УТВЕРЖДАЮ
И.о. министра
_____/Р.М. Самбу-Хоо
«05» августа 2021 г.

ИНСТРУКЦИЯ
пользователя государственной информационной системы
Министерства по внешнеэкономическим связям и туризму Республики Тыва

1. Общие положения

1.1 Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами:

– Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Методический документ ФСТЭК России от 11.02.2014 г. «Меры защиты информации в государственных информационных системах»;

– ....

1.2 Пользователями государственной информационной системы Министерства по внешнеэкономическим связям и туризму Республики Тыва, являются должностные лица, выполняющие свои должностные обязанности с использованием информации, информационных технологий и технических средств ИС и которым в ИС присвоены учетные записи.

1.3 Настоящая Инструкция определяет права, обязанности, задачи и ответственность пользователей ГИС Министерства по внешнеэкономическим связям и туризму Республики Тыва.

2. Обязанности пользователя

2.1 Пользователь обязан знать и выполнять требования действующих нормативных правовых актов Российской Федерации, а также локальных актов Министерства по внешнеэкономическим связям и туризму Республики Тыва, регламентирующих деятельность по обработке и защите информации, содержащейся в ГИС, обеспечивать конфиденциальность информации ограниченного доступа, ставшей известной пользователю в результате выполнения им служебных (должностных) обязанностей.

2.2 При эксплуатации ГИС пользователь обязан:

2.2.1 Руководствоваться положениями настоящей инструкции.

2.2.2 Помнить личные пароли и идентификаторы и обеспечивать их конфиденциальность.

2.2.3 Соблюдать установленную технологию обработки информации в ГИС.

2.2.4 Использовать для вывода на печать документов, содержащих информацию ограниченного доступа, только устройства печати, разрешенные к использованию, сводя к минимуму возможность доступа к ним посторонних лиц. Пользователь обязан незамедлительно изымать распечатанные документы, содержащие информацию ограниченного доступа, из лотка принтера.

2.2.5 Исключить возможность неконтролируемого доступа к техническим средствам ГИС посторонних лиц, а также возможность просмотра посторонними лицами ведущихся на технических средствах работ. В случаях кратковременного отсутствия (перерыв, обед) при выходе в течение рабочего дня из помещения, в котором размещаются технические средства ГИС, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте или выключить техническое средство.

2.2.6 Соблюдать требования парольной политики.

2.2.7 Соблюдать требования антивирусной защиты.

2.2.8 Докладывать своему непосредственному руководителю и администратору системы ГИС:

– о фактах имевшегося или предполагаемого несанкционированного доступа к информации, содержащейся в ГИС, носителям информации, техническим средствам ГИС, помещениям, в которых располагаются технические средства ГИС;

– об утрате носителей информации, паролей и идентификаторов, ключей от помещений, где ведется обработка защищаемой информации;

– о попытках получения информации лицами, не имеющими к ним допуска;

– об иных нештатных ситуациях, связанных с угрозой конфиденциальности информации или безопасности ГИС.

2.2.9 При прекращении работ (трудовых отношений) все материальные носители, содержащие конфиденциальную информацию (флеш-накопители, компакт-диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные образцы и пр.), передать непосредственному руководителю.

2.2.10 Пользователи, имеющие выход в интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена – интернет.

2.3 Пользователю ЗАПРЕЩАЕТСЯ:

– нарушать установленные в Министерстве по внешнеэкономическим связям и туризму Республики Тыва правила обработки конфиденциальной информации;

– входить в систему или работать в ней под чужой учетной записью;

– подключать к техническим средствам ГИС нештатные устройства;

– сообщать устно, письменно или иным способом (показ и т.п.) другим лицам идентификаторы и пароли, передавать ключи от помещений и другие реквизиты доступа к ГИС;

– оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии);

– оставлять без присмотра или неубранными в специальные хранилища (шкаф, сейф) носители или документы, содержащие конфиденциальную информацию;

– самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы;

– самовольно подключать компьютер к ЛВС Организации, изменять IP-адрес, MAC-адрес и иные настройки сети компьютера;

– самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать;

– пересылать сведения конфиденциального характера по каналам связи в открытом виде, в том числе интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования или шифрования и электронной подписи).

– осуществлять действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей;

– в случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения;

– удалять или искажать программы и файлы с конфиденциальной информацией и иной важной информацией (например, системной, необходимой для функционирования информационных систем);

– препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации;

– использовать для записи информации ограниченного доступа неучтенные машинные носители информации;

– производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, узлам сети интернет, в том числе:

– действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);

– установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;

– действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;

– уничтожение, модификация программного обеспечения или данных без согласования с непосредственным руководителем или владельцами этого ресурса;

– попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;

– умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам, либо на нарушение целостности и работоспособности этих систем.

3. Порядок работы с носителями информации

3.1 Допускается использование только учтенных носителей информации, которые являются собственностью Министерства по внешнеэкономическим связям и туризму Республики Тыва и подвергаются регулярной ревизии и контролю.

3.2 Учет и выдачу съемных носителей информации осуществляет администратор ИС. Факт выдачи носителя фиксируется в журнале учета съемных носителей информации.

3.3 Возможность подключения носителей информации, а также получение учтенных носителей информации предоставляются Пользователям по инициативе руководителей структурных подразделений в случаях:

– необходимости выполнения вновь принятым работником своих должностных обязанностей;

– возникновения у Пользователя производственной необходимости.

3.4 При использовании носителей информации необходимо:

– использовать носители информации исключительно для выполнения своих служебных обязанностей;

– бережно относиться к носителям конфиденциальной информации;

– обеспечивать физическую безопасность носителей информации;

– извещать администраторов о фактах утраты (кражи) носителей информации.

3.5 При использовании носителей конфиденциальной информации запрещено:

– использовать носители конфиденциальной информации в личных целях;

– передавать носители конфиденциальной информации другим лицам (за исключением администраторов);

– хранить съемные носители с конфиденциальной информацией на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– выносить съемные носители с конфиденциальной информацией из служебных помещений для работы с ними на дому и т. д.

3.6 В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициируется служебная проверка, проводимая комиссией, состав которой определяется подразделением по защите информации. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Министерства по внешнеэкономическим связям и туризму Республики Тыва и действующему законодательству РФ.

3.7 При отправке или передаче конфиденциальной информации адресатам на съемные носители записываются только предназначенные адресатам данные.

3.8 Вынос съемных носителей конфиденциальной информации для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

3.9 Съемные носители конфиденциальной информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссией, состав которой определяется руководителем подразделения по защите информации. По результатам уничтожения носителей составляется акт.

3.12 В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются и делаются соответствующие пометки в журнале учета носителей.

4. Права

4.1 Пользователь ГИС имеет право:

4.1.1 Использовать ГИС для выполнения служебных обязанностей.

4.1.2 Обращаться к администратору безопасности ГИС по любым организационным и техническим вопросам, касающимся обработки и защиты информации в ГИС (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению безопасности информации).

4.1.3 Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости замены старых версий на новые).

4.1.4 Направлять предложения по установке нового (а также дополнительного) программного обеспечения (с указанием цели использования, преимуществ перед существующими аналогами).

4.1.5 Получать консультации и разъяснения по нормативным документам, регламентирующим работу с конфиденциальной информацией в ГИС.

5. Ответственность

5.1. На пользователя возлагается персональная ответственность:

– за соблюдение установленной технологии обработки информации;

– за соблюдение режима конфиденциальности информации;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ГИС;

– за соблюдение требований локальных актов оператора по вопросам обработки и защиты информации в ГИС.

5.2 Пользователь несет ответственность за свои действия или бездействие, которые повлекут за собой разглашение конфиденциальной информации, а также за нарушение нормального функционирования ИС или ее отдельных компонентов, несанкционированный доступ к информации в соответствие с законодательством Российской Федерации и локальными нормативными актами Министерства по внешнеэкономическим связям и туризму Республики Тыва.

УТВЕРЖДАЮ
И.о. министра
_____/Р.М. Самбу-Хоо
«_05_» августа 2021 г.

АКТ
классификации государственной информационной системы Министерства по внешнеэкономическим связям и туризма Республики Тыва с учётом требуемого уровня защищенности персональных данных

Комиссия в составе:
Председателя:
_____

Члены комиссии:
_____
_____

1. Рассмотрев исходные данные (Таблица 1) на государственную информационную систему в соответствии с требованиями приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственный информационных системах», «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 и моделью угроз безопасности информации, обрабатываемой в государственной информационной системе,

Таблица 1. – Исходные данные для определения уровня защищенности

Наименование ИС	**Категория обрабатываемых данных**	**Кол-во субъектов ПДн**	**Тип актуальных угроз безопасности информации**
			Третий

Р Е Ш И Л А:

Установить для ГИС уровень защищенности ПДн - **третий (У3З)**.

Председатель комиссии: <ФИО> _____

Члены комиссии: <ФИО> _____
<ФИО> _____

2. Рассмотрев исходные данные (Таблица 2) на государственную информационную систему <Наименование ИС> в соответствии с порядком определения класса защищенности, утвержденным Приказом ФСТЭК России от 11.02.2013 г. № 17 «Об

утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

Таблица 2. – Исходные данные для определения класса защищенности

Наименование ИС	**Уровень защищенности ПДн**	**Уровень значимости информации**	**Масштаб ИС**
	3	2	Региональный

Р Е Ш И Л А :

Установить для ГИС класс защищенности – **второй (К2)**;

Председатель комиссии: _____

Члены комиссии: _____

_____