УДК [004.7+004.056.5]:930.25(477)

Тарас Купрунець

НОВИЙ ПОГЛЯД НА СИСТЕМИ ТЕРМІНАЛЬНОГО ДОСТУПУ ЯК ЗАСІБ ПОКРАЩЕННЯ ПОКАЗНИКІВ НАДІЙНОСТІ, СУКУПНОЇ ВАРТОСТІ ВОЛОДІННЯ ТА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ В АРХІВНІЙ ГАЛУЗІ УКРАЇНИ

У статті проаналізовано метод побудови інформаційно-комунікаційних систем на основі термінальної системи, визначено позитивні та негативні сторони термінальних систем у цілому та особливості їхнього використання в державних установах України, окреслено перспективи впровадження цих систем при створенні інформаційно-комунікаційних систем в архівній галузі.

Ключові слова: процес інформатизації, інформаційно-комунікаційна система, термінальна система, термінальний сервер, тонкий клієнт, інформаційна безпека.

Початок XXI ст. для України ознаменувався значними зрушеннями в сфері інформатизації суспільства[1]. Комерційний сектор інтенсивно розвивався в інформаційно-технічному плані ще з кінця XX ст.[2], що було обумовлено жорстким конкурентним середовищем, яке диктувало необхідність постійного поліпшення ефективності прийняття й виконання управлінських рішень, а це неможливо здійснити без підвищення швидкості отримання та опрацювання інформації. Натомість, у державному секторі ці процеси розвивалися дещо повільніше. Це пов'язано із зміщенням акцентів з оптимізації прийняття управлінських рішень у бік створення та розвитку самого процесу державного управління[3]. Однак, протягом останнього десятиріччя розвиток інформаційно-технічних засобів у державному секторі активізувався. Перед організаціями, підприємствами, установами (далі – установами) України державної форми власності все гостріше почали поставати завдання підвищення ефективності вже впроваджених механізмів керування документаційними процесами та надання електронних послуг, забезпечення їхньої більшої прозорості та доступності для громадян[4].

Класичним варіантом створення інформаційних систем переважної більшості установ в Україні була ситуація, коли обладнання закуповувалося не системно, а в міру надходження коштів. Зазвичай, першими комп'ютерами забезпечувалися керівники організацій, потім, відповідно до оновлення комп'ютерного парку, відбувалась низхідна ротація техніки – від керівників вищої до керівників середньої ланки та рядових працівників. У таких умовах було досить складно організувати роботу інформаційних систем організацій, оскільки поряд із сучасними персональними комп'ютерами використовувались уже застарілі системні блоки, які часто виходили з ладу, їхніх потужностей не вистачало для встановлення необхідного програмного забезпечення. Нерідко процес розвитку інформаційних систем установ ішов шляхом вирішення нагальних проблем: заміна комплектуючих системних блоків, копіювальної техніки, заміна чи заправка витратних матеріалів. Спрогнозувати виникнення їх при безсистемному підході до комплектування мережі робочими станціями і, відповідно, запланувати заходи щодо їхнього попередження було складно[5]. На це витрачалися основні матеріальні та людські ресурси установ, що забезпечували короткочасний, а тому й малоефективний результат. Через недостатнє фінансування рідко доходило до комплексного підходу до розвитку інформаційно-комунікаційних систем, що потребував значно більших капіталовкладень на початковому етапі, хоча в перспективі дозволив би отримати значно більший та триваліший позитивний ефект. Такий підхід передбачає моніторинг роботи системи, аналіз її загального стану на відповідність вимогам до діловодних процесів та підготовки документів до передавання на архівне зберігання, її апаратно-технічне і програмне забезпечення та вдосконалення на основі результатів проведеного аналізу отриманих даних.

Усвідомлення того, що без якісного інформаційно-технічного забезпечення ефективність виконання державними установами їхніх функцій у сучасному суспільстві є недостатньою, якраз і призвело до необхідності використання комплексного підходу до розвитку інформаційно-комунікаційних систем у державному секторі[6].

Нині, під час проектування інформаційно-комунікаційних систем, значна увага приділяється розробленню програмних продуктів. Це, переду-

сім, системи електронного документообігу, що оптимізують діловодство, системи обміну електронними документами між установами, так звані архівні модулі, які забезпечують в установах підготовку електронних документів до передавання на архівне зберігання, та веб-портали, котрі покращують взаємодію з громадянами тощо. Звичайно, це неможливо здійснити без активного впровадження серверних майданчиків, що забезпечують промислове використання цих програмних продуктів. Що ж до організації робочих місць користувачів системи, то, здебільшого, використовується класична модель, яка передбачає встановлення кожному користувачеві персонального комп'ютера з програмним забезпеченням та набором периферійних пристроїв, що забезпечують його роботу як у складі системи, так й автономно. Ці прилади об'єднуються в мережі для взаємодії між собою та серверами, однак такий підхід не забезпечує повного використання обчислювальних ресурсів робочих станцій. До зазначених ресурсів відносяться дискова та оперативна пам'ять, обчислювальні можливості мікропроцесорів тощо.

Для отримання максимального ефекту від апаратно-технічної складової інформаційно-комунікаційної системи пропонується використання іншого підходу до організації робочих місць користувачів, який передбачає концентрацію в одному місці всіх обчислювальних ресурсів. Для цього створюється термінальна система, в якій загальні ресурси концентруються на термінальному сервері. Кожний користувач, підключившись до такого сервера, отримує можливість виконувати операції із створення та опрацювання інформації на самому сервері. На робочому місці відображається лише результат виконання команд користувача сервером, тоді як всі дії зі створення, видалення, редагування інформації виконуються з використанням обчислювальних ресурсів сервера. Таким чином, користувач отримує у своє розпорядження стільки ресурсів, скільки йому потрібно для виконання конкретного завдання[7].

Цей підхід набув широкої популярності в комерційному секторі[8]. Зокрема, дуже популярною є концепція хмарних обчислень, яка дає змогу користувачам, наприклад, через мережу Інтернет, отримати доступ до програмних засобів, що використовують ресурси віддалених серверів. Згідно з таким принципом побудовані сервіси Google docs та Google drive, де за допомогою веб-інтерфейсу кожному користувачеві надається доступ до місця для створення власних електронних інформаційних ресурсів: створення та збереження текстових та аудіовізуальних документів, баз даних тощо[9]. Всі дії виконуються з допомогою програмних засобів, які надає Google в режимі он-лайн через веб-інтерфейс, та не потребує встановлення на персональний комп'ютер користувача.

Отже, якщо приватний сектор вже повною мірою використовує переваги термінальних систем та надає на їхній основі різноманітні електронні послуги суспільству, то у державному вони ще не набули достатнього поширення. Термінальні системи могли б бути використані для надання електронних послуг населенню, при створенні робочих місць діловодів та архівістів, в роботі читальних залів тощо.

Найбільш усталеним визначенням термінальної системи є таке: це – інформаційно-комунікаційна система, в якій створення, опрацювання та зберігання інформації здійснюється на віддаленому термінальному сервері[10]. Агрегація* обчислювальних потужностей в одному місці і є основною відмінністю від інформаційно-комунікаційних систем побудованих на персональних комп'ютерах.

Проаналізуємо запропоновану модель інформаційно-комунікаційних систем.

Робота користувача в такій системі організовується через тонкого клієнта (спеціалізований пристрій, який не має жорсткого диска, використовує для завантаження або мережевий інтерфейс, або спеціалізовану локальну операційну систему, одним із завдань якої є організація сесії з термінальним сервером для роботи користувача, не має у своєму складі рухомих деталей, виконується в спеціалізованих корпусах із повністю пасивним охолодженням)[11], який за допомогою мережевого інтерфейсу підключається до термінального сервера та слугує засобом введення-виведення інформації.

На створення тонкого клієнта слід звернути окрему увагу, адже він має низку значних переваг перед стандартним системним блоком. Особливості будови промислових моделей тонких клієнтів (це не стосується системних блоків, що використовуються як тонкі клієнти) обумовлені покладеними на них функціями. Використання файлової системи сервера для збереження користувацької інформації та файлів операційної системи призводить до того, що тонкі клієнти не містять власних носіїв енергонезалежної пам'яті

* Агрегація (лат. *aggregatio* – приєднання) – процес об'єднання елементів в одну систему.

(жорсткі диски, usb-накопичувачі тощо). Окремим випадком є встановлення на тонкому клієнті незначного обсягу енергонезалежної пам'яті для запису в неї спеціальної версії операційної системи з обмеженим функціоналом, за допомогою якої відбувається підключення тонкого клієнта до термінального сервера. Опрацювання інформації на стороні термінального сервера призводить до того, що тонкий клієнт використовує власні обчислювальні потужності (процесор та оперативну пам'ять) лише на етапі завантаження та підключення до сервера терміналів. За таких обставин у виробників тонких клієнтів немає необхідності комплектувати свої пристрої потужними процесорами та оперативною пам'яттю значного обсягу. Малопотужні процесори та оперативна пам'ять невеликого обсягу, а також повна або часткова відсутність пристроїв енергонезалежної пам'яті дає могу використовувати в тонких клієнтах лише пасивне охолодження. Це дозволяє підтримувати необхідний температурний режим роботи тонкого клієнта без використання вентиляторів, які створюють шум, характерний для роботи персонального комп'ютера.

Завдяки підвищеному інтересу до термінальних систем серед комерційних організацій є багато програмних засобів, за допомогою яких можна розгорнути та обслуговувати інформаційно-комунікаційні системи на базі терміналів. Однак, усі вони зводяться до одного принципу – на тонкому клієнті відбувається початкове завантаження для ініціалізації обладнання, після чого він, за допомогою мережевого інтерфейсу, автоматично зв'язується з термінальним сервером, який надає йому у користування копію ядра операційної системи. За допомогою мережевих протоколів ядро завантажується на тонкий клієнт та підключається файлова система. Між термінальним сервером та тонким клієнтом встановлюється робоча сесія, під час якої команди, введені на клієнті, передаються для виконання на сервер, а назад повертаються результати виконання даних команд, що відображаються на терміналі. З цього моменту тонкий клієнт використовує файлову систему термінального сервера та його обчислювальні потужності як свої власні.

На ринку інформаційних технологій представлені рішення, які по-різному автоматизують процес розгортання термінального сервера та встановлення зв'язку між ним і термінальними клієнтами. Вони, залежно від ступеня автоматизації процесу та подальшої підтримки, поділяються на комерційні та безкоштовні. Комерційні створюються на основі пропрієтарного програмного забезпечення, наприклад, Microsoft Windows Terminal Server[12]. Безкоштовні базуються на вільному програмному забезпеченні, наприклад, Linux Terminal Server Project[13]. Зазначений ринок апаратно-програмних рішень також пропонує послуги низки організацій з проектування та впровадження в промислову експлуатацію термінальних систем та їх подальшого супроводу, що базуються як на комерційному, так і на вільному програмному забезпеченні.

До переваг тонких клієнтів відносять наступне:

– Відсутність механічних деталей. Найчастіше в комп'ютерній техніці виходять з ладу комплектуючі, які в своїй конструкції мають рухомі частини. Як правило, це жорсткі диски, вентилятори охолоджувальної системи, оптичні приводи тощо. В тонких клієнтах такі пристрої відсутні з описаних вище причин. Тому середній термін експлуатації для кожного пристрою за заявами їхніх виробників складає близько 8 років. Із тих же причин тонкі клієнти відносяться до систем з низьким енергоспоживанням.

– Простота адміністрування. Внаслідок того, що тонкі клієнти використовують операційну систему та програмне забезпечення термінального серверу, немає необхідності фізичного доступу до тонких клієнтів для встановлення програмного забезпечення чи додаткового налаштування операційної системи. Процес інсталяції (встановлення) та оновлення програмного забезпечення здійснюється тільки на термінальному сервері, а не на кожному робочому місці.

– Збереження інформації. Вихід із ладу термінального клієнта, наприклад, внаслідок збою в електромережі, мережевого устаткування чи фізичного впливу, не спричиняє втрату даних, адже внаслідок їх опрацювання та збереження на термінальному сервері користувачу достатньо просто відновити роботу, наприклад, пересівши за інший термінальний клієнт, у якому налагоджено електропостачання, мережеве підключення тощо. При відновленні робочої сесії користувач отримає доступ до опрацьованої інформації точно в тому ж вигляді, що і до припинення роботи сесії. Відсутність ризику втрати даних при знеструмленні мережі позбавляє необхідності комплектувати тонкі клієнти дорогими джерелами безперебійного живлення.

– Питання безпеки. Системний адміністратор має можливість керувати політиками доступу до інформації та встановлених програмних додатків централізовано, через термінальний

сервер. Збереження інформації в одному місці дає змогу ефективніше проводити резервне копіювання користувацьких даних, що підвищує надійність та швидкість їхнього відновлення. Крім того, підвищений рівень захисту досягається завдяки тому, що навіть при фізичному доступі до тонкого клієнта неможливо отримати фізичний доступ до файлів операційної системи, адже вони розміщуються на сервері. Це означає, що неможливо внести зміни у файли конфігурації системи для отримання привілейованих прав користувача чи важливої інформації, доступ до якої обмежений.

– Гнучка функціональність. Здебільшого значний функціонал персональних комп'ютерів або не потрібний, або може використовуватись не для виробничих цілей (наприклад, пристрої зчитування оптичних дисків можуть бути використані як для завантаження користувацьких даних, так і для завантаження з оптичного диску операційної системи, відмінної від встановленої з правами суперкористувача, що дає змогу повністю контролювати персональний комп'ютер). Зазвичай, на тонких клієнтах присутній лише мережевий інтерфейс, який використовується для підключення до термінального сервера та інших мережевих пристроїв (наприклад, мережевих принтерів), присутніх в мережі.

– Простота масштабування. Завдяки особливостям функціонування термінальної системи, підключення нових тонких клієнтів регламентується лише створенням нових облікових записів на термінальному сервері й політик доступу до інформації та програмного забезпечення. Відсутність необхідності встановлення на кожному робочому місці операційної системи, драйверів, програмних продуктів, необхідних для виконання користувачем поставлених завдань, забезпечує легкість та швидкість розгортання нових робочих місць. Звичайно, за умови достатньої потужності термінального сервера. Якщо потужності для обслуговування нових тонких клієнтів не вистачає, то необхідна його модернізація.

– Плавний перехід. На початковому етапі переходу до термінальної системи можливе використання застарілих системних блоків, обчислювальних потужностей яких уже не вистачає для виконання завдань, що вирішуються в установі, але достатньо, щоб підключитись до термінального сервера та виконувати функції тонкого клієнта. Перевага можливості плавного переходу до термінального доступу, коли кошти виділяються поетапно і спочатку розгортається термінальний сервер, а застарілі робочі станції матимуть можливість працювати з новими додатками та операційними системами в термінальному режимі, є особливо актуальною саме для державних установ. Однак, це має бути тимчасовим рішенням, адже процес виходу з ладу застарілих системних блоків, що виконують функції тонких клієнтів, не зупиниться внаслідок фізичного старіння та зношування складових цих блоків.

– Економічна ефективність. Порівняно з персональними комп'ютерами тонкі клієнти мають меншу закупівельну вартість. Також, внаслідок відсутності рухомих деталей, вони використовують значно менше електроенергії, за наявною статистикою майже не виходять із ладу, а отже не потребують ремонту і, як зазначалося вище, мають довший строк експлуатації. Внаслідок використання обчислювальних ресурсів термінального сервера моральне старіння тонких клієнтів майже не впливає на їхню працездатність. При необхідності модернізації обладнання не потрібно купувати нові деталі на кожне робоче місце, а тільки достатньо здійснити модернізацію термінального сервера, щоб підвищити ефективність тонких клієнтів відповідно до поточних потреб. Тонкі клієнти займають значно меншу площу. При використанні пропрієтарного програмного забезпечення вартість ліцензування, у перерахунку на одне робоче місце, буде нижчою, ніж якби купувалися повноцінні операційні системи. Внаслідок відсутності власної енергонезалежної пам'яті та розміщення всієї інформації на сервері терміналів, ризик втрати інформації у разі фізичного пошкодження або викрадення тонкого клієнта відсутній.

До недоліків тонких клієнтів та побудованих на їхній основі термінальних систем відносять наступне:

– брак енергонезалежної пам'яті, потужного мікропроцесора та оперативної пам'яті не дають змоги працювати користувачам системи без підключення до термінального сервера;

– до термінального сервера підвищуються вимоги щодо продуктивності, адже його ресурсами мають користуватись десятки або й сотні тонких клієнтів;

– до термінального сервера та мережевого обладнання зростають вимоги щодо відмовостійкості, адже при виході з ладу хоча б одного із вищезазначених компонентів усі тонкі клієнти втратять можливість функціонування;

– до термінального сервера підвищуються вимоги щодо захищеності, адже на його дисковому просторі зберігається інформація всіх користувачів;

– відсутня можливість встановлення індивідуального програмного забезпечення, операційної системи на окремі тонкі клієнти. Термінальна система надає доступ до операційної системи та набору програмного забезпечення, стандартного для всіх користувачів. При такому підході індивідуальні побажання користувачів до встановлення програмного забезпечення виключаються, якщо якийсь продукт встановлюється, він стає потенційно доступним усім користувачам термінальної системи. Виключення можуть бути лише при забороні доступу окремих користувачів за допомогою політики безпеки. Хоча, на наш погляд, це не є недоліком, адже дозволяє формалізувати перелік програмних засобів, які використовуються в установі;

– зручність адміністрування, яка полягає в централізованості всіх налаштувань на термінальному сервері, несе за собою і небезпеку того, що будь-яка помилка адміністратора в конфігурації операційної системи чи програмного засобу вплине на роботу не окремих користувачів, а відразу всіх користувачів системи.

Використання термінальної моделі побудови інформаційно-комунікаційних систем може бути доречною при дотриманні певних умов. Економічна доцільність такого рішення залежить від кількості робочих місць у майбутній інформаційно-комунікаційній системі, адже термінальна модель системи, на відміну від класичної клієнт-серверної моделі, відрізняється наявністю додаткового сервера терміналів. Вартість сервера терміналів повинна компенсуватися розгортанням достатньої кількості тонких клієнтів, вартість придбання та обслуговування яких є меншою від вартості придбання та обслуговування персональних комп'ютерів. Також, економічний ефект напряму залежить від програмного забезпечення, що використовується для побудови термінальної системи. Звичайно, при використанні вільного програмного забезпечення цей ефект буде максимальним. Однак, слід пам'ятати, що розгортання термінальних систем на базі вільного програмного забезпечення більш трудомісткий процес, який вимагає від персоналу організації по роботі з інформаційними технологіями достатнього рівня кваліфікації для впровадження та подальшого обслуговування зазначених технологій.

Виходячи з переваг використання термінальної моделі, використання термінальних систем як основи при проектуванні інформаційно-комунікаційних систем саме для архівної галузі є досить перспективним. Це випливає з організації роботи в архівах, яка орієнтована на однотипну роботу кінцевих користувачів, спрямовану на обробку інформації, на централізоване її зберігання, з можливістю надання керованого доступу, та на специфічні вимоги, що ставляться перед робочими місцями, з яких цей доступ надається (місця в читальних залах тощо).

[1] *Тертична К. О.* Інформаційна складова соціально-економічного розвитку України // Вісник Бердянського університету менеджменту і бізнесу. – Бердянськ, 2011. – № 3. – С. 123–128.

[2] *Грипич С. Н.* Інформатизація сучасного суспільства: стан, проблеми, перспективи // Філософія. Педагогіка. Суспільство: зб. наук. пр. Рівнен. держ. гуманіт. ун-ту. – Рівне, 2012. – № 2. – С. 286–298.

[3] Україна – незалежна держава: проблеми становлення [Електронний ресурс]. – Режим доступу: http://ukr-history.com/ukrana_v_umovah_komandno-admnstrativno_sistemi_srsr_19451985rr-ukrana_nezalejna_derjava_problemi_stanovlennya.html. – Назва з екрана.

[4] Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27. – Ст. 182.

[5] *Рубан И. В., Бондарь В. И., Копытчук Н. Б.* Терминальные системы на базе GNU/LINUX // Труды Одесского политехнического университета. – Одесса, 2006. – № 1. – С. 85–87.

[6] *Резченко Є. О.* Організаційне забезпечення процесів інформатизації органів державної влади в Україні [Електронний ресурс] // Державне будівництво. – 2009. – № 2. – Режим доступу: http://www.nbuv.gov.ua/e-journals/Debu/2009-2/doc/1/08.pdf. – Назва з екрана.

[7] *Васютинський С. В.* Аналіз технології тонкий клієнт. Переваги та недоліки термінального доступу [Електронний ресурс] // Університет економіки і підприємництва, Україна. – Режим доступу: http://www.rusnauka.com/15_APSN_2011/Informatica/1_87881.doc.htm. – Назва з екрана.

[8] Amazon EC2 [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Amazon_EC2. – Загл. с экрана; Google Docs [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Google_Docs. – Загл. с экрана; Яндекс.Диск [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Яндекс.Диск. – Загл. с экрана.

[9] Огляд Диска Google [Electronic resource]. – Mode of access: https://support.google.com/drive/bin/answer.py?hl=uk&answer=2424384&ctx=cb&src=cb&cbid=qnu0mkhohuj2. – Title from screen.

[10] *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд. – СПб.: Питер, 2010. – 943 с.

[11] Тонкий клієнт [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Тонкий_клієнт. – Назва з екрана.

[12] Microsoft Server and Cloud Platform [Electronic resource]. – Mode of access: http://www.microsoft.com/en-us/

server-cloud/windows-server/virtual-desktop-infrastructure.aspx. – Title from screen.

[13] LTSP Linux server terminal projekt [Electronic resource]. – Mode of access: http://wiki.ltsp.org/wiki/Concepts. – Title from screen.

В статье сделан анализ метода построения информационно-коммуникационных систем на основе терминальной системы, определены позитивные и негативные стороны терминальных систем в целом и особенности их использования в государственных учреждениях Украины, очерчены перспективы внедрения терминальных систем при создании информационно-коммуникационных систем в архивной отрасли.

Ключевые слова: процесс информатизации, информационно-коммуникационная система, терминальная система, терминальный сервер, тонкий клиент, информационная безопасность.

This article analyzes the method of creation information-communication systems based on terminal system. Identify positive and negative aspects of terminal systems in general and of the use in states institutions of Ukraine. Determined by the prospects of using terminal systems to create information - communication systems in the archives of Ukraine.

Key words: informatization process, information-communication system, terminal system, terminal server, thin client, information security.

УДК [005.92:004.63]: 681.188

Вадим Малиновський

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИПТОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Розглянуто особливості застосування програмної та апаратної реалізації криптографічних засобів захисту електронних документів відповідно до вимог законодавчої бази України щодо захисту електронних документів, окреслено перспективи розвитку криптографічних засобів захисту електронного документообігу.

Ключові слова: системи електронного документообігу, електронний цифровий підпис, криптографічні засоби захисту електронних документів.

Нині майже не існує систем електронного документообігу, які б не містили засобів криптографічного захисту інформації (далі – КЗІ), зокрема засобів, що дають змогу використовувати в електронному документообігу електронний цифровий підпис. Слід зазначити, що й сам електронний цифровий підпис отримують за результатом криптографічного перетворення набору електронних даних, як визначено у ст. 1 Закону України «Про електронний цифровий підпис»[1].

Однак, як для суб'єктів захисту електронних документів, так і для розробників засобів криптографічного (далі – криптозасобів) захисту їх ще й дотепер не вирішено низку проблем:

– створення об'єктивної, оптимальної системи оцінок безпеки електронних документів та криптографічної стійкості засобів шифрування і електронного цифрового підпису;

– вдосконалення методів та способів ефективної апаратної і програмної реалізації криптографічних алгоритмів;

– розробка високоефективних систем криптоаналізу для дослідження сучасних систем криптозахисту даних[2];

– створення інформаційних систем у державних архівах та формування підходів і вимог до забезпечення їхньої безпеки.

Метою статті є аналіз сучасних криптозасобів захисту електронних документів, а саме – їх шифрування, накладання електронного цифрового підпису, та визначення перспективних напрямів дослідження зазначених методів і засобів захисту електронного документообігу.

Безсумнівно, основним позитивним показником засобу КЗІ є його криптостійкість, але в більшості практичних завдань при виборі криптографічних алгоритмів особливий інтерес становляють не тільки кількісні показники їхньої ефективності, а й функціонування у різних критичних умовах – загрозах, спектр яких при сучасних досягненнях науки та техніки може бути дуже широким.

Засоби КЗІ можуть мати апаратний, програмно-апаратний, або програмний спосіб реалізації. А тому низка критеріїв – надійність, якість, продуктивність та ін. – залежатиме від способу