



И.о. министра

Р.М. Самбу-Хоо
«05» августа 20 11 г.

Правила идентификации и аутентификации субъектов доступа и объектов доступа в информационной системе Министерства по внешнеэкономическим связям и туризму Республики Тыва

1. Общие положения

1.1. Данные Правила регламентируют порядок и процедуры присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности), а также организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах Министерства по внешнеэкономическим связям и туризму Республики Тыва и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

2.1. При доступе в ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва осуществляется идентификация и аутентификация пользователей, являющихся работниками Министерства по внешнеэкономическим связям и туризму Республики Тыва (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. К внутренним пользователям относятся должностные лица Министерства по внешнеэкономическим связям и туризму Республики Тыва:

- администратор ИС;
- администратор информационной безопасности (ИБ);
- ответственные работники по работе с ИС, выполняющие свои должностные обязанности (функции) в соответствии с должностными регламентами (инструкциями), утвержденными в организации и которым в <Наименование организации> присвоены учетные записи.

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с

организационно-распорядительными документами Министерства по внешнеэкономическим связям и туризму Республики Тыва. Для каждого внутреннего пользователя в ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва должны быть заведены учетные записи.

2.2. Пользователи ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва

2.3. Аутентификация пользователя в ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва осуществляется с использованием паролей. Также на усмотрение администратора ИБ могут применяться аппаратные средства в случае многофакторной (двухфакторной) аутентификации.

2.4. В ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

2.5. В ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва обеспечена многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов; пользователей), с использованием сети связи общего пользования, в том числе сети Интернет и с правами непривилегированных учетных записей (пользователей) с использованием сети связи общего пользования, для локального доступа в систему с правами привилегированных учетных записей (администраторов; пользователей).

3. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

3.1. В ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) осуществляется идентификация и аутентификация устройств (технических средств).

3.2. Идентификации и аутентификации до начала информационного взаимодействия подлежат следующие типы устройств:

- АРМ пользователя;
- Серверы;
- Ноутбуки;
- Тонкие клиенты;
- Принтер;
- Сканер.

3.3. Идентификация устройств в ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-

адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства. Аутентификация устройств в ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

4. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

4.1. В ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва устанавливаются и реализуются следующие функции управления идентификаторами пользователей и устройств:

- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года.
- блокирование идентификатора пользователя после 90 дней неиспользования.

4.2. В качестве ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств определен Администратор ИБ.

5. Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

5.1. В ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва устанавливаются и реализуются функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств:

- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты Министерства по внешнеэкономическим связям и туризму Республики Тыва;
- выдача средств аутентификации пользователям;
- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
- установление характеристик пароля: длина пароля не менее шести символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на 5 минут, смена паролей не более чем через 180 дней;
- блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;
- назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

- обновление аутентификационной информации (замена средств аутентификации) с периодичностью не более, чем через 90 дней;
- защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

5.2. В случае компрометации личного пароля пользователя ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

- Внеплановая смена личного пароля или удаление учетной записи пользователя ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться Администратором ИБ немедленно после окончания последнего сеанса работы данного пользователя с системой.

- Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) Администратора ИБ и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва.

5.3. В качестве ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации устройств определен Администратор ИБ.

6. Защита обратной связи при вводе аутентификационной информации

6.1. В ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

6.2. Защита обратной связи «система – субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.

7. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре (при наличии)

7.1. В ИС Министерства по внешнеэкономическим связям и туризму Республики Тыва обеспечивается идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администратора ИС в соответствии с настоящими Правилами, в том числе:

- идентификация и аутентификация администратора ВИ;
- идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;
- блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования;
- защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;
- идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

7.2. Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с настоящими Правилами.

8. Ответственность при организации идентификации и аутентификации

8.1. Ответственность за реализацию правил идентификации и аутентификации субъектов доступа и объектов доступа в соответствии с требованиями настоящих Правил возлагается на Администратора ИБ.

8.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящих Правил возлагается на Администратора ИБ и пользователей Министерства по внешнеэкономическим связям и туризму Республики Тыва

8.3. Периодический контроль за выполнением всех требований настоящих Правил осуществляется комиссией по проведению мероприятий по защите информации.

Лист ознакомления

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				