УТВЕРЖДАЮ
И.о. министра
_____ /Р.М. Самбу-Хоо
«26» августа 2021 г.

ПОЛИТИКА
организации парольной защиты в государственной информационной системе Министерства по внешнеэкономическим связям и туризму Республики Тыва

1. Целью настоящей политики является регламентирование организационно-технического обеспечения процессов генерации, использования, смены и прекращения действия паролей (удаления учетных записей пользователей) в государственной информационной системе (далее – ГИС), а также процесса контроля за действиями пользователей системы при работе с паролями с целью соблюдения требований, предъявляемых к государственным информационным системам второго класса защищенности.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ГИС и контроль за действиями пользователей системы при работе с паролями возлагается на отдел бухгалтерского учета, правового и кадрового обеспечения.

3. В Министерстве по внешнеэкономическим связям и туризму Республики Тыва установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе:

– определено должностное лицо (администратор)/подразделение, ответственное за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

– изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;

– выдача средств аутентификации пользователям;

– генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

– установление характеристик пароля:

а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

б) задание минимального количества измененных символов при создании новых паролей;

в) задание максимального времени действия пароля;

г) задание минимального времени действия пароля;

д) запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;

– 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, установленной оператором;

– защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

4. Личные пароли пользователей должны генерироваться и распределяться централизованно либо выбираться пользователями ГИС самостоятельно с учетом следующих требований:

– длина пароля не менее шести символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

– пароль не должен содержать имя учетной записи пользователя или какую-либо его часть или включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER и т.п.);

– алфавит пароля не менее 70 символов;

– максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 8 попыток;

– блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут;

– смена паролей не более чем через 90 дней.

5. Пользователям информационной системы запрещается сообщать кому-либо свой пароль.

6. Пользователям информационной системы запрещается хранить пароли в открытом виде (записывать пароли на бумаге и других носителях информации).

7. Пользователь обязан помнить свой пароль. В случае утраты пароля пользователь обязан сообщить системному администратору.

8. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

9. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников Министерства по внешнеэкономическим связям и туризму Республики Тыва. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

10. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

11. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение и т. д.) должна производиться уполномоченными сотрудниками Министерства по внешнеэкономическим связям и туризму Республики Тыва немедленно после окончания последнего сеанса работы данного пользователя.

12. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и т. д.) администраторов средств защиты и других сотрудников, которым были предоставлены полномочия по управлению парольной защитой информационной системы.

13. Учетная запись пользователя, ушедшего в длительный отпуск (более <...> дней), должна блокироваться администратором с момента получения письменного уведомления от кадрового подразделения.

14. Удаление учетных записей пользователей, уволенных или переведенных в другое структурное подразделение должно производиться администратором немедленно с момента получения письменного уведомления из кадрового подразделения.

15. В случае возникновения необходимости в смене пароля в виду компрометации пользователь должен немедленно известить администратора информационной системы или <подразделение по защите информации/ответственного за защиту информации>.

16. За разглашение парольной информации, сотрудник привлекается к ответственности в соответствии с действующим законодательством Российской Федерации.

17. Учет выданных паролей ведется в журнале выдачи паролей.

18. Журнал выдачи паролей пользователям государственной информационной системы должен храниться в надежно запираемом сейфе администратора.

Консультант _____ Ч.К. Сарыглар