**Система управления идентификацией и доступом «AtomID»**

Система управления идентификацией и доступом АтомID является программным средством обеспечения безопасности информационных технологий. Система применяется для защиты информации в значимых объектах критической информационной инфраструктуры 3 категории, в государственных информационных системах 3 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, а также для обеспечения до 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 3-го типа.

АтомID осуществляет идентификацию и аутентификацию операторов, администраторов и пользователей подключаемых систем. Аутентификация осуществляется с использованием паролей, идентификация осуществляется по идентификатору, связанному с учетной записью оператора, администратора и пользователя подключаемых систем. АтомID осуществляет блокировку доступа для субъектов, не прошедших процедуру аутентификации. (мера защиты ИАФ.1).

АтомID обеспечивает возможность использования двухфакторной аутентификации. (мера защиты ИАФ.1, усиление 1).

АтомID может выступать в качества брокера идентификации с поддержкой протоколов SAML 2.0, OIDC и SPNEGO/Kerberos.

АтомID обеспечивает формирование (создание) идентификатора, который однозначно идентифицирует пользователя. АтомID обеспечивает предотвращение повторного использования идентификатора. (мера защиты ИАФ.3).

АтомID обеспечивает 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 минимальной длины пароля;
* задание максимального времени действия пароля;
* запрет использования логина в качестве пароля;
* запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей.

АтомID обеспечивает блокирование (прекращение действия) и замену утерянных, скомпрометированных паролей.

АтомID обеспечивает обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором.

АтомID обеспечивает защиту аутентификационной информации от неправомерных доступа к ней и модифицирования (мера защиты ИАФ.4).

В АтомID осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации. Вводимые символы пароля отображаются условными знаками «•» (мера защиты ИАФ.4).

В АтомID осуществляется однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) (мера защиты ИАФ.6).

АтомID осуществляет ролевое управление доступом для:

* субъектов доступа:

1. администраторы;
2. операторы;
3. пользователи подключаемых систем.

* объектов доступа:

1. информационные ресурсы, обрабатываемые в AtomID;
2. информационные ресурсы, обрабатываемые в подключаемых системах.

АтомID осуществляет ролевое управление доступом, основываясь на:

* идентификаторе субъекта доступа;
* идентификаторе объекта доступа;
* правилах разграничения доступа субъекта доступа к объекту доступа (мера защиты УПД.2).

АтомID обеспечивает ограничение количества неуспешных попыток входа путем блокирования учетной записи при превышении ограничения количества неуспешных попыток входа (мера защиты УПД.6).

В АтомID обеспечивается блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) или по запросу (мера защиты УПД.10).

В АтомID блокируются любые действия пользователей до идентификации и аутентификации (мера защиты УПД.11).

АтомID обеспечивает регистрацию следующих событий безопасности:

* вход/выход или попытку входа оператора или администратора в АтомID;
* вход/выход или попытку входа пользователей в подключаемые системы;
* любые изменения в настройках АтомID;
* доступ субъектов к объектам доступа в подключаемых системах.

Состав и содержание информации, подлежащей регистрации, включает:

* дату и время события;
* тип события;
* идентификатор субъекта и объекта доступа;
* результат события (успешный или неуспешный);
* IP-адрес источника события (мера защиты РСБ.3).

АтомID ограничивает доступ к записям аудита и функциям управления механизмами регистрации (аудита) в соответствии с УПД.2 (мера защиты РСБ.7).

АтомID предоставляет возможность просмотра и анализа информации о действиях отдельных пользователей (мера защиты РСБ.8).

АтомID предоставляет возможность импорта конфигурации на машинные носители информации (мера защиты ОДТ.4).

АтомID предоставляет возможность восстановления конфигурации из ранее импортированного файла (мера защиты ОДТ.5)