РОССТАТ

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ГОСУДАРСТВЕННОЙ СТАТИСТИКИ ПО АСТРАХАНСКОЙ ОБЛАСТИ И РЕСПУБЛИКЕ КАЛМЫКИЯ (АСТРАХАНЬСТАТ)

П Р И К А З

9 октября 2020г. № 254

Астрахань

Об утверждении правил внутреннего контроля соответствия обработки защищаемой информации, в том числе персональных данных, требованиям безопасности информации и перечня мероприятий по контролю за обеспечением безопасности информации, в том числе персональных данных, в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня

Во исполнение Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и в целях обеспечения защиты информации, содержащейся в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня (далее – ИСПДн Росстата РУ) в Управлении Федеральной службы государственной статистики по Астраханской области и Республике Калмыкия (далее - Астраханьстат) п р и к а з ы в а ю :

1. Утвердить прилагаемые:

— Правила внутреннего контроля соответствия обработки защищаемой информации, в том числе персональных данных, требованиям безопасности информации в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня (далее - Правила) (Приложение № 1);

— Перечень мероприятий по контролю за обеспечением безопасности информации, в том числе персональных данных, в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня (далее - Перечень) (Приложение № 2).

2. Ответственному за организацию защиты персональных данных в ИСПДн Росстата РУ, Администраторам безопасности ИСПДн Росстата РУ и Администраторам ИСПДн Росстата РУ ознакомиться с Правилами и Перечнем под роспись в листе ознакомления.

3. Контроль за исполнением настоящего приказа возложить на заместителя руководителя С.Н. Цапко.

Руководитель Л.Я. Окунь

Приложение № 1

УТВЕРЖДЕНЫ
приказом Астраханьстата
от 9 октября 2026 г. № 254

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки защищаемой информации, в том числе персональных данных, требованиям безопасности информации в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня

1. Общие положения

1.1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки защищаемой информации, в том числе персональных данных, требованиям безопасности информации в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня (далее – Правила) в Управлении Федеральной службы государственной статистики по Астраханской области и Республике Калмыкия (далее - Астраханьстат) определяются процедуры, направленные на выявление и предотвращение нарушений установленных требований по защите информации в ИСПДн Росстата РУ.

1.2. Настоящие Правила определяют порядок внутреннего контроля соответствия обработки защищаемой информации, в том числе персональных данных, требованиям безопасности информации в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня (далее - ИСПДн Росстата РУ) и действуют постоянно.

2. Требования к организации внутреннего контроля

2.1. В целях осуществления внутреннего контроля обеспечения безопасности информации в ИСПДн Росстата РУ организуется проведение периодических проверок условий обработки защищаемой информации.

Проверка включает в себя:

— контроль реализации правил разграничения доступа, полномочий пользователей в ИСПДн Росстата РУ;

— контроль соблюдения пользователями ИСПДн Росстата РУ правил организации парольной защиты;

— контроль соблюдения пользователями ИСПДн Росстата РУ установленных правил антивирусной защиты;

— контроль соблюдения установленных в ИСПДн Росстата РУ правил работы с машинными носителями информации;

— контроль соблюдения порядка доступа в помещения, где расположены элементы ИСПДн Росстата РУ и ведется обработка защищаемой информации;

— контроль соблюдения порядка резервирования информации и хранения резервных копий;

— контроль соблюдения порядка работы со средствами защиты информации;

— контроль знания и соблюдения пользователями ИСПДн Росстата РУ внутренних документов по защите информации.

2.2. Проверки осуществляются Ответственным за организацию защиты персональных данных совместно с Администраторами ИСПДн Росстата РУ и Администратором безопасности ИСПДн Росстата РУ (далее - Комиссия).

2.3. Проверки проводятся на основании утвержденного приказом руководителя Астраханьстата «Перечня мероприятий по контролю за обеспечением безопасности информации, в том числе персональных

данных, в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня».

2.4. При проведении проверки обеспечения безопасности информации в ИСПДн Росстата РУ установленным требованиям должны быть полностью объективно и всесторонне установлены:

— порядок и условия применения организационных и технических мер по защите информации, исполнение которых обеспечивает установленный уровень защищенности информации в ИСПДн Росстата РУ;

— соответствие состава и структуры программно-технических средств ИСПДн Росстата РУ документированному составу и структуре средств, представленному в техническом паспорте ИСПДн Росстата РУ;

— порядок и условия применения средств защиты информации;

— порядок и условия допуска лиц в помещения, где размещены средства ИСПДн Росстата РУ;

— порядок организации и правильности учета машинных носителей информации;

— соблюдение установленных правил доступа субъектов доступа к объектам доступа;

— соблюдение установленного порядка использования мобильных технических средств;

— наличие (отсутствие) фактов несанкционированного доступа к информации и принятие необходимых мер;

— соблюдение установленных правил организации парольной и антивирусной защиты;

— знание персоналом базы нормативно-методических документов по защите информации.

2.5. При проведении внутренней проверки комиссия имеет право:

— запрашивать у сотрудников Астраханьстата, допущенных к работе в ИСПДн Росстата РУ, информацию, необходимую для реализации полномочий;

— принимать меры по приостановлению или прекращению обработки защищаемой информации, осуществляемой с нарушением требований законодательства Российской Федерации;

— вносить руководителю Астраханьстата предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности информации;

— вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в области защиты информации.

2.6. Мероприятия, проведенные в ходе внутреннего контроля, должны быть занесены в Журнал учета мероприятий по контролю за обеспечением защиты информации в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня (Приложение № 1).

2.7. В отношении информации, ставшей известной комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

2.8. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений составляется Протокол результатов проведения внутренней проверки обеспечения безопасности информации в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня (Приложение № 2).

Приложение № 1
к Правилам осуществления внутреннего контроля
соответствия обработки защищаемой информации,
в том числе персональных данных, требованиям
безопасности информации в сегменте
ИСПДн Федеральной службы государственной
статистики регионального уровня
«__»_____20__ года № _____

Журнал

учета мероприятий по контролю за обеспечением защиты информации в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня

(форма)

Журнал начат «____» _____ 20__ г.

_____ /Должность/
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20__г.

_____ /Должность/
_____ / ФИО должностного лица /

На _____ листах

20__ г

№ п/п	Мероприятие	Дата	Исполнитель	Результат

В настоящем журнале прошнуровано,

пронумеровано и скреплено

___ листов

Ответственный за ведение журнала

_____

_____

Приложение № 2
к Правилам осуществления внутреннего контроля
соответствия обработки защищаемой информации,
в том числе персональных данных, требованиям
безопасности информации в сегменте
ИСПДн Федеральной службы государственной
статистики регионального уровня
«__»_____20__ года № _____

П Р О Т О К О Л
результатов проведения внутренней проверки
обеспечения безопасности информации в ИСПДн Росстата РУ
(форма)

Настоящий Протокол составлен в том, что «___» _____ 20__ года комиссией в составе: Ответственного за организацию защиты персональных данных/Администратора ИСПДн Росстата РУ/Администратора безопасности ИСПДн Росстата РУ была проведена плановая внутренняя проверка обеспечения безопасности информации в сегменте ИСПДн Росстата РУ.

Проверка осуществлялась в соответствии с требованиями Правил осуществления внутреннего контроля соответствия обработки защищаемой информации, в том числе персональных данных, требованиям безопасности информации и Перечня мероприятий по контролю за обеспечением безопасности информации, в т.ч. персональных данных, в сегменте ИСПДн Росстата РУ

В ходе проверки проверено:

_____
_____
_____

Выявленные нарушения:

_____
_____
_____

Меры по устранению нарушений:

_____
_____
_____

Срок устранения нарушений: _____.

Проверку провели:

Ответственный за организацию обработки и
обеспечение защиты информации ИСПДн Росстата РУ подпись, ФИО

Администратор ИСПДн Росстата РУ подпись, ФИО

Администратор безопасности ИСПДн Росстата РУ подпись, ФИО

Приложение № 2

УТВЕРЖДЕН
приказом Астраханьстата
от 9 октября 2020 г. № 254

ПЕРЕЧЕНЬ
мероприятий по контролю за обеспечением безопасности информации, в том числе персональных данных, в сегменте информационной системы персональных данных Федеральной службы государственной статистики регионального уровня

Мероприятие	Периодичность	Исполнитель
Выявление (поиск), анализ и устранение уязвимостей в ИСПДн Росстата РУ	1 раз в месяц	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ, Администратор безопасности ИСПДн Росстата РУ
Проверка соответствия состава и структуры программно-технических средств ИСПДн Росстата РУ документированному составу и структуре средств, представленному в техническом паспорте ИСПДн Росстата РУ	1 раз в 6 месяцев	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ, Администратор ИСПДн Росстата РУ, Администратор безопасности ИСПДн Росстата РУ
Проверка выполнения требований по условиям расположения СВТ в помещениях, в которых размещены элементы ИСПДн Росстата РУ	1 раз в 6 месяцев	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ, Администратор ИСПДн Росстата РУ
Проверка целостности опечатывания системных блоков и других ТС, участвующих в обработке информации	1 раз в 6 месяцев	Администратор безопасности ИСПДн Росстата РУ
Проверка организации допуска лиц в помещения, где размещены средства ИСПДн Росстата РУ, в т. ч. перечня лиц, имеющих право доступа в помещения ИСПДн Росстата РУ	1 раз в 3 месяца	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ, Администратор безопасности ИСПДн Росстата РУ

Мероприятие	Периодичность	Исполнитель
Проверка актуальности перечня лиц, допущенных к работе в ИСПДн Росстата РУ	1 раз в 3 месяца	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ, Администратор безопасности ИСПДн Росстата РУ
Проверка соответствия реального уровня полномочий по доступу к информации различных пользователей, установленному в матрице доступа в соответствии с разрешительной системой доступа	1 раз в 3 месяца	Администратор безопасности ИСПДн Росстата РУ
Проверка организации учета средств защиты информации, используемых в ИСПДн Росстата РУ	1 раз в 6 месяцев	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ
Проверка наличия документов, подтверждающих возможность применения технических и программных средств защиты информации (сертификатов соответствия и других документов)	1 раз в 6 месяцев	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ, Администратор безопасности ИСПДн Росстата РУ
Проверка неизменности настроенных параметров средств защиты информации ИСПДн Росстата РУ	1 раз в месяц	Администратор безопасности ИСПДн Росстата РУ
Контроль состава программного обеспечения ИСПДн Росстата РУ	1 раз в 3 месяца	Администратор ИСПДн Росстата РУ
Контроль правил заведения и удаления учетных записей пользователей	1 раз в 6 месяцев	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ, Администратор безопасности ИСПДн Росстата РУ
Проверка соблюдения установленных правил организации парольной защиты	1 раз в 6 месяца	Администратор безопасности ИСПДн Росстата РУ
Контроль соблюдения установленных правил организации антивирусной защиты	1 раз в 3 месяца	Администратор безопасности ИСПДн Росстата РУ
Проверка работоспособности системы резервного копирования	1 раз в 6 месяцев	Администратор ИСПДн Росстата РУ
Проверка организации учета и условий хранения машинных носителей информации	1 раз в 6 месяцев	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ, Администратор безопасности ИСПДн Росстата РУ

Мероприятие	Периодичность	Исполнитель
Проверка работоспособности и контроль соблюдения правил эксплуатации СКЗИ, в соответствии с эксплуатационной документацией на СКЗИ, проведение контрольных проверок ViPNet Client	1 раз в месяц	Ответственный за обеспечение функционирования и безопасность СКЗИ
Проверка знаний персоналом базы нормативно-методических документов по защите информации	1 раз в 6 месяцев	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ
Организация анализа и пересмотра имеющихся угроз безопасности информации ИСПДн Росстата РУ, а также предсказание появления новых, еще неизвестных, угроз	Не реже 1 раз в год	Ответственный за организацию защиты персональных данных в ИСПДн Росстата РУ, Администратор безопасности ИСПДн Росстата РУ