Руководство по эксплуатации Flexberry Security

1. Введение

Настоящий документ предназначен для администраторов и разработчиков, ответственных за эксплуатацию системы разграничения прав доступа в приложениях, построенных на **Программной платформе Flexberry**, с использованием технологического компонента **Flexberry Security**.

Документ содержит информацию, необходимую для выполнения повседневных задач управления безопасностью: настройку политик доступа, управление пользователями и ролями, интеграцию с приложениями и диагностику.

Примечание: Вопросы установки, развертывания и системных требований описаны в отдельном документе «Руководство по установке Flexberry Security».

2. Общие принципы работы

Flexberry Security реализует систему безопасности на основе ролей (RBAC — Role-Based Access Control). Основные сущности системы:

- **Пользователь (Subject)**: учетная запись, соответствующая человеку или системе.
- **Роль (Role)**: набор полномочий. Пользователю может быть назначено несколько ролей.
- **Операция (Operation)**: действие над объектом (например, Чтение, Запись, Удаление, Выполнение).
- **Тип (Type)**: класс или тип объекта данных, к которому регулируется доступ.
- **Право (Access)**: правило, связывающее **Роль**, **Операцию** и **Тип**. Определяет, разрешена или запрещена операция.

Процесс авторизации: когда пользователь пытается выполнить действие в приложении, система безопасности:

1. Определяет роли, назначенные пользователю.
2. Ищет право, соответствующее запрашиваемой операции и типу объекта для каждой роли.
3. Применяет политику (разрешить, если найдено хотя бы одно разрешающее правило, и т.д.) и возвращает решение.

3. Управление безопасностью через интерфейсы администратора

Для управления настройками безопасности используются web-интерфейсы, входящие в состав платформы.

3.1. Доступ к интерфейсу управления

После успешной установки и настройки компонента, интерфейс управления доступен по URL, аналогичному: https://<ваш-сервер>/<ваше-приложение>/permissions

Для доступа необходима учетная запись с ролью, включающей права на операции Изменение и Чтение для типов Пользователь, Роль, Право доступа.

3.2. Управление пользователями

Раздел **«Пользователи»** позволяет:

- **Создать пользователя**: указать логин, пароль (согласно политике сложности), ФИО, email, статус (активен/заблокирован).
- **Редактировать профиль**: изменить атрибуты пользователя, сбросить пароль.
- **Назначить роли**: в карточке пользователя через интерфейс связей назначить одну или несколько существующих ролей.

- **Заблокировать/активировать**: отключить возможность входа без удаления учетной записи.
- **Удалить пользователя** (с подтверждением).

3.3. Управление ролями

Раздел **«Роли»** позволяет:

- **Создать роль**: задать уникальное имя и описание роли (например, МенеджерОтделаПродаж, АдминистраторСистемы).
- **Редактировать роль**: изменить ее описание.
- **Назначить права роли**: в карточке роли добавить правила доступа (Права), определяющие, какие операции над какими типами данных разрешены данной роли.
- **Удалить роль** (с подтверждением).

3.4. Управление правами доступа (Access Rights)

Права назначаются **ролям**. Для создания правила необходимо:

1. Выбрать **Тип объекта** (например, Клиент, Договор).
2. Выбрать **Операцию** (Чтение, Создание, Изменение, Удаление, Выполнение).
3. Установить флаг **Доступ** (Разрешить).

4. Программный API (для разработчиков)

Для интеграции механизмов безопасности в бизнес-логику приложения используется серверный API из пакета NewPlatform.Flexberry.Security.

Детальная информация по использованию API системы полномочий приведена в документации разработчика.

5. Интеграция с клиентскими приложениями

Клиентские платформы Flexberry (Ember, ASP.NET, Next) автоматически интегрируются с серверной системой безопасности.

- **Автоматическая проверка прав в UI**: элементы интерфейса (кнопки, меню, ссылки) могут скрываться или блокироваться на основе прав текущего пользователя. Настройка осуществляется через метаданные приложения.
- **Авторизация запросов к API**: все запросы к серверным API (REST, OData) проходят автоматическую проверку прав. Запрос, нарушающий политику безопасности, получает HTTP-ответ 403 Forbidden.
- **Передача контекста пользователя**: контекст безопасности (логин, роли) передается через стандартные механизмы аутентификации (cookie, токены) и доступен на сервере для принятия решений.

6. Рекомендации по эксплуатации и устранение неполадок

6.1. Типовые сценарии администрирования

1. **Новый сотрудник**:
    - Создать учетную запись пользователя.
    - Назначить одну или несколько ролей, соответствующих его должности.
    - Сообщить учетные данные.
2. **Смена должности сотрудника**:

- Отредактировать список ролей пользователя: удалить старые, добавить новые.

3. **Создание нового функционального модуля (типа данных)**:
    - Определить необходимые операции (Чтение, Запись и др.).
    - Для каждой роли, которой требуется доступ, создать соответствующие разрешающие права в разделе управления ролями.

6.2. Диагностика проблем

Симптом	Возможная причина	Действия по устранению
Пользователь не может войти.	Неверный логин/пароль, учетная запись заблокирована.	Проверить активность учетной записи в интерфейсе администратора. Инициировать сброс пароля.
Пользователь не видит данные или кнопки в интерфейсе.	Отсутствуют разрешающие права на операцию или тип данных.	1. Проверить список ролей пользователя. 2. Проверить, есть ли у этих ролей права на нужную операцию и тип.
Ошибка **403 Forbidden** при выполнении действия.	Запрос отклонен серверной системой безопасности.	Проверить логи сервера приложений для деталей. Убедиться, что право.

6.3. Ведение журналов (Logging)

Рекомендуется настроить ведение журналов событий безопасности на уровне сервера приложений (IIS, Kestrel) и в самой базе данных. Ключевые события для аудита:

- Успешные и неуспешные попытки входа.
- Изменения в конфигурации безопасности (добавление/удаление пользователей, ролей, прав).
- Критичные нарушения доступа (попытки выполнить запрещенную операцию).

7. Контакты для получения технической поддержки

- По вопросам приобретения лицензий и технической помощи обращайтесь по адресу support@flexberry.net.