Система анализа и мониторинга состояния ИБ DATAPK

Тема 6. Настройка системы управления доступом.

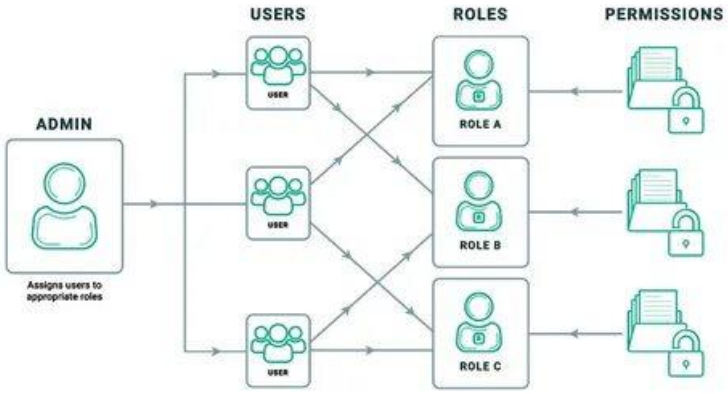
udv|group

Общие сведения

Продукт администрируется через веб-интерфейс (уровень Management).

На Supervision тоже свой веб-интерфейс (в данном курсе не рассматривается).

На сенсоре нет веб-интерфейса.



В продукте реализована ролевая модель доступа:

- **Администратор** – полный доступ
- **Инженер** – работа с активами, сетевыми соединениями, конфигурациями
- **Просмотр веб-интерфейса** – просмотр данных без возможности редактирования
- **Просмотр панели мониторинга** – только просмотр страницы «Панель мониторинга» (с бесконечным временем жизни сессии)

Таймаут по бездействию настраивается в консоли (**/usr/share/udv/datap/manager.env**, переменная **USER_SESSION_INACTIVITY_TIMEOUT** – задается в секундах (по умолчанию 600), распространяется для всех ролей, кроме «Просмотр панели мониторинга»

Сервисный SSH-доступ здесь не рассматривается – это настраивается средствами ОС Альт СП.

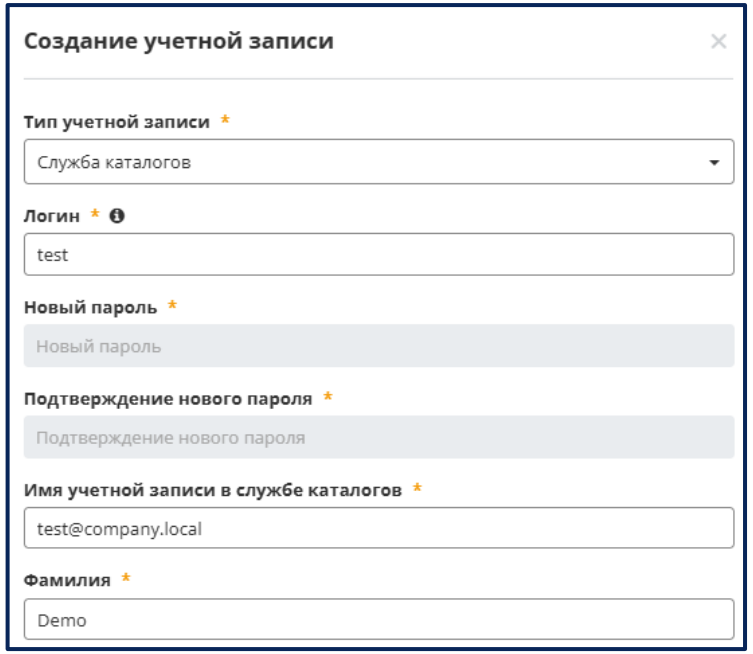
Необходимо сразу внедрять DATAPK с безопасными настройками пользователей в соответствии с политикой организации – **не использовать простые пароли/пароли по умолчанию**

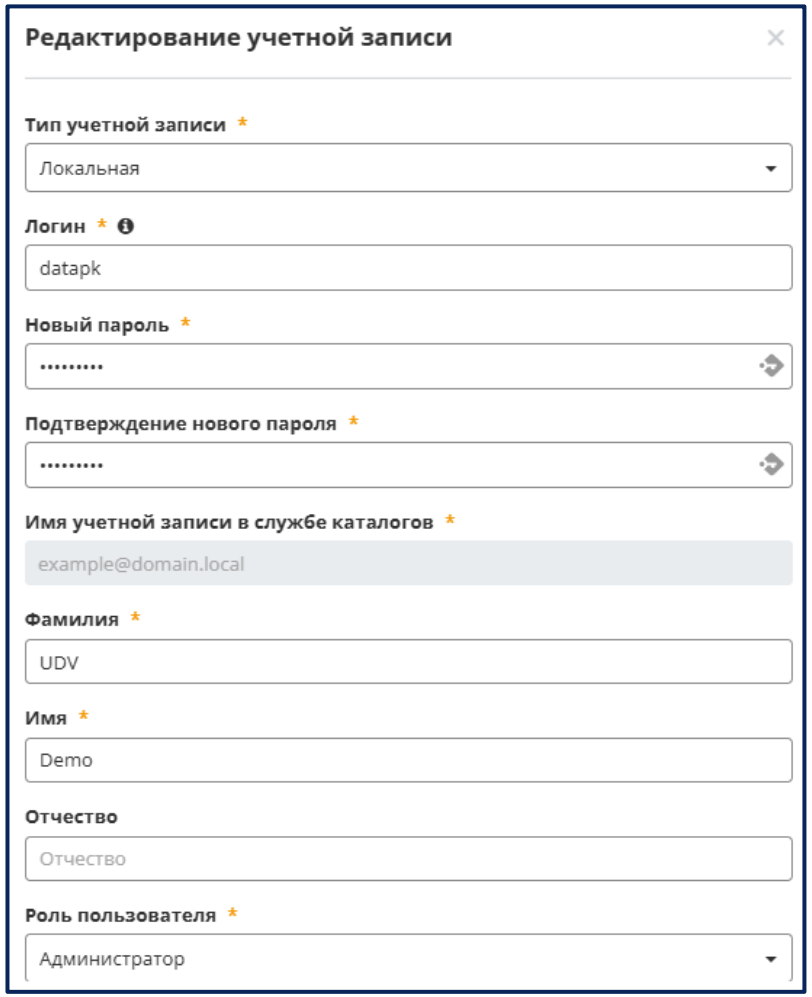
CyberLympha®

Учетные записи

Учетные записи в DATAPK могут быть:

- локальные
- служба каталогов (пароль проверяется LDAP-сервером), настройки LDAP – в **manager.env** переменные **LDAP_CONNECTION_STRING** (строка подключения к серверу LDAP) и **LDAP_TLS** (рекомендуется всегда ставить в **true** и использовать шифрованный LDAP), работает с MS AD и RED ADM
- централизованное управление с уровня Supervision (не рассматривается в курсе)





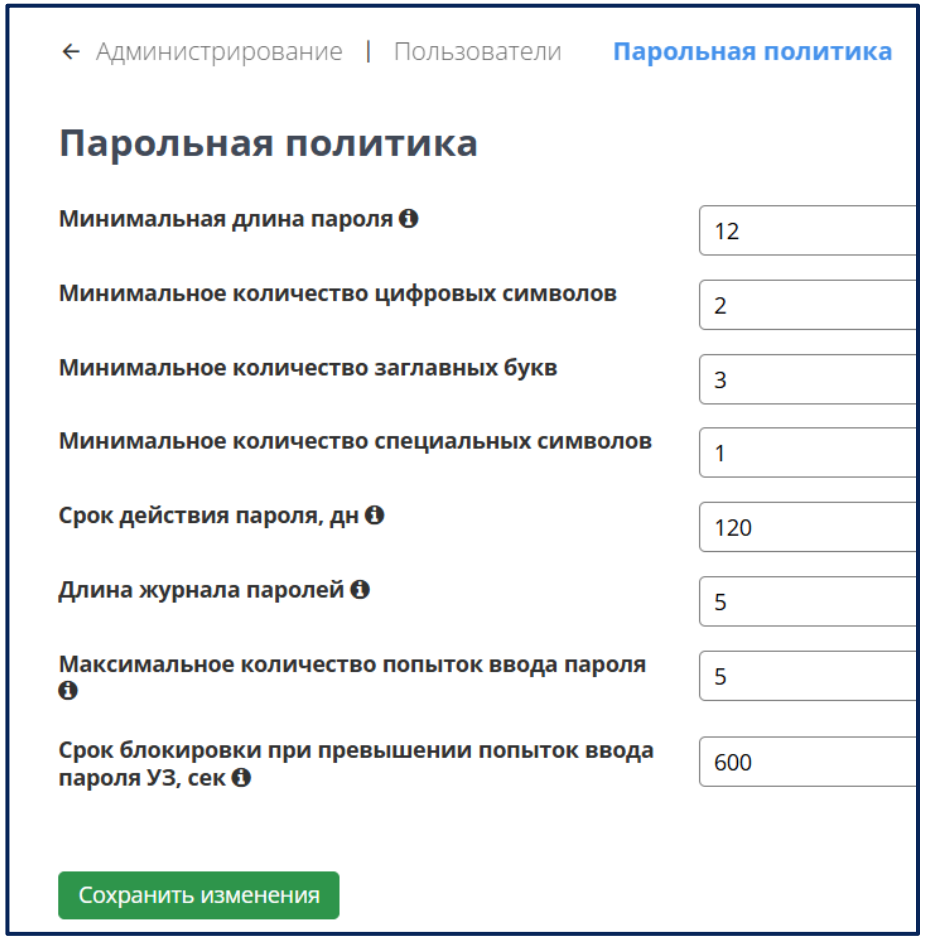
Парольная политика

Для локальных УЗ есть возможность настроить парольную политику и политику блокировки (Администрирование\Парольная политика).

По умолчанию парольная политика мягкая (6 символов, 1 цифра, 365 дней, 1 прошлый пароль, после 3 неуспешных попыток блокирование на 15 мин. (900 секунд)), поэтому ее надо откорректировать под нужные задачи.

Парольная политика не распространяется на учетные записи с типом «Служба каталогов» - они подчиняются настройкам контроллера домена

В централизованном управлении с Supervision подход схожий, только парольная политика и учетные записи распространяются с верхнего уровня – так же есть локальные / «служба каталогов» УЗ с доступами к определенным Managements с требуемыми ролями (и при включенном централизованном управлении локальные УЗ на данных Managements использовать нельзя).



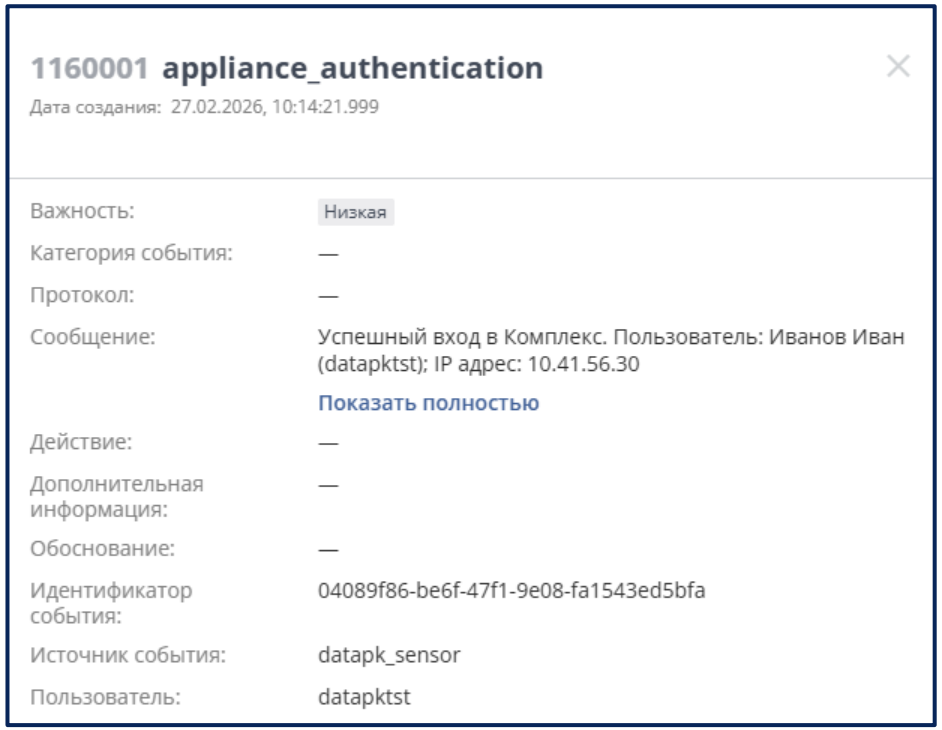
CyberLympha®

Аудит действий пользователей

Система фиксирует действия пользователей (источник **User Action Control**, типы событий **user_action_detected** и **appliance_authentication**):

- успешная/неуспешная авторизация
- успешное создание/редактирование учетных записей
- успешное редактирование парольной политики.

Дата создания	Важность	Описание
27.02.2026, 13:19:22.681	Низкая	Успешный вход в Комплекс
27.02.2026, 13:19:18.994	Низкая	Неудачная попытка входа в Комплекс
27.02.2026, 13:19:18.467	Низкая	Неудачная попытка входа в Комплекс
27.02.2026, 13:19:15.200	Низкая	Успешный выход из Комплекса
27.02.2026, 13:18:55.936	Низкая	Пользователь создан
27.02.2026, 11:44:21.663	Низкая	Успешный вход в Комплекс
27.02.2026, 11:44:16.861	Низкая	Успешный выход из Комплекса



Информация о пользователе так же фигурирует в событиях от других подсистем (редактирование инцидентов, активов, правил сессий и пр.)

Вопросы?

udv|group