УТВЕРЖДАЮ

И.о. министра

_____ /Р.М. Самбу-Хоо

«05» августа 20 21 г.

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации государственной информационной системы Министерства по внешнеэкономическим связям и туризму Республики Тыва

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации определяет действия (далее – Инструкция), связанные с функционированием государственной информационной системы Министерства по внешнеэкономическим связям и туризму Республики Тыва, меры и средства поддержания непрерывности работы и восстановления работоспособности ГИС.

Целью настоящего документа является регламентирование защиты элементов ГИС от предотвращения потери защищаемой информации.

Задачами данной Инструкции являются:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей Министерства по внешнеэкономическим связям и туризму Республики Тыва, имеющих доступ к ресурсам ГИС, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в три года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается <должность> ГИС.

2. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ГИС, предоставляемых пользователям ГИС, а также потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей.

– в результате преднамеренных действий пользователей и третьих лиц.

– в результате нарушения правил эксплуатации технических средств ГИС.

– в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале регистрации событий, связанных с отказами функционирования технических средств».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники, предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

3. МЕРЫ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ РАБОТЫ И ВОССТАНОВЛЕНИЯ РЕСУРСОВ ПРИ ВОЗНИКНОВЕНИИ ИНЦИДЕНТОВ

3.1 Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

– системы жизнеобеспечения;

– системы обеспечения отказоустойчивости;

– системы резервного копирования и хранения данных;

– системы контроля физического доступа.

Системы жизнеобеспечения ГИС включают:

– пожарные сигнализации и системы пожаротушения;

– системы вентиляции и кондиционирования;

– системы резервного питания.

Все критичные помещения Министерства по внешнеэкономическим связям и туризму Республики Тыва (помещения, в которых размещаются элементы ГИС и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ГИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ГИС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

– дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

– резервные линии электропитания в пределах комплекса зданий;
– аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

– кластеризация;
– технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ГИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ГИС должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2 Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для обрабатываемой конфиденциальной информации – не реже раза в неделю;
– для технологической информации – не реже раза в месяц;
– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ГИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

4. ОРГАНИЗАЦИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ

Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности государственной информационной системы (ГИС) в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

Резервному копированию подлежит информация следующих основных категорий:

– персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;

– информация, обрабатываемая пользователями в ГИС, а также информация, необходимая для восстановления работоспособности ГИС, в т.ч. систем управления базами данных (СУБД) общего пользования и справочно-информационные системы общего использования;

– рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ГИС, СУБД, серверов и рабочих станций;

– информация, необходимая для восстановления серверов и систем управления базами данных ГИС, локальной вычислительной сети, системы электронного документооборота;

– регистрационная информация системы информационной безопасности ГИС;

– другая информация ГИС, по мнению пользователей и администратора безопасности, являющаяся критичной для работоспособности ГИС.

Для каждого сегмента ГИС разрабатывается отдельный Регламент резервного копирования в зависимости от следующих требований:

– состав и объем копируемых данных, необходимая периодичность проведения резервного копирования;

– максимальный срок хранения резервных копий;

– требований к надежности и защищенности хранения резервных копий;

– требований к резервируемым аппаратным средствам ГИС.

Допускается составление одного Регламента для нескольких сегментов ГИС в случае идентичности требований к их резервированию.

Резервные копии хранятся вне пределов серверного помещения, доступ к резервным копиям ограничен. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только работники Министерства по внешнеэкономическим связям и туризму Республики Тыва указанные в Списке лиц, имеющих доступ к резервируемым программным и аппаратным средствам ГИС. Изменение прав доступа к резервируемым техническим средствам, массивам и носителям информации производится на основании Заявки руководителя подразделения. О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, сообщается <должность/ответственному> служебной запиской в течение рабочего дня после обнаружения указанного события.

4.1. Общие требования к резервному копированию

В Регламенте резервного копирования описываются действия при выполнении следующих мероприятий:

– резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);

– контроль резервного копирования:

– хранение резервных копий;

– полное или частичное восстановление данных.

Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к

резервному копированию. Система резервного копирования обеспечивает производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью.

Требования к техническому обеспечению систем резервного копирования:

– система представляет собой комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;

– имеется возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации:

– средства вычислительной техники отвечают действующим на момент сертификации российским и международным стандартам и рекомендациям.

Требования к программному обеспечению систем резервного копирования:

– лицензионное системное программное обеспечение и программное обеспечение резервного копирования;

– программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

Сопровождение системы резервного копирования возлагается на <должность>, которые(й) обязаны следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование, в соответствии с их инструкциями по эксплуатации.

Предварительный учет магнитных носителей архивных копий производится в отдельном журнале учета магнитных носителей для архивного копирования, который находится в <подразделении по ЗИ> (форма журнала приведена в Приложении №2). Все магнитные носители с архивными копиями маркируются, на них указывается предназначение носителя. В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

Хранение отдельных магнитных носителей архивных копий организуется в отдельном от используемых данных помещении. Физический доступ к архивным копиям строго ограничен. Контроль за физическим доступом возлагается на <администратора безопасности>.

Доступ к носителям архивных копий имеют только <уполномоченные работники подразделений…>, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

Магнитные носители для архивных копий изымаются для работы только работником, непосредственно осуществляющим резервное копирование, под роспись в журнале учета магнитных носителей архивных копий. Передача магнитных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

4.2 Периодичность резервного копирования

Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

Информация, содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:

– ежедневно проводится копирование измененной и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели;

– еженедельно проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца;

– ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

4.3 Контроль результатов резервного копирования

Контроль результатов всех процедур резервного копирования осуществляется <ответственными должностными лицами>, в срок до __ часов рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает руководителю подразделения по ЗИ до __ часов текущего рабочего дня.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

4.4 Замена носителей резервных копий

Система резервного копирования обеспечивает возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивает восстановление текущей информации ГИС в случае отказа любого из устройств резервного копирования.

Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются ответственным работником подразделения по ЗИ. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

4.5 Восстановление информации из резервных копий

В случае необходимости восстановление данных из резервных копий производится ответственным работником по ЗИ.

Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

5. ОТВЕТСТВЕННОСТЬ

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в государственных информационных системах возлагается <должность>.

Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на уполномоченных работников подразделения по ЗИ, осуществляющих резервное копирование.

Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующего Регламента, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности.

В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, сообщается в подразделение по ЗИ служебной запиской в течение рабочего дня после обнаружения указанного события.

Консультант _____

Приложение № 1 к Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации государственной информационной системы от «___» _____ 20__ г.

Список лиц, имеющих доступ к резервируемым программным и аппаратным средствам ГИС

№ п/п	Должность	Фамилия, имя, отчество работника
1		
2		
3		
…		
№		

Приложение № 2 к Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации государственной информационной системы от «___» _____ 20__ г.

Типовая форма журнала учета магнитных носителей для архивного копирования информации

УТВЕРЖДАЮ
И.о. Министра
_____/Р.М. Самбу-Хоо
«____» _____ 20__ г.

Журнала учета магнитных носителей для архивного копирования информации Министерства по внешнеэкономическим связям и туризму Республики Тыва

Журнал начат «___» _____ 20__ г.
Ответственный за ведение журнала (должность)
/_____/_____
Журнал завершен «___» _____ 20__ г.
Должность и Ф.И.О.
/_____/_____
Журнал составлен на _____ листах
Место хранения в процессе работы
_____

№ п/п	Носитель (маркировка)	Кому выдан (ФИО, должность, подразделение)	Получен (дата, подпись)	Возвращен (дата, подпись)	Уничтожен (№ акта, ФИО работника, должность, подразделение, дата, подпись)	Примечание
1						
2						
…						
№						

Приложение № 3 к Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации государственной информационной от «___» _____ 20__ г.

Реестр резервных копий

№ п/п	Дата записи резервной копии	Вид и номер (серийный/ инвентарный) носителя информации	Место хранения резервной копии	Содержание резервной копии	Срок хранения резервной копии	Сведения о лице, создавшем резервную копию	Примечание
1							
2							
3							
...							
№							