УТВЕРЖДАЮ

И.о. министра

_____ /Р.М. Самбу-Хоо

«05» августа 2021 г.

Положение о разграничении прав доступа к информации, обрабатываемой в государственной информационной системе Министерства по внешнеэкономическим связям и туризму Республики Тыва

1.1 Настоящее Положение определяет правила управления доступом субъектов доступа к объектам доступа в государственной информационной Министерства по внешнеэкономическим связям и туризму Республики Тыва в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17 согласно установленному классу защищенности (К2).

1.2 В государственной информационной системе установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

– определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);

– объединение учетных записей в группы (при необходимости);

– верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

– заведение, активация, блокирование и уничтожение учетных записей пользователей; пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором;

– порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов; оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

– уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

– предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

1.3 Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для

проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

1.4 В информационной системе используются автоматизированные средства поддержки управления учетными записями пользователей.

1.5 В информационной системе осуществляется автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

1.6 В информационной системе осуществляется автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования: более 90 дней.

1.7 Для управления доступом субъектов доступа к объектам доступа в информационной системе реализуется(ются) следующий метод управления доступом:

– дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;

– ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);

– мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

1.8 Правила разграничения доступа реализуются на основе установленных списков доступа или матриц доступа.

1.9 В информационной системе правила разграничения доступа обеспечивают управление доступом субъектов при входе в информационную систему.

1.10 В информационной системе правила разграничения доступа обеспечивают управление доступом субъектов к техническим средствам, устройствам, внешним устройствам.

1.11 В информационной системе правила разграничения доступа обеспечивают управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением.

1.12 Управление информационными потоками должно обеспечивать разрешенный маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками. Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик,

несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

1.13 В информационной системе обеспечивается разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями).

1.14 В информационной системе обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя до 15 минут или по запросу пользователя.

1.15 Перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации:

–...;

–...;

–....

1.16 Администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

1.17 Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

1.18 Защита удаленного доступа обеспечивается при всех видах доступа и включает:

– установление видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы;

– предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

– мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы;

– контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации).

1.19 В информационной системе используется ограниченное (минимально необходимое) количество точек подключения к информационной системе при организации удаленного доступа к объектам доступа информационной системы.

1.20 В информационной системе исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации.

1.21 В информационной системе обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с информационной системой.

1.22 Регламентация и контроль использования технологий беспроводного доступа включают:

– ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление беспроводного доступа;

– предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

– мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной системы;

– контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой.

1.23 В информационной системе обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств;

1.24 В информационной системе исключается возможность изменения пользователем точек беспроводного доступа информационной системы.

1.25 Управление взаимодействием с внешними информационными системами включает:

– предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям;

– определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;

– определение системных учетных записей, используемых в рамках данного взаимодействия; определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;

– определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

1.26 Доступ к информационной системе предоставляется авторизованным (уполномоченным) пользователям внешних информационных систем или разрешение на обработку, хранение и передачу информации с использованием внешней информационной системы осуществляется при выполнении следующих условий:

– при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

– при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

1.27 В информационной системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки.

1.28 В информационной системе доверенная загрузка обеспечивает:

– блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;

– контроль доступа пользователей к процессу загрузки операционной системы;

– контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

1.29 В информационной системе осуществляется доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения.

Консультант _____ Ч.К. Сарыглар