залишається стабільною.

1. *Исаев Сергей.* Популярно о генетических алгоритмах. web: http://www.chat.ru/~saisa/index.html.
2. *Мельник А.О., Сокіл О.М.* Проектування оптимізованих структур комп'ютерних пристроїв підбором необхідних елементів бібліотеки з використанням генетичних алгоритмів // Вісник Нац. Ун-ту „Львівська політехніка". – 2004. - №523. – с.101-108.
3. *Теленик С.Ф., Ролик О.І., Букасов М.М., Лабунський А.Ю.* Моделі управління віртуальними машинами при серверній віртуалізації// Вісник НТУУ «КПІ»: Інформатика, управління та обчислювальна техніка. - К.: «ВЕК+», 2009. - № 51. - С. 147-152.
4. *Колодчак О.М., Мельник А.О.* Модифікований генетичний алгоритм для проектування цифрових пристроїв. // Комп'ютерні системи та мережі. Вісник НУ „Львівська політехніка". – №546. – Л.: 2005. – с.69-75.

Поступила 11.08.2014 р.

УДК 004.451.36:681.5

Сабат В. І., Українська академія друкарства, м. Львів

АНАЛІЗ РИЗИКІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ДОКУМЕНТООБІГУ

Анотація. У статті проаналізовано метод визначення рівнів ризику для загроз в автоматизованій системі документообігу (АСДО) на всіх етапах життєвого циклу документів.

Ключові слова. Системи документообігу, ризики, загрози, вразливості.

Abstract. The article analyzes the method of determining the level of risk to threats in an automated workflow system (AWS) at all stages of life cycle of documents.

Keywords. Workflow system, risks, threats, vulnerabilities.

Вступ. Функціонування будь-якої системи документообігу зводиться до забезпечення зручних та комфортних умов роботи з документами для усіх суб'єктів системи від замовника чи адміністратора до виконавця. Такі умови роботи з документами можливі лише при налагодженій, надійній та ефективній системі захисту і доступу до будь-якого документу в АСДО.

На сьогодні більшість систем документообігу окрім електронних документів містять паперові, для яких також існує розроблена певна процедура їхнього функціонування в інформаційній системі. Але для того, щоб забезпечити надійність та ефективність роботи з великими масивами інформації, що міститься в документах, необхідно здійснити перехід від паперових до

електронних документів. Це основна і необхідна передумова для подальшого ефективного впровадження системи електронного документообігу (СЕД).

Основна частина. Спільне використання систем електронного діловодства, мережі Інтернет та внутрішніх локальних мереж із серверами для баз даних документів, сховищ інформації, дозволяє систематизувати і поєднувати інформацію, що полегшує її пошук, аналіз і опрацювання. Усе це можливо лише в системі управління, побудованій на основі цілком електронного документообігу. Але такий підхід має також свої недоліки, які випливають із використання інформаційних технологій та ризиків пов'язаних з цим.

Кожен документ має свій життєвий цикл (ЖЦД) і стадії обробки (шлях проходження) до яких можна віднести: створення; візування та узгодження; затвердження, підписання, проставлення печаток; реєстрація; розгляд; маршрутизація; виконання; контроль виконання; списання в справу; зберігання; знищення. На всіх стадіях ЖЦД на підприємстві чи в організації повинні бути розроблені процедури опрацювання електронних документів згідно маршруту його руху. Це дозволяє пришвидшити обіг документів, зменшує час на їхнє опрацювання і ризики втрати документів. Для порівняння з паперовими документами, в умовах традиційної паперової технології 30% часу співробітників витрачається на пошук, узгодження й відправлення документів, 6–15% документів безповоротно губиться. Багато документів породжують інші документи, пов'язані з основним. Кожний внутрішній документ копіюється в середньому до 20 разів. Середньостатистичний службовець витрачає щорічно до 150 годин свого робочого часу на пошук загубленої інформації. Існують оцінки, що на роботу з документами доводиться витрачати до 40% трудових ресурсів і до 15% корпоративних доходів. [1]

Для виявлення ризику в сучасних АСДО необхідно визначити основні вразливості і загрози на стадіях життєвого циклу електронних документів, а також дослідити контрзаходи в системі безпеки.

Вразливості АСДО визначаються експертами із служб системи захисту на основі аналізу вразливих місць ЖЦД і моніторингу всіх процедур безпеки на етапі створення, маршрутизації та використання документів. При цьому необхідно визначити наявність можливих точок доступу до інформації (як у електронній, так і у фізичній формі) і надійність систем, що знаходяться в організації. До таких процедур можна віднести: з'єднання з Інтернетом; точки віддаленого доступу; з'єднання з іншими організаціями; фізичний доступ в приміщення організації; точки доступу користувачів; точки доступу через бездротову мережу. Для кожної точки необхідно провести оцінку інформації та систем і виявити способи доступу до них. Окрім того необхідно переконатись, що в цей список включені всі відомі вразливі місця операційних систем та прикладних програм.

Головна мета безпеки АСДО — захист інформації, яка міститься в документах від загроз. Загрози оцінюються відповідно до розміру збитків, яких може бути завдано СЕД внаслідок реалізації відповідних загроз. Збитки можуть полягати у втраті суспільної довіри або зниженні іміджу організації АСДО в суспіль-

стві, відповідальності перед законом, створення загрози безпеці персоналу та ін. Проте в кінцевому результаті вони так чи інакше зводяться до фінансових втрат. Можливість реалізації загрози характеризується рівнем ризику, який в свою чергу прямо пропорційно залежить від вразливості системи. Тобто для захисту документів та інформації, яка міститься в них, необхідно зменшити їх вразливість до припустимого граничного рівня. При цьому вартість заходів спрямованих на зменшення вразливості АСДО не повинна перевищувати розміру збитків, яких може бути завдано внаслідок реалізації загроз.

АСДО в інформаційній системі (ІС) розглядається як один з активів підприємства чи організації. В свою чергу АСДО складається з інших активів та підрозділів, які також потребують захисту. Оскільки цільове призначення АСДО важливе для здійснення організацією своєї діяльності, то для неї необхідно проведення детального аналізу ризику (рис.1).

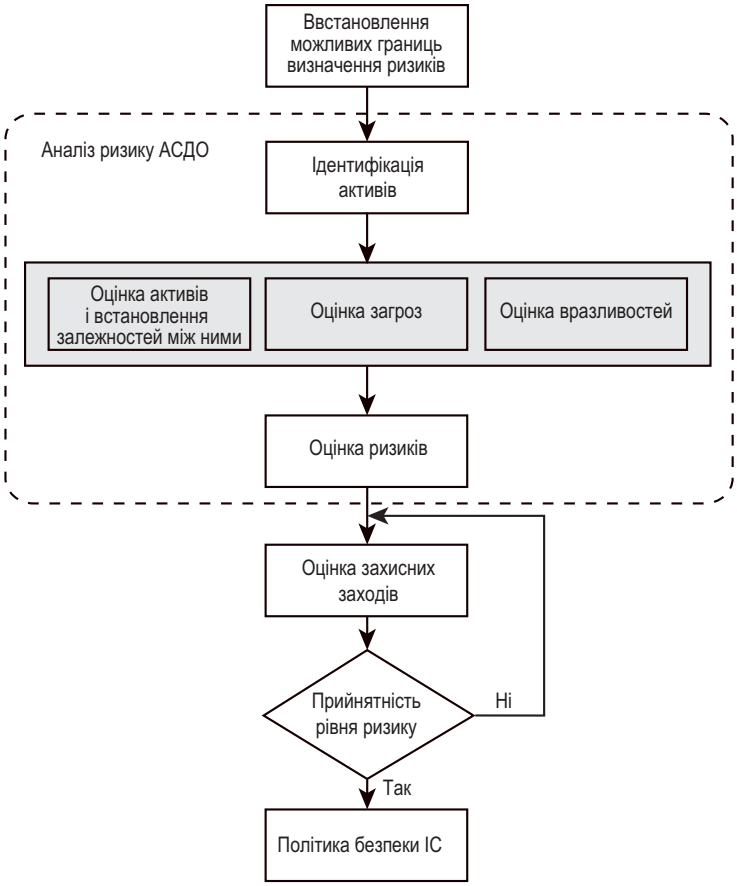

Рис. 1. Управління ризиком за методом детального аналізу ІС

Детальний аналіз загального ризику для ІС передбачає ідентифікацію всіх ризиків і оцінку їх рівня.

Встановлення можливих границь для розгляду ризиків має на меті чітке визначення того, які з ресурсів мають бути враховані при розгляді результатів аналізу ризиків. При розгляді ризиків АСДО необхідно враховувати такі фактори:

— активи інформаційних технологій (апаратні засоби, інформаційне забезпечення, інформацію, яка міститься в документах), оскільки вони складають програмну і апаратну базу для функціонування АСДО;
— персонал організації (який працює з АСДО і обслуговує її), як джерело можливих загроз;
— умови здійснення виробничої діяльності, оскільки вони впливають на нормальне функціонування АСДО;
— ділову діяльність, яка є основною метою функціонування АСДО.

Для детального аналізу ризиків представимо АСДО як сукупність трьох складових: інформаційної частини, організаційної роботи з персоналом і апаратної частини. Функціонування АСДО не можливе, якщо не буде функціонувати хоча б одна з її складових, тобто порушення нормальної роботи хоча б однієї з них спричинить порушення роботи решти складових і всієї системи загалом. Розглянемо детальніше кожну зі складових АСДО.

Інформаційна складова АСДО об'єднує всю інформацію, яка функціонує всередині АСДО, а також вхідні і вихідні інформаційні потоки документів (рис. 2 2).

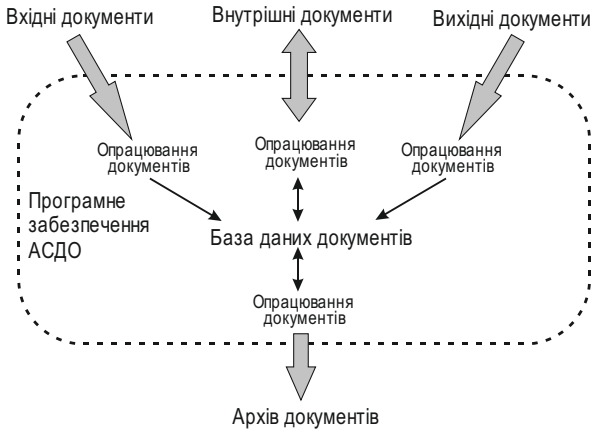

Рис. 2. Інформаційна складова АСДО

Програмне забезпечення (ПЗ) є окремою невід'ємною частиною інформаційної складової АСДО. За допомогою ПЗ здійснюється створення, передача і перетворення інформації, яка функціонує в АСДО. ПЗ можна умовно поділити на основне і допоміжне.

До основного ПЗ можна віднести програмні модулі для створення і

обробки інформації, яка функціонує в АСДО, а також центральну базу даних (БД) — ядро АСДО. Тут може зберігатися найрізноманітніша інформація потрібна в процесі роботи над документами.

Допоміжне ПЗ забезпечує роботу основного. Це операційна система, драйвери, різноманітні утиліти та ін.

Згідно схеми, зображеної на рис. 2, робота типової АСДО виглядає таким чином. Вхідна інформація (різноманітні вхідні документи та їхні реквізити, комерційна інформація, дані фінансового обліку) обробляється програмними модулями АСДО і заноситься в центральну БД. У процесі роботи до центральної БД через відповідні програмні модулі звертаються різноманітні внутрішні підрозділи підприємства — відбувається внутрішній інформаційний обмін. Також під час роботи АСДО відповідними модулями формується вихідна інформація (заявки на матеріали, документи, дані оперативного обліку). Для забезпечення надійності роботи інформація центральної БД періодично архівується.

При визначенні рівнів ризику програмного забезпечення слід враховувати його відповідність до вимог системи безпеки. Так, при використанні неліцензійних програм чи сторонніх додатків зростає ризик вірусних атак через т.зв. експлойти — на вразливі місця програмного забезпечення. Також слід приділити увагу на дотримання програмного оновлення операційних систем та усіх програмних засобів системи безпеки (у тому числі антивірусних програм та інших компонент захисту).

Апаратна частина АСДО. До апаратної частини АСДО належать пристрої, які забезпечують інформаційний обмін між компонентами всередині ІС, а також між АСДО і зовнішнім середовищем. Тобто до апаратної частини АСДО можна віднести:

— ресурси: сервери, робочі станції, мобільні комп'ютери;
— периферійне обладнання: принтери, сканери, веб-камери та ін.;
— устаткування для забезпечення зв'язку: мережі і мережеве обладнання;
— пристрої для зв'язку з виробничим устаткуванням: контроллери.

Під сервером будемо розуміти ресурс, який містить цінну інформацію і до якого можливий віддалений доступ. Відповідно робоча станція — це ресурс, який містить цінну інформацію і до якого можливий лише локальний доступ, мобільний комп'ютер — це ресурс, який містить цінну інформацію і може бути винесений користувачем за межі організації.

Для визначення рівнів ризику, які пов'язані із роботою апаратної частини АСДО варто враховувати не тільки можливість фізичного доступу до них, але й не забувати про можливість віддаленого контролю та віддаленого доступу через зовнішні мережі. Тому необхідно правильно настроїти модулі доступу на міжмережних екранах. В результаті сканування мережі через екран з фільтрацією пакетів, зазвичай, відобразиться більше число вразливостей, ніж при скануванні через міжмережний екран прикладного рівня. Також необхідно враховувати загрозу доступу до конфіденційної інформації при використанні бездротового зв'язку.

Персонал. Під поняттям «персонал» вважатимемо людей, що обслуговують АСДО (наприклад системні адміністратори), так і тих, які безпосередньо працюють з нею (користувачі, адміністратори та виконавці). При розробці політики безпеки будь-якої організації слід враховувати проведення організаційної роботи серед персоналу з питань підвищення засобів безпеки роботи в АСДО. Кожен працівник має володіти відповідними знаннями роботи з документами і виконувати свої службові обов'язки щодо дотримання усіх процедур розроблених в політиці безпеки. Чим більший рівень доступу конкретного суб'єкта системи захисту до захищених документів та об'єктів АСДО, тим більші вимоги до нього з дотримання правил і процедур політики безпеки. При цьому повинні бути задіяні усі служби системи захисту і здійснювати контроль та моніторинг виробничого процесу, адже через необізнаність персоналу в галузі безпеки, чи т.зв. «людський фактор» здійснюються найбільш нищівні та непрогнозовані атаки на ІС.

Отже для оцінки вразливостей необхідно провести їх ідентифікацію на усіх етапах ЖЦД. Проте саме існування вразливостей документів не завдає збитків АСДО, оскільки для цього необхідна наявність відповідної загрози документу. Наявність вразливості за відсутності такої загрози не вимагає вживання захисних заходів, але вразливість має бути зафіксована і надалі перевірена на випадок зміни ситуації. Слід зазначити, що захисні заходи безпеки, які некоректно використовуються або неправильно функціонують, можуть самі стати джерелами появи вразливостей. Оцінку вразливостей варто проводити лише для критичних загроз в АСДО, оскільки немає сенсу оцінювати вразливості для некритичних загроз, а також для тих, які виникають з дуже малою ймовірністю.

Ймовірність реалізації вразливостей й, відповідно, рівень ризику можна оцінювати за різними шкалами. Виокремлюють чотири зони ризику: безризикова зона, зона допустимого ризику, зона критичного ризику та зона катастрофічного ризику [2; 3]. У процесі прийняття економічних рішень про допустимість та доцільність ризику важливо з'ясувати ймовірність того, що збитки (ризик) не перевищать певного рівня та знаходяться в межах наперед визначеної зони, тобто: $R = p\left(x \le x_0\right)$, де x_0 – граничне значення певного рівня збитку. В. В. Вітлінський та Г. І. Великоіваненко вважають саме цей показник основним при оцінці ризику [2]. Описану методологію у більшості наукових праць прийнято називати «методом аналізу можливих збитків» [4].

Для вибору адекватних захисних заходів необхідно здійснити оцінку величини ризиків. Величина ризику АСДО залежить від вартості активу, критичності загрози, ймовірності і частоти виникнення загрози. Величина ризику визначатиметься за формулою:

$$R_{i,j} = V_j \times K_{j,i} \times P_{j,i} \times W_{j,i} \times Q_i^{\Sigma},$$

де V_j — вартість *j*-го активу;

$K_{j,i}$ — критичність *i*-ї загрози для *j*-го активу;

$P_{j,i}$ — ймовірність виникнення *i*-ї загрози для *j*-го активу;

$W_{j,i}$ — частота виникнення *i*-ї загрози для *j*-го активу протягом року;

Q_i^{Σ} — сумарна величина, отримана в результаті оцінки вразливостей для *i*-ї загрози. Вона визначається за формулою:

$$Q_i^{\Sigma} = \sum_{q=1}^{n} P_q^T,$$

де P_q^T — ймовірність реалізації вразливості *q* для *i*-ї загрози;

n — кількість вразливостей, які використовуються *i*-ю загрозою.

Величина сумарного ризику для *i*-ї загрози:

$$R_i^{\Sigma} = \sum_{j=1}^{s} R_{i,j},$$

де s — загальна кількість загроз.

Висновок. В результаті оцінки ризиків для кожної загрози визначається її числове значення, що характеризує ступінь ризику спричиненого цією загрозою в АСДО. Таким чином можна ранжувати загрози у порядку зменшення ризику, спричиненого ними і створювати адекватні захисні заходи в системі безпеки для протидії відповідним загрозам. Цей метод дозволяє розробити систему керування ризиками в системі безпеки не тільки для АСДО, але й для будь-якої організації, яка потребує захисту своїх активів.

1. *Золотарьова І. О.* Автоматизація документообігу. Навчальний посібник / І. О. Золотарьова, Р. К. Бутова. – Харків : Вид. ХНЕУ, 2008. – 168 с.
2. *Вітлінський В. В.* Ризикологія в економіці та підприємництві : [монографія] / В. В. Вітлінський, Г. І. Великоіваненко. – К. : КНЕУ, 2004. – 480 с.
3. *Клименко С. М.* Обгрунтування господарських рішень та оцінка ризиків : [навч. посібник] / С. М. Клименко, О. С. Дуброва. – К. : КНЕУ, 2005. – 252 с.
4. *Лук'янова В. В.* Економічний ризик : [навч. посіб.] / В. В. Лук'янова, Т. В. Головач. – К. : Академ-видав, 2007. – 464 с.

Поступила 14.08.2014 р.

УДК 004.72+004.032.6+378

Хамула О.Г., Васюта С.П., Яців М.Р.,
Українська академія друкарства, м. Львів

ОПТИМІЗАЦІЯ БАГАТОРІВНЕВОЇ МОДЕЛІ ФАКТОРІВ ВПЛИВУ НА ПРОЕКТУВАННЯ КОМПОЗИЦІЙНОГО ОФОРМЛЕННЯ ЕЛЕКТРОННОГО ВИДАННЯ ДЛЯ ДІТЕЙ З ВАДАМИ ЗОРУ

Анотація: На основі проаналізованих критеріїв, які впливають на композиційне оформлення електронного видання для дітей з вадами зору та розробленого графу взаємозв'язків між цими критеріями, які ієрархічно

