Приложение №1
к приказу № 94 от «10» 09 2026 г.

ПОЛОЖЕНИЕ

о внутреннем аудите соответствия обработки персональных данных установленным требованиям в Государственном бюджетном учреждении Ивановской области «Ивановский государственный театральный комплекс (ГБУ «ИГТК»)

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о внутреннем аудите соответствия обработки персональных данных установленным требованиям (далее – Положение) определяет процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок проведения внутреннего контроля соответствия обработки персональных данных в структурных подразделениях ГБУ «ИГТК» (далее – Организация или Оператор) требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных») и принятыми в соответствии с ним правовыми актами.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и принятыми в соответствии с ними нормативными правовыми актами.

1.3. В настоящем Положении используются основные понятия в значениях, определенных статьей 3 Федерального закона «О персональных данных».

II. ОБЩИЕ ТРЕБОВАНИЯ К ВНУТРЕННЕМУ АУДИТУ

2.1. Целями осуществления внутреннего аудита являются:

- оценка общего состояния выполнения Оператором требований по обработке и защите персональных данных, закрепленных законодательно, а также в локальных актах Организации;

- выявление и предотвращение нарушений законодательства в сфере персональных данных.

2.2. Внутренний аудит соответствия обработки персональных данных в структурных подразделениях Оператора требованиям к защите персональных данных (далее – внутренний аудит) осуществляется путем проведения проверок лицом, ответственным за организацию обработки персональных данных Оператора (далее – ответственный за организацию обработки персональных данных), или комиссией по проведению внутреннего контроля соответствия обработки персональных данных в структурных подразделениях Оператора требованиям к защите персональных данных (далее – комиссия).

2.3. Ответственный за организацию обработки персональных данных назначается приказом руководителя Оператора.

2.4. Состав комиссии утверждается приказом руководителя Оператора.

2.5. В состав комиссии могут входить работники Оператора. В проведении проверки не может участвовать работник Оператора, прямо или косвенно заинтересованный в ее результатах.

2.6. Члены комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность

персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

III. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО АУДИТА

3.1. Проверки соответствия обработки персональных данных установленным требованиям в Организации проводятся на основании утвержденного руководителем Оператора плана осуществления внутреннего аудита соответствия обработки персональных данных установленным требованиям или на основании поступившего Оператору письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

3.2. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- наличие мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

3.3. Ответственный за организацию обработки персональных данных в администрации Организации (либо комиссия) имеет право:

- запрашивать у сотрудников Оператора информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных работников Оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить руководителю Оператора предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить руководителю Оператора предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

3.4. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю Оператора докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

3.5. Руководитель Оператора, назначивший внеплановую проверку, осуществляет контроль за своевременностью и правильностью ее проведения.

Приложение № 1
к Положению о внутреннем аудите
соответствия обработки персональных данных
установленным требованиям в (ГБУ «ИГТК»),
утв. Приказом № 94 от «10» 09 2026 г.

Форма акта внутреннего аудита соответствия обработки персональных данных требованиям к защите персональных данных в ГБУ «ИГТК»

УТВЕРЖДАЮ
Директор «ГБУ «ИГТК»

_____Соколов С.Н.

«___» _____ 20__ года

АКТ
внутреннего аудита соответствия обработки персональных данных требованиям к защите персональных данных в ГУБ «ИГТК»

1. Настоящий Акт составлен в том, что «___» _____ 20__ года ответственным за организацию обработки персональных данных (комиссией в составе: _____) проведена проверка (внутренний аудит) соответствия обработки персональных данных требованиям к защите персональных данных в ГБУ «ИГТК».

2. Проверка осуществлялась в соответствии с требованиями:
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Положения об обработке и защите персональных данных работников, утвержденного приказом № _____ от «____» _____ 20 ____ года.

3. Результаты рассмотрения вопросов по предметам аудита:

Предмет аудита	**Результат рассмотрения**	**Примечание**

Выявленные нарушения:

_____
_____
_____
_____
_____

Меры по устранению нарушений:

_____
_____
_____
_____
_____

Срок устранения нарушений: _____.

Ответственный за организацию обработки персональных данных _____

(Комиссия в составе:
- председатель: _____
- члены: _____).

Приложение №2
к приказу №94 от 10.09.2026

ФОРМА

УТВЕРЖДАЮ

Директор
Государственного бюджетного учреждения
Ивановской области «Ивановский
государственный театральный комплекс»

_____ Соколов С.Н.

ПЛАН
внутреннего контроля соответствия обработки персональных данных требованиям защиты персональных данных на период с «___» ____ 20 ___ г. по «___» ____ 20 ___ г. в Государственном бюджетном учреждении Ивановской области «Ивановский государственный театральный комплекс» (ГБУ «ИГТК»)

ОБЩИЕ ПОЛОЖЕНИЯ

План внутреннего контроля соответствия обработки персональных данных требованиям защиты персональных данных содержит перечень внутренних проверок, сроки их исполнения и исполнителей.

План распространяется на все информационные системы персональных данных ГБУ «ИГТК».

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный
Контроль соблюдения организационно-режимных требований в помещениях, в которых осуществляется обработка персональных данных			
1	Проверка актуальности перечня должностных лиц, имеющих право самостоятельного доступа в помещения, где обрабатываются или хранятся персональные данные		
2	Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных		
3	Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными		
4	Наличие жалюзи на окнах		
5	Установка дополнительных запирающих устройств на места хранения документов с персональными данными		

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный
6	Проверка исполнения режима доступа в серверное помещение		
Контроль доступа к приложениям информационных систем, в которых осуществляется обработка персональных данных			
1	Контроль фактов подачи заявок на блокирование доступа к информационным данным увольняемых работников и своевременность подачи таких заявок		
2	Контроль использования предоставленных прав доступа (в том числе и право удаленного доступа)		
3	Соответствие используемых пользователями информационных данных, полномочий параметрам (матрице) доступа		
Контроль порядка обращения с носителями персональных данных			
1	Проверка корректности ведения журнала учета машинных носителей и соответствия записей в журнале записям в автоматизированной системе контроля съемных магнитных носителей информации		
2	Проверка наличия съемных носителей персональных данных и соблюдения пользователями правил работы с ними		
3	Своевременность проведения мероприятий по уничтожению персональных данных		
4	Контроль отсутствия конфиденциальных документов, содержащих персональные данные, без присмотра на рабочих столах работников		
Проверка выполнения запросов субъектов персональных данных			
1	Проверка своевременности исполнения запросов субъектов персональных данных		
2	Контроль актуальности ведения журнала учета обращений субъектов персональных данных по вопросам обработки их персональных данных		
3	Наличие необходимых согласий субъектов персональных данных		
Контроль выявления и нейтрализации угроз информационной безопасности			
1	Проверка корректности ведения базы данных, инцидентов информационной безопасности		
2	Актуальность заполнения отчетов об инцидентах и их нейтрализации		

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный
3	Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты персональных данных		
4	Проверка фиксации неудачных попыток входа в систему в системном журнале		
Контроль соблюдения требований режима обработки персональных данных			
1	Соблюдение порядка работы со средствами защиты информации		
2	Соблюдение пользователями требований антивирусной защиты		
3	Соблюдение порядка резервирования баз данных, иной защищаемой информации и хранения резервных копий		
4	Контроль за внесением изменений в программное обеспечение, за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах информационных систем		
5	Подготовка предложений по приобретению и установке новых лицензионных программных продуктов		
6	Контроль сохранности пломб на технических средствах передачи и обработки персональных данных, а также на устройствах их защиты		
Контроль соблюдения пользователями информационных систем парольной политики			
1	Проверка сроков действия паролей		
2	Проверка пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей		
Анализ и пересмотр имеющихся угроз безопасности персональных данных			
1	Анализ и пересмотр имеющихся угроз безопасности персональных данных, а также предсказание появления новых, еще не известных угроз		
2	Корректировка частных моделей угроз безопасности персональных данных при их обработке в информационных системах		
3	Моделирование (при необходимости) новых моделей угроз безопасности персональных данных в соответствии с действующими нормативными правовыми актами и методическими документами ФСТЭК и ФСБ		

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный
Обучение и проверка работников по вопросам обеспечения безопасности персональных данных			
1	Контроль ознакомления вновь принимаемых работников с локальными нормативными актами, регламентирующими обработку персональных данных		
2	Проверка знания пользователями информационных систем о своих действиях во внештатных ситуациях		
3	Проверка знаний и соблюдения работниками положений действующего законодательства Российской Федерации в области персональных данных и локальных актов учреждения		
4	Обучение руководителей и работников в области обработки и защиты персональных данных		

С планом ознакомлены(а):

_____ _____ _____

_____

_____ _____ _____

_____