Versium — типовые сценарии автоматизации ИБ и ИТ

Платформа Versium представляет из себя гибкий конструктор для автоматизации процессов ИБ и ИТ. Ниже описаны основные этапы и модули, через которые обычно проходит реализация типовой задачи: от проектирования сущностей и UI до интеграций, действий, виджетов, рабочих процессов и настроек безопасности.

Модель данных

Основу любой автоматизации в Versium составляет модель данных: сущности, их атрибуты и связи.

- Создание и редактирование сущностей
  - Навигация: Администрирование → Системные таблицы.
  - Можно «на горячую», без перезагрузки, создавать новые таблицы (сущности) — например, «Договоры», «Инциденты».
  - Добавляйте атрибуты (типы: строка и др.) и настраивайте связи (ссылки между сущностями, например, ИТ-актив → Договор).
- Таблицы-расширения (one-to-one)
  - Для хранения специфических атрибутов подмножества записей используйте таблицы-расширения, связанные с базовой таблицей 1:1.
  - Пример: часть инцидентов приходит из MaxPatrol — создайте расширение «Инциденты MaxPatrol» к основной таблице «Инциденты» и храните только профильные поля в расширении.
  - В UI атрибуты расширений прозрачно видны как часть основной сущности, а в БД — лежат отдельно и подгружаются по необходимости, снижая нагрузку.
- История изменений
  - На уровне атрибута доступна опция «Сохранять историю».
  - Изменения по отмеченным полям доступны на системной странице «История» формы объекта.

Пользовательские интерфейсы (экраны)

В Versium UI строится через сущности «экраны»: экраны списков и экраны форм. Создаются/редактируются во встроенном редакторе форм (drag-and-drop)

- Экран списка
  - Навигация: Администрирование → Системные таблицы → выбрать таблицу → Экраны → Создать → Тип «Экран списка».
  - Табличное представление записей с настраиваемым набором колонок.
- Экран формы
  - Навигация: Администрирование → Системные таблицы → выбрать таблицу → Экраны → Создать → Тип «Экран формы».
  - Можно управлять расположением и размером полей, группировать их по «страницам» (вкладкам), менять порядок вкладок.
  - Доступны 4 системные страницы (можно включать/скрывать):
    - Комментарии — обсуждение по текущей записи, вложения (файлы) к комментариям.
    - История — изменения атрибутов с включенной опцией «Сохранять историю».
    - Документы — артефакты, прикрепленные к записи (включая вложения из комментариев).
    - Рабочие процессы — визуальная схема активных процессов и текущий шаг по записи.

Интеграции

Интеграции в Versium делятся на два подхода: внешний интеграционный сервис и встроенные модули.

- Навигация: Администрирование → Интеграционные сервисы.
- Внешний интеграционный сервис
  - Разворачивается рядом с платформой как Windows-служба или Linux-daemon (.NET-приложение, исходный код открыт).
  - Администратор реализует логику получения данных из REST API, БД, файлов и т. п., приводит их к формату Versium и отправляет в платформу.
  - В Versium настраивается интеграционный мэппинг: сопоставление входящих полей с полями БД, заполнение ссылок/атрибутов, правила поиска и обновления. Встроенный редактор кода имеет функции автодополнения, позволяющий упрощать написания подобных мэппингов.
  - Поиск записей по ключам:
    - Поддерживаются простые и составные ключи (например, серийный номер + MAC-адрес).
    - Возможны каскадные сценарии поиска: по серийному номеру, если не найдено — по MAC, если не найдено — по IP.

    - Управление режимами: только обновление найденных в Versium записей / создание новых при отсутствии.
- Встроенные интеграционные модули
    - Реализованы в ядре Versium для типовых систем: например, Kaspersky Security Center (KSC), Kaspersky Anti Targeted Attack (KATA), MaxPatrol, PT NAD, Active Directory и др.
    - Не требуют развертывания отдельного сервиса: достаточно выбрать и настроить мэппинг в интерфейсе.
- Учетные записи (секреты)
    - Объект «Учетная запись» хранит параметры подключения (логин, пароль, строка подключения и пр.) в зашифрованном виде.
    - Доступ к данным учетных записей ограничен администраторами.
    - Конкретная учетная запись выбирается в настройках интеграции и передается при вызове.
- Запуск интеграций по расписанию
    - В Versium можно создавать периодические задачи для вызова интеграционных сервисов (например, каждую субботу в 06:00 — загрузка сотрудников из Active Directory).
    - Навигация: Администрирование → Периодические задачи.

Динамические API-сервисы

Подход для входящих интеграций с инициированием на стороне внешней системы или для предоставления данных наружу.

- Навигация: Администрирование → API сервисы.
- Входящие вызовы (webhook-сценарии)
    - Создайте новый endpoint, определите входной JSON и обработку скриптом (.NET), написанным во встроенном редакторе кода.
    - Скрипт может создавать/изменять объекты в Versium с учетом логики любой сложности.
- Исходящие сценарии (данные для BI и др.)
    - Реализуйте endpoint, который по GET/POST возвращает агрегированные данные, сформированные в скрипте.
- Безопасность API
    - Доступ к динамическим API-сервисам — только после авторизации с использованием JWT-токена.
    - Права доступа проверяются на уровне пользователя и конкретного API-сервиса.

Системные действия

Механизм расширения логики работы с объектами без переписывания базовых экранов. Типы действий:

- Навигация: Администрирование → Действия.
- Мастер (wizard)
  - XML-разметка для описания UI + .NET-код для логики.
  - Поддерживает пошаговые сценарии (next → next → finish), поля, таблицы, валидации, кнопки, виджеты.
  - Встроенный редактор кода с автодополнением (IntelliSense).
- Скрипт
  - Чистый .NET-код без UI, выполняется в фоне или по кнопке.
  - Примеры: отправка письма, массовые перерасчеты, технические операции.

Контекстные действия

- Если системное действие привязано к таблице контекста, кнопка действия появляется на форме соответствующей записи.
- Примеры: «Назначить ответственного» для договора, «Привязать инциденты к ИТ-активу».

Виджеты

Визуальные компоненты для агрегирования и отображения данных.

- Навигация: Администрирование → Виджеты.
- Бесконтекстные
  - Размещаются на главной странице/дашбордах.
  - Пример: круговая диаграмма по статусам всех инцидентов, таблица с инцидентами в статусе "Новый".
- Контекстные
  - Добавляются на форму объекта в редакторе экрана формы.
  - Пример: диаграмма по статусам дочерних инцидентов для открытого ИТ-актива.

Рабочие процессы

Визуальный движок для автоматизации маршрутов обработки сущностей.

- Навигация: Администрирование → Рабочие процессы.
- Редактор процессов
  - Графическая схема, где шагом может быть Мастер или Скрипт.
  - Для каждого шага задаются условия переходов.
- Условия старта
  - Запуск после создания, после изменения или после создания/изменения записи.
  - При наступлении события проверяется что для текущей записи (например, договора) нет данной запущенной схемы. Если нет, то проверяется условие перехода на первый шаг. Если условие выполняется, процесс инициируется.

    - Для уже запущенных схем, при обновлении объекта проверяются условия перехода на следующие шаги. Например, переход на следующий шаг при статусе "В работе".
- Назначение задач
    - Шаг-мастер назначается на пользователя/группу.
    - Поддерживаются режимы «каждый из группы» (массовое согласование) и «любой из группы».
    - У пользователя появляется задача; индикатор виден в интерфейсе, в хедере, в правом верхнем углу.
- Визуализация
    - Текущий процесс и шаг отображаются на системной странице «Рабочие процессы» формы объекта.

Модель безопасности и доступов

Два уровня разграничения: роли и группы доступа.

- Роли
    - Навигация: Администрирование → Роли.
    - Права на объекты (видеть/создавать/редактировать/удалять).
    - Привязка конкретных экранов формы/списка для роли (разные представления для разных ролей, например, без финансовых полей).
    - Права на пункты меню, действия, виджеты, API-сервисы.
    - Мэппинг внешних ролей: привязка групп Active Directory к ролям Versium для автоматического назначения при входе (см. гостевой вход).
- Группы доступа (разграничение на уровне записей)
    - Навигация: Администрирование → Группы доступа.
    - Иерархические группы для сегментации данных (например, по филиалам).
    - Если у записи заполнена ссылка на группу доступа, её видят только пользователи с этой группой или группой более высокого уровня.
    - Если ссылка не заполнена, запись видна всем (механизм опционален — используйте при необходимости).

Практический пример: «Договор»

1. Модель данных:
   - Создать таблицу «Договоры».
   - Добавить атрибуты: Номер договора (строка), Контрагент, Дата начала/окончания, Ответственный и др.
   - Настроить связи: ИТ-актив → Договор (ссылка много-к-одному).
2. UI:
   - Создать экран списка с колонками: Номер, Контрагент, Статус, Ответственный, Даты.
   - Создать экран формы; разнести поля по страницам. Включить системные страницы «Комментарии», «Документы», «История», «Рабочие процессы».
3. Интеграция:
   - Настроить интеграционный мэппинг для загрузки договоров из внешней системы.
   - Создать периодическую задачу для выполнения интеграции
   - Ключ поиска: Номер договора (или составной ключ).
4. Системные действия:
   - Мастер «Назначить ответственного» с валидациями (например, обязательность заполнения перед переходом на следующий этап).
5. Рабочий процесс:
   - Схема согласования: Старт «после создания или изменения», шаги «Проверка данных» (скрипт) → «Утверждение бюджета» (мастер) → «Финальное согласование».
   - Назначение задач на роли/группы.
6. Доступы:
   - Роль «Специалист по учету» — просмотр, без удаления; роль «Финконтролер» — расширенная форма с финансовыми полями.
   - Группы доступа по филиалам.

Рекомендации и лучшие практики

- Планируйте ключи интеграции
  - Отдавайте предпочтение устойчивым ключам (серийный номер + MAC). Используйте каскадный поиск, если это оправдано.
- Используйте таблицы-расширения
  - Для редких/специфических полей применяйте 1:1-расширения — это уменьшит нагрузку на основную таблицу.
- Включайте историю точечно

    - Отмечайте «Сохранять историю» только для действительно важных атрибутов, чтобы не раздувать объем хранения.
- Разграничение прав
    - Сочетайте роли (функциональные права) и группы доступа (сегментация данных) для принципа наименьших привилегий.
- Тестируйте системные действия и процессы
    - Используйте встроенный редактор с автодополнением. Валидируйте сценарии на тестовых данных до публикации.

См. также

- Ссылки пока не реализованы
- Модель данных: системные таблицы
- Экраны: списки и формы
- Интеграции и мэппинги
- Динамические API-сервисы
- Системные действия: Мастер и Скрипт
- Редактор рабочих процессов
- Роли и группы доступа

Если вам нужен пошаговый гайд по конкретному сценарию, начните с Практического примера и адаптируйте его под ваши сущности и процессы.