

ПРАВИЛА
осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите
персональных данных, политике оператора в отношении
обработки персональных данных

1. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее – контроль, внутренний контроль) проводится на основании приказа учреждения.

2. При проведении контроля учреждение руководствуется нормативными правовыми актами Российской Федерации, регламентирующими работу с персональными данными, а также Положением об организации работы с персональными данными в учреждении.

3. Предметом контроля являются:
проверка соответствия информационных систем персональных данных параметрам, указанным в актах классификации информационных систем персональных данных;

соблюдение работниками учреждения мер по защите персональных данных;
соблюдение организационных мер и средств защиты информации, обеспечивающих безопасную обработку персональных данных;

проверка соответствия сведений о лицах, допущенных к обработке персональных данных, и уровне их доступа;

проверка соответствия сведений о составе и структуре обрабатываемых персональных данных.

4. Плановый контроль осуществляется не реже одного раза в три года по графику, утвержденному заведующим учреждением.

5. Внеплановый контроль осуществляется при наличии существенного нарушения функционирования работы в сфере персональных данных.

6. На время проведения контроля создается комиссия из числа работников учреждения.

7. Проверка информационной системы персональных данных включает:
наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;

наличие резервных копий общесистемного программного обеспечения;
наличие резервных копий носителей персональных данных;

наличие информационных ресурсов (баз данных, файлов и других), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

проверку системы контроля физического доступа к информационной системе;
проверку существующих технологических мер защиты персональных данных;
проверку разграниченных прав доступа лиц к обрабатываемым персональным данным;

проверку состава и структуру объектов защиты;
проверку конфигурации и структуры информационной системы;
проверку режима обработки персональных данных;
проверку перечня лиц, участвующих в обработке персональных данных;
моделирование угроз безопасности персональных данных, оценку вероятность их реализации, реализуемость, опасность и актуальность.

8. По итогам проверки:
вносятся изменения в План мероприятий по обеспечению защиты персональных данных;
уточняется перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним;
формируются новые модели угроз безопасности персональных данных;
составляется список необходимых мер защиты персональных данных;
вносятся изменения в локальные нормативные акты учреждения по вопросам обработки персональных данных.

ПРАВИЛА
осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите
персональных данных, политике оператора в отношении
обработки персональных данных

1. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее – контроль, внутренний контроль) проводится на основании приказа учреждения.

2. При проведении контроля учреждение руководствуется нормативными правовыми актами Российской Федерации, регламентирующими работу с персональными данными, а также Положением об организации работы с персональными данными в учреждении.

3. Предметом контроля являются:

 проверка соответствия информационных систем персональных данных параметрам, указанным в актах классификации информационных систем персональных данных;

 соблюдение работниками учреждения мер по защите персональных данных;

 соблюдение организационных мер и средств защиты информации, обеспечивающих безопасную обработку персональных данных;

 проверка соответствия сведений о лицах, допущенных к обработке персональных данных, и уровне их доступа;

 проверка соответствия сведений о составе и структуре обрабатываемых персональных данных.

4. Плановый контроль осуществляется не реже одного раза в три года по графику, утвержденному заведующим учреждением.

5. Внеплановый контроль осуществляется при наличии существенного нарушения функционирования работы в сфере персональных данных.

6. На время проведения контроля создается комиссия из числа работников учреждения.

7. Проверка информационной системы персональных данных включает:

 наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;

 наличие резервных копий общесистемного программного обеспечения;

 наличие резервных копий носителей персональных данных;

 наличие информационных ресурсов (баз данных, файлов и других), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

 проверку системы контроля физического доступа к информационной системе;

 проверку существующих технологических мер защиты персональных данных;

 проверку разграниченных прав доступа лиц к обрабатываемым персональным данным;

 проверку состава и структуру объектов защиты;

 проверку конфигурации и структуры информационной системы;

 проверку режима обработки персональных данных;

 проверку перечня лиц, участвующих в обработке персональных данных;

 моделирование угроз безопасности персональных данных, оценку вероятность их реализации, реализуемость, опасность и актуальность.

8. По итогам проверки:

вносятся изменения в План мероприятий по обеспечению защиты персональных данных;

уточняется перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним;

формируются новые модели угроз безопасности персональных данных;

составляется список необходимых мер защиты персональных данных;

вносятся изменения в локальные нормативные акты учреждения по вопросам обработки персональных данных.