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

ИНСТРУКЦИЯ
администратора безопасности информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет обязанности администратора безопасности информации, обрабатываемой в государственной информационной системе (далее - администратора безопасности).

1.2. Администратор безопасности назначается приказом руководителя Министерства по внешнеэкономическим связям и туризму Республики Тыва из числа подготовленных работников подразделения по защите информации (ЗИ).

1.3. Администратор безопасности по вопросам обеспечения безопасности информации подчиняется руководителю подразделения по ЗИ, являющемуся структурным подразделением, назначаемым ответственным за обеспечение безопасности информации в Министерства по внешнеэкономическим связям и туризму Республики Тыва.

1.4. Администратор безопасности отвечает за поддержание установленного уровня защищенности обрабатываемой в информационной системе информации, в том числе персональных данных.

1.5. Администратор безопасности осуществляет методическое руководство деятельностью пользователей ГИС в вопросах обеспечения безопасности информации.

1.6. Требования администратора безопасности, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ГИС.

1.7. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ГИС, состояние и поддержание установленного уровня защиты информации, обрабатываемой в ГИС.

2. ЗАДАЧИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

2.1. Основными задачами администратора безопасности являются:

– поддержание необходимого уровня защищенности обрабатываемых в сегментах ГИС персональных данных от несанкционированного доступа (НСД) к информации;

– обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации;

– установка средств защиты информации и контроль выполнения правил их эксплуатации;

– сопровождение средств защиты информации (СЗИ) от НСД и основных технических средств и систем (ОТСС) ГИС;

– периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов ИБ;

– оперативное реагирование на нарушения требований по ИБ в ГИС и участие в их прекращении.

2.2. В рамках выполнения основных задач администратор безопасности осуществляет:

– текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;

– текущий контроль технологического процесса автоматизированной обработки конфиденциальной информации, в том числе персональных данных;

– участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности защищаемой информации;

– контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации в структурных подразделениях Министерства по внешнеэкономическим связям и туризму Республики Тыва и территориальных органах Министерства по внешнеэкономическим связям и туризму Республики Тыва;

– методическую помощь всем работникам Министерства по внешнеэкономическим связям и туризму Республики Тыва и территориальных органов Министерства по внешнеэкономическим связям и туризму Республики Тыва по вопросам обеспечения безопасности защищаемой информации.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Администратор безопасности обязан:

3.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ГИС.

3.2. Участвовать в установке, настройке и сопровождении программных средств защиты информации.

3.3. Участвовать в приемке новых программных средств обработки информации.

3.4. Обеспечить доступ к защищаемой информации пользователям ГИС согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

3.5. Вести контроль осуществления резервного копирования информации.

3.6. Анализировать состояние защиты ГИС.

3.7. Контролировать правильность функционирования средств защиты информации и неизменность их настроек.

3.8. Контролировать физическую сохранность технических средств обработки информации.

3.9. Контролировать исполнение пользователями ГИС введенного режима безопасности, а также правильность работы с элементами ГИС и средствами защиты информации.

3.10. Контролировать исполнение пользователями правил парольной политики.

3.11. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

3.12. Не допускать установку, использование, хранение и размножение в ГИС программных средств, не связанных с выполнением функциональных задач.

3.13. Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) ГИС.

3.14. Оказывать помощь пользователям ГИС в части применения средств защиты и консультировать по вопросам введенного режима защиты.

3.15. Периодически представлять руководству отчет о состоянии защиты ГИС и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.16. В случае отказа работоспособности технических средств и программного обеспечения ГИС, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.17. В случае выявления нарушений режима безопасности информации (ПДн), а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

3.18. Принимать участие в проведении работ по оценке соответствия ГИС требованиям безопасности информации.

4. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности имеет право:

4.1. Отключать от ресурсов ГИС работников, осуществивших НСД к защищаемым ресурсам ГИС или нарушивших другие требования по ИБ.

4.2. Давать работникам обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ГИС.

4.4. Организовывать и участвовать в любых проверках по использованию пользователями Министерства по внешнеэкономическим связям и туризму Республики Тыва и территориальных органов Министерства по внешнеэкономическим связям и туризму Республики Тыва телекоммуникационных ресурсов.

4.5. Осуществлять контроль информационных потоков, генерируемых пользователями ГИС при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.6. Осуществлять взаимодействие с руководством и персоналом Министерства по внешнеэкономическим связям и туризму Республики Тыва и территориальных органов Министерства по внешнеэкономическим связям и туризму Республики Тыва по вопросам обеспечения ИБ.

4.7. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

4.8. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ защищаемой информации, обрабатываемой в ГИС.

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности несет ответственность (дисциплинарную, гражданскую, административную, уголовную и иную, предусмотренную законодательством Российской Федерации ответственность):

5.1. За организацию защиты информационных ресурсов и технических средств ГИС.

5.2. За качество проводимых работ по контролю действий пользователей и администраторов ГИС, состояние и поддержание необходимого уровня защиты информационных и технических ресурсов ГИС.

5.3. За разглашение сведений ограниченного доступа (коммерческая тайна, персональные данные и иная защищаемая информация), ставших известными ему по роду работы.

6. ДЕЙСТВИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НСД

6.1. К попыткам НСД относятся:

– сеансы работы с телекоммуникационными ресурсами Министерства по внешнеэкономическим связям и туризму Республики Тыва и территориальных органов Министерства по внешнеэкономическим связям и туризму Республики Тыва незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;

– действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ГИС с использованием учетной записи администратора или другого пользователя ГИС, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

6.2. При выявлении факта/попытки НСД администратор безопасности обязан:

– прекратить доступ к информационным ресурсам со стороны выявленного участка НСД:

– доложить руководству подразделения по ЗИ о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

– известить Руководителя структурного подразделения Министерства по внешнеэкономическим связям и туризму Республики Тыва и/или территориальных органов Министерства по внешнеэкономическим связям и туризму Республики Тыва ,в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

– проанализировать характер НСД;

– по решению руководства подразделения по ЗИ осуществить действия по выяснению причин, приведших к НСД;

– предпринять меры по предотвращению подобных инцидентов в дальнейшем.