Адміністративна цілісність	ЦА-1	ЦА-1	ЦА-1	ЦА-2	ЦА-1	[4]
Відкат	ЦО-1	ЦО-1	ЦО-1	ЦО-1	ЦО-1	(=)
Цілісність при обміні	(-)	(-)	(-)	ЦВ-2	ЦВ-2	[4],[5]

ВИСНОВКИ

13

Однією із ефективних форм створення, накопичення і обміну інформацією та її використання у процесі управлінської діяльності є технологія електронного документообігу.

Встановлено, що під захищеним документообігом розуміється контрольований рух конфіденційної документованої інформації з регламентованих пунктів прийому, обробки, розгляду, виконання, використання і збереження в жорстких умовах організаційного забезпечення безпеки як носія інформації, так і самої інформації.

Розглянуто нормативно-правові підстави ведення діловодства та електронного документообігу в Україні. Проаналізовано переваги і недоліки систем електронного документообігу. Встановлено, що загрозами інформації в системах електронного документообігу є загрози конфіленційності, доступності, цілісності інформації.

Описано вимоги до безпеки систем електронного документообігу, а також додаткові вимоги до захищених систем такого типу. Досліджено систему забезпечення захисту електронного документообігу на базі Lotus Notes.

З технологічної точки зору система електронного документообігу являє собою інтеграційну систему, що охоплює діловодство і підготовку документів і поєднує їх із зовнішнім середовищем електронного обміну.

Практична цінність роботи полягає у тому, що модель СЕД може бути використаною у діяльності реального підприємства для підвищення ефективності його роботи.