

**ПРАВИЛА  
ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ  
ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ  
ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ «О ПЕРСОНАЛЬ-  
НЫХ ДАННЫХ», ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ  
ПРАВОВЫМИ АКТАМИ, В ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ  
КУЛЬТУРЫ СТАВРОПОЛЬСКОГО КРАЯ «СТАВРОПОЛЬСКАЯ КРАЕВАЯ УНИ-  
ВЕРСАЛЬНАЯ НАУЧНАЯ БИБЛИОТЕКА  
ИМ. М. Ю. ЛЕРМОНТОВА»**

1. Настоящие Правила устанавливают порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном учреждении культуры Ставропольского края «Ставропольская краевая универсальная научная библиотека им. М.Ю. Лермонтова» (далее соответственно - внутренний контроль, библиотека).

2. Осуществление внутреннего контроля в библиотеке осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в том же значении, что и в Федеральном законе № 152-ФЗ.

4. Целью настоящих Правил является обеспечение защиты персональных данных граждан от несанкционированного доступа, неправомерного их использования или утраты в библиотеке.

5. Настоящие Правила устанавливают:  
виды и периодичность внутреннего контроля;  
порядок создания комиссии для осуществления внутреннего контроля;  
порядок проведения внутреннего контроля.

6. Внутренний контроль обработки персональных данных (далее - ПДн) делится на текущий и комиссионный.

7. Текущий внутренний контроль осуществляется на постоянной основе ответственным за организацию обработки ПДн в библиотеке в ходе мероприятий по обработке ПДн.

Ответственный за организацию обработки ПДн в библиотеке имеет право:

требовать от сотрудников библиотеки, имеющих доступ к ПДн, выполнения установленной технологии обработки ПДн, инструкций и других нормативных правовых актов по обеспечению безопасности ПДн;

участвовать в разработке мероприятий по совершенствованию безопасности ПДн в библиотеке;

инициировать проведение служебных расследований по фактам нарушения сотрудниками библиотеки, имеющими доступ к ПДн, установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемых ПДн;

обращаться к директору библиотеки о приостановке процесса обработки ПДн в библиотеке или отстранению от работы сотрудников библиотеки, имеющих доступ к ПДн, в

случаях нарушения установленной технологии обработки или нарушения режима конфиденциальности ПДн.

8. Комиссионный внутренний контроль осуществляется комиссией, образуемой приказом библиотеки из числа сотрудников библиотеки, и носит периодический характер (далее - комиссия). Периодичность проведения комиссионного внутреннего контроля - не реже одного раза в год.

Комиссионный внутренний контроль проводится в библиотеке на основании утвержденного директором плана осуществления комиссионного внутреннего контроля соответствия обработки ПДн установленным требованиям, разрабатываемого председателем комиссии, или на основании поступившего в библиотеку письменного заявления о нарушении правил обработки ПДн.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в ее результатах.

9. При проведении внутреннего контроля должны быть полностью, объективно и всесторонне установлены соответствия по следующим положениям:

наличие, учет, порядок хранения и обезличивания ПДн;

порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке;

порядок и условия применения средств защиты ПДн;

эффективность принимаемых мер по обеспечению безопасности ПДн;

состояние учета машинных носителей ПДн;

соблюдение правил доступа к ПДн;

наличие (отсутствие) фактов несанкционированного доступа к ПДн;

мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности ПДн.

10. В отношении ПДн, ставших известными членам комиссии или ответственному за организацию обработки ПДн в ходе проведения мероприятий внутреннего контроля, должно обеспечиваться конфиденциальность ПДн.

11. Срок проведения внутреннего контроля не может составлять более 30 дней со дня принятия директором решения о его проведении.

12. Результаты проверки отражаются в протоколе проведения внутреннего контроля условий обработки персональных данных в библиотеке по форме согласно приложению к настоящим Правилам.

13. При выявлении в ходе проверки нарушений ответственным за организацию обработки ПДн в библиотеке либо председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

14. Протоколы хранятся у ответственного за организацию обработки ПДн в течение текущего года, когда был осуществлен внутренний контроль. Уничтожение протоколов проводится ответственным за организацию обработки ПДн самостоятельно в январе года, следующего за проверочным годом.

15. О результатах проведенного внутреннего контроля и мерах, необходимых для устранения нарушений, директору докладывает ответственный за организацию обработки ПДн в библиотеке или председатель комиссии.

Приложение

к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами, в библиотеке

ФОРМА

**ПРОТОКОЛ**  
проведения внутреннего контроля условий обработки персональных данных в ГБУК «СКУНБ им. Лермонтова»

Настоящий Протокол составлен «\_\_\_» \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_ (кем проводится проверка: ответственным за организацию обработки персональных данных или комиссией по внутреннему контролю)  
проведена проверка \_\_\_\_\_ (тема проверки)

Проверка осуществлялась в соответствии с требованиями \_\_\_\_\_ (наименование документа)

В ходе проверки проверено: \_\_\_\_\_

Выявленные нарушения: \_\_\_\_\_

Меры по устранению нарушений: \_\_\_\_\_

Срок устранения нарушений: \_\_\_\_\_

\_\_\_\_\_ (кто проводил проверку: ответственный за организацию обработки персональных данных или комиссия по внутреннему контролю (председатель и члены комиссии), подписи, Ф.И.О. проверяющих)

С протоколом ознакомлен:

\_\_\_\_\_ (руководитель проверяемого подразделения: должность, подпись, Ф.И.О.)