ПЕРША ДЕРЖАВНА СИСТЕМА

Формальна модель та програмна архітектура
функціонального верифікованого мовного забезпечення
для побудови інфраструктурних процесінгових систем
орієнтованих на державну модель управління:
процесами для проведення зовнішнього аудиту,
різними видами розподілених сховищ,
телекомунікаційними та реєстровими фреймворками,
інтернет-утворюючими сервісами зокрема та для
автоматизації захищених автономних офісів і
державних підприємств України у цілому.

Максим Сохацький
ДП «ІНФОТЕХ», Київ, Україна
4 січня 2023

УДК 002
УДК 004.4, 004.6, 004.9

Присвячується всім державним
службовцям України

Система управління державними підприємствами ERP.UNO визначає формальну специфікацію та її імплементацію для сучасних оптимізованих підприємств які вимагають сучасних засобів контролю операцій та цілістності даних.

Телекомунікаційна платформа Erlang/OTP від Ericsson успішно застосовується в індустрії мобільними операторами понад 30 років, а її віртуальна машина досі вважається однією з найкращих в галузі. Системи ERP на її базі також уже не один рік використовується у банківській сфері, процесінгу транзакцій, розподілених системах повідомлень, в IoT секторі. Ви можете переглянути демо модулі системи ERP.UNO в нашому захищеному середовищі зі своїм центром випуску ECC X.509 сертифікатів. У цій книзі ви знайдете класичну авторську монографію на тему архітектури та імплементації такої системи, побудованої на міжнародних та державних стандартах України:

RFC: 7363, 6350, 4180, 5126, 5652, 8567, 9006, 9011, 9019, 9159, 9100, 8323, 7815, 7228, 6455, 8927, 8259, 4627, 7493, 7159, 4227, 3288, 6025, 5911, 4120, 4122, 7363, 6537, 6940, 7890, 2251-2256, 6960, 5280, 1034-1035, 4033-4035.

ISO: 19510, 19514, 42010, 18033, 14888, 10118, 10116, 15946, 29146, 9075, 27001, 19464, 20922, 21823, 27402, 30161, 30165, 20452, 42010, 19501, 19505, 8824-8825.

NIST: 800-162.

ДСТУ: 28147, 15946, 9798, 4145, 319-422, 319-122.

Постійне посилання твору: https://axiosis.top/sep/
Видавець: Державний науково-дослідний інститут МВС України

ISBN — 978-617-8027-23-0

Підготовлено до друку на Подолі, м. Київ.

Зміст

Розділ 1

Вступ

Формальна модель та програмна архітектура функціонального верифікованого мовного забезпечення для побудови інфраструктурних процесінгових систем орієнтованих на державну модель управління: процесами для проведення зовнішнього аудиту, різними видами розподілених сховищ, телекомунікаційними та реєстровими фреймворками, інтернет-утворюючими сервісами зокрема та для автоматизації захищених автономних офісів і державних підприємств України у цілому.

Система управління державними підприємствами ERP.UNO (State Enterprise Prime) визначає формальну специфікацію та її імплементацію для сучасних оптимізованих підприємств які вимагають сучасних засобів контролю операцій та цілістності даних.

Телекомунікаційна платформа Erlang/OTP від Ericsson успішно застосовується в індустрії мобільними операторами понад 30 років, а її віртуальна машина досі вважається однією з найкращих в галузі. Системи ERP на її базі також уже не один рік використовується у банківській сфері, процесінгу транзакцій, розподілених системах повідомлень, в IoT секторі. Ви можете переглянути демо модулі системи ERP.UNO в нашому захищеному середовищі зі своїм центром випуску ECC X.509 сертифікатів. У цій книзі ви знайдете перелік модулів системи та основні сутності схеми.

Універсальна платформа для створення та забезпечення функціонування інформаційних реєстрів баз (банків) даних різних масштабів, — від базових міжсистемних довідників та класифікаторів, до високонавантажених корпоративних, місцевих та державних ресурсів.

Розділ 2

Фреймворк

По аналогії зі стандартом ISO 42010 «Фреймворку Закмана», фреймворк ДП «ІНФОТЕХ» визначає та уточнює архітектурні рівні з яких складаються сучасні корпоративні інформаційні системи:

— Юридично-документальний рівень
— Обліково-реєстровий рівень
— Зв'язність людей та пристроїв
— Телекомунікаційна платформа
— Схема та метаінформація
— Безпека інтернету

2.1 Юридично-документальний рівень

Згідно фреймворку верхній шостий рівень визначає BPMN процеси згідно яких здійнюється відзеркалення юридично-правивих відносин електронного документообігу. Кожен крок такого процесу, та усі його документи підписуються особистим ключем КЕП посадової особи, що дає змогу проведення диспутів та розслідувань Міністерством юстиції України. Окрім того цей рівень системи орієнтований на аналітику у взаємодії з громадянами через СЕВ ОВВ.

У 2022 році юридично-документальні системи ERP.UNO будуються на сховищі з єдиним простором ключів Facebook RocksDB, що здатне працювати через Intel SPDK на NVMe дисках, наприклад у складі таких сховищ як CEPH. Обсяг обігу документів на великих підприємствах сягає 1ТБ на рік.

2.2 Обліково-реєстровий рівень

Обліково-реєстровий рівень пропонує низькорівневе масштабоване розподілене журнальне сховище даних та метаданих, яке може бути побудоване на реляційних базах даних, базах даних з єдиним простором ключів з гарантіями консистентності (chain-hash) або їх комбінаціях.

Класичні представники цього рівня в системах управління підприємствами: система управління людськими та матеріальними ресурсами, банківські системи PCI DSS, складські системи, системи управління поставками та виробництвом, системи сервісних послуг, системи управління проектами, тощо.

2.3 Зв'язність людей та пристроїв

Рівень зв'язності людей та пристроїв визначає комунікаційні протоколи та технології, які об'єднують головні ресурси підприємства (пристрої та людей) у одну телекомунікаційну мережу. Як правило виробництво складається з багатьох пристроїв що підключаються до промислових шин як MQTT, та робочих місць користувачів.

З точки зору продуктів цей рівень представляється зазвичай корпоративними комунікаторами та дашбордами де здійнюється моніторинг роботизованого обладнання: пристрої, датчики, тощо. Ресурси підприємства — люди та пристрої як правило зберігаються в LDAP директорії підприємства.

2.4 Телекомунікаційна платформа

Рівень платформи визначає засоби мастшабування пам'яті (персистентної та волатильної) та обчислювальних ресурсів (за допомогою процесінгових брокерів доставки повідомлень). Це рівень визначає реляційні бази даних та бази даних з єдиним простором ключів, а також стандарти та протоколи передачі інформації у промислових ERP системах, такі як CSV, JSON, SOAP, BERT, ASN.1, тощо.

2.5 Схема та метаінформація

Рівень схеми даних визначає модель зберігання даних як з точки зору об'єктів-сутностей та і з точки зору технологій та протоколів, які необхідні для їх опису. Головним чином це Фреймворк Закмана та сімейство стандартів які описують UML.

2.6 Безпека інтернету та інфраструктури

Рівень безпеки визначає схему функціонування основного центрального засвідчувального орнагу, акредитованих центрів сертифікації ключів, протоколи шифрування та підпису, директорію підприємства, інтернет протоколи найменування ресурсів. Усе визначено згідно ASN.1 специфікації. Компанія ІНФОТЕХ є утримувачем та автором усіх імплементації.

Розділ 3

Специфікація та сертифікація

3.1 Законодавча база

3.1.1 Загальні положення

Базова версія «МІА: Документообіг» керується наступними загальними положеннями які виражені законами України:

— 2657-XII, Про інформацію[1],
— 7498-ВР, Про Національну програму інформатизації[2],
— 39396-ВР, Про звернення громадян[3],
— 2939-VI, Про доступ до публічної інформації[4]
— 2155-VIII, Про електронні довірчі послуги[5],
— 851-IV, Про електронні документи та електронний документообіг[6],

та розпорядженнями і постановами Кабінету Міністів України:

— 386-2013-р, Розпорядження КМУ #3860-Р [7],
— 373-2006-п, Постанова КМУ #373 [8].

[1] https://zakon.rada.gov.ua/laws/show/2657-XII
[2] https://zakon.rada.gov.ua/laws/show/74/98-вр
[3] https://zakon.rada.gov.ua/laws/show/393/96-вр
[4] https://zakon.rada.gov.ua/laws/show/2939-17
[5] https://zakon.rada.gov.ua/laws/show/2155-19
[6] https://zakon.rada.gov.ua/laws/show/851-15
[7] https://zakon.rada.gov.ua/laws/show/386-2013-р
[8] https://zakon.rada.gov.ua/laws/show/373-2006-п

3.1.2 Базова версія «МІА: Документообіг»

Продукт «МІА: Документообіг» в основному базується на Поставі #55 Кабінету Міністрів України та інших постановах КМУ:

— 55-2018-п, КМУ. Постанова #55 Деякі питання документування управлінської діяльності [9],
— 749-2018-п, КМУ. Постанова #749 Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності[10],
— v0144774-20, ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості". Наказ #144 Про прийняття та скасування національних стандартів ДСТУ 4163:2020 та ДСТУ 9031:2020[11],

але платформа продукту базується на наказаї Міністерства юстиції України, Міністерства цифрової трансформації, Міністерства освіти і науки, та Законами України:

— z1854-12, Міністерство юстиції України. Наказ #16005 Про затвердження Порядку роботи з електронними документами через систему електронної взаємодії органів виконавчої влади з використанням електронного цифрового підпису[12],
— z1039-20, Міністерство цифрової трансформації України. Адміністрація державної служюи спеціального зв'язку та захисту інформації України. Наказ #140614[13],
— z1306-11, Міністерство освіти і науки, молоді та спорту України. Наказ #1207 Про вимоги до форматів даних електронного документообігу в органах державної влади. Формат електронного повідомлення[14],
— z1421-14, Міністерство юстиції України. Наказ #1886/5 Про затвердження Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання[15], — 851-IV, Про електронні документи та електронний документообіг[16],
— 8094-ВР, Про захист інформації в інформаційно-телекомунікаційних системах[17],

---

[9] https://zakon.rada.gov.ua/laws/show/55-2018-п
[10] https://zakon.rada.gov.ua/laws/show/749-2018-п
[11] https://zakon.rada.gov.ua/rada/show/v0144774-20
[12] https://zakon.rada.gov.ua/laws/show/z1854-12
[13] https://zakon.rada.gov.ua/laws/show/z1039-20
[14] https://zakon.rada.gov.ua/laws/show/z1306-11
[15] https://zakon.rada.gov.ua/laws/show/z1421-14
[16] https://zakon.rada.gov.ua/laws/show/851-15
[17] https://zakon.rada.gov.ua/laws/show/80/94-вр

3.1.3 Розширення та додаткові модулі

Розширення «MIA: Провадження»

— 4651-VI, Кримінальний процесуальний кодекс України[18],
— v0298905-20, Офіс генерального прокурора. Наказ #298 Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення[19],

Розширення «MIA: Закупівлі»

— 922-19, Закон України про публічні закупівлі[20],

Розширення «MIA: Зброя»

— 5708, Проект Закону про право на цивільну вогнепальну зброю[21], — 5709, Проект Закону про внесення змін до Кодексу України про адміністративні правопорушення та Кримінального кодексу України для реалізації положень Закону України "Про право на цивільну вогнепальну зброю"[22],

[18] https://zakon.rada.gov.ua/laws/show/4651-17
[19] https://zakon.rada.gov.ua/laws/show/v0298905-20
[20] https://zakon.rada.gov.ua/laws/show/922-19
[21] http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2pf3516=5708skl=10
[22] http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2pf3516=5709skl=10

3.2 Класифікація вимог

3.2.1 Вимоги до інтерфейсу користувача

3.2.2 Вимоги до адміністрування системи

3.2.3 Вимоги типових ділопроцесів системи

3.2.4 Вимоги процесінгової системи

3.2.5 Вимоги інтеграції з зовнішніми системами

3.2.6 Вимоги до розподіленої роботи

3.2.7 Вимоги до комплексу засобів захисту (КЗЗ)

3.2.8 Технічні вимоги до зберігання даних

3.3 Відповідність міжнародним стандартам

3.3.1 Стандарти RFC

3.3.2 Стандарти ISO

3.3.3 Національні стандарти ДСТУ та NIST

3.4 Засоби захисту та ступені гарантії безпеки

3.4.1 Мануальна наочна верифікація

3.4.2 Інтеграційне тестування

3.4.3 Математична верифікація

Розділ 4

Юридично-документальний рівень

4.1 Вступ

Друге видання КНИГИ ERP (англ. ERP BOOK VOL.3 Blue Book) визначає формальну бізнес специфікацію та її імплементацію для сучасних оптимізованих підприємств. Системи ERP на її базі також уже не один рік використовується у банківській сфері, процесінгу транзакцій, розподілених системах повідомлень, в IoT секторі.

4.2 Модулі підприємства

ERP.UNO є комплексом бібліотек (N2O.DEV) та підсистем додатків (ERP.UNO), який використовує загальну шину і загальну розподілену базу даних для швидкіснх операційних вітрин.

ERP — Даний модуль обліково-реєстраційного рівня зберігає основну ієрархічну структуру підприємства, її схему, метаінформацію про типи даних, а також сам інформіцію: записи про персонал, інвентар, компанії та офіси підприємства.

CRM — Система управління зв'язками з громадськістю та органами виконавчої влади: являє собою базову реалізацію постанови #55 КМУ.

CART — Система управління клієнтами: являє собою розширення більш абстрактного додатку CHAT.

4.3 Управління ресурсами

Головним чином інформаційна структура нашого підприємства складається з обчислювальних ресурсов (додатки, запущені в

шині) та накопичувальних ресурсів (дані, збережені в базі даних). SOA архітектура в якості моделі управління обчислювальними ресурсами пропонує асинхронний протокол віддаленого виклику на шинах. Разом з N2O можно використовувати MQTT та інші шини, за допомогою наступних протоколів: TCP, WebSocket. Ці асинхронні протоколи часто називають протоколами реального часу, оскільки в них функції відправки повідомлень завжди миттєво повертають результат. Що ж стосується протоколів для публікації і доступу до даних, то тут може виявитися доречним використання синхронного HTTP протоколу.

4.4 Обчислювальні ресурси

Для SOA архітектури традиційно використовуються асинхронні протоколи доступу до обчислювальних ресурсів. Зазвичай це серверні воркери, які підключені до шини і обслуговують API певного додатку. Кожен додаток має власне консистентне хеш-кільце воркерів. В мережі одночасно працює багато кілець-додатків.

```
config :n2o,
  tcp_services: ['ldap'],
  ws_services: ['chat'],
  mqtt_services: ['erp', 'bpe']
```

за допомогою config.exs файлу можна налаштувати необхідну конфігурацію серії консистентних кілець, кожне з яких працює на власному транспортному протоколі. В даному прикладі показано карту Erlang серверів, які обслуговують черги додатків в шині:

```
> PLM.vnodes
[
  {{:tcp, '/ldap/tcp/4'}, [:n2o_tcp]},
  {{:tcp, '/ldap/tcp/3'}, [:n2o_tcp]},
  {{:tcp, '/ldap/tcp/2'}, [:n2o_tcp]},
  {{:tcp, '/ldap/tcp/1'}, [:n2o_tcp]},
  {{:ws, '/chat/ws/4'}, [:n2o_ws]},
  {{:ws, '/chat/ws/3'}, [:n2o_ws]},
  {{:ws, '/chat/ws/2'}, [:n2o_ws]},
  {{:ws, '/chat/ws/1'}, [:n2o_ws]},
  {{:mqtt, '/erp/mqtt/4'}, [:n2o_mqtt]},
  {{:mqtt, '/erp/mqtt/3'}, [:n2o_mqtt]},
  {{:mqtt, '/erp/mqtt/2'}, [:n2o_mqtt]},
  {{:mqtt, '/erp/mqtt/1'}, [:n2o_mqtt]},
  {{:mqtt, '/bpe/mqtt/4'}, [:n2o_mqtt]},
  {{:mqtt, '/bpe/mqtt/3'}, [:n2o_mqtt]},
  {{:mqtt, '/bpe/mqtt/2'}, [:n2o_mqtt]},
  {{:mqtt, '/bpe/mqtt/1'}, [:n2o_mqtt]},
  {{:caching, 'timer'}, [:n2o]}
]
```

Завдяки такій деталізації можна проектувати гетерогенні системи, включаючи необхідний набір протоколів на портах потрібних машин. Ця же система дозволяє отримати балансування навантаження, підключаючи фізичні ресурси до певних черг шини даних.

В нашій моделі асинхронні протоколи використовуються для управління обчислювальними ресурсами підприємства.

4.5 Накопичувальні ресурси

Розподілені хеш-кільця використовуються не тільки для розподілених обчислень, але і для зберігання даних. Деякі бази даних, наприклад RocksDB та Cassandra, використовують глобальний простір ключів для даних (на відміну від таблично-орієнтованих баз). Саме для таких баз і створено библиотеку KVS, де в якості синхронного транзакційного інтерфейсу — API ланцюжків з гарантією консистентності. Нижче наведено приклад структури ланцюжків екземпляру системи PLM:

```
> :kvs.all :writer
[
  {:writer, '/bpe/proc', 2},
  {:writer, '/erp/group', 1},
  {:writer, '/erp/partners', 7},
  {:writer, '/acc/synrc/Kyiv', 3},
  {:writer, '/chat/5HT', 1},
  {:writer, '/bpe/hist/1562187187807717000', 8},
  {:writer, '/bpe/hist/1562192587632329000', 1}
]
```

В нашій моделі синхронні протоколи використовуються для управління накопичувальними ресурсами підприємства і транзакційного процесингу.

4.6 Типові специфікації

Протоколи визначаються типовими специфікаціями і генеруються для наступних мов: Java, Swift, JavaScript, Google Protobuf V3, ASN.1. Також ми генеруємо валідатори даних по цих типових анотаціях і вбудовуємо ці валідатори в тракт наших розподілених протоколів, тому ми ніколи не дозволимо клієнтам зіпсувати сторадж. Для веб додатків у нас развинута система валідації — як для JavaScript, так і на стороні сервера. Бізнес логіка повністью ізольована в нашій системі управління бізнес процесами, де кожен бізнес процесс є процесом віртуальної машини. Всі ланцюжки модифікуються атомарним чином, підтримують flake адресацію, і не вимагають додаткової ізоляції у своєму примітивному використанні. Тому ви можете трактувати базу як розподілений кеш і використовувати її з фронт додатків для примітивних випадків.

4.7 Архітектура CRM системи

4.7.1 Сторінки

4.7.2 Елементи

4.7.3 Комболукап

4.7.4 Сервіси

4.7.5 CEB OBB

4.7.6 Шаблони

4.7.7 Дерева

4.7.8 Процеси

4.7.9 Документи

4.7.10 Редактори

Розділ 5

Обліково-реєстраційний рівень

5.1 Вступ

Друге видання КНИГИ ERP (англ. ERP BOOK VOL.3 Blue Book) визначає формальну бізнес специфікацію та її імплементацію для сучасних оптимізованих підприємств. Системи ERP на її базі також уже не один рік використовується у банківській сфері, процесінгу транзакцій, розподілених системах повідомлень, в IoT секторі.

5.1.1 Види реєстрів

5.1.2 Функціональні можливості

5.2 Модулі підприємства

ERP.UNO є комплексом бібліотек (N2O.DEV) та підсистем додатків (ERP.UNO), який використовує загальну шину і загальну розподілену базу даних для швидкіснх операційних вітрин.

FIN — Фінансовий модуль підприємства для бухгалтерії, зберігає бізнес процеси, які представляють собою рахунки учасників системи: персонал (для нарахування зарплат), рахунки та субрахунки підприємства (для здійснення економічної діяльності) і зовнішні рахунки в платіжних системах.

ACC — Система управління персоналом: зарплатні відомості, календар підприємства, відпустки, декретні відпустки, інші календарі.

SCM — Система управління ланцюжком поставок: головний БП системи — експедиційний процес доставки товарів ланцюжку одержувачів за допомогою транспортних компаній.

PLM — Система управління життєвим циклом проектів і продуктів. Також містить CashFlow та P&L звіти.

PM — Система управління проектами підприємства з деталізацією часу і протоколів прийому-передачі (прийняті коміти в гит-хабі).

WMS — Система управління складом та деталями.

TMS — Система управління транспортом підприємства.

5.3 Архітектура CART системи

Розділ 6

Технологічний рівень зв'язності людей та пристроїв

6.1 Вступ

Архітектурна компанія SYNRC розробляє та підтримує систему автоматизації підприємства N2O.DEV, побудовану згідно формальної специфікації яка призначена для розробки багатофункціональних гетерогенних платформ для додатків та сервісів на основі шини та розподіленої бази даних. N2O.DEV уже використовується у банках, системах повідомлень, державних підприємствах та інших менших чисельних організаціях в Америці, Європі та Азії.

Друге видання КНИГИ N2O (англ. N2O BOOK Vol. 2 Green Book) визначає форамальну специфікацію на програмне забезпечення усіх рівнів моделі Закмана для підприємств ISO-42010, містить широкий спектр прикладів, розказує про складові компоненти та є вичерпним авторським стартовим посібником для курсу навчання розробки технологічних програм для платформи Erlang.

6.2 Структура виробничого процесу

6.3 Інтерфейс NITRO

6.4 Сховище KVS

6.5 Логіка BPMN

6.6 Додатки MQTT та WebSocket

Розділ 7

Рівень телекомунікаційної платформи

Розділ 8

Схема даних, типи, валідація та генерація

8.1 Графічні мови представлення метаінформації UML

8.2 Алгебраїчні мови та System F

8.3 Моделі процесів

8.4 Верифікація типів

8.5 Генерація SDK та конекторів

8.6 Базова схема підприємства ERP.UNO

Розділ 9

Інфраструктурний рівень безпеки інтернету

Розділ 10

Апробація

ЄРЗ (Єдиний реєстр зброї НПУ), СУСЗЦЗ (Система управління силами та засобами цивільного захисту ДСНС), ЄІС (Єдина інформаційна система МВС), ФП МТРЗ (Функціональна підсистема матеріально-технічного та ресурсного забезпечення МВС), ГСЦ (Головний сервісний центр МВС).