УДК 681.3.06

Головань С.М., Мелешко О.О., Щербак Л.М.

КОНЦЕПЦІЯ СТВОРЕННЯ СИСТЕМИ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Вступ

З давніх часів людство передавало свої знання із покоління в покоління. Вся отримана і створена інформація відповідним чином фіксувалась. Матеріальні носії, що містять у зафіксованому вигляді інформацію, оформлену у заведеному порядку, є документи. Документи виконують офіційну, ділову і оперативну функції, оскільки вони – письмовий доказ, джерело відомостей. Із віку в вік не було цінності більшої, чим документи. Наш вік – вік інформаційних технологій, інформаційно-телекомунікаційних систем і інформаційних систем управління у різних галузях народного господарства України. Проблеми створення, обробки, передавання, одержання, зберігання, використання та знищення документів встають на новий, більш якісний рівень. З прийняттям законів „Про електронні документи та електронний документообіг", „Про електронний цифровий підпис" та ряд інших директивних документів, в тому числі стандарт ДСТУ 4145-2002 на електронний цифровий підпис [1...3]. Сучасні документи не тільки носії інформації, але ще мають властивість губитися, не виконуватися в строк та ставатися все більше вразливими з різних причин, а саме:

– збільшується обсяг збережених і переданих документів з обмеженим доступом;

– збільшується коло користувачів, які мають доступ до ресурсів інформаційної системи і документам;

– ускладнюється режим експлуатації інформаційних систем.

Тому все більшу важливість набуває проблема захисту інформації з обмеженим доступом від несанкціонованого доступу під час підготовки та зберігання документів. Суть цієї проблеми – постійна боротьба спеціалістів по захисту інформації з обмеженим доступом із своїми „опонентами".

В даній роботі розглянуті основні положення створення електронних документів та захист інформацію з обмеженим доступом, що міститься в них.

Електронний документ

Закон України „Про електронні документи та електронний документообіг" встановлює основні організаційно-правові засади використання електронних документів.

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які містять, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами – обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили, у тому числі з електронно цифровим підписом автора. Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора або підписувала електронного документа іншими суб'єктами електронного документообігу.

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором (фізична або юридична особа, яка створила електронний документ) створюються ідентичні за документальною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу.

Впровадження інформаційних технологій обробки документів повинен здійснюватися

фахівцями у даній сфері, оскільки будь-яка управлінська діяльність, а особливо діяльність фахівців які здійснюють обробку документів з обмеженим доступом, потребує знань як в системі документообігу, так і стосовно новітніх технологій обробки і захисту інформації з обмеженим доступом. Обробку документів в системі доцільно поділити на модулі, один для введення і редагування переліку користувачів, інші для реєстрації документів, проведення щоденних перевірок тощо [4]. Схему алгоритму створення електронного документа ілюструє рис. 1.

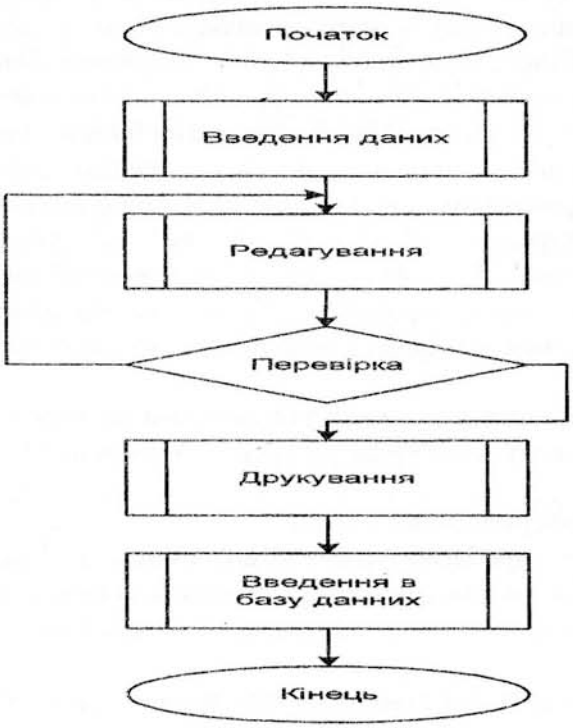

Рис. 1. Схема алгоритму створення електронного документа

Кожний електронний документ в процесі свого життєвого циклу проходить різні стадії і попадає до свого виконавця в різних якостях. Загальну модель життєвого циклу електронного документа ілюструє рис. 2.

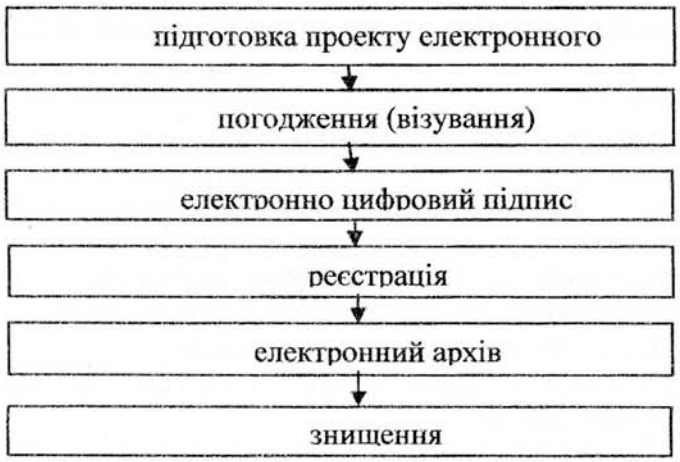

Рис. 2. Загальна модель життєвого циклу електронного документа

На етапі створення електронного документа, він не має юридичної сили, а є проектом електронного документа. Після того як документ створений – погоджений (завізований),

підписаний (затверджений) проект стає документом, наданням електронного підпису завершується створення електронного документа, і з цього моменту і до кінця життєвого циклу він має юридичну силу.

Електронний архів – система призначена для фізичного зберігання електронних документів та їх пошуку. Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері. Зберігання документів здійснюється або в файловій системі, або в базі даних інформаційної системи. Пошук документів повинен здійснюватися, як за реквізитам, так і за документальною інформацією.

Концепція безпеки інформації з обмеженим доступом в електронному документі

Концепція базується:

– на створенні єдиної інформаційної системи документообігу в межах одної організації системи організацій міністерства, відомства на організаційно-правових засад електронного документообігу з використання електронних документів на основі упорядкованої системи документування управлінської діяльності;

– сучасних інформаційно-телекомунікаційних та інформаційних системах;

– класифікація інформаційних потоків на відкриті та з обмеженим доступом;

– ієрархічної структури системи для реалізації різних форм обмеження доступу до інформації (конфіденційної та таємної інформації);

– відповідних технічних та нормативних методів захисту інформації з обмеженим доступом.

Комплексна система захисту інформації повинна представляти сукупність правових (законодавчих), організаційних і технічних засобів та норм, направлених на попередження або унеможливлення нанесення збитків інтересам авторів електронного документа.

Політику безпеки інформації в інформаційній системі і її складових частинах визначає автора (користувача інформаційної системи).

Об'єктами захисту в інформаційній системі і її складових частинах є:

– документація і інформаційні процеси в інформаційних системах;

– інформація про інформаційну систему і її елементи;

– управляючі процеси в інформаційній системі;

– ресурси інформаційної системи і її складових частин (засоби зв'язку і управління, інформаційно-програмне забезпечення, лінії зв'язку тощо).

Циркулюючі в інформаційній системі електронні документи і інформація по забезпеченню функціонування системи (підсистеми, елемента), як об'єкти захисту, мають різний статус:

– відкрита інформація;

– інформація з обмеженим доступом (конфіденційна і таємна інформація. До таємної інформація належить інформація, що містить відомості, які становлять державну таємницю, а також інша передбачена законом таємницю).

Щоб гарантувати безпеку інформаційній системі, необхідно застосовувати таке програмне забезпечення, яке дозволяє пересвідчитися у відсутності елементів, що уможливлюють дистанційний контроль за роботою системи, або несанкціоноване зняття інформації. Саме тому код програми повинен бути доступним під час перевірки, оскільки знання його усуває ризик застосування програм, до яких вбудовано інші програми (підпрограми). Відкрите (вільне) програмне забезпечення дозволяє повну і всеосяжну інспекцію механізмів за допомогою яких таке програмне забезпечення обробляє дані, усебічно вивчити програму – чудовий механізм безпеки.

Відкрите програмне забезпечення дозволяє:

– використання програм для будь-якої мети;

– безперешкодний доступ до програмного коду або набору інструкцій;

– будь-яке вивчення механізмів (принципів) функціонування програм;

– можливість використання механізмів (принципів) функціонування і будь-яких

довільних частин коду програми (програм, програмних комплексів) для створення інших програм або адаптації до власних потреб;

– можливість зміни і вільного поширення як оригінальної програми так і зміненої, за тими ж умовами, під які підпадає і оригінальна програма.

По появі і положенню джерела виникнення загроз відносно складових частин інформаційної системи і її елементів загрози групуються в класи. В свою чергу класи загроз включають сукупність загроз, згруповані по каналам реалізації. Виходячи з переліку можливих загроз, комплексна система захисту інформації інформаційної системи повинна забезпечити [5]:

– цілісність електронних документів на всіх етапах її обертання при любих загрозах;

– підтвердження справжності електронних документів на всіх етапах їх обробки при усієї безлічі потенційних загроз;

– скритність інформації з обмеженим доступом яка циркулює в інформаційній системі;

– захист від несанкціонованого доступу до захищеної інформації і ресурсів інформаційної системи;

– організаційно-технічні засоби захисту інформації з обмеженим доступом від витоку.

Реалізація функцій і задач комплексної системи захисту інформацій з обмеженим доступом в інформаційній системі може забезпечуватися комплексним використанням методів і засобів криптографічного і технічного захисту інформації з обмеженим доступом.

Комплекс правових (законодавчих), організаційних (адміністративних), технічних і фізичних засобів, що реалізують функції і задачі комплексної системи захисту інформації в інформаційній системі, повинен забезпечувати:

– попередження появи загроз;

– виявлення появи загроз;

– попередження впливу загроз на інформаційну систему;

– виявлення впливу загроз на інформаційну систему;

– локалізацію впливу загроз на інформаційну систему;

– ліквідацію наслідків впливу загроз на інформаційну систему.

Забезпечення безпеки інформації в складових частинах та інформаційній системі в цілому повинен здійснюватися комплексом правових (законодавчих), організаційних (адміністративних), технічних і фізичних засобів, реалізуючих наступні методи забезпечення безпеки:

– перешкоду (фізична перешкода шляху);

– управління доступом (регулювання використання всіх ресурсів інформаційної системи);

– маскування (закриття змісту електронного документа криптографічними засобами);

– регламентація (створення умов, мінімізуючи умови несанкціонованого доступу до електронних документів);

– примушення (дотримання встановлених правил використання ресурсів системи у тому числі документів під загрозою відповідальності);

Забезпечення безпеки інформації в інформаційній системі може бути ефективним тільки в тому випадку, коли захист інформацій з обмеженим доступом буде представляти собою безперервний і цілеспрямований процес, постійно здійснений на всіх етапах життєвого циклу документа. Так комплексна система захисту інформації інформаційної системи крім функцій, задач і засобів власне забезпечення захисту документів повинна включати функції, задачі і засоби управління в якості одного із основних компонентів.

Комплексна система захисту інформації інформаційної системи та її складових повинна реалізуватися на принципах:

– системності;

– комплектності;

– адекватності;

– функціональній самостійності;

– зручності користування;
– обмеження доступ до інформації ;
– повний контроль за роботою інформаційної системи;
– своєчасне реагування на появу загроз;
– економічності.

Висновки

Наведений матеріал є частиною теоретичної методології підготовки і розробки відкритих та з обмеженим доступом електронних документів. Представлено методологічні основи концепції безпеки інформації з обмеженим доступом в електронному документі.

Список літератури

1. Закон України „Про електронні документи та електронний документообіг". Закон України від 22.05.03 № 851-IV // Відомості Верховної Ради України. – 2003. – № 35. – Ст. 275.

2. Закон України „Про електронний цифровий підпис". Закон України від 22.05.03 № 852-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276.

3. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах". Закон України від 11.05.43 № 1703-IV // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

4. *Головань С.М., Давиденко А.М., Душеба В.В., Щербина В.П.* Підвищення ефективності процесу діловодства / Науково-технічний журнал „Захист інформації", –2004.– № 1. – С. 66-71.

5. *Бондаренко М.Ф., Черных С.П., Горбенко И.Д.* и др. Методологические основы концепции и политики информационных технологий // Радиотехника: Всеукр. межвед. науч-техн. сб. 2001. Вып. 119. С.5-16.

Надійшла 19.01.2005р.

УДК 621.396.96

Ксендзук А.В.

КОДОВЫЕ СИГНАЛЬНЫЕ ГРУППЫ В МНОГОПОЗИЦИОННЫХ СИСТЕМАХ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ

Постановка задачи и связь с научными и практическими задачами.

Одной из наиболее важных задач в многопозиционных системах с синтезированием апертуры антенны (МПРСА) является обеспечение высоких энергетических отношений сигнал/помеха, которое необходимо для эффективного комплексирования. Фактором, оказывающим существенное влияние на энергетические показатели системы, является степень ортогональности пространственно-временных процессов в различных приемных элементах.

Количественно степень ортогональности можно определить с помощью величины межканальной помехи на выходе оптимального устройства обработки. Использование различных групп сигналов позволяет уменьшить межканальные помехи в МПРСА. В данной работе рассмотрено использование кодовой группы сигналов, - сигналов, отличающихся комплексной огибающей. Такой ансамбль сигналов обеспечивает высокую степень защиты данных систем ДЗ, высокую помехозащищенность и скрытность. Однако при этом происходит существенное повышение взаимных помех в системе дистанционного зондирования, которые должны быть уменьшены путем оптимизации вида сигналов и выбором пространственной конфигурации элементов МПРСА.

Анализ публикаций и исследований по данной теме.

Вопрос о необходимости использования групп сигналов, позволяющих эффективно