

**ИНСТРУКЦИЯ**  
**по порядку обращения со средствами защиты информации**  
**в информационных системах Государственного комитета по охране**  
**объектов животного мира Республики Тыва**

**1. Общие положения**

1.1. Инструкция по порядку обращения со средствами защиты информации в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва (далее – ИС Госкомохотнадзора РТ) (далее – Инструкция) регламентирует порядок обращения со средствами защиты информации в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации.

1.2. Настоящая Инструкция подготовлена в соответствии с требованиями нормативных и методических документов ФСТЭК России и ФСБ России по защите информации ограниченного доступа, не содержащую сведения, составляющие государственную тайну.

1.3. В настоящей Инструкции используются следующие понятия и определения:

1.3.1. Доступ к информации – возможность получения информации и ее использования.

1.3.2. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.3.3. Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

1.3.4. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации, не являющееся криптосредством.

1.4. Для обеспечения безопасности информации при ее обработке в ИС Госкомохотнадзора РТ должны использоваться СЗИ, прошедшие в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

## 2. Учет СЗИ

2.1. Инсталлирующие СЗИ носители и установленные СЗИ подлежат поэкземплярному учету администратором информационной безопасности (далее – ИБ).

2.2. Программные СЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СЗИ учитываются также совместно с соответствующими аппаратными средствами.

2.3. Эксплуатационная и техническая документация к СЗИ подлежит поэкземплярному учету администратором ИБ.

2.4. СЗИ, а также эксплуатационная и техническая документация к СЗИ должны быть упакованы в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия.

2.5. Полученные упаковки с СЗИ, а также с эксплуатационной и технической документацией к ним, вскрываются администратором ИБ. Администратор ИБ проверяет целостность упаковки и содержимого.

2.6. Уничтожение СЗИ:

2.6.1. СЗИ уничтожаются (утилизируются) по решению комиссии по проведению мероприятий по защите информации совместно с администратором ИБ.

2.6.2. Намеченные к уничтожению (утилизации) СЗИ изымаются из аппаратных средств, с которыми они функционировали. При этом СЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СЗИ процедура удаления программного обеспечения СЗИ, и они полностью отсоединены от аппаратных средств.

2.6.3. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения используются после уничтожения СЗИ без ограничений.

2.7. Эксплуатационная и техническая документация к СЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин.

## 3. Эксплуатация хранилищ

3.1. Инсталлирующие СЗИ носители, эксплуатационная и техническая документация к СЗИ должна храниться в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

## 4. Контроль безопасности СЗИ

4.1. Текущий контроль за организацией и обеспечением

функционирования СЗИ возлагается на ответственного за обработку и защиту информации и администратора ИБ в пределах их полномочий.

## 5. Управление конфигурацией

5.1. Все изменения конфигурации ИС Госкомохотнадзора РТ должны производиться только на основании заявок пользователей ИС Госкомохотнадзора РТ на имя администратора ИБ.

5.2. Право внесения изменений в конфигурацию ИС Госкомохотнадзора РТ предоставляется:

- в отношении системных и прикладных программных средств, а также в отношении аппаратных средств – уполномоченному администратору ИС;

- в отношении СЗИ – уполномоченному администратору ИБ.

5.3. Изменение конфигурации ИС Госкомохотнадзора РТ, кроме уполномоченных работников, запрещено.

5.4. В рамках управления конфигурацией ИС подлежат изменению:

- программно-аппаратные средства;
- программные средства, включая средства защиты информации;
- их настройки;
- программный код;
- эксплуатационная документация;
- интерфейсы;
- файлы и иные документы, подлежащие изменению и контролю.

5.5. В ходе управления конфигурацией ИС Госкомохотнадзора РТ и ее системы защиты информации осуществляются:

- поддержание конфигурации ИС Госкомохотнадзора РТ и их системы защиты информации (структуры системы защиты информации ИС Госкомохотнадзора РТ, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИС Госкомохотнадзора РТ и их системы защиты информации);

- управление изменениями базовой конфигурации ИС Госкомохотнадзора РТ и их системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИС Госкомохотнадзора РТ и их системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИС Госкомохотнадзора РТ и их системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИС Госкомохотнадзора РТ и их системы защиты информации, сохранение данных об изменениях базовой конфигурации ИС Госкомохотнадзора РТ и их системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИС Госкомохотнадзора РТ и их системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС Госкомохотнадзора РТ и их системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС Госкомохотнадзора РТ;

– определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС Госкомохотнадзора РТ и их системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации ИС Госкомохотнадзора РТ и их системы защиты информации в эксплуатационную документацию на систему защиты информации ИС Госкомохотнадзора РТ.

5.6. Установка, изменение (обновление) и удаление системных и прикладных программных средств производится администратором ИС Госкомохотнадзора РТ.

5.7. Подготовка модификаций программного обеспечения (далее – ПО) средств вычислительной техники (далее – СВТ), тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в архив эталонных дистрибутивов, и другие необходимые действия производятся администратором ИС.

5.8. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

5.9. После установки (обновления) ПО администратором ИС администратор ИБ должен проверить работоспособность ПО и правильность настройки средств управления доступом к компонентам программного средства в соответствии с установленными правилами разграничения прав доступа.

5.10. При изъятии СВТ из состава ИС Госкомохотнадзора РТ его передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как администратор ИБ снимет с данной СВТ средства защиты и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках СВТ. Факт уничтожения защищаемой информации, находившейся на диске СВТ, оформляется актом за подписью администратора ИБ.

## **6. Экстренная модификация (обстоятельства форс-мажор)**

6.1. В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на СВТ. Факт внесения изменений в ПО СВТ фиксируется актом за подписями администратора ИС, администратора ИБ и пользователя данного СВТ. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо(а),

проводившее изменения.

6.2. В течение следующего дня после составления акта администратором ИС, администратором ИБ при участии пользователей ИС Госкомохотнадзора РТ выясняются причины и состав проведенных экстренных изменений, и принимается решение о необходимости подготовки исправительной модификации ПО или восстановления ПО СВТ с эталонной копии. Необходимость участия в разбирательстве пользователя ИС Госкомохотнадзора РТ определяется руководством. Результат разбирательства оформляется в виде согласованного решения и хранится у администратора ИС, копии передаются администратору ИБ.

## **7. Ответственность**

7.1. Пользователи ИС Госкомохотнадзора РТ несут персональную ответственность за сохранность полученных СЗИ, эксплуатационной и технической документации к СЗИ, за соблюдение положений настоящей Инструкции.

7.2. Ответственный за обработку и защиту информации в ИС Госкомохотнадзора РТ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки информации с использованием СЗИ лицензионным требованиям и условиям эксплуатационной и технической документации к СЗИ, а также настоящей Инструкции.

Лист ознакомления  
с Инструкцией по порядку обращения со средствами защиты информации 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.				
20.				