



Дата подготовки: 14.06.2024

Заключение № 4942

Подготовлено: А.М. Келлерманн
Ведущий аудитор ISO / IEC 27001

Заключение

Комитета по информационной и правовой безопасности о результатах внешней проверки исполнения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (с изменениями на 06 февраля 2023 года) и иных требований нормативно-правовых актов по защите персональных данных в МОУ СОШ №8



Содержание

Введение, основные термины и определения:	3-4
• кто является оператором персональных данных	
• что является обработкой персональных данных	
• кто осуществляет контроль за соблюдением закона о персональных данных	
Изменения в сфере защиты персональных данных, «новый» закон о персональных данных	4
Сводная информация по результату внешней проверки в отношении МОУ СОШ №8	5-6
Требования по наличию организационно-распорядительной документации	6-11
• перечень организационно-распорядительной документации по защите персональных данных, предусмотренный действующим законодательством	
Требования по направлению уведомления, для включения в реестр операторов персональных данных	11
• новые требования к форме уведомления на 2024 год	
Ответственность и штрафы за нарушения на 2024 год	12-14
• таблица ответственности и штрафов за нарушения законодательства в области персональных данных (в редакции КоАП, действующей с 27.03.2021)	
О специфике и результатах деятельности Комитета по информационной и правовой безопасности	14
Необходимые меры по подготовке МОУ СОШ №8 к требованиям законодательства по защите персональных данных	15



1. Введение, основные термины и определения

Комитет по информационной и правовой безопасности (далее - Комитет) уведомляет Вас, что по результатам мониторинга, проведенного в отношении оператора персональных данных МОУ СОШ №8, выявлены нарушения требований действующего законодательства в сфере защиты персональных данных, предусмотренных ч. 3, ч. 7 ст. 22, ч. 1 ст. 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных).

Закон о персональных данных претерпел множество изменений за последние несколько лет, и для того, чтобы помочь Вам сэкономить финансовые средства и разобраться, какие требования Государство предъявляет к Вашей организации, эксперты Комитета подготовили Заключение о результатах внешней проверки (далее – Заключение).

Данный документ является руководством, описывающим действия МОУ СОШ №8, которые необходимо предпринять ответственным лицам для соответствия законодательству, регулиющему отношения, связанные с обработкой персональных данных.

Кто является оператором персональных данных

❗ В соответствии пунктом 2 статьи 3 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

При этом указанные органы и лица являются операторами персональных данных с момента регистрации в Федеральной Налоговой службе, независимо от включения в реестр операторов, осуществляющих обработку персональных данных, который ведет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Что является обработкой персональных данных

В силу требований действующего законодательства, на МОУ СОШ №8 возложена обязанность обработки персональных данных текущих и уволенных работников, включая руководителя организации (так как его персональные данные фигурируют в кадровых и учредительных документах), а также должностных лиц контрагентов и иных физических лиц, что в соответствии со ст. 3 п. 3 Закона о персональных данных является обработкой персональных данных.

❗ Использование данных руководителя, работников, клиентов и иных физических лиц в профессиональной деятельности (фамилия, имя, отчество, адрес, паспортные данные, ИНН, номер телефона), ведение кадрового и бухгалтерского учета, заключение и оформление договоров, сбор анкет (резюме) кандидатов на работу, направление третьим лицам (органам) списков сотрудников при оформлении им медицинских полисов, перечисление денежных средств на зарплатные счета в банк, предоставление в военный комиссариат списков военнообязанных сотрудников, сбор и использование персональных данных клиентов, осуществление видеонаблюдения, ведение журнала контрольно-пропускного пункта и т.д. в соответствии с п.3 ст. 3 Федерального закона №152-ФЗ является обработкой персональных данных.



Кто осуществляет контроль за соблюдением закона о персональных данных

Ответственными ведомствами (регуляторами) за соблюдение правомерности обработки персональных данных являются:

- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) - контроль и надзор за соответствием обработки персональных данных требованиям законодательства.
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России) устанавливает методы и способы защиты информации в информационных системах не криптографическими методами.
- Федеральная служба безопасности (ФСБ России) устанавливает методы и способы защиты информации в информационных системах криптографическими методами.



❗ Обращаем внимание, что несмотря на действующий мораторий в отношении плановых проверок на 2024 г., порядок проведения контрольно-надзорных мероприятий Роскомнадзора определен Постановлением Правительства Российской Федерации от 29 июня 2021г. № 1046, предусматривая следующие формы надзора: инспекционный визит, документарная проверка и выездная проверка.

2. Изменения в сфере защиты персональных, «новый» закон о персональных данных

В 2022 году произошли одни из самых масштабных изменений в сфере защиты персональных данных. Их стали часто называть «новый закон о персональных данных 2022 года».

❗ Новшества вступили в силу 01 сентября 2022 года. Но есть ряд изменений, которые начали действовать гораздо позже – 01 марта 2023 года.

Речь идет о Федеральном законе от 14.07.2022 № 266-ФЗ. Он вносит изменения в другой закон, который уже давно регулирует вопросы обработки и защиты персональных данных - Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (далее – Закон).

Также, с 26.12.2022 года, с вступлением в силу Приказа Роскомнадзора №180 от 28.10.2022 г. «Об утверждении новых форм уведомлений о намерении осуществлять обработку персональных данных» операторы персональных данных будут обязаны использовать новые формы уведомлений для направления в Роскомнадзор:

- о намерении осуществлять обработку персональных данных;
- об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных;
- о прекращении обработки персональных данных.



3. Сводная информация по результату внешней проверки в отношении МОУ СОШ №8 *

*На соответствие требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Отчет сформирован при взаимодействии с информационными ресурсами Федеральной Налоговой службы и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

❗ Так как МОУ СОШ №8 на момент проверки, по состоянию на 14.06.2024 имеет статус «Действующее», с указанной численностью работников – 50 чел., то является оператором персональных данных согласно п.2 ст.3 Закона о персональных данных.

Основные реквизиты

Краткое наименование	МОУ СОШ №8
Статус	Действующее
Юридический адрес	442240, Россия, Приволжский Федеральный округ, Пензенская обл, Каменка, ул Ворошилова зд. 18А
ДИРЕКТОР	Рябов Александр Николаевич
Численность работников	50 чел.
Основной вид деятельности по ОКВЭД	85.14 Образование среднее общее
ИНН	5802100930
Форма собственности	Муниципальное бюджетное учреждение

❗ Проверка экспертами Комитета по информационной и правовой безопасности, проведенная 14.06.2024 в отношении МОУ СОШ №8 (ИНН: 5802100930) показала, что проверяемая организация имеет значительный уровень нарушений в отношении соответствия требованиям Закона о персональных данных.

Результаты мониторинга

✓	Информация по организации в ФНС	Найдена
✓	Обязанность подачи уведомления об обработке персональных данных в Роскомнадзор	Организация обязана уведомить Роскомнадзор перед началом обработки персональных данных
⚠	Наличие организации в реестре операторов Роскомнадзора	Требуется уточнение сведений, в соответствии с требованиями Приказа Роскомнадзора №180 от 28.10.2022 г
⚠	Наличие необходимой организационно-распорядительной документации	Требуется сверка перечня имеющихся документов с п.4 Заключения «Требования по наличию организационно-распорядительной документации»
❗	Максимальный штраф при проверке по ст.13.11 КоАП РФ	От 1 до 6 млн. руб.

Сведения данного отчета являются аналитическим показателем, рассчитываемым на основе публично доступной информации о деятельности юридического лица и данных, полученных при заполнении заявки на сайте <https://kpib.ru>. Данная оценка является рекомендательным мнением и



не даёт каких-либо гарантий или заверений третьим лицам

4. Требования по наличию организационно-распорядительной документации

По результатам мониторинга деятельности МОУ СОШ №8, было выявлено, что Ваша организация не выполнила необходимых организационно-технических мер по организации сбора и обработки персональных данных для соответствия требованиям Закона о персональных данных, что является грубейшим нарушением с установленной административной ответственностью в соответствии со ст.13.11 Кодекса Российской Федерации об административных правонарушениях.

- ❗ На 14.06.2024 в МОУ СОШ №8 должны быть приняты правовые, организационные и технические меры по обеспечению безопасности персональных данных, в соответствии с требованиями, предусмотренными ст. 18.1, ст. 19 Закона о персональных данных, включая разработку и издание комплекта организационно-распорядительной документации.

Документы должны быть у каждой компании, ИП, физического лица, государственного или муниципального органа и прочих организаций, которые занимаются обработкой персональных данных. Их тщательно изучают в рамках проверок сотрудники Роскомнадзора и Трудовой инспекции и при выявлении нарушений накладывают штрафы.

Требования, предъявляемые МОУ СОШ №8 к обработке и защите персональных данных, отражены в следующих нормативно-правовых актах, регламентирующих создание организационно-распорядительной документации (ОРД) организации:

- Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ;
- Постановление Правительства РФ от 15.09.2008 N 687;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21;
- Приказ ФСБ Российской Федерации от 10 июля 2014 г. N 378.

- ❗ **Требуемый пакет документов должен разрабатываться квалифицированным специалистом по информационной безопасности, имеющим необходимые разрешения, аккредитацию, или сертификацию.**

Применение шаблонных инструкций, размещенных в открытом доступе недопустимо, в связи с тем, что они не учитывают специфику деятельности МОУ СОШ №8 и могут содержать неактуальные требования устаревших нормативных актов.

Перечень организационно-распорядительной документации по защите персональных данных, предусмотренный действующим законодательством

Выполняемые мероприятия	Нормативно-правовой акт (основание для требования)
Акт определения уровня защищенности ИСПДн	Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление Правительства № 1119); пункт 5 части 1 статьи 18.1 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных»
Акт оценки потенциального вреда субъектам персональных данных	Приказ Роскомнадзора от 27.10.2022 № 178 «Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения



	Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ о базах данных информации, содержащей персональные данные. Приложения к документу: <ul style="list-style-type: none">Сведения о месте нахождения баз данных информации, содержащей персональные данные граждан Российской Федерации, обрабатываемые в информационных системах персональных данных.	Пункт 10.1 части 3 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ о безопасности материальных носителей ПДн. Приложения к документу: <ul style="list-style-type: none">Перечень мест хранения материальных (бумажных и машинных) носителей персональных данных и лиц, ответственных за реализацию мер по обеспечению безопасности персональных данных;Инструкция ответственного за реализацию мер по обеспечению безопасности персональных данных в части исключения несанкционированного доступа при хранении материальных (бумажных и машинных) носителей персональных данных.	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
Приказ о вводе в действие комплекта организационно-распорядительной документации по организации обработки и защиты персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
Приказ о вводе информационной системы персональных данных в эксплуатацию	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ о комиссии по уничтожению персональных данных. Приложения к документу: <ul style="list-style-type: none">Положение о комиссии по уничтожению персональных данных;Типовая форма акта об уничтожении персональных данных.	Требования к подтверждению уничтожения персональных данных, утвержденными приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных» в целях реализации положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ об утверждении перечней персональных данных, обрабатываемых в информационных системах персональных данных. Приложения к документу: <ul style="list-style-type: none">Перечень персональных данных, обрабатываемых в	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении



информационной системе персональных данных	требований к защите персональных данных при их обработке в информационных системах персональных данных»
Приказ об утверждении перечня лиц, имеющих право доступа в помещения, в которых размещены информационные системы персональных данных. Приложения к документу: <ul style="list-style-type: none">Перечень лиц, имеющих право доступа в помещения, в которых размещены информационные системы персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ об утверждении перечней лиц, доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей. Приложения к документу: <ul style="list-style-type: none">Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ о назначении ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных. Приложения к документу: <ul style="list-style-type: none">Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ о назначении ответственного за организацию обработки персональных данных. Приложения к документу: <ul style="list-style-type: none">Инструкция ответственного за организацию обработки персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ о предоставлении пользователям доступа к информационным ресурсам информационных систем персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ о комиссии по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных. Приложения к документу: <ul style="list-style-type: none">Положение о комиссии по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данныхТиповая форма акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Приказ об оценке вреда, который может быть причинен субъектам персональных данных, персональные данные которых обрабатываются в информационных системах персональных данных	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»» в целях реализации пункта 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ об утверждении границ контролируемой зоны информационных систем персональных данных и перечней помещений, в которых размещены информационные системы персональных данных. Приложения к документу: <ul style="list-style-type: none">Перечень помещений, в которых размещена информационная система персональных данныхПеречень материальных носителей, содержащих персональные данные	Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 01.11.2012 №1119
Приказ об утверждении матриц доступа пользователей к информационным системам персональных данных. Приложения к документу: <ul style="list-style-type: none">Матрица доступа пользователей к информационной системе	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Приказ об утверждении перечня информационных систем персональных данных. Приложения к документу: <ul style="list-style-type: none">Перечень информационных систем персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»



данных	
Приказ об утверждении перечня персональных данных, обрабатываемых без использования средств автоматизации. Приложения к документу: <ul style="list-style-type: none">Перечень персональных данных, обрабатываемых без использования средств автоматизации	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ об утверждении Политики в отношении обработки персональных данных. Приложения к документу: <ul style="list-style-type: none">Политика в отношении обработки персональных данныхПеречень персональных данных, обрабатываемых в информационной системе персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Правила обработки персональных данных информационных системах персональных данных. Приложения к документу: <ul style="list-style-type: none">Типовая форма согласия субъекта на обработку персональных данныхТиповая форма согласия субъекта на передачу персональных данныхТиповая форма согласия законного представителя на обработку персональных данных несовершеннолетнегоТиповая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить персональные данные и (или) дать согласие на их обработкуТиповая форма обязательства о неразглашении персональных данныхТиповая форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространенияТиповая форма информирования о факте обработки персональных данных без использования средств автоматизации	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (при наличии смешанной обработки ПДн или обработки ПДн без использования средств автоматизации).
Правила рассмотрения запросов субъектов персональных данных или их представителей. Приложения к документу: <ul style="list-style-type: none">Типовая форма запроса на предоставление информации об обработке персональных данныхТиповая форма заявления об отзыве согласия на обработку персональных данныхТиповая форма запроса на уточнение персональных данныхТиповая форма возражения против принятия решений на основании исключительно автоматизированной обработки персональных данныхТиповая форма журнала обращений субъектов персональных данных или представителей субъектов персональных данныхПравила по формированию и ведению журнала обращений субъектов персональных данных или представителей субъектов персональных данныхТиповая форма уведомления о прекращении обработки ПДнТиповая форма отказа в предоставлении сведений об обработке ПДнТиповая форма уведомления о невозможности отзыва согласия на обработку ПДнТиповая форма уведомления о произведении уточнения ПДнТиповая форма ответа на возражение против принятия решений на основании исключительно автоматизированной обработки персональных данныхТиповая форма уведомления о блокировании персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ); постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – постановление Правительства РФ № 687); постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – постановление Правительства РФ № 1119); приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»; приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения



	<p>Федерального закона «О персональных данных»»; приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»; приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 №180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»; приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – приказ ФСТЭК России № 21); приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» (далее – приказ ФСТЭК России № 77).</p>
Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных. Приложения к документу:	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
• Типовая форма акта проведения внутренней проверки условий обработки персональных данных	
План внутреннего контроля обработки и защиты персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
План мероприятий по защите персональных данных информационных систем персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Инструкция о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных. Приложения к документу:	
• Типовая форма журнала запросов уполномоченного органа по защите прав субъектов персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
• Правила по формированию и ведению журнала запросов уполномоченного органа по защите прав субъектов персональных данных	
Инструкция пользователя информационных систем персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказ ФСБ России от 10.07.2014 № 378 Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для



	выполнения установленных Правительством Российской Федерации требованиям к защите персональных данных для каждого из уровней защищенности»; приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Положение о порядке организации и проведении работ по защите персональных данных, обрабатываемых в информационных системах персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Инструкция по идентификации и аутентификации пользователей информационных систем персональных данных. Приложения к документу: <ul style="list-style-type: none">• Типовая форма журнала учета выдачи первичных паролей информационной системы персональных данных• Правила по формированию и ведению журнала учета выдачи первичных паролей информационной системы персональных данных• Типовая форма журнала учета аппаратных средств аутентификации• Правила по формированию и ведению журнала учета аппаратных средств аутентификации	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Инструкция по управлению доступом к информационным системам персональных данных. Приложения к документу: <ul style="list-style-type: none">• Типовая форма журнала учета разрешенных средств удаленного доступа• Правила по формированию и ведению журнала учета разрешенных средств удаленного доступа• Типовая форма журнала учета разрешенных мобильных технических средств• Правила по формированию и ведению журнала учета разрешенных мобильных технических средств	Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных», постановление Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Инструкция по защите машинных носителей персональных данных. Приложения к документу: <ul style="list-style-type: none">• Типовая форма журнала учета машинных носителей персональных данных• Правила по формированию и ведению журнала учета машинных носителей персональных данных• Типовая форма заявления на право использования съемного машинного носителя информации• Типовая форма акта технической экспертизы состояния машинного носителя информации• Типовая форма акта проверки наличия и состояния машинных носителей информации	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказ ФСБ России от 10.07.2014 № 378 Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для



	выполнения установленных Правительством Российской Федерации требованиям к защите персональных данных для каждого из уровней защищенности»; приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;
Инструкция по управлению событиями информационной безопасности информационных систем персональных данных. Приложения к документу: <ul style="list-style-type: none">• Типовая форма журнала событий информационной безопасности информационной системы персональных данных• Правила по формированию и ведению журналов событий информационной безопасности информационных систем персональных данных• Перечень регистрируемых событий информационной безопасности информационных систем персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Инструкция по антивирусной защите информационных систем персональных данных. Приложения к документу: <ul style="list-style-type: none">• Рекомендации по защите компьютера от программ-шифровальщиков	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Инструкция по контролю (анализу) защищенности персональных данных информационных систем персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Инструкция по защите технических средств информационных систем персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных



	системах персональных данных».
Технологический процесс обработки и защиты персональных данных в информационных системах персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Порядок доступа в помещения, в которых размещены информационные системы персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Рекомендации по внесению изменений в должностные (трудовые) обязанности работников в части обеспечения безопасности персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Проект модели угроз безопасности персональных данных	ст.19 п.2 Федерального закона от 27.07.2006 г. № 152-ФЗ; п.2 Постановления Правительства Российской Федерации от 1.11.2012 г. № 1119; п.9 Приказа ФСБ РФ от 10 июля 2014 г. № 378; п. 3.8 СТР-К
Уведомление об обработке (о намерении осуществлять обработку) персональных данных	ч. 1 ст. 22 Федерального закона от 27.07.2006 г. № 152-ФЗ

5. Основные требования по направлению уведомления, для включения в реестр операторов персональных данных

В соответствии с ч.1 ст.22 Закона о персональных данных, МОУ СОШ №8 обязано направить Уполномоченный орган уведомление об обработке (о намерении осуществлять обработку) персональных данных, указав дату начала такой обработки на дату регистрации в ЕГРЮЛ(ИП).

Согласно ч. 2.1. ст. 25 Закона о персональных, операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, должны были представить в Уполномоченный орган сведения, указанные в п.п. 5, 7.1, 10 и 11 ч. 3 ст. 22 Закона о персональных данных в срок до 1 января 2013г. или на дату регистрации организации в ЕГРЮЛ(ИП).

❗ **Категорически запрещено** направлять уведомление об обработке (о намерении осуществлять обработку) персональных данных, если организацией не выполнены требования, согласно п.4 Заключения «Требования по наличию организационно-распорядительной документации», поскольку в уведомлении необходимо описать принятые организационно-технические меры для защиты персональных данных.

Описание мер, предусмотренных
статьями 18.1. и 19 Федерального
закона «О персональных данных» *



Новые требования к форме уведомления на 2024 год

С выходом Приказа Роскомнадзора №180 от 28.10.2022 г. «Об утверждении новых форм уведомлений о намерении осуществлять обработку персональных данных», к формам уведомлений появились новые требования.

С 1 сентября 2022 года можно не уведомлять Уполномоченный орган о намерении обрабатывать персональные только в трёх ситуациях:

Заключение Комитета по информационной и правовой безопасности о результатах внешней проверки исполнения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (с изменениями на 14 июля 2022 года) и иных требований нормативно-правовых актов по защите персональных данных в МОУ СОШ №8.



- персональные данные включены в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка — например, автоматизированные дактилоскопические информационные системы (АДИС) полиции;
- обработка личной информации производится исключительно без средств автоматизации, то есть без использования вычислительной техники (компьютеров, принтеров, телефонов и др);
- персональные данные используются в случаях, предусмотренных законами о транспортной безопасности. Например, записи с видеокамер систем видеонаблюдения в аэропортах и на ж/д вокзалах.

6. Ответственность и штрафы за нарушения на 2024 год

❗ С 27 марта 2021 года вступили в силу новые штрафные санкции за нарушения в области персональных данных в соответствии с Федеральным законом от 24.02.2021 г. №19-ФЗ. Суммы штрафов **увеличены в 2 раза и более**. Кроме этого, по некоторым статьям введено увеличенное наказание за повторное нарушение.

Также увеличился и срок давности привлечения к административной ответственности за нарушения в области персональных данных. Вместо трех месяцев теперь он составляет один год.

Административная ответственность по статье 13.11 на 2024 год предусматривает дифференциацию в зависимости от последствий нарушения. Так ответственность для юридического лица предусматривает наложение штрафа в размере от 30 тысяч до 6 миллионов рублей, а при повторном нарушении — до 18 миллионов рублей.

Максимальный совокупный штраф для должностного лица составляет 336 тысяч рублей, а при повторном нарушении может превышать 1 миллион рублей.

Таблица ответственности и штрафов за нарушения законодательства в области персональных данных (в редакции КоАП, действующей с 27.03.2021):

Статья	Содержание статьи КоАП	Сумма штрафа (тысяч рублей)			
		Физ.лицо (самозаня- тый)	Должностное лицо	ИП	Юр. лицо
13.11 ч.1	Обработка персональных данных в случаях, не предусмотренных законодательством РФ в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи, если эти действия не содержат уголовно наказуемого деяния	2-6	10-20	60-100	60-100
13.11 ч.1.1	Повторное совершение административного правонарушения, предусмотренного частью 1 настоящей статьи	4-12	20-50	50-100	100-300
13.11 ч.2	Обработка персональных данных без согласия в письменной форме субъекта персональных данных	6-10	20-40	30-150	30-150



	на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством РФ в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных				
13.11 ч.2.1	Повторное совершение административного правонарушения, предусмотренного частью 2 настоящей статьи	10-20	40-100	100-300	300-500
13.11 ч.2.1	Невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных	1,5-3	6-12	10-20	30-60
13.11 ч.4	Невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	2-4	8-12	20-30	40-80
13.11 ч.5	Невыполнение оператором в сроки, установленные законодательством РФ в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	2-4	8-20	20-40	50-90
13.11 ч.5.1	Повторное совершение административного правонарушения, предусмотренного частью 5 настоящей статьи	12-30	30-50	50-100	300-500
13.11 ч.6	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством РФ в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении	1,5-4	8-20	20-40	50-100



	персональных данных, при отсутствии признаков уголовно наказуемого деяния				
13.11 ч.7	Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством РФ в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных	—	6-12	—	—
13.11 ч.8	Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», предусмотренной законодательством РФ в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ	30-50	100-200	1-6 млн	1-6 млн
13.11 ч.9	Повторное совершение административного правонарушения, предусмотренного частью 8 настоящей статьи	50-100	50-100	50-100	50-100

7. О специфике и результатах деятельности Комитета по информационной и правовой безопасности

Наша организация прочно закрепилась на рынке с 2016 года и успешно работает уже более 7 лет. За это время:

- наши эксперты провели аудит и проконсультировали на предмет обработки и защиты персональных данных более 33000 организаций от Калининграда до Чукотки;
- более 2785 частных, муниципальных и государственных организаций по всей России доверили нам разработку систем менеджмента по обработке и защите персональных данных, включая:



Открытое Акционерное Общество
«Автодор Санкт-Петербург»



Федеральное государственное
бюджетное учреждение «Российский
НИИ гематологии и трансфузиологии
ФМБА России»



Контрольно-Счетный Комитет
Беломорского Муниципального района
Республики Карелия



Федеральное бюджетное учреждение
«Государственный региональный центр
стандартизации, метрологии и
испытаний
в Нижегородской области»



Комитет финансов администрации МО
«Всеволожский муниципальный район»
Ленинградской области»



Белгородский областной фонд
поддержки малого и среднего
предпринимательства

- более 1200 организаций находятся по постоянной поддержке от наших экспертов по вопросам защиты персональных данных и взаимодействия с Роскомнадзором;
- помогли клиентам устранить риски в части административной ответственности и потенциальных штрафов на сумму более 3 млрд рублей.



8. Необходимые меры по подготовке к требованиям законодательства по защите персональных данных

С учетом вышеизложенного, рекомендуем незамедлительно приступить к процедуре по приведению деятельности МОУ СОШ №8 в соответствии с требованиями закона, не дожидаясь проверки, по результатам которой вы получите предписание об устранении нарушений и штраф.

Осторожно! Вам важно доверить взаимодействие с контролирующими органами специалистам, которые смогут дать гарантию того, что вашу организацию внесут в реестр операторов персональных данных, а документы будут подготовлены по текущим требованиям законодательства, с учетом специфики деятельности МОУ СОШ №8.



Проанализируем, как вы работаете с персональными данными, определим необходимый уровень защищенности.



Сертифицируем вашу организацию, что уменьшит риск проведения проверки.



Разработаем все документы по защите персональных данных для организации именно вашего профиля.



Уведомим вас, если требования закона изменятся и внесем корректировки в ваши документы.



Сформируем за вас уведомление в Роскомнадзор в электронном виде с учетом всех актуальных требований.



Бесплатно дадим рекомендации и материалы: «как вести себя в случае проверки».



Для осуществления деятельности, нами была зарегистрирована первая в Российской Федерации система сертификации экспертов и организаций в области защиты персональных данных «Национальный центр информационной безопасности». Свидетельство о регистрации системы сертификации № РОСС RU.32827.04НЦИ выдано Федеральным агентством по техническому регулированию и метрологии «Росстандарт» без ограничения срока действия.

Оказание услуг по разработке организационно-распорядительной документации и формирование уведомления для постановки на учет в реестр операторов персональных данных для МОУ СОШ №8, составляет **55 000 р. 00 копеек**.

Срок оказания услуг определен в договоре и составляет **10 рабочих дней**.



С уважением,
Александр Келлерманн
Генеральный директор Комитета по информационной
и правовой безопасности
+7 (812)240-9297
<http://kpib.ru>





Комитет по информационной
и правовой безопасности

Справочная: +7 (812) 240-9297
(с 9:00 до 16:00 по Москве)
Интернет-приемная: kpib.ru
welcome@kpib.ru

195112, Санкт-Петербург проспект
Энергетиков, дом 3, литера А, пом. 301



МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ
И ТОРГОВЛИ РОССИЙСКОЙ ФЕДЕРАЦИИ
**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО
ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И
МЕТРОЛОГИИ**
(Росстандарт)

Пресненская набережная, д. 10, стр. 2, Москва, 123112
Тел: (495) 547-51-51; факс: (495) 547-51-60
E-mail: info@rst.gov.ru
<http://www.rst.gov.ru>

ОКПО 00091089, ОГРН 1047706034232
ИНН/ КПП 7706406291/770301001

ООО «Комитет по информационной
и правовой безопасности»

195112, город Санкт-Петербург, пр-кт
Энергетиков, д. 3 литера А, помещ. 301

welcome@kpib.ru

08.06.2023 № 7253-ИК/03

На №

О регистрации системы добровольной
сертификации экспертов и организаций
в области защиты персональных данных
«Национальный центр информационной
безопасности»
(рег. РОСС RU.32827.04НЦИО
от 7 июня 2023 г.)

Управление стандартизации Федерального агентства по техническому регулированию и метрологии рассмотрело заявление ООО «Комитет по информационной и правовой безопасности» о регистрации системы добровольной сертификации экспертов и организаций в области защиты персональных данных «Национальный центр информационной безопасности» (далее – Система) и представленные к регистрации документы в соответствии с Административным регламентом предоставления Федеральным агентством по техническому регулированию и метрологии государственной услуги по ведению единого реестра зарегистрированных систем добровольной сертификации (далее – Единый реестр), утвержденным приказом Минпромторга России от 10 октября 2012 г. № 1440, и сообщает: Система зарегистрирована в Едином реестре 7 июня 2023 г., регистрационный № РОСС RU.32827.04НЦИО.

Дополнительно уведомляем, что регистрация системы добровольной сертификации в соответствии с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» не заменяет аккредитации, регулируемой Федеральным законом от 28 декабря 2013 г. № 412-ФЗ «Об аккредитации в национальной системе аккредитации». Одновременно Росстандарт информирует, что функционирование системы добровольной сертификации экспертов и организаций в области защиты персональных данных «Национальный центр информационной безопасности» должно осуществляться в строгом соответствии с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

Начальник
Управления стандартизации

И.А.Киреева

М.А.Мартиросян
Тел. 8 (495)-547-51-52 (50-403)

Подлинник электронного документа, подписанного ЭП,
хранится в системе электронного документооборота
Федеральное агентство по техническому регулированию и
метрологии.

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 73D3C7C4AF1E708F9D072909A4DDF831
Кому выдан: Киреева Ирина Александровна
Действителен: с 20.12.2022 до 14.03.2024