СЛУЖБА ПО ФИНАНСОВО-БЮДЖЕТНОМУ НАДЗОРУ РЕСПУБЛИКИ ТЫВА

ПРИКАЗ

№ 13/од

г. Кызыл «30» января 2026 г.

Об обеспечении информационной безопасности

Для обеспечения информационной безопасности в Службе по финансово-бюджетному надзору Республики Тыва (далее – Служба) и с целью выполнения требований:

• Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

• Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну содержащихся в государственных информационных системах»;

• Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

• Руководящего документа (Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации), утвержденного решением председателя Гостехкомиссии России от 30.03.1992,

ПРИКАЗЫВАЮ:

1. Утвердить следующие документы:

• Политика защиты информации в Службе (Приложение № 1);

• Журнал ознакомления сотрудников с документами в области обеспечения информационной безопасности в Службе (Приложение № 2);

• Журнал поэкземплярного учета средств защиты информации (СЗИ), эксплуатационной и технической документации к ним, ключевых документов в Службе (Приложение № 3);

• Перечень информационных систем в Службе (Приложение № 4);

• Инструкция пользователя информационных систем Службы (Приложение №5);

• Инструкция по организации парольной защиты в информационных системах Службы (Приложение № 6);

• Инструкция по организации антивирусной защиты в информационных системах Службы (Приложение № 7);

• Инструкция по выявлению инцидентов и реагированию на них в информационных системах Службы (Приложение № 8);

• Карточка данных об инциденте безопасности обработки персональных данных в информационных системах Службы (Приложение № 1 к Инструкции по выявлению инцидентов и реагированию на них в информационных системах Службы);

• Журнал реагирования на инциденты информационной безопасности в Службе (Приложение № 2 к Инструкции по выявлению инцидентов и реагированию на них в информационных системах Службы);

• План практических занятий и тренировок с персоналом информационной системы по блокированию угроз безопасности информации и реагированию на инциденты (Приложение № 3 к Инструкции по выявлению инцидентов и реагированию на них в информационных системах Службы);

• Перечень лиц, ответственных за выявление инцидентов и реагирование на них (Приложение № 4 к Инструкции по выявлению инцидентов и реагированию на них в информационных системах Службы);

• Правила управления конфигурацией информационной системы и системы защиты информации информационной системы (Приложение № 9);

• Правила контроля и мониторинга за обеспечением уровня защищенности информации, содержащейся в информационной системе (Приложение № 10);

• Инструкция по защите информации при выводе из эксплуатации информационной системы или об окончании обработки информации (Приложение № 11);

• Инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах Службы (Приложение № 12):

◦ Журнал резервирования информационных ресурсов Службы (Приложение № 1 Инструкции по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах Службы);

• Порядок контроля выполнения мероприятий по обеспечению защиты информации в информационных системах Службы (Приложение № 13):

◦ План мероприятий по защите информации (Приложение № 1 к Порядку контроля выполнения мероприятий по обеспечению защиты информации в информационных системах Службы);

◦ Журнал проведения мероприятий по защите информации в Службе (Приложение № 2 к Порядку контроля выполнения мероприятий по обеспечению защиты информации в информационных системах Службы);

• Регламент по использованию в Службе технологий беспроводного доступа (Приложение № 14);

• Регламент по использованию мобильных технических средств (Приложение № 15);

• Регламент взаимодействия с иной информационной системой (Приложение № 16);

• Инструкция о порядке работы при подключении к сетям общего пользования и (или) международного обмена в Службе (Приложение № 17):

• Правила по работе в локальной сети (Приложение № 1 к Инструкции о порядке работы при подключении к сетям общего пользования и (или) международного обмена в Службе);

• Правила работы с электронной почтой (Приложение № 2 к Инструкции о порядке работы при подключении к сетям общего пользования и (или) международного обмена в Службе);

• Правила по работе в сети Интернет (Приложение № 3 к Инструкции о порядке работы при подключении к сетям общего пользования и (или) международного обмена в Службе);

• Журнал ознакомления сотрудников с документами в области обеспечения информационной безопасности с использованием средств защиты информации (СЗИ) в информационных системах Службы (Приложение № 18);

• Инструкция по действиям персонала во внештатных ситуациях при обработке защищаемой информации в информационных системах Службы (Приложение № 19);

• Источник угроз (Приложение № 1 к Инструкция по действиям персонала во внештатных ситуациях при обработке защищаемой информации в информационных системах Службы);

• Правила ведения журналов в части защиты информации в Службе (Приложение № 20).

2. Контроль за своевременным ведением и актуализацией организационно-распорядительной документации по обеспечению информационной безопасности возлагается на администратора информационной безопасности.

3. Контроль исполнения настоящего приказа оставляю за собой.

Руководитель Службы Т.Х. Монгуш

С приказом ознакомлен (ы): Монгуш Т.Х.