Увеличение плотности записи вызывает появление ошибок чтения данных, и производители HDD стали применять сложные корректирующие коды, исправляющие пакеты многократных ошибок. Типичный привод может иметь в каждом секторе 512 байт данных, 4 байта CRC и 11 байт корректирующего кода (ECC). Такой корректирующий код способен исправлять одиночные пакетные ошибки длиной до 22 бит, двойные пакетные ошибки длиной до 11 бит и обнаруживать одиночные пакетные ошибки длиной до 51 бит [1].

Поэтому, даже если некоторые данные гарантировано удалены, существует теоретическая возможность их восстановления, используя возможности коррекции ошибок.

Выводы

С развитием методов записи информации на HDD развиваются и методы восстановления потерянных (удаленных) данных. Поэтому актуальной задачей является осознание особенностей хранения важных данных на HDD, резервирования их, а также осознание надежного удаления их с магнитного носителя.

Список литературы

1. Gutmann, Peter. Secure Deletion of Data from Magnetic and Solid-State Memory. University of Auckland, 1996.

2. Upgrading and repairing PCs. Tenth Anniversary Edition. Scott Mueller, Craig Zacker. Que Corporation, 1998.

Поступила 1.11.2004г.

УДК 681.3.06

Головань С.М., Давиденко А.М., Мелешко О.О.,
Щербак Л.М., Щербина В.П.

СТВОРЕННЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Вступ

На сьогодні впровадження інформаційних технологій, інформаційно-аналітичних систем і інформаційних систем, управління у різні галузі народного господарства України є важливою і актуальною науково-технічною проблемою. У 2003 році прийняті закони „Про електронні документи та електронний документообіг", „Про електронний цифровий підпис". Введено в дію ряд інших директивних документів, в тому числі стандарт ДСТУ 4145-2002 на електронний цифровий підпис [1...3]. В даній роботі розглянуті основні проблеми створення системи електронного документообігу, які також є актуальними та важливою складовою комплексного вирішення державних науково-технічних проблем. Застосування механічних і електричних друкарських машинок, на сьогодні інформаційні (автоматизовані) системи (організаційно-технічна система, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється) стали відповідними етапами розвитку систем документообігу.

Прийнято вживати два поняття – діловодство та документообіг. Відмітимо, що поняття діловодство (цей термін з'явився в другій половині XVIII ст.) позначало діяльність, якою займалась не тільки і не стільки канцелярія, скільки весь апарат підприємства, установи, організації в цілому. Термін „діловодство" походить від словосполучення слів „ведення діл", а під „ділом" в той час розумілась не папка з документами, як в сучасному значенні цього слова, а розгляд і вирішення питання, „ведення діл" (виробництво справ) – це не що інше, як вирішення справи. Оскільки всяке вирішення передбачає його письмову фіксацію на всіх стадіях, то природно, діловодство розумілось і як „правила, якими канцелярія керувалась в складанні доповідних записок, ведення журналів обліку паперів, визначень та актів взагалі, і виконання паперів". В свою чергу документообіг – переміщення

(рух) документів на підприємстві в установі та організації з моменту їх отримання чи створення і до завершення виконання чи відправки.

Автоматизація діловодства – це процес впровадження новітніх інформаційних технологій для заміни паперового документообігу електронним документообігом (сукупність процесів створення, оброблення, відправлення, передання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержанням таких документів) з метою підвищення швидкості реєстрації та контролю виконання документів (повідомляється про приближення строку виконання), зберігання документів в інформаційній системі, підтримуються шаблони документів, здійснюється пошук документів, автоматично формується реєстр на відправку документів, ведеться класифікація документів (по типу, виду тощо), ведуться справи документів, відправлення документів до справи, передача справи на зберігання до архіву, складаються необхідні звіти (річний звіт по діловодству) тощо. Будь-яке фундаментальне технічне або технологічне нововведення, надаючи можливості для розв'язання одних проблем і відкриваючи широкі перспективи їхнього розвитку, завжди викликає загострення інших або породжує нові, раніше невідомі проблеми, стає для суспільства джерелом нових потенційних небезпек. Якщо належною мірою не подбати про нейтралізацію супутніх процесів негативних факторів, то ефект від упровадження новітніх досягнень науки і техніки може виявитися негативним. Іншими словами, без належної уваги до питань забезпечення безпеки наслідки переходу до новітніх технологій документообігу можуть бути тупіковими.

Задачі системи електронного документообігу

Наведемо спрощену структурну схему системи електронного документообігу, яка зображена на рисунку 1.

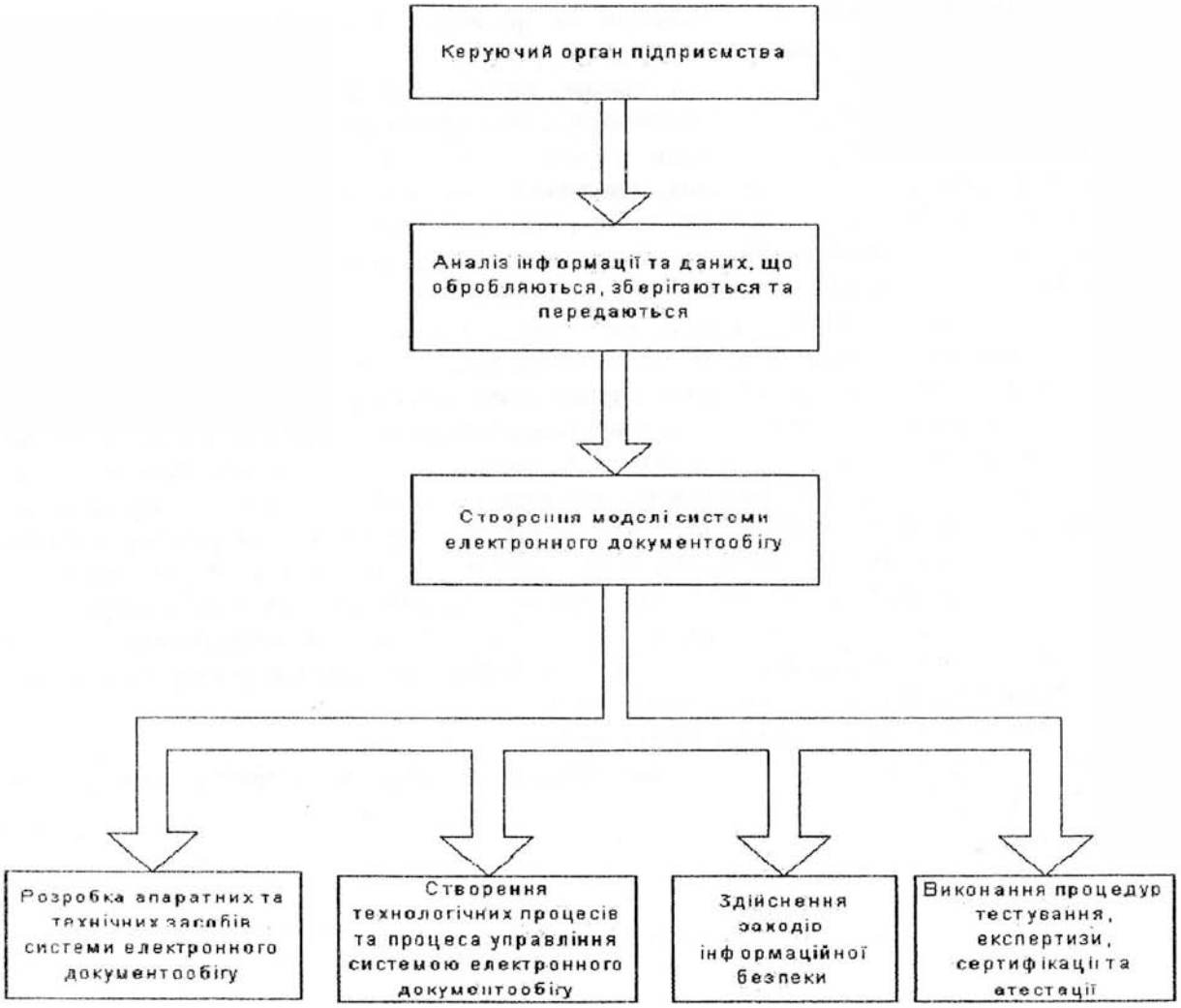

Рис. 1. Спрощена структурна схема системи електронного документообігу

Зупинимось більш детально на основних проблемах створення системи електронного документообігу.

Електронний документообіг повинен здійснюватися на основі упорядкованої системи документування управлінської діяльності, а її засоби повинні бути сумісними і передбачати можливість їх об'єднання в єдину систему.

Склад програмного забезпечення і засобів, що використовуються для електронного документообігу та безпека інформації з обмеженим доступом, залежить від конкретних умов роботи апарату управління з документами, зокрема від структури управління, його розміщення, умов праці працівників, кількості і змісту документів, грифу обмеження доступу до документів, потреб в оперативній і ретроспективній інформації, ступеня централізації робіт з документами тощо.

Фундаментальну роль у забезпеченні безпеки електронного документообігу відіграє політика безпеки інформації з обмеженим доступом. Політика безпеки це основа створення та ефективного функціонування комплексної системи захисту інформації в інформаційній системі. Відсутність добре продуманої політики безпеки приводить до відсутності методологічного та організаційного фундаменту забезпечення безпеки інформації та інших цінних ресурсів інформаційної інфраструктури системи інформаційних технологій, автоматизованих систем, а також до безсистемності розв'язання задач захисту інформації з обмеженим доступом.

При розгляді проблеми забезпечення безпеки інформації з обмеженим доступом в інформаційній системі необхідно виходити з того, що існують дві основні протиборчі сторони – власник інформації в інформаційній системі, що має певну цінність і вимагає її захисту, і порушник (неавторизований користувач), який має мотиви і можливість для незаконного використання інформації, що може привести до нанесення збитків (морального, матеріального, економічного тощо) власнику інформації. Третьою, незалежною стороною, основними задачами якої є розгляд суперечок між користувачами інформаційної системи, перш за все коли один із них є внутрішнім порушником, а також між користувачами та власником інформації та ресурсів. Крім того, третя сторона може бути як довіреною стороною, так і порушником.

За збереження ресурсів відповідає її власник, яким в більшості випадків є органи державної влади, органи місцевого самоуправління, підприємства, установи і організації для яких ці ресурси мають цінність. У такому випадку ресурси може розглядатися як активи. Безпека інформаційної системи пов'язана перш за все із захистом інформаційних ресурсів системи. Необхідно чітко розуміти, що інформація (інформаційний ресурс) – це найбільш цінний актив власника інформаційної системи.

Під ресурсами слід розуміти, в широкому розумінні, все, що має цінність з токи зору власника інформаційної системи. Виділяють наступні класи ресурсів:

– обладнання інформаційної системи (фізичні ресурси);

– інформаційні ресурси (бази даних, файли, дані, що передаються каналами зв'язку, всі види документів);

– програмне забезпечення (системне, прикладне, утиліти, інші допоміжні програми);

– сервіс та підтримуюча інфраструктура (забезпечення необхідних умов експлуатації, енергопостачання тощо).

Порушник розглядається як джерело погроз безпеці інформації та ресурсам. Під погрозою будемо розуміти можливі події, дії (вплив), процес чи явище, реалізація яких може привести до нанесення збитку (втрат) власнику та користувачам ресурсів. Порушники мають певну зацікавленість у несанкціонованому використанні ресурсів інформаційної системи і прагнуть їх використати, незважаючи на інтереси власника. Власник ресурсів повинен сприймати подібні погрози як потенціал впливу на ресурси, що призводить до пониження їх цінності і до різних видів збитків для власника. Основними загрозами в інформаційно-телекомунікаційній системі є:

– загроза порушення конфіденційності інформації (ознайомлення з інформацією неавторизованими користувачами або процесами);

– загроза порушення цілісності інформації (несанкціонована модифікація інформації неавторизованим користувачем);

– загроза порушення доступності інформаційних ресурсів (порушення доступу до інформаційних ресурсів для користувачів, що володіють відповідними повноваженнями);

– загроза порушення спостережності (обмеження можливостей інформаційно-телекомунікаційної системи контролювати користувачів, процеси і пасивні об'єкти з метою забезпечення установленої політики безпеки).

Для забезпечення конфіденційності, цілісності і доступності інформації, а також спостережності інформаційної системи необхідно захищати інформацію не тільки від несанкціонованого доступу, але і виключити можливість негативного впливу на інформацію, втручання у процес її обробки, порушення працездатності інформаційної системи. Таким чином, захищати необхідно всі компоненти інформаційної системи: апаратуру та обладнання, програми, дані, персонал.

Процес виявлення погроз інформації, можливість їхнього здійснення для несанкціонованого впливу на інформацію повинен групуватися за такими критеріями:

– всі погрози поділяються на загрози, що визначаються природними та техногенними факторами. Природні фактори виникають внаслідок стихійних природних явищ та

об'єктивних фізичних процесів. Техногенні фактори є наслідком діяльності людини, технічних засобів і систем;

– техногенні фактори поділяються на випадкові і навмисні. Випадкові спричиняються помилками проектування інформаційної системи, збоями і відмовами апаратури та систем забезпечення, персоналу. Навмисні обумовлені цілеспрямованими діями порушників;

– за місцем розміщення джерела загроз відносно інформаційної системи, що реалізуються дистанційно і контактно. До дистанційних відносяться ті, джерело яких знаходиться за межами контрольованої зони. Контактні загрози здійснюються в межах контрольованої зони, як правило при проникненні у приміщення де розташовані засоби обробки та збереження інформації..

Власник інформаційної системи аналізує можливі загрози з метою виявлення, які з них дійсно мають місце у середовищі експлуатації системи. Як результат такого аналізу визначається ризик інформаційної безпеки. Аналіз може допомогти при виборі контрзаходів для протистояння погрозам та зниження ризиків до придатного рівня. Контрзаходи застосовуються для зменшення вразливості та реалізації політики безпеки власника ресурсів. Однак і після введення таких контрзаходів можуть зберігатися залишкові вразливості. Такі вразливості можуть використовуватися порушниками становлячи рівень залишкового ризику для актів. Власник ресурсів повинен мінімізувати цей ризик, задаючи додаткові обмеження.

Оцінка політика безпеки з точки зору її впливу на функціонування інформаційної системи у цілому, на досягнення поставлених цілей безпеки і розв'язання задач захисту, а також оцінити діяльність власника стосовно впровадження у життя положень політики безпеки і реалізації принципів забезпечення безпеки інформації необхідно оцінюівати: результативність, ефективність, адекватність, гнучкість, доцільність, здійсненність та простоту в адміністративному забезпеченні [4].

Результативність визначає, в якій мірі може і чи може взагалі впровадження політики безпеки та окремих її положень або правил привести до досягнення поставленої цілі безпеки та розв'язання визначених задач захисту.

Під ефективністю слід розуміти співвідношення результатів досягнутих за впровадження політики безпеки, і витрат, необхідних для досягнення цих результатів. Ефективність в основному вимірюється в грошовому еквіваленті. Основним підходом до визначення ефективності є підрахунок витрат на виконання комплексу організаційних заходів, проведення технічних робіт, закупку технічних та інших засобів, які мають безпосереднє відношення до захисту інформації з обмеженим доступом. Політика безпеки є ефективною, якщо вона досягає максимальної результативності за мінімальних затрат.

Адекватність визначає, що даний рівень результативності дійсно відповідає ситуації, яка склалася відносно існуючих погроз безпеці і задовольняє потребам власника інформаційних ресурсів відносно забезпечення безпеки інформації з обмеженим доступом. Політика безпеки є адекватною, якщо правила безпеки і рівень їх реалізації адекватні погрозам безпеки для даного об'єкту захисту і сприяє надійному запобіганню виявлених погроз та зниженню ризиків до придатного рівня.

Доцільність пов'язана із визначенням, чи є протиріччя між задачами і основними положеннями політики безпеки та загальними задачами об'єкту захисту. Доцільність уточнює питання, чи необхідні цілі безпеки і задачі захисту в конкретній системі чи нема протиріч між загальними задачами, що стоять перед нею.

Гнучкість пов'язана із оцінкою здатності політики безпеки задовольнити потреби власника інформаційних ресурсів у відношенні безпеки інформації в умовах обстановки, що змінюється. Політика безпеки повинна бути здатною адекватно реагувати на зміни умов функціонувати об'єкту інформації, зміни цілей і задач функціонування, інтересів і потреб власника інформаційних ресурсів. Політика безпеки називається гнучкою, якщо вона здатна задовольнити потреби в безпеці інформації з обмеженим доступом у будь-яких умовах функціонування інформаційної системи.

Здійсненність пов'язана із визначенням умов здійсненності конкретної політики безпеки в конкретних умовах при заданих обмеженнях у конкретній інформаційній системі. Вона враховує здійсненність політики безпеки і впровадження її на різних рівнях забезпечення безпеки інформації з обмеженим доступом і у зв'язку з цим має різні аспекти. Безпека інформації забезпечується на правовому, адміністративному процедурному і програмно-технічному рівнях. Таким чином необхідно розглядати здійсненність політики безпеки на цих рівнях.

На правовому рівні необхідно оцінювати політику безпеки з точки зору її легітимності. Чи можуть конкретні положення політики безпеки бути реалізовані на даному об'єкті з точки зору правового поля держави в області захисту інформації з обмеженим доступом.

Здійсненність політики безпеки на адміністративному рівні залежить від ступеня розуміння керівництвом цілей безпеки і задач захисту. Усвідомлення реальності погроз безпеці, реалізація яких може понести збитків, рівня сформованості потреб у розв'язанні таких задач захисту.

На процедурному рівні здійсненність політики безпеки залежить від ступеня технологічної і організаційної готовності об'єкта інформатизації до впровадження правил безпеки. Тут важливе місце набуває готовність персоналу виконувати вимоги безпеки. Така готовність залежить від багатьох чинників: розуміння персоналом необхідності виконання цих вимог, рівня усвідомлення і дисциплінованості персоналу, рівня його професійної підготовленості.

Іншими чинниками, що мають істотний вплив на здійсненність політики безпеки, це якість системи управління безпекою на об'єкті інформатизації. Якість практичних робіт щодо реалізації положень політики і досягнення цілей безпеки залежить не тільки від придбання ефективних засобів захисту інформації з обмеженим доступом, але й від ефективного управління безпекою на об'єкті, планування захисту, визначення конкретного переліку робіт щодо реалізації правил безпеки, впровадження системи контролю та оцінки виконання цих робіт.

На програмно-технічному рівні на здійсненність політики безпеки має вплив можливість закупки необхідних заходів захисту і технічні можливості їх застосування на об'єкті інформатизації. На здійсненність впливають розмір фондів, що виділяються на реалізацію програми забезпечення безпеки інформації з обмеженим доступом і планів захисту, наявності на ринку відповідних засобів захисту потрібної якості, технологічний рівень процесів обробки інформації з обмеженим доступом на об'єкті інформатизації (стан парку обчислювальної та іншої спеціальної техніки, рівень комп'ютеризації та інформатизації технологічних процесів тощо).

Висновки

Таким чином, можна констатувати, що створення системи електронного документообігу це поєднання наукових, технічних, правових та організаційних заходів. Політика безпеки є здійсненною, якщо на правовому, адміністративному, процедурному та програмно-технічному рівнях забезпечення безпеки інформації з обмеженим доступом створені всі умови для здійснення правил безпеки.

Така властивість документообігу як простота в адміністративному забезпеченні розглядає політику безпеки з точки зору її придатності для адміністрування, тобто враховує наявність достатнього адміністративного персоналу для впровадження політики безпеки, рівень професіоналізму, організаційних здібностей та навичок персоналу, що відповідає за реалізацію політики безпеки і організацію ефективного захисту інформації з обмеженим доступом. Політика безпеки є простою в адміністративному забезпеченні, якщо вона потребує мінімальних витрат на організаційно-штатні зміни в структурі підприємства.

Таким чином, з точки зору діяльності політика безпеки повинна бути стабільною, цілеспрямованою, організованою, керованою, узгодженою та мотивованою, забезпечити максимальну результативність і ефективність при досягненні цілей безпеки і розв'язанні

задач захисту, бути адекватною погрозам безпеки, доцільною та гнучкою в реалізації, здійсненною на різних рівнях забезпечення безпеки інформації з обмеженим доступом, достатньо простою у адміністративному забезпеченні.

Загальними задачами на вирішення яких направлена політика безпеки є:

– забезпечення конфіденційності, цілісності, доступності і спостережності інформації в інформаційній системі;

– управління інформацією та ресурсами з метою вдоволення експлуатаційних вимог інформаційної системи;

– здійснення цілеспрямованої та структурованої діяльності з тестування і оцінки безпеки за реалізації розроблених та запропонованих до застосування функцій та механізмів безпеки;

– здійснення аудиту безпеки, сертифікації компонентів інформаційної системи для прийняття рішення про можливість функціонування системи в захищеному режимі з необхідним рівнем ризику.

Список літератури

1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99, ДСТЗІ СБ України, Київ, 1999.

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

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

4. *Бондаренко М.Ф., Потій О.В., Лавріненко В.Г., Горбенко Ю.І.* Визначення та обґрунтування суті політики інформаційної безпеки // Радіотехніка: Всеукр. межвед. науч-техн. сб. 2003. Вип.134. С.9 – 25.

Надійшла 21.10.2004р.

УДК 655.002

Азарсков В.Н., Ситник А.Г.

СОВРЕМЕННЫЕ МЕТОДЫ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА НА ОСНОВЕ ИССЛЕДОВАНИЙ ДЕЙСТВИЙ ПОСЛЕВОЕННЫХ ЗАПАДНЫХ СПЕЦСЛУЖБ И ДРЕВНИХ СПОСОБОВ РАЗВЕДКИ В СТРАНАХ АЗИИ. ЧАСТЬ I

Исследование проблемных вопросов информационного противоборства сторон начнем с цитаты Джона Баккана [1] о жизни агента в информационной войне: "Впереди дни и ночи в постоянном напряжении сил, подтачивающим нервы в изнурительной борьбе. Страшная работа, слишком бесчеловечная для человека"

В своем изложении будем исходить из накапливания: фактов, наблюдений и впечатлений и не будем торопиться с выводами, поскольку «наблюденный факт», по выражению Л.Н. Гумелева это основной метод ведения исследований в науке о происходящих изменениях в современном мире. Пусть наши выводы будут напоминать скорей беллетристические фрагменты рассуждений, чем сухие отчеты статистики.

Сегодня в науке в качестве основного метода информационно-аналитического исследования (МИАИ) [2] политических событий: переворотов, политических заговоров и убийств, информационных войн, военных конфликтов, операций антитеррористической деятельности и т. д. используется рассмотрение событий непосредственно «по горячим следам». Считается, что чем меньше времени нас отделяет от происшедшего политического события, тем более современен и актуален автор исследования, ему присваиваются