### Требования к паролям

|  |  |  |
| --- | --- | --- |
| Параметр | Требование | Обоснование |
| **Состав пароля** |  |  |
| Минимальная длина | 8 символов | Базовая защита |
| Обязательные символы | Заглавная буква, строчная буква, цифра | Увеличение сложности |
| Специальные символы | Рекомендуются | Дополнительная защита |
| Запрещенные пароли | Словарные слова, простые последовательности | Защита от брутфорса |
| **Срок действия** |  |  |
| Срок действия пароля | 90 дней | Регулярная смена |
| История паролей | Последние 5 паролей | Предотвращение повторного использования |
| Блокировка после попыток | 5 неудачных попыток | Защита от взлома |

### Правила сброса, смены и восстановления пароля

|  |  |  |  |
| --- | --- | --- | --- |
| Операция | Процедура | Время действия | Дополнительные условия |
| **Смена пароля** |  |  |  |
| Плановая смена | В личном кабинете с вводом старого пароля | Немедленно | Уведомление на email |
| Принудительная смена | При первом входе или истечении срока | До смены пароля | Невозможность использования системы |
| **Восстановление пароля** |  |  |  |
| По email | Ссылка на email с временным токеном | 30 минут | Действует один раз |
| По SMS | Код подтверждения на телефон | 15 минут | Максимум 3 попытки в час |
| **Сброс администратором** |  |  |  |
| Для сотрудников | Генерация временного пароля | До первого входа | Обязательная смена при входе |
| Уведомление | SMS + Email пользователю | Немедленно | О факте сброса пароля |

### Многофакторная аутентификация

|  |  |  |
| --- | --- | --- |
| Категория действий | Действия, требующие МФА | Порядок аутентификации |
| **Вход в систему** |  |  |
| Менеджеры и администраторы | Все входы в систему | 1. Логин/пароль  2. SMS-код или Google Authenticator |
| Мастера | Первый вход, вход с нового устройства | 1. Логин/пароль  2. SMS-код |
| **Критические операции** |  |  |
| Изменение настроек уведомлений | Для всех ролей | 1. Подтверждение пароля  2. SMS-код |
| Доступ к отчетам | Менеджеры | 1. Текущая сессия  2. SMS-код |
| Изменение ролей пользователей | Администраторы | 1. Подтверждение пароля  2. Google Authenticator |

### Логирование

|  |  |  |
| --- | --- | --- |
| Категория операций | Конкретные операции | Логируемые данные |
| **Операции с записями** |  |  |
| Создание записи | Запись клиента на услугу | Дата/время, ID клиента, ID мастера, услуга, IP-адрес |
| Отмена записи | Отмена клиентом или менеджером | Дата/время, ID записи, инициатор отмены, причина |
| Изменение записи | Перенос времени, смена мастера | Дата/время, старые/новые данные, инициатор |
| **Административные операции** |  |  |
| Изменение расписания | Ввод/корректировка расписания мастеров | Дата/время, ID мастера, изменения, ID менеджера |
| Управление пользователями | Создание, изменение ролей, блокировка | Дата/время, ID пользователя, изменения, ID администратора |
| **Безопасность** |  |  |
| Вход/выход | Все аутентификации | Дата/время, ID пользователя, IP-адрес, результат |
| Неудачные попытки входа | Ошибки аутентификации | Дата/время, логин, IP-адрес, тип ошибки |

### Требования к паролям

|  |  |  |
| --- | --- | --- |
| Параметр | Требование | Обоснование |
| **Состав пароля** |  |  |
| Минимальная длина | 10 символов | Повышенная безопасность для финансовых операций |
| Обязательные символы | Заглавная буква, строчная буква, цифра, спецсимвол | Максимальная сложность |
| Энтропия | Минимум 60 бит | Защита от современных атак |
| **Срок действия** |  |  |
| Администраторы | 60 дней | Высокие привилегии требуют частой смены |
| Диспетчеры | 90 дней | Доступ к операционным данным |
| Курьеры | 180 дней | Меньше критичных операций |
| История паролей | Последние 8 паролей | Предотвращение циклического использования |

### Правила сброса, смены и восстановления пароля

|  |  |  |  |
| --- | --- | --- | --- |
| Операция | Процедура | Время действия | Дополнительные условия |
| **Смена пароля** |  |  |  |
| В мобильном приложении | Биометрическое подтверждение + старый пароль | Немедленно | Push-уведомление на все устройства |
| В веб-интерфейсе | Двухфакторная аутентификация | Немедленно | Logout с других устройств |
| **Восстановление пароля** |  |  |  |
| Через администратора | Личная верификация с документами | До 24 часов | Только в офисе компании |
| Экстренный сброс | Для курьера на маршруте | 1 час | Подтверждение диспетчером |
| **Безопасность** |  |  |  |
| Компрометация | Немедленная блокировка всех сессий | Немедленно | Уведомление службы безопасности |

### Многофакторная аутентификация

|  |  |  |
| --- | --- | --- |
| Категория действий | Действия, требующие МФА | Порядок аутентификации |
| **Первоначальная настройка** |  |  |
| Первый вход в мобильное приложение | Регистрация биометрии курьера | 1. Логин/пароль  2. SMS-код  3. Настройка биометрии |
| Регистрация нового устройства | Для всех ролей | 1. Логин/пароль  2. Код из email  3. Подтверждение администратором |
| **Административные функции** |  |  |
| Доступ к админ-панели | Администраторы | 1. Логин/пароль  2. Google Authenticator  3. Push-уведомление |
| Переназначение заказов | Диспетчеры | 1. Текущая сессия  2. SMS-код |
| **Финансовые операции** |  |  |
| Просмотр финансовых отчетов | Администраторы | 1. Подтверждение пароля  2. Hardware token |
| Изменение тарифов | Администраторы | 1. Подтверждение пароля  2. Email-подтверждение  3. SMS-код |

### Логирование

|  |  |  |
| --- | --- | --- |
| Категория операций | Конкретные операции | Логируемые данные |
| **Операции с заказами** |  |  |
| Все изменения статусов | Создание, принятие, выполнение, отмена заказов | Дата/время, номер заказа, старый/новый статус, ID пользователя, геолокация |
| Переназначение заказов | Смена курьера диспетчером | Дата/время, номер заказа, старый/новый курьер, причина, ID диспетчера |
| **Финансовые операции** |  |  |
| Расчеты с курьерами | Начисление оплаты за доставку | Дата/время, ID курьера, сумма, номера заказов, ID администратора |
| Расчеты с партнерами | Передача данных в бухгалтерию | Дата/время, ID партнера, сумма, период, тип операции |
| **Административные операции** |  |  |
| Управление пользователями | Регистрация курьеров, назначение прав | Дата/время, ID пользователя, изменения прав, ID администратора |
| Системные операции | Изменение настроек, обновления | Дата/время, тип изменения, параметры, ID пользователя |
| **Геолокация и безопасность** |  |  |
| Трекинг курьеров | Геолокация при работе с заказами | Дата/время, ID курьера, координаты, статус заказа |
| Доступ к персональным данным | Просмотр данных клиентов/курьеров | Дата/время, ID просматриваемого, ID просматривающего, тип данных |

## Сравнительная таблица подходов к безопасности

|  |  |  |
| --- | --- | --- |
| Аспект | Барбершоп | Доставка заказов |
| **Уровень безопасности** | Стандартный | Повышенный |
| **Длина пароля** | 8 символов | 10 символов |
| **Срок действия пароля** | 90 дней для всех | 60-180 дней по ролям |
| **МФА** | Для администраторов и критичных операций | Для всех административных функций |
| **Биометрия** | Не используется | Обязательна для мобильного приложения |
| **Геолокация в логах** | Не требуется | Обязательна для курьеров |
| **Восстановление паролей** | Email/SMS | Только через администратора |
| **Экстренные процедуры** | Стандартные | Специальные для курьеров на маршруте |

## Дополнительные меры безопасности

### Барбершоп

* Шифрование персональных данных клиентов
* Регулярные аудиты безопасности (ежеквартально)
* Обучение сотрудников основам информационной безопасности

### Доставка заказов

* End-to-end шифрование геолокационных данных
* Блокчейн для аудита финансовых операций
* Автоматическое обнаружение аномальной активности
* Соответствие PCI DSS для обработки платежей
* Регулярные пентесты (ежемесячно)
* SOC (Security Operations Center) 24/7