ПРИЛОЖЕНИЕ № 7
к приказу
от 6 августа 2024 г.
№ 65-ос

ПОЛОЖЕНИЕ
об управлении доступом субъектов доступа к объектам доступа в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва

1. Термины и определения

Аутентификационная информация (информация аутентификации): информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе.

Аутентификация: проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

Идентификатор: представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе.

Идентификация: присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Локальный доступ: доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).

Многофакторная аутентификация: аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации.

Непривилегированная учетная запись: учетная запись пользователя (процесса, выполняемого от его имени) информационной системы.

Объект доступа: единица информационного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Пользователь: лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

Привилегированная учетная запись: учетная запись администратора информационной системы.

Роль: предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.

Субъект доступа: пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Удаленный доступ: процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

Управление доступом: ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

2. Принятые сокращения

ИБ – информационная безопасность
ИС – информационная система
КЗ – контролируемая зона
НСД – несанкционированный доступ
ОС – операционная система
ПО – программное обеспечение
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СКЗИ – средство криптографической защиты информации
СУБД – система управления базой данных
ТС – техническое средство

3. Общие положения

3.1. Настоящее положение определяет права и привилегии субъектов доступа, описывает разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва (далее – ИС Госкомохотнадзора РТ) правил разграничения доступа, а также контроль соблюдения этих правил.

3.2. Разграничение прав осуществляется на основании Модели угроз безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, при её обработке в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва, а также исходя из характера и режима обработки информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – Информация) в ИС Госкомохотнадзора РТ.

3.3. Уровень прав доступа представлен в Таблице 1.

Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, осуществляется в соответствии с их должностными обязанностями. Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с матрицей доступа.

Таблица 1 – Уровень прав доступа.

№ п/п	Группа	Уровень доступа к Информации, ТС, прикладному ПО и СЗИ	Разрешенные действия
1.	Администратор ИС	Доступ на правах администратора к Информации, ТС и прикладному ПО. Без доступа к СЗИ	– модернизация, настройка и мониторинг работоспособности комплекса ТС (серверов, рабочих станций); – установка, модернизация, настройка и мониторинг работоспособности системного и базового ПО; – установка, настройка и мониторинг прикладного ПО; – соблюдение правил, оговоренных в инструкции администратора
2.	Администратор ИБ	Доступ на правах администратора к СЗИ. Без доступа на изменение к Информации, ТС и прикладному ПО	– разработка, управление и реализация эффективной политики информационной безопасности системы; – управление (администрирование) системой защиты информации ИС; – выявление инцидентов и реагирование на них; – управление конфигурацией ИС и ее системы защиты; – контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИС; – управление правами доступа пользователей к функциям системы; – проверка состояния используемых СЗИ от НСД, проверка правильности их настройки; – обеспечение функционирования и поддержание работоспособности СЗИ; – проведение инструктажа эксплуатационного персонала и пользователей СВТ по правилам работы с используемыми СЗИ; – контроль и предотвращение несанкционированного изменения целостности ресурсов; – контроль аппаратной конфигурации защищаемых компьютеров и предотвращение попытки ее несанкционированного изменения
3.	Администратор резервного копирования	Доступ на правах администратора к прикладному ПО и ТС. Без доступа на изменение Информации и СЗИ	– Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы; – периодическое резервное копирование информации на резервные машинные носители информации; – контроль работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий; – восстановление информации из резервных копий
4.	Ответственный за эксплуатацию СКЗИ	Доступ на правах администратора к сертифицированным СКЗИ. Без доступа на изменение к Информации, ТС, прикладному ПО, СЗИ	– поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним; – контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией; – учет Пользователей криптосредств;

№ п/п	Группа	Уровень доступа к Информации, ТС, прикладному ПО и СЗИ	Разрешенные действия
			– надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей дистрибутивов криптосредств, бумажных и машинных носителей Информации; – расследования и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации; – разработка и принятие мер по предотвращению возможных негативных последствий нарушений
5.	Ответственный за обработку и защиту информации	Доступ на правах пользователя к Информации, ТС, прикладному ПО и СЗИ. Без доступа на изменение ПО, СЗИ и ТС	– контроль (мониторинг) за обеспечением уровня защищенности информации – информирование пользователей о требованиях законодательства Российской Федерации об Информации, локальных актов по вопросам обработки и защиты Информации. – внутренний контроль (проверки) над соблюдением законодательства Российской Федерации об Информации, в том числе требований к защите Информации
6.	Пользователь	Доступ на правах пользователя к Информации, ТС, прикладному ПО и СЗИ. Без доступа на изменение ПО, СЗИ и ТС	– сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, предоставление записей, содержащих Информацию

3.4. Должен быть утвержден Перечень лиц, имеющих доступ в помещения, в которых расположены технические средства информационных систем, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва (далее – Помещения), в соответствии с минимально необходимыми для выполнения ими своих должностных обязанностей. Должен быть исключен неконтролируемый доступ в Помещения.

3.5. Работники Госкомохотнадзора РТ, которые в рамках своих должностных обязанностей обрабатывают Информацию, должны быть внесены в Перечень лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации в ИС.

4. Правила разграничения доступа

4.1. В ИС Госкомохотнадзора РТ организовано (реализовано):

4.1.1. Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей, возлагается на администратора ИБ путем следующих функций:

– определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная);

– объединение учетных записей в группы (при необходимости);

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

– заведение, активация, блокирование и уничтожение учетных записей пользователей (при необходимости);

– пересмотр и, при необходимости, корректировка учетных записей не реже одного раза в три месяца;

– порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

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

– предоставление пользователям прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней ИС;

– использование автоматизированных средств поддержки управления учетными записями пользователей;

– автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

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).

Заведение временных учетных записей осуществляется на основании подписанного администратором ИБ и ответственным за обработку и защиту Информации, утвержденного и. о. руководителя (председателя) Госкомохотнадзора РТ соответствующего Акта, содержащего цель, место, наименование и сроки их использования, по истечении которых осуществляется автоматическое блокирование временных учетных записей пользователей.

4.1.2. 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). Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей).

Правила разграничения доступа реализуются на основе матрицы доступа и обеспечивают управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к ТС, устройствам (в том числе внешним), объектам файловой системы, запускаемым и исполняемым модулям, объектам СУБД, параметрам настройки СЗИ, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации.

В ИС Госкомохотнадзора РТ правила разграничения доступа должны обеспечивать:

– управление доступом субъектов при входе в ИС;

– управление доступом субъектов к ТС, устройствам, внешним устройствам;

– управление доступом субъектов к объектам, создаваемым общесистемным (общим) ПО.

4.1.3. В ИС Госкомохотнадзора РТ осуществляется управление информационными потоками, которое обеспечивает разрешенный маршрут прохождения информации между пользователями, устройствами в рамках информационной системы и между информационными системами или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). 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.

4.1.4. Ограничение неуспешных попыток входа в ИС (доступа к ИС), равное 5 (пяти), при этом должно быть обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в ИС (доступа к ИС) не менее чем на 5 (пять) минут.

4.1.5. Блокирование сеанса доступа в ИС Госкомохотнадзора РТ после 15 минут бездействия (неактивности) пользователя или по его запросу.

Блокирование сеанса доступа пользователя в ИС обеспечивает временное приостановление работы пользователя с СВТ, с которого осуществляется доступ к ИС Госкомохотнадзора РТ (без выхода из ИС Госкомохотнадзора РТ).

Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в ИС Госкомохотнадзора РТ сохраняется до прохождения им повторной идентификации и аутентификации.

4.1.6. Запрет всех действий пользователей до прохождения процедур идентификации и аутентификации в ИС (кроме необходимых для прохождения процедур идентификации и аутентификации).

Администратору ИБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИС в случае сбоев в работе или выходе из строя отдельных ТС (устройств).

4.1.7. Регламентация и контроль использования в информационной системе технологий беспроводного доступа.

В ИС Госкомохотнадзора РТ обеспечивается регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе.

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;

– 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;

– аутентификация подключаемых с использованием технологий беспроводного доступа устройств.

4.1.8. Контроль использования в ИС мобильных технических средств

В ИС допускаются проводные (коммутируемые), беспроводные и широкополосные доступы к объектам доступа информационной системы с

использованием мобильных технических средств: съемных машинных носителей информации, портативных вычислительных устройств и устройств связи с возможностью обработки информации.

Контроль использования мобильных технических средств в ИС Госкомохотнадзора РТ включает:

– использование в составе ИС для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с правилами обращения с машинными носителями информации и мобильными техническими средствами в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва;

– ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ИС, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств;

– мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС;

– запрет возможности запуска без команды пользователя в информационной системе ПО (программного кода), используемого для взаимодействия с мобильным техническим средством;

– применение мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), в соответствии с требованиями Правил обращения с машинными носителями информации и мобильными техническими средствами в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

4.1.9. Управление взаимодействием с ИС сторонних организаций (внешними ИС)

В ИС Госкомохотнадзора РТ управление взаимодействием с внешними ИС возлагается на ответственного за обработку и защиту Информации совместно с администратором ИБ и администратором ИС, и включает:

– предоставление доступа к ИС только авторизованным (уполномоченным) пользователям;

– определение типов прикладного ПО ИС, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних ИС;

– определение системных учетных записей, используемых в рамках данного взаимодействия;

– определение порядка предоставления доступа к ИС Госкомохотнадзора РТ авторизованными (уполномоченным) пользователями из внешних ИС;

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

Госкомохотнадзор РТ предоставляет доступ к ИС Госкомохотнадзора РТ авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней информационной системы при выполнении следующих условий:

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

б) 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).

Лист ознакомления
с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва

№ 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.				