Подп. и дата	
Инв.№ дубл.	
Взам. инв. №	
Подп. и дата	
Инв.№ подл.	

ПРОГРАММНЫЙ КОМПЛЕКС

«Bars.Up.Access Manager»

Руководство пользователя

RU.83470944.501410-01 97 01

Листов 27

2022 г.

СОДЕРЖАНИЕ

АННОТАЦИЯ

Данный документ представляет собой Руководство пользователя к системе защиты от несанкционированного доступа к информации прикладных web-приложений — программного комплекса "Bars.Up.Access Manager".

1. ВВЕДЕНИЕ

Настоящее руководство предназначено для ознакомления пользователя с техническими характеристиками и функциональными возможностями Программного комплекса «Bars.Up.Access Manager», децимальный номер RU.83470944.501410-01.

В основной части документа приведены сведения о назначении Программного комплекса «Bars.Up.Access Manager» (далее – ПК, ПК «Bars.Up.Access Manager», Изделие) и его основных возможностях, об условиях применения ПК, а также об описании процесса работы и доступа различных пользователей к ПК.

2. ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ

− идентификация и аутентификация пользователей;

− управление идентификаторами пользователей;

− управление средствами аутентификации (аутентификационной информацией) пользователей ПК «Bars.Up.Access Manager»;

− обеспечение защиты обратной связи при вводе аутентификационной информации;

− управление (создание, активация, блокирование и удаление) учетными записями пользователей;

− управление доступом субъектов доступа посредством реализации ролевого метода управления доступом;

− ограничение неуспешных попыток входа в ПК «Bars.Up.Access Manager»;

− предупреждение пользователя при его входе в ПК «Bars.Up.Access Manager» о реализации в Изделии мер защиты информации;

− отображение пользователю, после успешного входа в ПК «Bars.Up.Access Manager», информации о его предыдущем входе в Изделие;

− ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя ПК «Bars.Up.Access Manager»;

− блокирование сеанса доступа в ПК «Bars.Up.Access Manager» после установленного времени бездействия (неактивности) пользователя или по запросу;

− сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

− формирование журнала администрирования для мониторинга администратором (просмотр, анализ) результатов регистрации событий безопасности и реагирования на них.

Основные принципы работы ПК

Программный комплекс «Bars.Up.Access Manager» является программным средством защиты информации прикладных web-приложений (информационных/ автоматизированных систем) от несанкционированного доступа и предназначено для решения следующих задач:

- реализация технологии единой точки доступа (Single Sign-On, SSO) к информационным системам;
- идентификация и аутентификация пользователей;
- управление доступом;
- регистрация событий безопасности.

ПК может применяться для защиты конфиденциальной информации, в том числе в государственных информационных системах до 1 класса защищенности включительно, а также для обеспечения защиты персональных данных до 1 уровня защищенности включительно.

Аудит событий информационной безопасности

Информация о событиях безопасности фиксируется в «Журнале событий» и «Журнале администрирования».

Журнал событий представлен в виде таблицы с полями: «Дата и время», «Категория», «Тип», «Система», «Пользователь», «IP адрес», «Ошибка». Журнал фиксирует все типы события безопасности, а именно:

- Категория «Безопасность»:
  - Вход;
  - Ошибка входа;
  - Регистрация;
  - Ошибка регистрации;
  - Выход;
  - Ошибка выхода;
  - Получение маркера;
  - Ошибка получения маркера
  - Аутентификация системы;
  - Ошибка аутентификации системы;
  - Создание связи с провайдером идентификации;
  - Ошибка создания связи с провайдером идентификации;
  - Удаление связи с провайдером идентификации;
  - Ошибка удаления связи с провайдером идентификации;
  - Изменение адреса электронной почты;
  - Ошибка изменения адреса электронной почты;
  - Изменение профиля;
  - Ошибка изменения профиля;
  - Изменение пароля;
  - Ошибка изменения пароля;
  - Изменение маркера TOTP;
  - Ошибка изменения маркера TOTP;
  - Подтверждение адреса электронной почты;

  - Ошибка подтверждения адреса электронной почты;
  - Удаление маркера TOTP;
  - Ошибка удаления маркера TOTP;
  - Отзыв разрешения;
  - Сброс пароля;
  - Ошибка сброса пароля;
  - Первичный поток входа через провайдера идентификации;
  - Ошибка первичного потока входа через провайдера идентификации;
  - Поток после входа через провайдера идентификации;
  - Ошибка потока после входа через провайдера идентификации;
  - Смена пользователя.
- Категория «Конфигурация»:
  - Регистрация системы;
  - Ошибка регистрации системы;
  - Обновление системы;
  - Ошибка обновления системы;
  - Удаление системы;
  - Ошибка удаления системы.
- Категория «Система»:
  - Запрос подтверждения адреса электронной почты;
  - Ошибка запроса подтверждения адреса электронной почты;
  - Запрос сброса пароля;
  - Ошибка запроса сброса пароля;
  - Запрос подтверждения связи с провайдером идентификации;
  - Ошибка запроса подтверждения связи с провайдером идентификации;
  - Выполнение настраиваемого действия;
  - Ошибка выполнения настраиваемого действия;
  - Выполнение действия;
  - Ошибка выполнения действия.

Журнал администрирования представлен в виде таблицы с полями «Дата и время», «Ресурс», «Тип», «Домен», «Система», «Пользователь», «IP адрес» и отвечает за регистрацию всех учетных записей пользователей, совершающих действия, которые влекут за собой совершение события безопасности.

Доступ к журналам открыт только пользователям с соответствующими правами. При доступе к журналам ПК позволяет осуществлять фильтрацию по полях таблицы. При первичной настройке ПК ведение журналов отключено, поэтому Администратором безопасности необходимо включить ведение журнала для осуществления функции аудита событий безопасности. Подробнее о настройке и работе журналов описано в документе «Программный комплекс «Bars.Up.Access Manager» Руководство по КСЗ» RU.83470944.501410-01 91 01.

3. УСЛОВИЯ ФУНКЦИОНИРОВАНИЯ

3.1 Требования к составу и параметрам технических и программных средств

Необходимо обеспечить наличие на клиентских рабочих местах интернет-браузеров:

- Google Chrome 84 и выше;
- Mozilla Firefox 79 и выше;
- Microsoft Edge 83 и выше;
- Yandex 21.6 и выше.

3.2 Требования к персоналу

Пользователи ПК должны обладать навыками работы с одной из следующих операционных систем: Microsoft Windows, Unix (Linux), Apple MacOS, а также навыками работы с веб-браузерами.

Каждый пользователь в соответствии со своими правами должен обладать необходимыми знаниями в предметной области для корректной работы с предоставляемой информацией.

Для работы с программой пользователю необходимо изучить настоящее руководство.

3.3 Режимы работы ПК

Работа в ПК осуществляется в одном стандартном штатном режиме функционирования, при котором ПК поддерживает выполнение всех заявленных функций. В этом режиме ПК поддерживает работу всех компонентов в круглосуточном режиме.

4. РАБОТА С ПК

4.1 Работа в «Профиле пользователя»

4.1.1 Вход в ПК

Начало работы с ПК содержит следующую последовательность действий:

1) запустите любой web-браузер;

2) в адресной строке браузера введите ссылку на сайт ПК, которую предоставляет Администратор безопасности, и перейдите по ссылке;

3) в открывшемся окне входа в ПК (см. рисунок 1) заполните поля:

– «Имя пользователя или адрес электронной почты» – введите имя пользователя или адрес электронной почты, полученное Администратором безопасности;

– «Пароль» – введите пароль, полученный Администратором безопасности.

Рисунок 1 — Окно входа в ПК.

4) После заполнения полей нажмите кнопку «Вход».

Если данные введены верно, то в окне web-браузера откроется интерфейс личного кабинета пользователя ПК.

Если данные введены неверно, пользователь увидит оповещение, представленное на рисунке 2.

5) При нажатии на кнопку «ЭЦП» пользователь может воспользоваться ключом электронной подписи, при этом ПК предложит пользователю подключить цифровой носитель с ключом к компьютеру. Выполните данное действие и нажмите кнопку «Вход».

В появившемся окне выберите сертификат, зарегистрированный в ПК, и нажмите на него (см. рисунок 3). После чего откроется интерфейс личного кабинета пользователя.

Рисунок 2 — Неверный ввод имени пользователя или пароля.

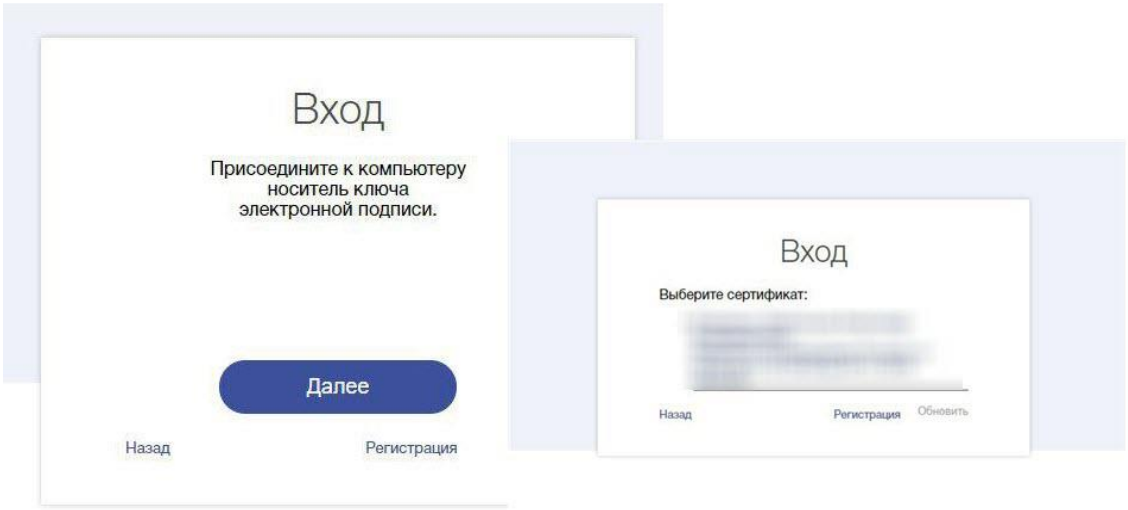

Рисунок 3 — Вход в ПК с использованием ключа электронной подписи

4.1.2 Парольная политика

ПК реализует возможность настройки Политики паролей. Пользователь с правами администратора может корректировать настройки параметров Политики паролей, при этом учитывая обязательное выполнение требований к Политике паролей.

При первичной установке ПК реализованы следующие требования к паролям пользователей:

- длина пароля не менее восьми символов;
- алфавит пароля не менее 70 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) от трех до четырех неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки;
- блокировка учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на период времени от 15 до 60 минут;
- смена паролей не более чем через 60 дней.

4.1.3 Общий вид интерфейса системы

После входа в ПК откроется личный кабинет пользователя, который представлен на рисунке 4. Информация в окне разбита по следующим вкладкам:

- «Аккаунт» — вкладка содержит основную информацию пользователя: имя пользователя, электронную почту, ФИО пользователя.;
- «Пароль» — в данной вкладке пользователю доступна смена пароля для входа в ПК;
- «Сертификат» — вкладка содержит сертификат ключа проверки;
- «Сессии» — вкладка содержит журнал с информацией об открытых сессиях на разных компьютерах под данной учетной записью пользователя;
- «Журнал» — во вкладке содержатся записи событий для пользователя.

4.1.3.1 Вкладка «Аккаунт»

Вкладка «Аккаунт» (см. рисунок 4) содержит основную информацию пользователя: имя пользователя, электронную почту, ФИО пользователя.

Поле «Имя пользователя» описывает имя учетной записи, и по умолчанию оно недоступно для редактирования. В «Административной консоли» в настройках домена можно редактировать возможность изменения этого поля (см п. 5.1)

Остальная информация доступна для редактирования всем пользователям: внесите изменения в нужные поля, после чего нажмите кнопку «Сохранить».

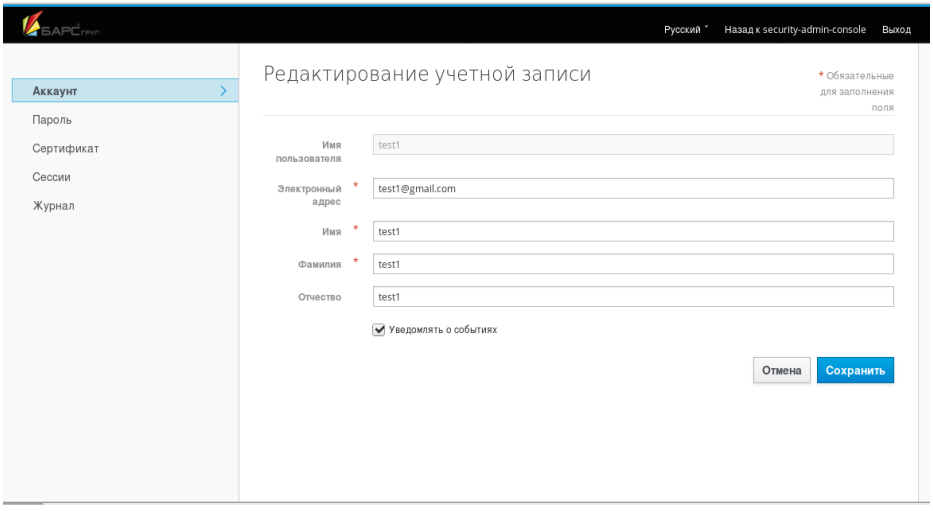

Рисунок 4 — Окно профиля пользователя

4.1.3.2 Вкладка «Пароль»

В данной вкладке пользователю доступна смена пароля для входа в ПК (см. рисунок 5). Для этого заполните следующие поля:

- «Старый пароль» – укажите текущий пароль пользователя;

- «Новый пароль» – укажите новый пароль;
- «Подтверждение» – повторно введите новый пароль.

После чего нажмите кнопку «Сохранить».

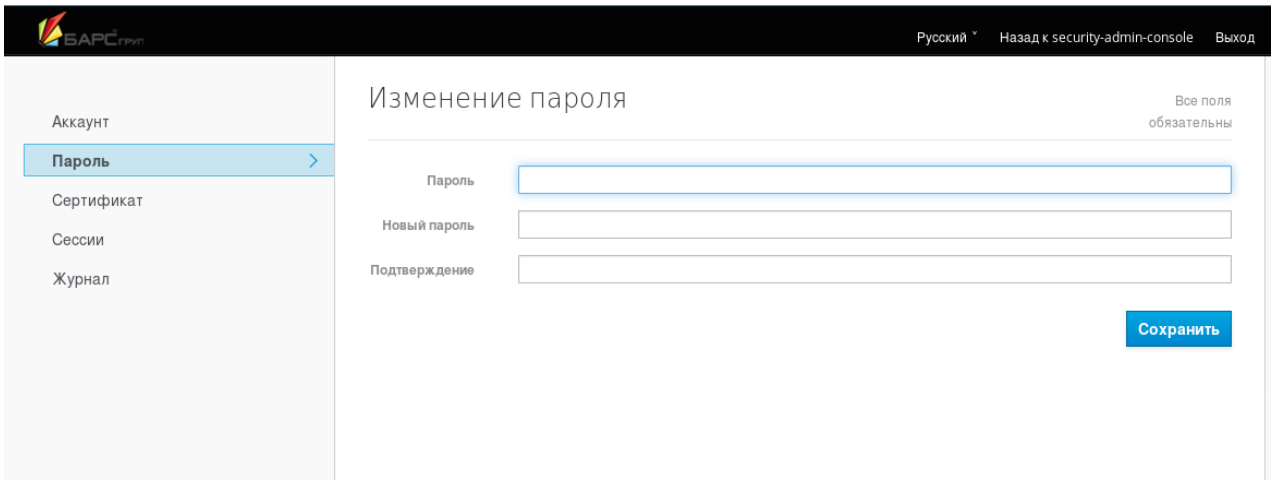

Рисунок 5 — Изменение пароля

4.1.3.3 Вкладка «Сертификат»

В процессе электронного документооборота ЭЦП обеспечивает проверку целостности и конфиденциальности документов, а также устанавливает отправителя документов.

Вкладка «Сертификат» содержит сертификат ключа проверки – электронный документ (либо документ на бумажном носителе), который выдаётся удостоверяющим центром и подтверждает, что ключ подписи действительно принадлежит владельцу сертификата (см. рисунок 6).

При генерации ключа данные о его владельце сохраняются, и полученный таким образом файл именуется сертификатом ключа подписи. Данный документ обязательно включает открытый ключ («Алгоритм подписи»), а также информацию о владельце ЭЦП («Владелец») и удостоверяющем центре («Издатель»), выдавшем этот ключ.

Сертификат ключа подписи выдаётся на 1 год («От» и «До»), и по истечении данного срока более не действует, а обмен документами становится невозможен. Для того чтобы продолжить работать в системе электронной документации, следует продлить сертификат.

При любом изменении реквизитов владельца ключа (смена руководителя организации, названия и т. д.), а также компрометации закрытого ключа требуется отозвать текущий сертификат и оформить новый.

По умолчанию поля во вкладке «Сертификат» недоступны для редактирования. Управление редактированием возможно в «Административной консоли» в подразделе «Домен» (подробнее см. п. 5.1).

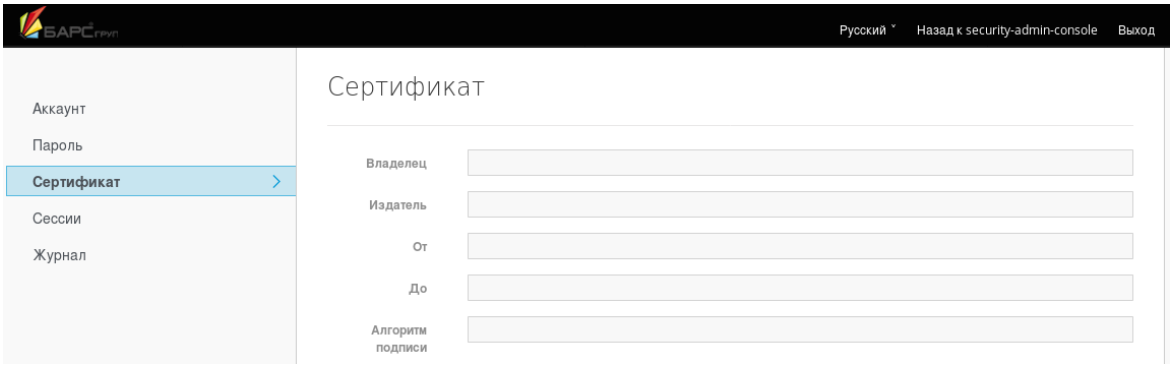

Рисунок 6 — Вкладка «Сертификат»

В ПК сертификат учетной записи пользователя загружается через «Административную консоль». Загрузка сертификата доступна пользователям с правами администратора (см. рисунок 7). Описание загрузки сертификата ЭЦП и его настройки см. в п. 5.1.

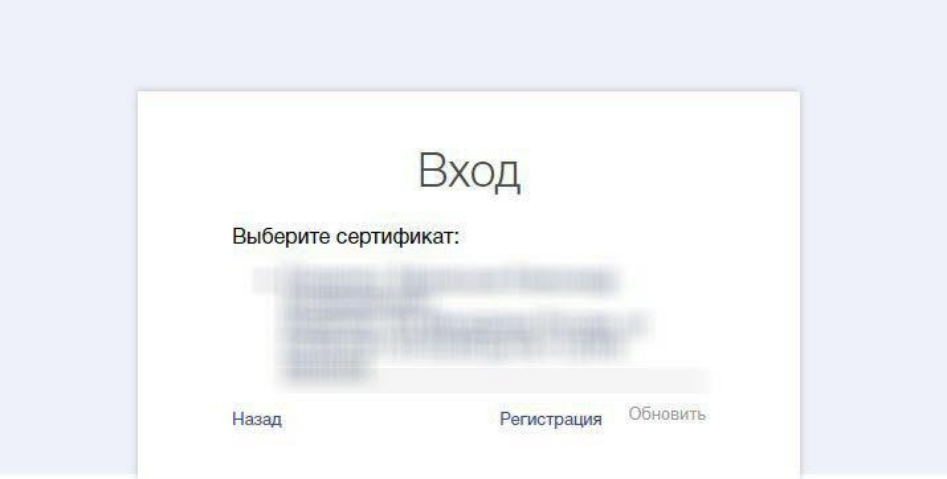

Рисунок 7 — Пример загруженного сертификата

4.1.3.4 Вкладка «Сессии»

Вкладка содержит журнал с информацией об открытых сессиях на разных компьютерах под данной учетной записью пользователя (см. рисунок 8).

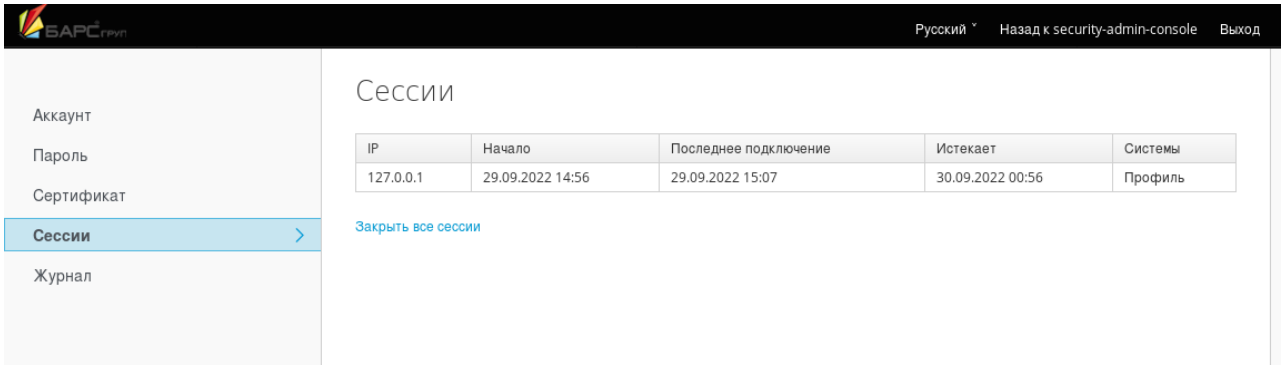

Рисунок 8 — Вкладка «Сессии»

При нажатии на кнопку «Закрыть все сессии» все открытые сессии под данной учетной записью будут закрыты. Для продолжения работы с ПК пользователю необходимо заново пройти авторизацию.

4.1.3.5 Вкладка «Журнал»

Вкладка содержит информацию о действиях пользователя в ПК и внешних системах (см. рисунок 9).

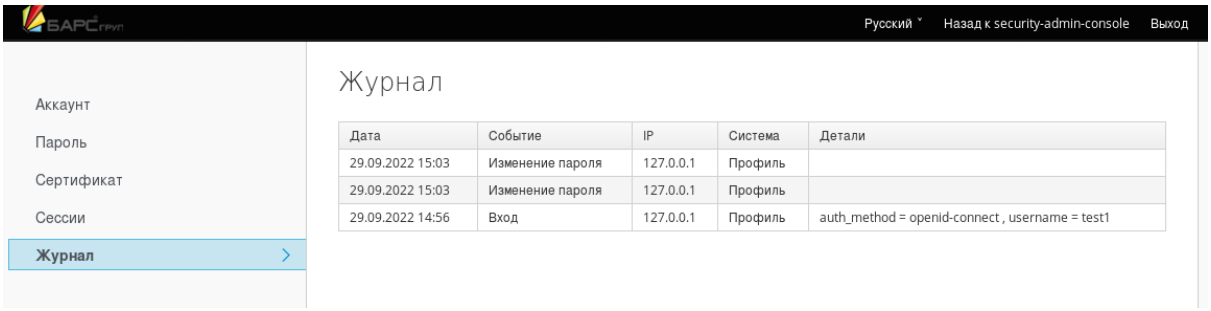

Рисунок 9 — Вкладка «Журнал»

4.1.4 Завершение работы

Для корректного завершения работы с ПК нажмите кнопку «Выход» в правом верхнем углу окна (см. рисунок 10).

Рисунок 10 — Кнопка «Выход»

4.2 Работа в «Административной консоли»

Переход в «Административную консоль» происходит через вкладку «Системы» в «Профиле пользователя». По умолчанию для нового пользователя доступен только просмотр настроек Домена и Системы. Изменение настроек доступно пользователю с правами администратора (admin). Подробное описание работы в системе «Административная консоль» представлено в документе «Программный комплекс «Bars.Up.Access Manager». RU.83470944.501410-01 97 01 Руководство по КСЗ».

Интерфейс «Административной консоли» представлен на рисунке 11.

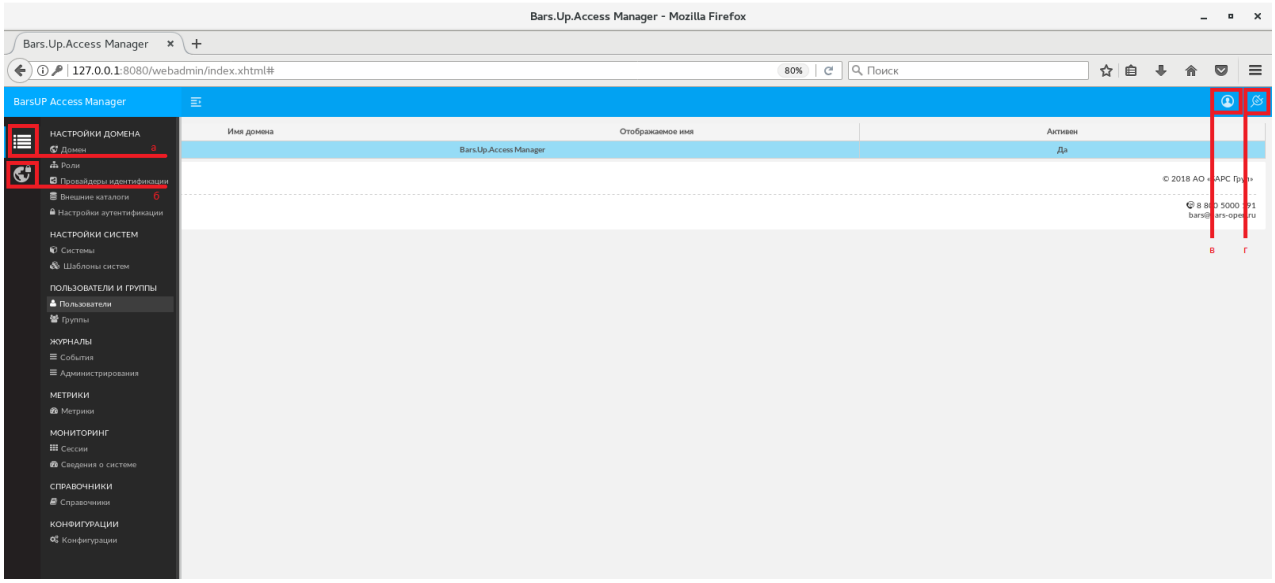

Рисунок 12 — Интерфейс «Административной консоли».

Интерфейс «Административной консоли» включает в себя:

– кнопку (рисунок 11,а), открывающую перечень разделов для просмотра и настройки выбранного домена;

– кнопку (рисунок 11,б), открывающую список доступных к просмотру или редактированию доменов;

– рабочую область;

– кнопку (рисунок 11,в) перехода в систему «Профиль пользователя»;

– кнопку (рисунок 11,г) выхода из ПК.

Разделы для просмотра и настройки выбранного домена:

– Настройки домена:

– Домен — настройка домена в системе: метода объединения проектов в независимые группы;

– Роли — в данном разделе содержится список ролей домена и информация по этим ролям;

– Провайдеры идентификации — провайдер идентификации аутентифицирует пользователя и предоставляет сервис-провайдеру информацию, которая проверяет аутентичность пользователя;

– Внешние каталоги — настройка каталогов, в которых лежат данные внешних информационных систем (службы каталогов);

– Настройки аутентификации — включает в себя параметры потоков событий и связей потоков, настройку обязательных действий, настройку параметров политики паролей, политики одноразовых паролей.

- Настройки системы:
  – Системы — раздел содержит список систем доступных в данном домене: как внешних, так и систем ПК;
  – Шаблоны системы — создание шаблона системы для дальнейшего его использования при настройке внешних систем.
- Пользователи и группы:
  – Пользователи — раздел содержит список пользователей домена и информацию о них: имя учетной записи пользователя, ФИО пользователя, e-mail, а также параметр его активности;
  – Группы — создание групп пользователей.
- Журналы:
  – События — содержит журнал событий, в котором отражается информация о совершенных событиях безопасности;
  – Администрирования — содержит журнал администрирования, в котором отражается информация об учетных записях пользователей, и событиях безопасности, совершенных данными пользователями.
- Мониторинг:
  – Сессии — данный раздел содержит информацию об открытых сессиях в ПК и внешних системах с указанием количества активных пользователей;
  – Сведения о системе — данный раздел содержит информацию об операционной системе (виртуальной машине), на которой развернуто ПК.
- Справочники:
  – Справочники — данный раздел содержит список справочников, необходимых для того, чтобы можно было не передавать информацию длинными строками, а загружать справочник в систему и при необходимости использовать идентификатор из внутреннего справочника.

4.2.1 Регистрация нового пользователя

Для возможности авторизации и работы с Программным комплексом пользователю в ПК должна быть присвоена учетная запись с уникальным идентификатором пользователя.

Алгоритм создание нового пользователя написан в п.4.3.8 документа «Программный комплекс «Bars.Up.Access Manager» Руководство по КСЗ» RU.83470944.501410-01 91 01.

4.3. Роли пользователей

В ПК реализован ролевой метод управления доступом. Распределение ролей между пользователями в ПК организовано путем создания в «Административной консоли» в разделе «Домен» новых ролей, либо использования ролей по умолчанию. При регистрации нового пользователя по умолчанию ему присваиваются роли:

- manage_account — управление профилем;
- view_profile — просмотр профиля.

Данные роли присваиваются пользователю автоматически после его регистрации в ПК и служат для разграничения прав пользователей не имеющих дополнительных настроек ролевой модели. Настройка набора прав, которые присваиваются пользователю при самостоятельной регистрации, реализуется в «Административной консоли» Администратором безопасности.

Дальнейшее присвоение прав пользователю происходит в «Административной консоли» пользователем с правами администратора (admin). Подробно процесс присвоения ролей описан в п. 3.4.2 документа «Программный комплекс «Bars.Up.Access Manager». Руководство по КСЗ» RU.83470944.501410-01 91 01.

В зависимости от присвоенных ролей у пользователя могут быть права, указанные в Таблице 1.

Таблица 1 – Роли с указанием прав

Имя роли	**Описание**
Роли уровня домена	
Offline-access	оффлайн доступ
View-dicts	просмотр справочников
Manage-dicts	управление справочниками
Create-realm	создание домена
User	пользователь
Admin	администратор
Роли уровня системы	
Create-client	создание системы

Disable user	заблокировать пользователя
Enable user	разблокировать пользователя
Impersonation	смена пользователя
Manage-clients	управление системами
Manage-events	управление событиями;
Manage-group-memberships	управление членством в группах
Manage-identify-providers	управление провайдером идентификации
Manage-realm	управление доменом
Manage-users	управление пользователями
View-clients	просмотр систем
View-events	просмотр событий
View-identify-providers	просмотр провайдеров идентификации
View-realm	просмотр домена
View-users	просмотр пользователей
Read-token	чтение токена
Manage-account	управление профилем
View profile	просмотр профиля

Программным комплексом также предусмотрена возможность создания новой составной роли. Роль является составной, если она имеет в своем составе другие роли. Право создавать новые роли и присваивать их пользователям есть у пользователя с правами администратора (admin). Подробный процесс создания и присвоения роли описан в п. 3.4.2 документа «Программный комплекс «Bars.Up.Access Manager» Руководство по КСЗ» RU.83470944.501410-01 91 01.

4.3.1 Создание и редактирование роли

Для создания новой роли необходимо обладать правами администратора (admin) в данном домене. Во вкладке «Системы» необходимо перейти в систему «Административная консоль» (см. рисунок 11).

ПК перейдет в систему «Административная консоль», главная страница которой представлена на рисунке 12.

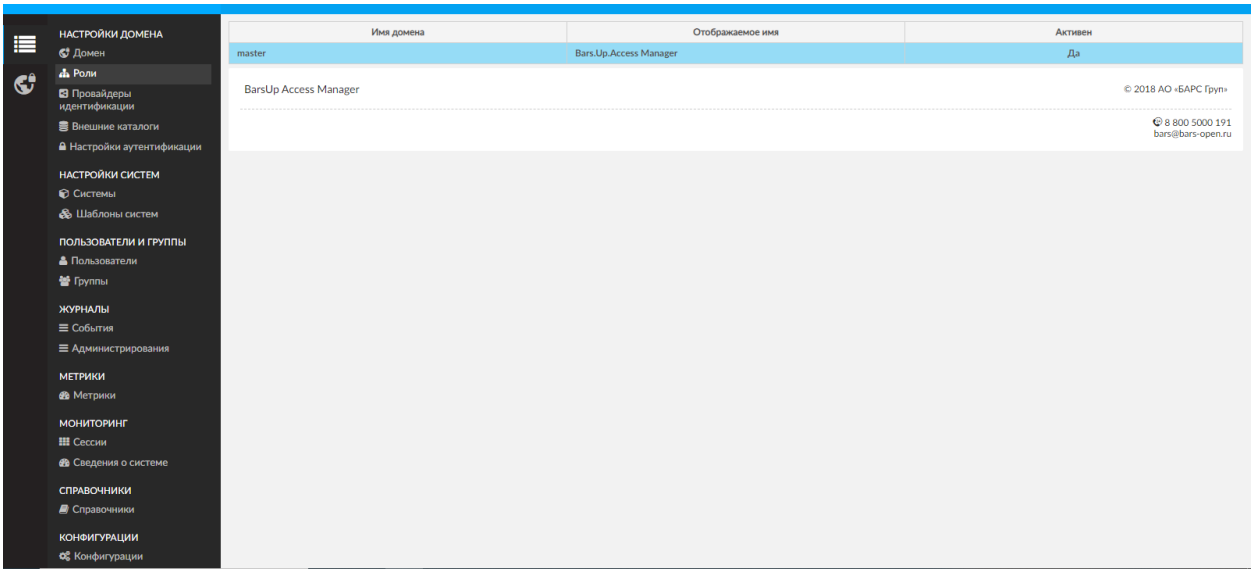

Рисунок 12 — Система «Административная консоль»

Подробно процесс создания и присвоения ролей описан в п. 3.4.2 документа «Программный комплекс «Bars.Up.Access Manager» Руководство по КСЗ» RU.83470944.501410-01 91 01.

5. СООБЩЕНИЯ ОБ ОШИБКАХ

Описание ошибок действий при эксплуатации средства приведены в таблице 2.

Таблица 2 - Описание действий после сбоев и ошибок

№ п/п	Ошибка	Способ решения для пользователя ПК
1	Ошибка входа	Необходимо проверить корректность ввода данных.
2	Ошибка регистрации	Необходимо проверить корректность ввода данных при регистрации пользователя в системе.
3	Ошибка выхода	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
4	Ошибка изменения адреса электронной почты	Необходимо проверить корректность ввода почты пользователя в ПК
5	Ошибка изменения профиля	Необходимо проверить все ли данные, указанные в настройках пользователя, имеют верное значение, при необходимости проверить журнал администрирования.
6	Ошибка изменения пароля	Необходимо проверить, что заданный пароль соответствует требованиям настроек безопасности в ПК
7	Ошибка подтверждения адреса электронной почты	Необходимо проверить корректность адреса электронной почты в ПК
8	Ошибка запроса подтверждения адреса электронной почты	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
9	Ошибка запроса сброса пароля	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
10	Ошибка сброса пароля	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
11	Неверная подпись	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.

№ п/п	Ошибка	Способ решения для пользователя ПК
12	Ошибка запроса данных пользователя	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
13	Ошибка выполнения действия	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
14	Ошибка выполнения настраиваемого действия	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
15	Ошибка запроса данных системы	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
16	Ошибка регистрации системы	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
17	Ошибка обновления системы	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.
18	Ошибка удаления системы	Очистить кеш/куки, обновить браузер и повторить попытку. Если ошибка повторяется, необходима эскалация в службу технической поддержки.

Описание типов событий безопасности, связанных с доступными пользователю функциями средства представлено в таблице 3.

Таблица 3 - Описание типов событий безопасности, связанных с доступными пользователю функциями средства

№ п/п	Тип события безопасности	Возможный результат события безопасности
1	Вход	Вход выполнен успешно
2	Ошибка входа	Ошибка выполнения входа
3	Регистрация	Регистрация пользователя выполнена успешно
4	Ошибка регистрации	Регистрация пользователя завершилась ошибкой
5	Выход	Выход выполнен успешно

№ п/п	Тип события безопасности	Возможный результат события безопасности
6	Ошибка выхода	Ошибка выполнения выхода, пользователь не получил доступ в приложение
7	Создание связи с провайдером идентификации	Создание связи с провайдером идентификации
8	Ошибка создания связи с провайдером идентификации	Ошибка создания связи с провайдером идентификации
9	Удаление связи с провайдером идентификации	Удаление связи с провайдером идентификации
10	Ошибка удаления связи с провайдером идентификации	Ошибка удаления связи с провайдером идентификации
11	Изменение адреса электронной почты	Изменения адреса электронной почты в настройках пользователя
12	Ошибка изменения адреса электронной почты	Изменения адреса электронной почты, завершилось ошибкой
13	Изменение профиля	Изменение настроек пользователя
14	Ошибка изменения профиля	Ошибка изменения настроек пользователя
15	Изменение пароля	Изменение пароля пользователя
16	Ошибка изменения пароля	Ошибка изменения пароля пользователя
17	Подтверждение адреса электронной почты	Подтверждение адреса электронной почты
18	Ошибка подтверждения адреса электронной почты	Ошибка подтверждения адреса электронной почты
29	Пользователь разблокирован	Пользователь разблокирован
20	Пользователь заблокирован	Пользователь заблокирован
21	Сброс пароля	Сброс пароля выполнен успешно
22	Ошибка сброса пароля	Ошибка сброса пароля
23	Вход через провайдера идентификации	Вход через провайдера идентификации выполнен успешно
24	Ошибка входа через провайдера идентификации	Ошибка входа через провайдера идентификации
25	Смена пользователя	Смена пользователя

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Расшифровка
IP	Internet Protocol — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.
IP-адрес	Сетевой адрес в цифровом виде, уникальное число, назначающееся каждому компьютеру, подключенному к Интернет.
SSO	Single Sign-On - технология, при использовании которой пользователь переходит из одного раздела портала в другой без повторной аутентификации.
Администратор	Пользователь, которому присвоена роль администратора в одном домене с привилегиями администратора только в группе проектов этого домена.
Администратор безопасности	Сотрудник, отвечающий за настройку и поддержание в рабочем состоянии ПК «Bars.Up.Access Manager»
БД	База данных
Домен	Метод объединения проектов в независимые группы.
Интернет-браузер, web-браузер	Программный комплекс для поиска, просмотра веб-страниц (преимущественно из сети Интернет), для их обработки, вывода и перехода от одной страницы к другой. Например, Microsoft Internet Explorer, Mozilla Firefox и т.п.
Маркер аутентификации	Информация, которая проверяет аутентичность пользователя.
ОО	Объект оценки
ПК	Программный комплекс
Пользователь	Сотрудник, который использует программный комплекс «Bars.Up.Access Manager».
Провайдер идентификации	Аутентифицирует пользователя и предоставляет сервис-провайдеру маркер аутентификации
РД	Руководящий документ
Система	Информационная система, доступ к которой осуществляется через ПК «Bars.Up.Access Manager» путем реализации технологии единой точки доступа (Single Sign-On, SSO) к информационным системам.

Событие безопасности	Идентифицированное возникновение состояния системы, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью
Токен	Средство идентификации пользователя или отдельного сеанса работы в компьютерных сетях и приложениях.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ изм.	Новых листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	изъятых					