

**ПРАВИЛА**  
**осуществления в Законодательной Думе Томской области**  
**внутреннего контроля соответствия обработки персональных данных**  
**требованиям по защите персональных данных**

**1. Общие положения**

1.1. Настоящие правила осуществления в Законодательной Думе Томской области внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных (далее – Правила) определяют порядок и методику проведения внутренних проверок соответствия обработки персональных данных (ПДн) в Думе требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов.

1.2. Настоящие Правила могут пересматриваться и дополняться по мере необходимости ответственным лицом за организацию обработки персональных данных. Все изменения и дополнения в настоящие Правила вносятся соответствующим распоряжением Председателя Думы.

1.3. Контроль за соблюдением настоящих Правил возлагается на ответственного за организацию обработки ПДн.

**2. Порядок проведения внутренних проверок**

2.1. Проведение внутренних проверок в Думе организует ответственный за организацию обработки ПДн.

2.2. Проверки могут быть плановыми – в соответствии с Планом мероприятий по обеспечению безопасности персональных данных и внеплановыми (при изменении состава и структуры ИСПДн, при изменении существенных условий обработки и категорий, обрабатываемых персональных данных в Думе), но не реже, чем один раз в год. При невозможности выполнения проверки в установленные сроки (отсутствие/занятость ответственных лиц и др.), сроки проведения проверки могут быть перенесены по согласованию с ответственными лицами, но не более чем на один месяц.

2.3. Проверки проводятся постоянной комиссией в области обработки персональных данных в Думе, либо сотрудниками, указанными в распоряжении о проведении проверки. В таком распоряжении также устанавливаются сроки проведения проверки и необходимый перечень отчетной документации по результатам проверки.

2.4. По результатам проверки ответственным лицом за организацию обработки ПДн производится запись в «Журнале учета внутренних проверок в области обработки персональных данных» (приложение 1 к настоящим Правилам) и оформляется соответствующий Протокол проведения внутренней проверки (приложение 2 к настоящим Правилам).

2.5. В Протоколе проведения внутренней проверки производится отметка о соответствии/несоответствии проверяемых критериев (по организационной и технической частям), заданных методикой, а также запись о мероприятиях по устранению нарушений, сроках устранения выявленных нарушений и ответственных за устранение нарушений лицах.

2.6. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, ответственный за организацию обработки персональных данных докладывает руководителю аппарата Думы.

### 3. Методика проведения проверки

3.1. Проверки проводятся непосредственно на местах обработки персональных данных путем опроса либо путем осмотра рабочих мест сотрудников, допущенных к обработке персональных данных.

3.2. Проверка организационной части:

Обозначение критерия	Наименование критерия	Примечание
КО-1	Наличие действующего распоряжения о назначении ответственного лица за организацию обработки персональных данных.	152-ФЗ, ст.18.1, ч.1, п.1 152-ФЗ, ст.22.1, ч.1 ПП-211, п.1-а, п.1-б
КО-2	Наличие действующего распоряжения о назначении лица, ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн (администратора безопасности ИСПДн)	ПП-1119, п.14 Приказ №378 ФСБ
КО-3	Наличие действующего распоряжения о назначении постоянной комиссии по персональным данным в Думе.	Комиссия для установления уровней защищенности ПДн, проведения внутренних проверок и др. Для уничтожения носителей ПДн назначается отдельная комиссия.
КО-4	Наличие актуальной модели угроз безопасности ПДн при их обработке в ИСПДн	152-ФЗ, ст.19, ч.2, п.1
КО-5	Обеспечение сохранности носителей персональных данных. Наличие и ведение журнала учета машинных носителей ПДн	152-ФЗ, ст.19, ч.2, п.5 Приказ №378 ФСБ
КО-6	Наличие актуального перечня мест хранения носителей ПДн	ПП-687, ч.3, п.13
КО-7	Наличие актуального перечня сотрудников, допущенных к обработке ПДн	ПП-687, ч.3, п.13 ПП-211, п.1-б Приказ №378 ФСБ
КО-8	Наличие актуального перечня ИСПДн	ПП-211, п.1-б
КО-9	Наличие актуального перечня ПДн	ПП-211, п.1-б
КО-10	Проверка наличия и актуальности внутренних организационно-распорядительных документов, определяющих политику Думы в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. (Правила, положения, инструкции, регламенты, план мероприятий).	152-ФЗ, ст.18.1, ч.1, п.2 ПП-211, п.1-б
КО-11	Проверка наличия актуальных документов, определяющих политику обработки ПДн в общедоступных источниках	152-ФЗ, ст.18.1, ч.2 ПП-211, п.2

Обозначение критерия	Наименование критерия	Примечание
КО-12	Проверка наличия документов, подтверждающих факт ознакомления допущенных к обработке сотрудников с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, с документами, определяющими политику Думы в отношении обработки ПДн, с локальными актами по вопросам обработки ПДн и (или) обучения указанных сотрудников.	152-ФЗ, ст.18.1, ч.1, п.6 ПП-211, п.1-е
КО-13	Наличие актуального (полного и достоверного) отправленного в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) Уведомления об обработке ПДн (письма о внесении изменений в Уведомление)	152-ФЗ, ст.22 ПП-211, п.1-ж
КО-14	Наличие согласий работников на обработку и распространение их ПДн	152-ФЗ, ст.6, ч.1, п.1 152-ФЗ, ст.9, 152-ФЗ, ст.10.1, ПП-211, п.1-б
КО-15	Наличие письменных обязательств сотрудников, допущенных к обработке ПДн, о неразглашении ПДн	ПП-211, п.1-б
КО-16	Определение уровней защищенности ПДн при их обработке в ИСПДн в зависимости от угроз безопасности этих данных. Наличие актуальных Актов установления уровней защищенности ПДн при их обработке в ИСПДн	152-ФЗ, ст.19, ч.2, п.2 ПП-1119
КО-17	Наличие соглашений (существенных условий договоров) с контрагентами о соблюдении конфиденциальности передаваемых ПДн (в случае такой передачи по договору)	152-ФЗ, ст.6, ч.3
КО-18	Наличие согласий субъектов на опубликование их ПДн в общедоступных источниках	152-ФЗ, ст.8
КО-19	Наличие и ведение журнала запросов субъектов ПДн по вопросам обработки ПДн и наличие правил обработки таких запросов	152-ФЗ, ст.14
КО-20	Проверка соблюдения оператором правил работы (хранения и уничтожения) с носителями ПДн	ПП-687
КО-21	Внутренний контроль и аудит соответствия обработки персональных данных Федеральному закону 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике в отношении обработки ПДн, локальным актам по вопросам обработки ПДн. Наличие актуального плана мероприятий по обеспечению безопасности ПДн и ведение журнала внутренних проверок в области обработки ПДн	152-ФЗ, ст.18.1, ч.1, п.4 ПП-211, п.1-б, п.1-д
КО-22	Проверка соблюдения сотрудниками правил доступа в помещения, в которых происходит обработка и хранение бумажных носителей ПДн, а также в которых расположены компоненты ИСПДн	ПП-1119, п. 13-а ПП-211, п.1-б
КО-23	Выявление избыточных данных по отношению к целям обработки	152-ФЗ, ст.5, ч.5

<b>Обозначение критерия</b>	<b>Наименование критерия</b>	<b>Примечание</b>
КО-24	Своевременность проведения мероприятий по обезличиванию персональных данных	152-ФЗ, ст.5, ч.7 ПП-211, п.1-6, п.1-3
КО-25	Своевременность проведения мероприятий по уничтожению персональных данных	152-ФЗ, ст.5, ч.7
КО-26	Проведение оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых Думой мер, направленных на обеспечение выполнения обязанностей	152-ФЗ, ст.18.1, ч.1, п.5
КО-27	Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации	152-ФЗ, ст.19, ч.1, п.3
КО-28	Организация режима обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	Приказ №378 ФСБ

### 3.3. Проверка технической части:

<b>Обозначение критерия</b>	<b>Наименование критерия</b>
КТ-1	Идентификация и аутентификация субъектов доступа и объектов доступа (авторизация пользователей по логину и паролю, применение надежных паролей для доступа к ИСПДн)
КТ-2	Управление доступом субъектов доступа к объектам доступа (соблюдение порядка разграничения прав доступа пользователей к ИСПДн)
КТ-3	Соблюдение пользователями правил работы со съемными машинными носителями ПДн
КТ-4	Регистрация событий безопасности (применение сертифицированных СрЗИ в ИСПДн )
КТ-5	Применение антивирусной защиты в ИСПДн
КТ-6	Контроль (анализ) защищенности ПДн
КТ-7	Обеспечение доступности персональных данных (применение средств резервного копирования и восстановления в ИСПДн)
КТ-8	Защита среды виртуализации
КТ-9	Защита технических средств (расположение технических средств ИСПДн в пределах контролируемой зоны, исключающее случайный или преднамеренный несанкционированный просмотр выводимых данных)
КТ-10	Защита информационной системы, ее средств, систем связи и передачи данных (применение шифровальных средств для защиты информации при передаче ПДн по каналам связи за пределы контролируемой зоны Думы)
КТ-11	Соблюдение пользователями правил работы с шифровальными средствами
КТ-12	Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области

	обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз
КТ-13	Выявление инцидентов и реагирование на них (Выявление инцидентов, нештатных ситуаций, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей)
КТ-14	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
КТ-15	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

Приложение 1  
к Правилам осуществления в Законодательной  
Думе Томской области внутреннего контроля  
соответствия обработки персональных данных  
требованиям по защите персональных данных

**Форма Журнала учета внутренних проверок  
в области обработки персональных данных**

<b>№ п/п</b>	<b>Дата начала и окончания проверки</b>	<b>Исполнитель (Комиссия)</b>	<b>Результат проверки</b>	<b>Подпись ответственного за организацию обработки ПДн</b>	<b>Примечание</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>

Примечание.

Заполнение полей Журнала:

1 – порядковый номер проверки в данном Журнале.

2 – даты начала и окончания проверки.

3 – заносятся ФИО исполнителя (исполнителей) или наименование комиссии, назначенных распоряжением  
Председателя Думы, дата и номер распоряжения о проведении проверки, вид проверки (плановая/внеплановая (в связи  
с чем).

4 – указывается краткое описание результатов проведения проверки.

5 – подпись и расшифровка подписи (Ф.И.О.) ответственного лица за организацию обработки персональных  
данных.

6 – иная информация.

Приложение 2  
к Правилам осуществления в Законодательной  
Думе Томской области внутреннего контроля  
соответствия обработки персональных данных  
требованиям по защите персональных данных

**Форма Протокола о проведении внутренней проверки  
в области обработки персональных данных**

**ПРОТОКОЛ**

проведения внутренней проверки в области обработки персональных данных

Настоящий Протокол составлен в том, что в срок с «\_\_» \_\_\_\_\_ 20\_\_ г. по  
«\_\_» \_\_\_\_\_ 20\_\_ г. комиссией в составе:

Председатель комиссии:

- \_\_\_\_\_ ;

Члены комиссии:

- \_\_\_\_\_ ;

- \_\_\_\_\_ ;

- \_\_\_\_\_ ;

утвержденной распоряжением от \_\_\_\_\_ № \_\_\_\_\_, проведена внутренняя проверка в области  
обработки персональных данных на соответствие условий обработки ПДн требованиям  
Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии  
с ним нормативных правовых актов.

Проверка является плановой (внеплановой, в связи с \_\_\_\_\_) и осуществлялась  
на основании Правил проведения внутренних проверок (утв. распоряжением от \_\_\_\_\_  
№ \_\_\_\_\_) и Плана мероприятий по обеспечению безопасности персональных данных (утв.  
распоряжением от \_\_\_\_\_ № \_\_\_\_\_).

В ходе проверки было выявлено:

№ п/п	Критерий	Соответствие/ Несоответствие (+ / -)	Выявленное нарушение	Меры по устранению нарушений	Сроки устранения нарушений	Ответственный

Председатель комиссии:

\_\_\_\_\_ ;

Члены комиссии:

\_\_\_\_\_ ;

\_\_\_\_\_ ;

\_\_\_\_\_ .