Технічні вимоги

Обґрунтування впровадження єдиного рушія BPMN та ABAC в системах документообігу судової влади

2026

Зміст

Зміст

Анотація

У цьому документі наведено технічне та нормативне обґрунтування необхідності впровадження єдиного уніфікованого рушія управління бізнес-процесами (BPMN) та контролю доступу на основі атрибутів (ABAC) в інформаційних системах документообігу судової влади України (СЕД). Розглянуто архітектурний імператив Опорного монітора (Reference Monitor, NIST SP 800-53 AC-25) та фільтрації механізмів оркестровки (AC-4(29)), які виключають використання кількох незалежних рушіїв безпеки різними командами розробників. Запропоновано підхід до ізоляції документообігу загального судочинства та господарських судів на рівні єдиної платформи з використанням логічно розділених просторів імен (spaces) та бакетів (buckets) збереження даних.

1. Передумови та виклики розробки

Сучасна концепція розвитку Єдиної судової інформаційно-кодифікаційної системи (ЄСІКС) передбачає автоматизацію діловодства двох ключових напрямків:

1. Загальне судочинство (місцеві та апеляційні суди загальної юрисдикції, Верховний Суд);
2. Господарське судочинство (господарські суди всіх інстанцій).

У практичній реалізації часто виникає ситуація, коли розробку рішень для цих двох напрямків здійснюють різні команди розробників або різні підрядники. За відсутності жорстких системних обмежень це призводить до фрагментації інфраструктури безпеки: кожна команда прагне розгорнути власний рушій оркестрації процесів (BPMN) та власні локальні модулі перевірки прав доступу.

Такий підхід створює критичні вразливості, збільшує поверхню атаки та унеможливлює комплексну сертифікацію системи захисту (КСЗІ) відповідно до вимог Державної служби спеціального зв'язку та захисту інформації України.

2. Концепція Опорного монітора (NIST SP 800-53 AC-25)

За забезпечення єдиного централізованого ядра перевірки політик доступу, яке неможливо обійти, у класичній теорії комп'ютерної безпеки відповідає концепція Опорного монітора (Reference Monitor). У стандарті NIST SP 800-53 Rev. 5 цей принцип реалізовано через контроль AC-25 (Reference Monitor).

Відповідно до НД ТЗІ 3.6-006-24 та міжнародних стандартів проектування безпечних систем (ISO/IEC 15408 / Common Criteria), Опорний монітор має відповідати трьом фундаментальним вимогам:

1. Завжди викликається (Non-bypassable): Архітектура системи побудована так, що будь-який запит на доступ до даних або виконання кроку процесу проходить виключно через перевіряючий механізм. Не існує жодних обхідних шляхів, прямих запитів до бази даних або альтернативних рушіїв BPMN. Наслідки порушення: Наявність двох паралельних рушіїв автоматично порушує цю вимогу. Зловмисник або помилка конфігурації може дозволити виконати транзакцію в обхід суворіших правил одного з рушіїв.
2. Захищений від модифікації (Tamper-proof): Код, конфігурація та правила доступу рушія ізольовані від процесів користувачів і не можуть бути змінені чи зупинені прикладними компонентами.
3. Піддається аналізу та перевірці (Evaluatable): Механізм перевірки має бути компактним, структурованим та єдиним. Це дає змогу повністю протестувати його логіку, провести математичний аналіз коректності та гарантувати відсутність логічних помилок. Наслідки порушення: Дублювання рушіїв для різних судів збільшує складність аудиту експоненціально, роблячи повну верифікацію безпеки системи неможливою.

Таким чином, використання єдиного екземпляра рушія BPMн та ABAC є безальтернативною умовою виконання вимог контролю AC-25.

3. Фільтрація оркестровки та інформаційні потоки

У складних сервісно-орієнтованих архітектурах, де процеси оркеструються за допомогою BPMN, діють додаткові контроли сімейства керування доступом:

3.1. AC-4(29) — Фільтр механізмів оркестровки

Цей контроль вимагає, щоб будь-які механізми маршрутизації та оркестрування процесів проходили через централізований фільтр політик безпеки.

- Рушій BPMN виступає головним оркестратором переходів станів документів.
- Кожен перехід у схемі BPMN (наприклад, перехід справи від підготовки до слухання) є зміною інформаційного потоку.
- Єдиний фільтр політик безпеки перевіряє правомірність цієї зміни на основі атрибутів суб'єкта та об'єкта (ABAC) за допомогою контролю AC-3 (Access Enforcement) та AC-4 (Information Flow Enforcement).

3.2. AC-16 — Атрибути безпеки (Security Attributes)

Усі метадані документів (гриф секретності, належність до суду, категорія справи) повинні мати уніфікований формат. Єдиний ABAC-модуль зчитує ці атрибути для прийняття рішень щодо доступу. Якщо дві різні системи реалізують власні інтерпретації атрибутів, виникає неузгодженість політик.

3.3. Криптографічний захист зв'язків (SC-12 та SC-17)

Усі виклики до єдиного рушія перевірки від прикладних сервісів мають бути криптографічно автентифіковані (mTLS) з використанням сертифікатів безпеки, що виключає можливість підміни перевіряючого вузла.

4. Уніфікована архітектура: Один продукт, логічні простори

Для забезпечення відповідності нормам ТЗІ та стандартам NIST, архітектура СЕД повинна будуватися на таких принципах:

- Уніфікація технологічного стеку: Обидві команди розробників зобов'язані використовувати один і той самий BPMN-фреймворк та інтегруватися з єдиним централізованим ядром ABAC.
- Логічне розділення (Namespaces / Buckets): Замість створення фізично окремих інсталяцій рушіїв, ізоляція даних загального та господарського судочинства реалізується логічно:

- Спільний рушій BPMN обслуговує запити обох систем, але оперує різними схемами бізнес-процесів.
- Збереження документів здійснюється в єдиній системі зберігання (наприклад, ScyllaDB DHT або S3-сумісному сховищі), але у відокремлених логічних просторах імен (spaces / namespaces) та бакетах (buckets).
- ABAC-рушій автоматично додає обмеження простору імен до кожного запиту на основі атрибуту суду користувача.

Це гарантує повну ізоляцію конфіденційних матеріалів справ господарських і загальних судів на рівні сховищ при збереженні монолітності контролюючого ядра.

5. Впровадження через галузевий профіль безпеки ДСА

Найбільш дієвим механізмом забезпечення цієї вимоги є фіксація архітектурних обмежень на рівні регулятора.

Якщо Державна судова адміністрація (ДСА) України затверджує та підписує такі контроли у своєму Галузевому профілі безпеки (L2):

- AC-4 (Контроль інформаційних потоків);
- AC-16 (Керування атрибутами безпеки);
- SC-12 / SC-17 (Управління криптографічними ключами та сертифікатами);
- AC-25 (Опорний монітор безпеки);
- AC-4(29) (Обов'язкова фільтрація оркестровки).

То це автоматично створює імперативне техніко-юридичне обмеження. Будь-яка команда розробників, яка створює прикладне ПЗ для судової системи, зобов'язана використовувати виключно визначений ДСА єдиний централізований фреймворк BPMN/ABAC. Спроба розгорнути окремий рушій буде заблокована на етапі експертизи КСЗІ як невідповідність Галузевому профілю безпеки.

6. Висновки

Використання єдиного уніфікованого рушія BPMN та ABAC у поєднанні з логічним розділенням сховищ (namespaces/buckets) є єдино можливим способом побудови безпечної та сертифікованої СЕД. Такий підхід повністю задовольняє вимогам контролів AC-25 та AC-4(29) стандарту NIST SP 800-53, запобігає виникненню обхідних шляхів доступу до даних та створює надійну основу для захисту державної таємниці та службової інформації в судовій системі України.

Література

[1] NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations.

[2] Постанова Кабінету Міністрів України № 712 від 18 червня 2025 року. Про затвердження Порядку розроблення та затвердження профілів безпеки.

[3] ДСТУ ISO/IEC 15408. Інформаційні технології. Методи захисту. Критерії оцінки безпеки інформаційних технологій.

[4] Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems.

[5] НД ТЗІ 3.6-006-24. Профілі безпеки для об'єктів критичної інформаційної інфраструктури.