Программный комплекс

«Bars.Up.Access Manager»

Что такое WEBSSO?

WebSSO (Web Single Sign-On) — это технология, которая позволяет пользователям авторизовываться на нескольких сайтах без необходимости запоминать множество логинов и паролей. Вместо этого пользователь может использовать один и тот же логин и пароль для доступа к нескольким сайтам или приложениям, которые поддерживают WebSSO.

Когда пользователь входит в web - приложение, который поддерживает WebSSO, он автоматически получает доступ ко всем другим сайтам, которые также используют эту технологию. При этом каждый раз, когда пользователь заходит на новый сайт или web - приложение, ему не нужно вводить свой логин и пароль заново.

В целом, системы класса WebSSO позволяют упростить процесс авторизации на нескольких сайтах или web - приложениях и повысить безопасность пользователей, так как они не должны запоминать множество логинов и паролей.

Решение БАРС Груп BarsUP.AM является сертифицированным программным средством защиты информации прикладных web-приложений 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 и устройств;
- управление доступом субъектов доступа к информационным системам;

– регистрация событий безопасности.

BarsUP.AM 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.

Стандарты реализации единого входа в BarsUP.AM :

OpenID Connect (OAuth 2.0) — это протокол авторизации и аутентификации пользователей в интернете. Он позволяет пользователям давать доступ к своим данным на различных сайтах без необходимости каждый раз вводить логин и пароль. Вместо этого пользователь получает уникальный идентификатор, который он может использовать для доступа к своим данным на разных сайтах.

Security Access Markup Language (SAML) — это язык разметки, используемый для определения прав доступа к ресурсам и приложениям в среде безопасности. Он используется для создания и управления политиками безопасности, которые определяют, какие пользователи имеют доступ к каким ресурсам и приложениям. SAML предоставляет структурированный формат для описания политик безопасности, позволяя администраторам создавать и управлять политиками безопасности централизованно.

Возможности BarsUP.AM

BarsUP.AM предоставляет следующие возможности:

- идентификация и аутентификация пользователей и устройств;
- управление идентификаторами и средствами аутентификации (аутентификационной информацией) пользователей и устройств;
- идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа;
- возможность двухфакторной аутентификации, с использованием TOTP алгоритма
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

- управление доступом субъектов доступа посредством реализации ролевого метода управления доступом и правила разграничения доступа;
- назначение необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование BarsUP.AM;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирования на них;
- обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в BarsUP.AM;
- контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в BarsUP.AM;
- ограничение прав пользователей по вводу информации в BarsUP.AM;
- обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;
- обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов;
- обеспечение возможности активация/деактивация учетных записей пользователей.

Функциональное назначение BarsUP.AM

BarsUP.AM обеспечивает идентификацию пользователей по именам учетных записей пользователей. ПК BarsUP.AM обеспечивает аутентификацию пользователей с использованием паролей.

BarsUP.AM обеспечивает аутентификацию для следующих видов и субъектов доступа:

- удаленного доступа пользователей и администраторов при использовании сети связи общего пользования, в том числе сети Интернет;
- локального доступа администраторов и пользователей для локального доступа.

BarsUP.AM реализовывает следующие функции управления идентификаторами пользователей:

- формирование идентификатора, который однозначно идентифицирует пользователя;
- присвоение идентификатора пользователю;
- предотвращение повторного использования идентификатора пользователя, в течение установленного оператором периода времени;
- блокирование идентификатора пользователя после установленного оператором времени неиспользования.

BarsUP.AM:

- исключает повторное использование идентификатора пользователя в течение не менее трех лет;
- обеспечивает блокирование идентификатора пользователя не более чем через период времени неиспользования не более 45 дней.

BarsUP.AM реализовывает следующие функции управления аутентификационной информацией пользователей:

- генерация и выдача начальной аутентификационной информации;
- установление характеристик пароля:
- задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;
- задание минимального количества измененных символов при создании новых паролей;
- задание максимального времени действия пароля;
- запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей.
- блокирование (прекращения действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;
- обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором;

BarsUP.AM обеспечивает:

- длину 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.

BarsUP.AM осуществляет защиту аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

Защита осуществляется путем исключения отображения для пользователя действительного значения аутентификационной информации. Вводимые символы пароля отображаются условными знаками «•».

BarsUP.AM осуществляет управление учетными записями пользователей: заведение, активация, блокирование, уничтожение учетных записей.

BarsUP.AM осуществляет автоматическое блокирование временных учетных записей пользователей по окончании установленного времени для их использования, а также неактивных (неиспользуемых) учетных записей пользователей после периода время неиспользования более 45 дней.

BarsUP.AM устанавливает и реализовывает следующие функции управления учетными записями пользователей:

- объединение учетных записей в группы;
- временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования автоматизированной/информационной системы, для организации гостевого доступа.

BarsUP.AM реализовывает ролевой метод управления доступом субъектов доступа (пользователей) к объектам доступа на основе ролей субъектов доступа.

BarsUP.AM обеспечивает назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

BarsUP.AM предоставляет права и привилегии по доступу к функциям безопасности (параметрам настройки) исключительно администратору, наделенному полномочиями по администрированию.

BarsUP.AM обеспечивает установку ограничения количества неуспешных попыток входа пользователя в ПК и блокирование учетной записи пользователя при

превышении пользователем ограничения количества неуспешных попыток входа, с возможностью разблокирования только администратором.

BarsUP.AM предупреждает пользователя при его входе в ПК о том, что в нем реализованы меры по обеспечению защиты информации.

BarsUP.AM оповещает пользователя после успешного входа в ПК о его предыдущем входе.

BarsUP.AM обеспечивает ограничение числа параллельных сеансов доступа пользователей для каждой учетной записи пользователя.

BarsUP.AM предоставляет возможность контролировать и отображать администратору число параллельных сессий для каждой учетной записи пользователей.

BarsUP.AM обеспечивает блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя.

BarsUP.AM регистрирует вход (выход), а также попытки входа субъектов доступа в ПК.

В перечень событий безопасности, подлежащих регистрации, включены события, связанные с действиями от имени привилегированных учетных записей (администраторов) и с изменением привилегий учетных записей (регистрация входа и выхода администраторов, регистрация изменения параметров учетных записей администраторов).

BarsUP.AM обеспечивает срок хранения информации о зарегистрированных событиях безопасности, осуществляет хранение записей о выявленных событиях безопасности и записей системных журналов, которые служат основанием для регистрации события безопасности.

Состав и содержание информации о событиях безопасности обеспечивают возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

При регистрации входа (выхода) субъектов доступа в ПК BarsUP.AM состав и содержание информации включают дату и время входа (выхода) в автоматизированную/информационную систему (из автоматизированной/ информационной системы), результат попытки входа (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

BarsUP.AM осуществляется реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности.

BarsUP.AM имеется возможность просмотра и анализа информации о действиях отдельных пользователей.

Описание области применения BarsUP.AM

Портфолио приложений: системы WebSSO позволяют пользователям получать доступ к нескольким приложениям и сайтам, используя один аккаунт.

Управление доступом: системы WebSSO позволяют администраторам управлять правами доступа пользователей к различным ресурсам и приложениям.

Безопасность: системы WebSSO обеспечивают безопасность данных и защиту от несанкционированного доступа к информации.

Удобство использования: системы WebSSO упрощают процесс входа на сайты и приложения, что повышает удобство использования для пользователей.

Интеграция: системы WebSSO позволяют интегрировать различные приложения и сайты, чтобы пользователи могли получать доступ к информации и ресурсам из одного места.

Требования к техническому обеспечению BarsUP.AM

Требования к техническому обеспечению

Структуру комплекса технических средств должны составлять следующие группы технических средств:

- *серверная группа;*
- *клиентские рабочие места пользователей.*

Требования к техническому обеспечению серверов:

- *сервер БД: 2 CPU, 8GB RAM, 64GB HDD;*
- *сервер кластерного домена (Master Wildfly): 2 CPU, 4GB RAM, 40GB HDD;*
- *сервер кластера ядра платформы: 2 CPU, 8GB RAM, 40GB HDD (рекомендуется кластер из нескольких нод для повышения отказоустойчивости и производительности);*
- *веб-сервер: 2 CPU, 8GB RAM, 40GB HDD (рекомендуется кластер из нескольких нод для повышения отказоустойчивости и производительности);*
- *сервер-балансировщик: 1 CPU, 4GB RAM, 40GB HDD.*

Требования к программному комплексу серверов:

- *сервер БД:*
- *ОС CentOS 7 (x86/x64);*
- *СУБД PostgreSQL 9.5;*
- *Wget;*
- *ntpdate.*
- *сервер кластерного домена:*
- *ОС CentOS 7 (x86/x64);*
- *WildFly 10.0;*
- *Wget;*
- *ntpdate;*
- *NTP.*
- *сервер кластерного ядра платформы:*
- *ОС CentOS 7 (x86/x64);*
- *WildFly 10.0;*
- *Wget;*
- *ntpdate.*
- *веб-сервер:*
- *ОС CentOS 7 (x86/x64);*
- *WildFly 10.0;*
- *Wget;*
- *ntpdate.*
- *сервер-балансировщик:*
- *ОС CentOS 7 (x86/x64);*
- *WildFly 10.0;*
- *Wget;*
- *ntpdate;*
- *Nginx.*

Спецификация и технологический стек

Языки программирования

- **Java**

Фреймворки

- **EJB**

Серверная часть

- **Ubuntu**
- **Nginx**
- **WildFly**

Языки запросов к базе данных

- **SQL**

Среды разработки

- **IntelliJ Idea**

Сервер базы данных

- **PostgreSQL**

Сведения о сертификации BarsUP.AM

Программный комплекс «Bars.Up.Access Manager», разработанный АО «БАРС Груп», является программным средством со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом и регистрации событий безопасности, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, что подтверждено сертификатом соответствия **№4716 от 14.09.2023.**