|  |
| --- |
| **Система управления идентификацией и доступом****«AtomID»** |
|  |
| **ОПИСАНИЕ ЖИЗНЕННОГО ЦИКЛА** |
|  |
| **RU.ЕРТД.00101-01 91 01** |
|  |
| **Версия документа 1.0** |

**СОДЕРЖАНИЕ**

[1 ОБЩИЕ СВЕДЕНИЯ 3](#_Toc57911557)

[2 УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ 4](#_Toc57911558)

[2.1 Маркировка 4](#_Toc57911559)

[2.2 Список элементов конфигурации 5](#_Toc57911560)

[2.3 Порядок управления изменениями 7](#_Toc57911561)

[2.4 Отслеживание и исправление обнаруженных ошибок ПО 10](#_Toc57911562)

[2.5 Управление доступом к изменению конфигурации 11](#_Toc57911563)

[3 Инструментальные средства разработки 13](#_Toc57911564)

# Общие сведения

Настоящий документ содержит описание жизненного цикла Системы управления идентификацией и доступом «AtomID» (далее по тексту – Изделие, AtomID).

AtomID реализует технологию единого входа (Single Sign-On) для управления идентификацией и доступом пользователей. Функции по защите информации, реализованные в AtomID, описаны в разделе 2 настоящего документа. Общая схема работы Изделия представлена на Рисунке 1.

В Изделии должны быть реализованы следующие функций по защите информации:

* идентификация и аутентификация пользователей;
* ролевое разграничение доступа;
* регистрация событий безопасности;
* обеспечение доступности информации.

Изделие является программным средством обеспечения безопасности информационных технологий. Изделие может применяться для защиты информации в значимых объектах критической информационной инфраструктуры 3 категории, в государственных информационных системах 3 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, а также для обеспечения до 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 3-го типа.

Предприятие-разработчик и производитель: Акционерное общество «Гринатом» (АО «Гринатом»); адрес места нахождения: 119017, г. Москва, ул. Большая Ордынка, д. 24; адрес места осуществления лицензируемого вида деятельности: 115230, г. Москва, 1-й Нагатинский проезд, д. 10, стр. 1; лицензия на деятельность по разработке и производству средств защиты конфиденциальной информации № 1993 от 19.02.2021, действует бессрочно.

Рисунок 1

1. Пользователь обращается к защищаемому приложению (1). Если пользователь не прошел аутентификацию, происходит перенаправление на AtomID (2).
2. Пользователь автоматически переходит в веб-интерфейс AtomID (2). Далее, в зависимости от настроек Изделия, пользователь может ввести свои логин и пароль или осуществить вход через стороннего провайдера идентификации по протоколам SAML 2.0, OIDC или SPNEGO/Kerberos (7).
3. В случае успешной аутентификации, происходит обмен служебной информацией между AtomID и веб-приложением (3), пользователь становится авторизованным.
4. Администратор может настраивать AtomID с использованием веб-интерфейса Изделия или административного API (4).
5. Собственные данные (УЗ, группы, настройки клиентов и пр.) AtomID хранит в СУБД (5)
6. Учётные записи пользователей могут быть созданы вручную администратором, путем импорта из каталогов LDAP/AD (6), в ходе самостоятельной регистрации.

# Управление конфигурацией

## Маркировка

Маркировка осуществляется с учетом требований ЕСПД. Для маркировка программы и ее программного документа (Спецификации) применяются правила, указанные на Рисунке Рисунок 2. Допускается пропуск кода страны в случае, если не планируется поставка за рубеж.

Рисунок 2

Структура обозначения других программных документов представлена на Рисунке Рисунок 3:

Рисунок 3

Таким образом, Системе управления идентификацией и доступом «AtomID» присвоен номер **RU.ЕРТД.00101-01**. Коды программной документации представлены в Таблице Таблица 1.

Таблица 1

|  |  |  |
| --- | --- | --- |
| № | Код документа | Наименование документа |
|  | - | Спецификация |
|  | 30 | Формуляр |
|  | 32-1 | Руководство администратора, часть 1 |
|  | 32-2 | Руководство администратора, часть 2 |
|  | 32-3 | Руководство администратора, часть 3 |
|  | 50-59 | Зарезервировано для тестовой документации |
|  | 90 | Технические условия |
|  | 91 | Описание жизненного цикла |
|  | 92 | Процедура обновления |
|  | 93 | Описание архитектуры |
|  | 94 | Функциональная спецификация |
|  | 95 | Проектная документация |
|  | 96 | Процедуры тестирования при разработке безопасного программного обеспечения |
|  | 97 | Руководство по безопасной разработке |
|  | 98 | Модель угроз безопасности информации |

Для маркировки версий файлов в Gitlab используются метки, автоматически проставляемые при каждом новом изменении (Рисунок 4). Иные требования к маркировке в Gitlab не предъявляются.

Рисунок 4 Уникальная маркировка фала

Маркировка бинарных файлов, полученных в результате сборки из исходных текстов на локальном компьютере разработчика, осуществляется следующим образом. Номер версии состоит из трех чисел, разделенных точкой, например 1.2.33. При каждом обновлении Изделия номер версии увеличивается по следующим правилам:

* первое число — при значительных изменениях программного комплекса, которые вносятся независимо от заказчика;
* второе число — выпуск новой измененной версии без обратной совместимости с предыдущими версиями;
* третье число — выпуск новой измененной версии с сохранением обратной совместимости.

## Список элементов конфигурации

Список элементов конфигурации средства, включающий в том числе документацию, представлен в Таблице Таблица 2

Таблица 2

|  |  |  |
| --- | --- | --- |
| № | Обозначение | Наименование |
|  | RU.ЕРТД.00101-01 | Дистрибутив Системы управления идентификацией и доступом «AtomID» |
|  | RU.ЕРТД.00101-01 90 01 | Система управления идентификацией и доступом «AtomID». Технические условия.  |
|  | RU.ЕРТД.00101-01 30 01 | Система управления идентификацией и доступом «AtomID». Формуляр.  |
|  | RU.ЕРТД.00101-01 32 01 | Система управления идентификацией и доступом «AtomID». Руководство администратора. |
|  | RU.ЕРТД.00101-01 91 01 | Система управления идентификацией и доступом «AtomID». Описание жизненного цикла. |
|  | RU.ЕРТД.00101-01 92 01 | Система управления идентификацией и доступом «AtomID». Процедура обновления. |
|  | RU.ЕРТД.00101-01 93 01 | Система управления идентификацией и доступом «AtomID». Описание архитектуры безопасности. |
|  | RU.ЕРТД.00101-01 94 01 | Система управления идентификацией и доступом «AtomID». Функциональная спецификация. |
|  | RU.ЕРТД.00101-01 95 01 | Система управления идентификацией и доступом «AtomID». Проектная документация |
|  | RU.ЕРТД.00101-01 96 01 | Система управления идентификацией и доступом «AtomID». Процедуры тестирования при разработке безопасного программного обеспечения |
|  | RU.ЕРТД.00101-01 98 01 | Система управления идентификацией и доступом «AtomID». Модель угроз безопасности информации. |

## Порядок управления изменениями

Для управления конфигурацией используется Git - распределённая система контроля версий. В качестве системы управления репозиториями программного кода для Git используется программное обеспечение GitLab.

Центральный репозиторий GitLab функционирует на вычислительных мощностях АО «Гринатом». Локальная разработка ведется на ноутбуках программистов с последующей передачей исходных кодов в центральный репозиторий.

Роли и зоны ответственности

|  |  |  |
| --- | --- | --- |
| № | Роль | Описание |
|  | * Системный аналитик
 | * Уточнение, анализ, формализация системных требований на основании бизнес требований;
* Определение критериев готовности по каждой "истории";
* Коммуникации с разработчиками для поиска решения, постановка задач в OpenProject;
* Участие в проектирование REST API совместно с разработчиками и техлидом (новых методов/ необходимых изменений в существующих, описание контракта и логики работы);
* Описание работ на фронт (use case, поведение элементов интерфейса, какие api использовать);
* Разработка ERD;
* Саппорт команды разработки в течении спринта;
* Ревью тест кейсов, подготовленных тестировщиками;
* Тестирование, в рамках кроссфункциональности;
* Оценка трудоемкости задачи и сроков ее исполнения (участие в приоритезации бэклога);
* Выборка и анализ данных при помощи SQL запросов;
* Демонстрация результатов спринта.
 |
|  | * Тимлид системных аналитиков
 | * Управление группой системных аналитиков;
* Выстраивание процессов;
* Определение формата документации;
* Распределение задач;
* Контроль результатов;
* Обучение и помощь в выполнении поставленных задач;
* Проведение 1:1 с системными аналитиками;
* Выполнение функций системного аналитика по наиболее сложным задачам;
* Анализ резюме, проведение собеседований с системными аналитиками.
 |
|  | * Руководитель проекта (менеджер, администратор)
 | * Управление Проектом: Сроки , Качество, Объем, Бюджет;
* Планирование и анализ работ по проекту (сроки, ресурсы и объёмы работ);
* Формирование и контроль бюджета проекта;
* Постановка задач проектной команде (для команды разработки и аналитики постановка задач через Продуктового менеджера). Контроль выполнения, сроки выполнения, ресурсы;
* Обеспечение достижения результатов по проекту;
* Руководство проектной командой вне зависимости от административной подчиненности сотрудников;
* Обеспечение коммуникации со смежными подразделениями, участвующими в проекте. Контроль исполнения проектных задач этими подразделениями;
* Обеспечение коммуникации внутри проектной команды и информирование сотрудников о задачах и ходе Проекта, достигнутых результатах, принятых решений и изменений;
* Проведение коммуникаций с ключевыми заинтересованными сторонами на уровне ГК;
* Информирование о существующих отклонениях Руководства (Руководители ГА) и Заказчика. Участие в эскалации вопросов на уровне ГА, ГК;
* Управление рисками, отклонениями Проекта, влияющими на достижение ключевых вех и/или конечного результата Проекта (выявление, минимизация, исключение);
* Контроль рисков и критических вопросов;
* Контроль сроков разработки проектной документации.
 |
|  | * Техлид
 | * Проектирование сервисов (логика разбиения по областям ответственности, взаимодействие с другими сервисами, логирование);
* Описание подхода к взаимодействию с внешними системами;
* Описание системы to be (детально на несколько спринтов, общая схема готового решения);
* Процесс разработки (что тестируем, как подготавливаем версии продуктов, как доставляем решение пользователю);
* Поиск решения нестандартных задач. (SSO, права доступа);
* Контроль соблюдения договорённостей в коде.
 |
|  | * Тимлид разработки
 | * Список активностей
* 1:1 для поддержания команды в тонусе и понимая, что ее волнует;
* Регулярные синки по темам;
* Основные скрам процедуры;
* Дейлики - для информирования;
* PBR- помощь в оценке, если нужна;
* Ретро - сбор более общих проблем для решения, но это скорее сейчас про скрам-мастеров;
* Планирование - для информирования;
* Участие во встречах статусах;
* Анализ резюме и проведение собеседований;
* Обсуждения и проработка процессов для движения в правильном направлении;
* Проработка и “вытаскивание” каких-то вопросов на поверхность, связанных с разработкой нашего продукта;
* Фасилитация в команде;
* Онбординг;
* Участие в оценке конкретных задач (скорее, по требованию);
* Участие в крупноблочной оценке для построения планов;
* Проработка крупных задач до передачи их в разработку;
* Сбор и работы по техдолгу
* Зоны ответственности- команда разработки    - оценка задач    - соблюдение сроков    - качество работы    - помощь с техническими и продуктовыми решениями    - комфортная и продуктивная атмосфера    - проработка сложных кейсов, но тут скорее совместное и для того, чтобы подготовить их к передаче в команду разработки- команда    - найм    - онбординг (в HCM: Надя рассказывает про продукт, роудмап; Артем - технологическая часть; Леша - скрам, что и как)    - мотивация    - развитие- продукт    - делюсь экспертизой    - готовность что-то подхватить- тестирование    - делюсь экспертизой    - готовность что-то подхватить
 |
|  | * Менеджер продукта
 | * Контроль формирования и документального оформления функциональных требований к бизнес-процессам проектов;
* Организация методологического сопровождения разработки и внедрения и развития систем;
* Разработка видения продукта/процесса и доведение его до успешной реализации;
* Наблюдение, изучение, обсуждение и анализ требований конечных пользователей продукта/процесса;
* Сбор потребностей и их систематизация в виде "историй" (описания процесса с точки зрения пользовательского опыта);
* Формирование состава MVP1 c учетом имеющихся ограничений ресурсов и последовательного развития продукта/процесса;
* Создание, поддержка и приоритизация бэклога по продукту/процессу;
* Определение объема MLP по каждому эпику;
* Коммуникация требований команде и обеспечение понимания требований командой (через СА);
* Предоставление обратной связи по работе команды ее участникам и группе развития персонала;
* Обеспечение планирования релизов совместно с заинтересованными лицами;
* Создание и поддержание отношений с заинтересованными лицами;
* Отслеживание и измерение прогресса по продукту/процессу;
* Взаимодействие с разработчиками и дизайнерами на всех этапах проекта;
* Предоставление подробных рекомендаций при разработке продукта/процесса;
* Отслеживание за последними тенденциями рынка разрабатываемых продуктов;
* Общение с функциональным закзачиком и другими заказчиками;
* Постановка и контроль требований к дизайну и исследованиям.
 |
|  | * Тимлид группы тестирования
 | * Проведение 1:1 с тестировщиками и техническим писателем
* Определение формата тестовой документации
* Выстраивание процессов тестирования
* Управление группой тестирования
* Постановка задач техническому писателю (при отсутствии у него текущих задач)
* Помощь в выполнении задач
* Проведение обзорных показов системы вновь прибывшим в команду
* Анализ резюме, проведение собеседований
* Выявление и анализ багов, заведение багов
* Написание и анализ тест-кейсов до передачи их на ревью аналитиками
* Взаимодействие с ДКС для управления процессом НТ
* Формирование требований по нагрузке, сбор метрик, хранение и обработка метрик (влияние новых фич на систему)
* Стандартизация и выработка общего подхода по заведению багов (формат бага - как заводим, что содержит, какие логи прикладываем и т.д.)
* Стандартизация и выработка общего подхода к заведению тест-кейсов
* Коммуникация с девопсами
 |
|  | * Тестировщик
 | * Выполнение задач, поставленных тимлидом группы тестирования
 |
|  | * Бизнес-аналитик
 | * Сбор требований к системе от бизнес-пользователей (в зависимости от задачи: от БВП, Дивизионов, предприятий, ЦО по УП и т.д.) и анализ требований
* Уточнение деталей функционирования действующих систем отрасли (РЕКОРД, ИАСУП и т.д.) при необходимости
* Подготовка предложений по оптимизации бизнес-процессов
* Подготовка бизнес-требований и их согласование с ГК
* Передача бизнес-требований дизайнерам и системным аналитикам, доработка бизнес-требований при необходимости
* Планирование спринтов бизнес-аналитиков
* Участие в демонстрации макетов и готовой системы Заказчику
* Участие в подготовке проектных документов
 |
|  | * Тимлид бизнес-аналитиков
 | * Участие в проведении собеседований бизнес-аналитиков
* Проработка бизнес-анализа по наиболее сложным задачам (в том числе по миграции и интеграции)
* Проверка бизнес-кейсов (по запросу)
* Помощь в планировании спринтов бизнес-аналитиков
* Помощь в подготовке проектных документов
* Контроль важных писем от бизнес-аналитиков на ГК / УК / предприятия
* Консультирование по системе РЕКОРД (ETWeb) и прошлым проектам внедрения
* Проведение 1:1 с бизнес-аналитиками
* Контроль мероприятий по миграции данных
 |
|  | * Тимлид дизайнеров
 | * Менторство и обучение дизайнеров (курирование всех дизайнеров)
* Приведение системы к единообразию
* Проработка пути пользователя в интерфейсе, исходя из поставленных целей (итерациями);
* Формирование дизайн-системы (ui kit, guidline);
* интеграция дизайн-системы в продукт (+ревью результата);
* поддержка консистентности продукта
 |
|  | * Scrum-мастер
 | * Ответственность за управление Scrum процессами и координацией Scrum команд в соответствии с методологией Agile
* Ответственность за устранение возникающих препятствий в работе Scrum команд
* Планирование, проведение и фасилитиция Scrum церемоний: ежедневных stand-up митингов, PBR, Планирования, Демо
* Содействие в создании бэклога продукта и приведение его в состояние готовности к следующему спринту
* Защита интересов ѕсrum команд
* Управление командой и окружением проекта для обеспечения эффективности командной работы
* Помощь Владельцу Продукта в части разработки стратегии и целей проекта с привлечением всех заинтересованных сторон
 |
|  | * Лид Scrum-мастеров
 | * Масштабирование Scrum - Выстраивание процесса поставки с использованием SAFe, LeSS, Nexus илиSpotify. Помогает Владельцу Продукта в формировании дорожной карты работ на несколько кварталов с учетом приоритетов. Организует совместное квартальное планирование целей множества команд.
* Агент изменений - планирование и запуск организационных изменений в компании, подразделении или команде, реорганизации процессов, оргструктуры, трекинг трансформации. Запуск agile-направлений -Value Streams. Дизайн продуктовых команд.
* Agile коучинг – коучинг скрам мастеров, работа со стейхколдерами и владельцами продуктов, изучение с ними инструментов, которые помогут им в работе, фасилитация встреч.
 |

Процесс разработки

Таблица 3 Описание элементов разработки

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | * **Сущности (уровень абстракции)**
 | * **Наименование**
 | * **Объем работ**
 |
|  | * Высший уровень
 | * Strategic Themes (стратегические темы, проекты)
 | * несколько месяцев, квартал
 |
|  | * Первый уровень
 | * Epic (Функции)
 | * несколько спринтов
 |
|  | * Второй уровень
 | * Story, Task (Задача)
 | * один спринт
 |
|  | * Третий уровень
 | * SubTask (Подзадача)
 | * один день
 |

Описание статусов элементов разработки:

**Epic**

* To Do
* In Progress
* Done

**Task**

* To Do
* In Progress
* Done

**Story**

* ToDo
* Аналитика - этап, на котором работают аналитики с методологами, обсуждают с пользователями; формируется описание, критерии приемки, сценарии. (Business Analysis, System Analysis, Design)
* Согласование (Критерии приемки не меняются после согласования)
* Декомпозиция и Оценка (Команда декомпозирует Задачу на Подзадачи, затем оценивает)
* Backlog (готова к разработке)
* Development - этот статус включает все этапы разработки, пока хотя бы одна Подзадача истории находится в тестировании или Code Review история остается в статусе Development. Только когда все подзадачи протестированы, баги закрыты, тестировщик переводит ВСЮ историю в статус Review
* Review - принимается решение о готовности, если все ок, то закрываем ее и показываем на Демо спринта
* Done

**SubTask**

* ToDo
* Development
* Code Review
* Ready for Test
* Test
* Done

Контроль версий

Для контроля версий в Git используются метки (тэги). Метка – цифро-буквенный идентификатор, присваиваемый разрабатываемому программному обеспечению для его однозначной идентификации, а также для идентификации файлов, входящих в его состав.

Отслеживание изменений осуществляется с помощью штатных средств системы программного обеспечения GitLab. В журнал аудита заносятся все изменения, вносимые в репозиторий. Пример такой записи представлен на Рисунке Рисунок 5.

Рисунок 5

На случай возникновения нештатной ситуации ведется полное ежедневное резервное копирование данных, содержащихся в системе контроля версий.

## Отслеживание и исправление обнаруженных ошибок ПО

Все обнаруженные недостатки, включая недостатки безопасности, заносятся в систему управления процессами OpenProject. Каждой записи присваивается свой уникальный идентификатор. При исправлении недостатка, в запись добавляется ссылка на Merge request. В системе контроля версии GitLab также указывается идентификатор записи в OpenProject.

## Управление доступом к изменению конфигурации

Все фалы конфигурации AtomID хранятся в системе контроля версии GitLab, для доступа в которую необходимо пройти процедуры идентификации и аутентификации (Рисунок 5).

Рисунок 7 Окно приветствия Gitlab

Для элементов конфигурации AtomID отведен отдельный проект под названием IAM. Данный проект является приватным, доступ к нему ограничен определенным кругом лиц (Рисунок 8).

Рисунок 8 Ограниченный доступ к проекту

# Инструментальные средства разработки

В Таблице Таблица 3 представлена информация о инструментальных средствах, используемых в ходе разработки Система управления идентификацией и доступом «AtomID». Специальные настройки инструментальных средств не используются.

Таблица 4

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование | Разработчик | Ссылка на ЭД |
|  | IntelliJ IDEA 2021.1.3 | Jetbrains | <https://www.jetbrains.com> |
|  | Insomnia 2022.2.1 | Kong Inc | [https://insomnia.rest](https://insomnia.rest/) |
|  | Dbeaver Community 22.0.2.202204041542 | JKISS project | <https://dbeaver.io/> |
|  | Notepad++ 8.3.3 | Don Ho | <https://notepad-plus-plus.org/> |
|  | Docker Desktop 4.6.1 | Docker, Inc. | <https://www.docker.com/products/docker-desktop/> |
|  | Apache Directory Studio 2.0.0.v20210717-M17 | The Apache Software Foundation | <http://directory.apache.org/studio> |