

ИНСТРУКЦИЯ
администратора информационной безопасности информационных систем
Государственного комитета по охране объектов животного мира
Республики Тыва

1. Общие положения

1.1. Инструкция администратора информационной безопасности информационных систем Государственного комитета по охране объектов животного мира Республики Тыва (далее – ИС Госкомохотнадзора РТ) (далее – Инструкция) определяет функции, права и обязанности администратора информационной безопасности (далее – администратор ИБ) по вопросам обеспечения информационной безопасности при подготовке и исполнении документов в ИС Госкомохотнадзора РТ.

1.2. Администратор ИБ назначается из числа работников Госкомохотнадзора РТ приказом и.о. руководителя (председателя) и обеспечивает правильность использования и нормальное функционирование установленной системы защиты ИС Госкомохотнадзора РТ.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

1.4. Администратор ИБ обладает правами доступа к любым программно-аппаратным средствам защиты информации (далее – СЗИ) на технических средствах пользователей. Он несет ответственность за реализацию принятой политики безопасности.

2. Должностные обязанности

2.1. Администратор ИБ обязан:

2.1.1. Осуществлять учет и периодический контроль за составом и полномочиями пользователей ИС Госкомохотнадзора РТ.

2.1.2. Осуществлять оперативный контроль за работой пользователей ИС Госкомохотнадзора РТ, анализировать содержимое системных журналов средств вычислительной техники (далее – СВТ) и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов СВТ и надлежащий режим хранения данных архивов.

2.1.3. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в ИС Госкомохотнадзора РТ СЗИ.

2.1.4. Присутствовать при внесении изменений в конфигурацию

(модификации) аппаратно-программных средств защищенных СВТ, обеспечивать и контролировать установку и настройку СЗИ.

2.1.5. Не реже одного раза в месяц проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).

2.1.6. Управлять учётными записями пользователей, реализовывать правила разграничения доступа, а также осуществлять контроль соблюдения этих правил в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

2.1.7. Управлять идентификаторами (осуществлять создание, присвоение и уничтожение идентификаторов пользователей и устройств) и средствами аутентификации (аутентификационной информацией) внутренних пользователей в ИС Госкомохотнадзора РТ, обеспечивать соблюдение правил идентификации и аутентификации пользователей и устройств в соответствии с Правилами идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

2.1.8. Осуществлять контроль за хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации в соответствии с Правилами идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

2.1.9. Осуществлять контроль не реже одного раза в три месяца установленного (инсталлированного) в ИС Госкомохотнадзора РТ программного обеспечения в соответствии с Правилами по ограничению программной среды в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

2.1.10. Осуществлять мониторинг и контроль применения мобильных технических средств в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС.

2.1.11. Настраивать параметры журналов регистрации событий безопасности в соответствии с Правилами регистрации событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

2.1.12. Проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование на них не реже одного раза в неделю.

2.1.13. Управлять средствами антивирусной защиты в соответствии с Инструкцией по антивирусной защите в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

2.1.14. Осуществлять контроль уровня защищенности информации, обрабатываемой в ИС Госкомохотнадзора РТ, в соответствии с Инструкцией по контролю защищенности информации в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

2.1.15. Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков.

2.1.16. Обеспечивать сохранность СЗИ, эксплуатационной и технической документации к СЗИ, а также порядок обращения с СЗИ в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации в соответствии с Инструкцией по порядку обращения со средствами защиты информации в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

2.1.17. Проводить не реже одного раза в три месяца контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в соответствии с Правилами идентификации и аутентификации пользователей в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва и Инструкцией по контролю защищенности информации в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

2.1.18. Своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СЗИ, установленных на СВТ ИС Госкомохотнадзора РТ.

2.1.19. Осуществлять поэкземплярный учет в соответствующем журнале:

– СЗИ (носителей дистрибутивов, системных блоков с установленными СЗИ);

– эксплуатационной и технической документации к СЗИ.

2.1.20. Осуществлять хранение:

– носителей дистрибутивов СЗИ;

– лицензий и сертификатов на СЗИ.

2.1.21. Не реже одного раза в месяц осуществлять проверки:

– состояния защищенности информационных ресурсов от сбоя в системе электропитания (система резервирования и автоматического ввода резерва);

– состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатающих устройств, оборудования распределительных шкафов).

2.1.22. Проводить первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала ИС Госкомохотнадзора РТ по

вопросам работы с СЗИ.

2.1.23. Отвечать на вопросы обслуживающего и эксплуатирующего персонала ИС Госкомохотнадзора РТ, связанные с работой СЗИ.

2.1.24. Составлять инструкции по работе с СЗИ.

2.1.25. Докладывать руководству Госкомохотнадзора РТ об имевших место попытках несанкционированного доступа к информации и техническим средствам ИС.

2.1.26. Участвовать в выявлении инцидентов информационной безопасности и реагировании на них.

2.1.27. Управлять конфигурацией ИС Госкомохотнадзора РТ и их системой защиты информации.

2.1.28. В случае возникновения нештатных ситуаций и аварийных ситуаций принимать меры по реагированию в пределах функций и полномочий с целью ликвидации последствий. Оперативно докладывать вышестоящему руководству о случаях возникновения нештатных ситуаций и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС Госкомохотнадзора РТ. Предпринимаемые меры по возможности согласовывать с вышестоящим руководством.

3. Права

3.1. Администратор ИБ имеет право:

3.1.1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС Госкомохотнадзора РТ.

3.1.2. Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в ИС Госкомохотнадзора РТ при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.1.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех недостатках в работе ИС Госкомохотнадзора РТ и их системы защиты.

3.1.4. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.5. Подписывать и визировать документы в пределах своих обязанностей в соответствии с настоящей Инструкцией.

3.1.6. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей (в т.ч. вести мониторинг действий пользователей и обслуживающего персонала ИС Госкомохотнадзора РТ).

3.1.7. Вносить свои предложения по совершенствованию мер защиты информации в ИС Госкомохотнадзора РТ.

4. Ответственность

4.1. Администратор ИБ ИС Госкомохотнадзора РТ несет ответственность:

4.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.1.2. За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.1.3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Лист ознакомления
с Инструкцией администратора информационной безопасности
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.				
20.				