УДК 004.9

М. В. Турти, С. М. Нужний, А. П. Гунченко
Національний університет кораблебудування,
кафедра ЕОС та інформаційної безпеки

РОЗРОБЛЕННЯ БЛОКА ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ АСОД ДССЗЗІ

Обґрунтована необхідність вдосконалення автоматизованої системи обігу захищених документів для державних структур на основі АС-3 класу.

Ключові слова: захищений документообіг, АС-1, АС-3, блок прийняття рішення.

This paper substantiates the necessity of improving automated circulation system of protected documents for the state agencies on the basis of class 3automated systems.

Key words: protected document circulation, AS-1, AS-3, decision making unit.

Вступ

Постійне збільшення обсягів інформації, яка циркулює у суспільстві, вимагає контролю та обліку інформаційних ресурсів. Це стосується державних структур, де процеси інформатизації та впровадження сучасних технологій отримали новий імпульс розвитку з прийняттям в останні роки багатьох нормативних документів. Закон України “Про електронні документи та електронний документообіг” [1] встановлює, що відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, Цивільним кодексом України, законами України “Про інформацію”, “Про захист інформації в автоматизованих системах”, “Про державну таємницю”, “Про телекомунікації” та ін.

Державна служба спеціального зв’язку та захисту інформації згідно з [2] є складовою сектору безпеки і оборони України. Структура та умови використання системи захищеного електронного документообігу Національної системи конфіденційного зв’язку додатково регламентуються Постановою Кабінету Міністрів України № 303 [3], яка передбачає наявність у складі системи захищеного електронного документообігу акредитованого центру сертифікації ключів. Питання розроблення і впровадження захищених автоматизованих систем обігу документів (АСОД) також входять до сфери відповідальності Національного координаційного центру кібербезпеки, до функцій якого належить “розроблення і внесення … пропозицій щодо … проведення наукових досліджень у галузі кібербезпеки та кіберзахисту для потреб національної безпеки і оборони” [4, 5]. Діяльність цих організацій нерозривно пов’язана із застосуванням норм права, організацією та створенням автоматизованих систем управлінського призначення.

Питання комп’ютеризації та інформатизації правотворчої, правоохоронної, правозастосовної, правоосвітньої діяльності розглядають праці багатьох вітчизняних та зарубіжних учених [6–8]. Проте методологія розвитку системи інформаційного забезпечення процесу застосування норм права залишається недостатньо обґрунтованою без створення моделі управлінських відносин, яка враховувала б як технічний, так і організаційно-правовий бік процесів розроблення, впровадження та експлуатації АСОД. Побудова такої моделі ґрунтується на врахуванні таких типових чинників [6], як ступінь централізації та децентралізації функцій, обґрунтування кількості структурних підрозділів, типові структури і типові штати; порядок узгодження, візування, затвердження документів, який необхідний для ухвалення управлінських рішень. Для вироблення самих управлінських рішень в окремому (чи окремих) блоці АСОД потрібно враховувати розподіл інформаційних потоків в ієрархічній системі управління, наявність типових алгоритмів отримання інформації і рішення на її основі, а також наявність в автоматизованій системі програмно-апаратних засобів можливої реалізації цих алгоритмів.

Сьогодні в Україні успішно функціонують і використовуються користувачами системи інформаційно-аналітичного забезпечення узагальненої законотворчої та правозастосовної діяльності (“Право”, “Законодавство”, “Рада” тощо), а також інформаційні ресурси і пошукові системи, що є спеціалізованими у певній галузі і найчастіше є Інтернет-орієнтованими (як сайт Міністерства освіти і науки України, сайт ДССЗЗІ тощо). Однак ці діючі системи не містять процедур вироблення рішень, хоча відомі результати наукових досліджень [6], спрямованих на створення правозастосовних експертних систем на основі продукційної моделі з надання знань зі зворотними висновками, які уможливили автоматизувати рутинну частину діяльності експертів. Причому побудова таких систем повинна виходити з мережевоцентричної парадигми інформаційної безпеки інформаційних ресурсів [8], враховувати, що розроблювана система може бути глобальним розподіленим багатокористувацьким і багатодоменним комплексом, який обробляє інформацію різних категорій конфіденційності і різних власників. Домен включає ІТС класу 3, яка належить одному власнику і має свою КСЗІ, що захищає домен по периметру, свою систему управління інформаційною безпекою, свою систему попередження, виявлення, обробки і ліквідації інцидентів з інформаційною безпекою, свою єдину для домена політику безпеки. Парадигма кібербезпеки підприємств у цьому випадку розглядається як розвиток мережевоцентричної парадигми.

Особливість сучасних реалізацій функцій АСОД ДССЗЗІ зумовлена використанням у регіональних управліннях ДССЗЗІ АС 1-го класу і звітності ліцензіатів на паперових носіях, що істотно ускладнює процедуру управління, а відповідно й припускає можливість помилки. Тому за рекомендацією регіонального управління ДССЗЗІ в Національному університеті кораблебудування ім. адмірала Макарова на кафедрі Електрообладнання суден та інформаційної безпеки у межах ініціативної кафедральної теми проводиться розробка АСОД, яка може разом з іншими функціями контролювати і оптимізувати роботу безпосередньо самої служби, її ліцензіатів та ліцензістів, включаючи як відділи, так і групи технічного захисту інформації.

Мета роботи – проаналізувати можливості створення АСОД на основі АС 3-го класу з забезпеченням функцій оптимального керування.

Основна частина

У роботі проаналізовано структуру діяльності ДССЗЗІ, нормативно-правова база якої дає змогу визначити зовнішні для АСОД інформаційні ресурси та існуючі методи прийняття рішень, обрані методи, що лягли в основу розроблених алгоритмів. Завдання діяльності ДССЗЗІ можуть бути умовно поділені на дві групи: фахові завдання діяльності і завдання суспільної діяльності та визначення напрямків розвитку галузі. До фахових завдань діяльності належить ліцензування, сертифікація та експертиза для напрямків криптографічного і технічного захисту інформації, а також завдання державного контролю та регуляторної діяльності. До другої групи завдання належить міжнародна діяльність, питання державних закупівель, організація зв’язків з громадськістю та завдання, що стосуються розвитку галузевої науки, зокрема роботи науково-експертної ради, наукових установ та проведення наукових заходів (семінарів, конференцій тощо).

Проведений аналіз показав, що переважна більшість процесів обробки інформації під час виконання завдань діяльності ДССЗЗІ оперує структурованими якісними даними. Однак під час виконання завдань ліцензування, сертифікації, експертизи, державного контролю вхідні дані для блока прийняття рішень можуть бути подані у бінарному вигляді, що відповідає наявності чи відсутності конкретних умов для прийняття позитивного рішення. Тоді критерій прийняття рішення подається за наявності детермінованих даних в адитивній чи мультиплікативній формі:

$$F = F_{\max} = \sum_{i=1}^{N} x_i; \quad x \in \{0,1\}; \tag{1}$$

$$F \neq 0 \ \ or \ \ (F = 1); \ F = \prod_{i=1}^{N} x_i; \quad x \in \{0,1\}. \tag{2}$$

В умовах ризику критерієм прийняття рішення може виступати

$$F = \sum_{j=1}^{m} R_j \to \min \tag{3}$$

під час застосування методик визначення абсолютних ризиків або:

$$F = \frac{\sum_{j=1}^{m} R_j^{new}}{\sum_{j=1}^{m} R_j^{old}} \to \min,\ F < 1; \tag{4}$$

$$F = \frac{\sum_{j=1}^{m} R_j^{old}}{\sum_{j=1}^{m} R_j^{new}} \to \max,\ F > 1 \tag{5}$$

під час застосування методик визначення відносної ефективності рішення.

Критеріями прийняття рішення в умовах невизначеності можуть виступати критерій Вальда (песимістична оцінка), критерій Лапласа (за відсутності даних), критерій Севіджа (за визначеного максимально припустимого ризику), експертна оцінка альтернатив за сукупністю критеріїв якості рішення з врахуванням важливості критеріїв.

Зовнішнє інформаційне середовище АСОД (рис. 1) включає ресурси з різним ступенем довіри до інформації, тому разом з даними зберігається рівень їх достовірності, який використовується у процесах прийняття рішень.

Рис. 1. Об'єкти зовнішнього інформаційного середовища АСОД ДССЗЗІ

Розроблена у роботі структура АСОД (рис. 2) передбачає наявність модулів отримання первинних даних та їх попередньої обробки, довідкових модулів, модулів реєстрації подій, прийняття та видачі рішень, модулів керування роботою АСОД.

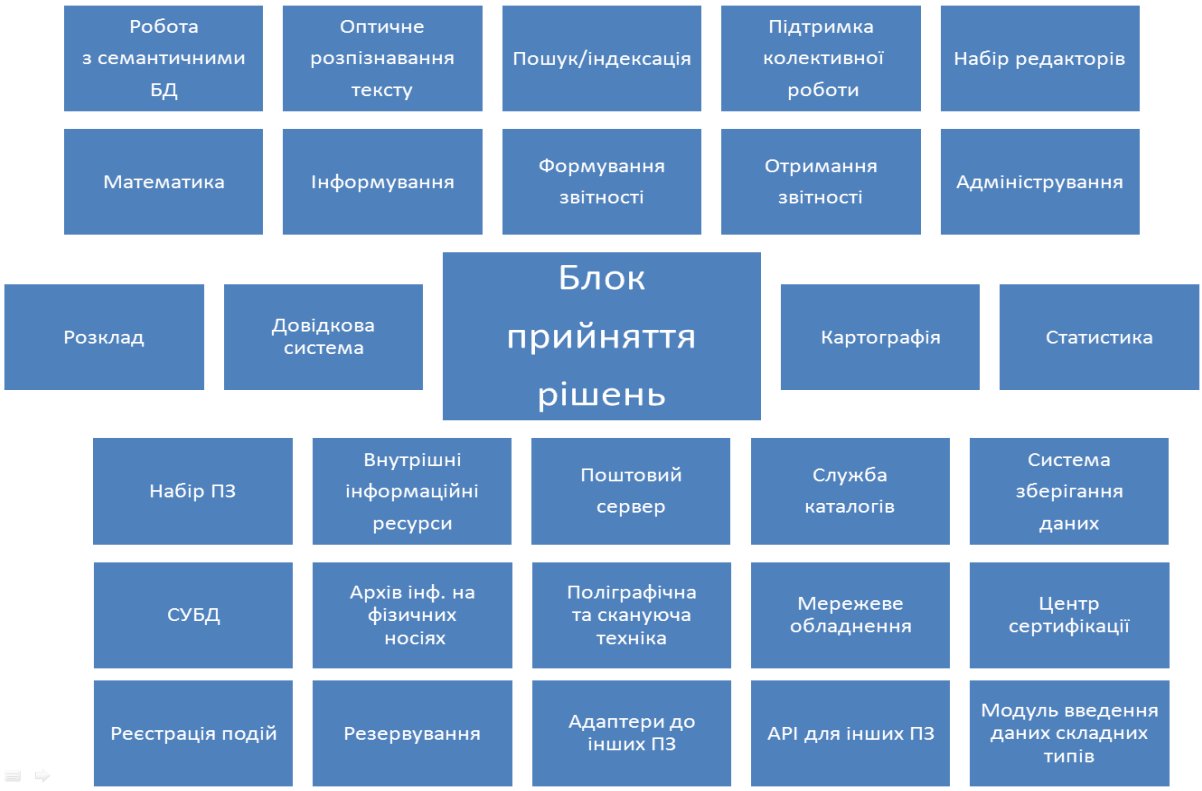

Рис. 2. Структура АСОД ДССЗЗІ

Основними джерелами інформації для блока прийняття рішень (рис. 3) є: модуль пошуку, модуль управління процесами, модуль управління ресурсами, розклад, картографічний модуль, бази даних загального і обмеженого доступу, засоби підтримки колективної роботи, модуль аналізу інформації з відкритих джерел, модуль реєстрації подій, бібліотека, модуль маршрутизації. У міжмодульній взаємодії усі завдання і процедури повинні мати пріоритет (некритичні завдання повинні виконуватися з нижчими пріоритетами) і виконуватися на наявних поточних ресурсах.

Математичний модуль реалізує операції обробки даних, зокрема математичні, операції з комбінованими даними, обробку виразів. Задля безпеки ІЗОД, що обробляється у виразі, екземпляр математичного модуля, що обробляє конкретний вираз, працює з правами користувача, який цей вираз створив, або спеціально створеного користувача.

Модуль управління ресурсами контролює наявні ресурси, отримує від модуля прогнозування прогнозовані потреби у ресурсах, приймає запити на ресурси, видає рекомендації відповідальним користувачам у разі досягнення граничнодопустимих запасів ресурсів, виділяє ресурси з урахуванням ефективності їх використання. До групи ресурсів належать людські ресурси, матеріально-технічні ресурси та фінансові ресурси. Інформація про матеріальні об’єкти (зокрема персонал) зберігається у модулі розкладу, а про фінансові ресурси – отримується з банку у реальному часі (наприклад, використовуючи API банку). Для оптимізації управління ресурсами використовується маска коефіцієнта корисності праці, що накладається на тижневий графік, чи за вимогою на графік для заданого терміну часу. Маска коефіцієнта корисності розраховується для окремого працівника та виду роботи, яку він виконує. Розрахунки виконуються модулем статистики на основі даних про вже виконані ним роботи того самого виду, а саме: графік виконання, час виконання, оцінка керівника, кількість повернень на доопрацювання, інтенсивність використання технічних засобів, інші непрямі показники.

Модуль авторизації призначений для надання і зняття прав за подією, наприклад, створення документа за шаблоном, для заповнення якого потрібно ознайомитись з ІЗОД, вирішення конфліктів прав/ролей для випадку, коли один користувач має багато ролей, реалізації процедур делегування повноважень.

Рис. 3. Структура блока прийняття рішень АСОД ДССЗЗІ

Управління процесами здійснюється окремим модулем, який, за запитом, створює процес, контролює його виконання, змінює дані у інших модулях, відповідно до завдань у схемі процесу. При цьому можливий автоматичний та ручний розподіл завдань. Із наближенням граничних термінів поступово підвищується пріоритет завдань процесу, але не вище від граничного для цього процесу. Час завершення процесу попередньо розраховується модулем прогнозування на основі статистики виконання тих самих завдань. Після завершення процесу статистика коригується на основі реальних додаткових даних.

Управління документами передбачає організацію процедур створення і редагування документів та їх версій, порівняння версій документів, управління правами доступу у плані блокування внесення повних чи часткових змін, вирішення колізій у разі сумісного редагування документів. Модуль перевірки документів контролює відповідність даних прийнятим стандартам, шаблонам, коректність даних з метою запобігання помилкам і зловживанням. Наприклад, розпорядження про видатки грошей повинно міститися у фінансовому документі (обіг яких містить відповідні процедури контролю), а якщо документ про фінансові витрати не належить до визначеної групи фінансових документів або надійшов від адресата, який не має прав генерувати такі документи, то підписання документа блокується та про це сповіщається відділ безпеки. Додатково можна перевірити коректність суми видатку за записом у системі керування ресурсами. Модуль управління документами на фізичних носіях приймає рішення про сканування, розпізнавання, збереження, створення фізичного носія, зокрема копіювання електронних документів та друк.

Модуль виявлення та прогнозування порушень виконує перевірку накопичених даних на наявність типових порушень, конфліктуючих даних, аномальних кореляцій, відхилень деяких величин від випадкового розподілу, інших статистичних аномалій. Для прогнозування порушень, що можуть бути скоєні об’єктом, використовуються як типові алгоритми пошуку, так і

прогнозування стану об'єкта з подальшими перевірками відповідності. У модулі можуть використовуватися алгоритми нечіткої логіки. Якщо результат має ймовірність вищу від заданої, модуль сповіщає відділ безпеки чи відсилає інформацію модулю планування контрольних перевірок. Результати пошуку та прогнозування нетипових порушень напряму залежать від витрачених обчислювальних ресурсів, тому ці операції можна виконувати безперервно з низьким пріоритетом.

Модуль прогнозування приймає вихідні значення, повертає прогнозовані. Емпіричні значення для алгоритмів прогнозування отримує від модулів статистики, картографії, роботи із семантичними БД, аналізу інформації з відкритих джерел.

Модуль планування контрольних перевірок ініціює процеси планових та позапланових контрольних перевірок, які обробляються модулем управління процесами. Позапланові перевірки ініціюються, якщо є дані про скоєне чи прогнозоване порушення, час перевірки обирається за критерієм максимальної ймовірності виявлення порушення.

Модуль перевірки відповідності використовується у завданнях фахової діяльності для встановлення відповідності об'єктів/суб'єктів вимогам нормативних документів (НД). Використовує правила, що ґрунтуються на вимогах НД та містять зв'язки з бібліотечним модулем, де зберігається текст НД. Бібліотечний модуль відстежує зміни НД на інформаційних ресурсах відповідних організацій та інформує про них інші модулі та відповідальних осіб.

Криптомодуль забезпечує шифрування, розшифрування повідомлень, інших даних, накладання та перевірку електронного цифрового підпису.

Модуль маршрутизації документів передбачає наявність жорсткої та вільної маршрутизації. Вільна маршрутизація дає змогу працівнику за умови наявності відповідних прав змінити маршрут проходження документа, реалізуючи послідовне чи паралельне візування документів.

Серед засобів управління роботою АСОД потрібно виділити модулі управління фільтрацією, самотестування та самовідновлення. Модуль управління фільтрацією керує поштовим сервером, реалізуючи антиспам, антивірусом, модулем мережевого обладнанням (який, своєю чергою, керує проксі, маршрутизаторами, комутаторами). Модуль самотестування здійснює контроль стану блоків та модулів, формування повідомлень адміністраторів. Модуль самовідновлювання у разі отримання інформації про збій виконує процедури відновлення працездатності.

Висновки

Запропоновано структуру АСОД та її блока прийняття рішень, проведено аналіз та визначено набір методів та критеріїв, застосування яких дасть змогу забезпечити виконання поставлених завдань. На прикладі процедури ліцензування досліджено процеси прийняття рішень, визначені джерела і атрибути вхідної та вихідної інформації, розроблені та апробовані алгоритми та процедури прийняття рішень.

1. Закон України "Про електроні документи та електронний документообіг" //http://zakon2. rada.gov.ua/laws/show/851-15. 2. Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України № 92/2016 від 14 березня 2016 року. 3. Постанова Кабінету Міністрів України № 303 від 14.05.2015 "Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку". 4. Стратегія кібербезпеки України, затверджена Указом Президента України № 96/2016 від 15 березня 2016 року. 5. Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України № 242/2016 від 7 червня 2016 року. 6. Павлишин О. В. Філософсько-правовий аналіз розробки і використання електронних експертних систем у правозастосовчій діяльності : автореф. дис. … канд. юрид. наук : спец. 12.00.12 "Філософія права" / О. В. Павлишин. – К., 2005. – 19 с. 7. Костюк Н. П., Степанець Д. С. Проблеми інформатизації процесу правозастосування // Криміналістичний вісник. – 2016. – № 1 (25). – С. 102–108. 8. Кононович В. Г. Еволюція парадигми інформаційної, соціально-психологічної та кібербезпеки // http://avia.nau.edu.ua/doc/ 2011/2/avia2011_2_10.pdf.