

АКТ
определения уровня защищённости информационных систем
персональных данных, оценки вреда субъектам персональных данных
и подтверждения выполнения требований по их защите

г. Тула

«02» июня 2025 г.

Настоящий Акт составлен лицом, ответственным за организацию обработки персональных данных, — директором ООО «ЗАКОН.ГУРУ» Лутиковой Викторией Гароевной:

- во исполнение постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее — ПП № 1119) — в части определения уровня защищённости и подтверждения выполнения требований;
- во исполнение пункта 5 части 1 статьи 18.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее — Закон) и требований к оценке вреда, утверждённых приказом Роскомнадзора от 27 октября 2022 года № 178 (далее — Требования № 178) — в части оценки вреда;
- во исполнение пункта 6 Приказа Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее — Приказ № 21) — в части оценки эффективности принятых мер защиты.

Часть I. Определение уровня защищённости

1. Сведения об информационной системе персональных данных

Параметр	Значение
Категория обрабатываемых ПД	Иные категории ПД (не специальные, не биометрические): ФИО, контактные данные, паспортные данные, СНИЛС, ИНН, сведения об образовании и занятости
Специальные категории ПД	Не обрабатываются
Биометрические ПД	Не обрабатываются
Субъекты ПД	Физические лица, не являющиеся сотрудниками Оператора (слушатели, контрагенты, участники

	мероприятий), а также сотрудники Оператора
Количество субъектов ПД (не сотрудники)	Менее 100 000 человек
Трансграничная передача	Отсутствует

2. Определение типа актуальных угроз (пункты 6–7 ПП № 1119)

Тип угроз	Актуальность	Обоснование
Угрозы 1-го типа — связанные с недокументированными возможностями в системном ПО	Не актуальны	Оператор не располагает сведениями о наличии таких угроз в используемом ПО
Угрозы 2-го типа — связанные с недокументированными возможностями в прикладном ПО	Не актуальны	Оператор использует лицензионное ПО, не имеет оснований полагать наличие в нём недокументированных возможностей
Угрозы 3-го типа — не связанные с недокументированными возможностями в ПО	Актуальны	Основные риски: несанкционированный доступ к данным по сети, ошибки персонала, утеря носителей

3. Определение уровня защищённости

На основании подпункта «б» пункта 12 ПП № 1119: при угрозах 3-го типа, обработке иных категорий ПД субъектов — не сотрудников Оператора — в количестве менее 100 000 человек — устанавливается 4-й (четвёртый) уровень защищённости.

Часть II. Оценка вреда субъектам персональных данных

4. Проверка факторов высокой степени вреда (подпункт 2.1 Требований № 178)

Фактор	Присутствует	Обоснование
Обработка биометрических ПД	Нет	Не осуществляется
Обработка специальных категорий ПД	Нет	Не осуществляется
Обработка ПД несовершеннолетних для заключения договоров	Нет	Программы ДПО предназначены для совершеннолетних специалистов
Обезличивание ПД в целях	Нет	Не осуществляется

скоринга или иных исследований		
Поручение иностранному лицу обрабатывать ПД граждан РФ	Нет	Обработка осуществляется исключительно директором Оператора на территории РФ
Сбор ПД с использованием баз данных за пределами РФ	Нет	Хостинг и базы данных расположены на территории РФ

5. Проверка факторов средней степени вреда (подпункт 2.2 Требований № 178)

Фактор	Присутствует	Обоснование
Распространение ПД на сайте или предоставление неограниченному кругу лиц	Нет	ПД субъектов на сайтах не публикуются
Обработка ПД в целях, отличных от первоначальной цели сбора	Нет	ПД обрабатываются строго в целях, для которых собраны
Продвижение услуг с использованием баз ПД иного оператора	Нет	Оператор использует только собственную базу данных
Получение согласия через сайт без последующей идентификации субъекта	Не применяется	Согласие оформляется исключительно при заключении договора в письменной форме
Согласие, содержащее право обрабатывать ПД в несовместимых целях	Нет	Согласия содержат строго определённые, совместимые цели

6. Проверка факторов низкой степени вреда (подпункт 2.3 Требований № 178)

Фактор	Присутствует	Обоснование
Ведение общедоступных источников ПД (статья 8 Закона)	Нет	Оператор не создаёт общедоступных источников ПД
Назначение ответственным лица, не являющегося штатным сотрудником	Нет	Ответственным назначен директор — штатный работник Оператора

7. Вывод по оценке вреда

Ни один из факторов высокой и средней степени вреда, предусмотренных подпунктами 2.1 и 2.2 пункта 2 Требований № 178, в деятельности Оператора

не выявлен. В соответствии с пунктом 6 Требований № 178 применяется наиболее высокая из выявленных степеней.

УСТАНОВИТЬ: степень вреда — НИЗКАЯ.

**Часть III. Выполнение требований 4-го уровня защищённости
(пункт 13 ПП № 1119)**

Требование (подпункт п. 13)	Фактическое состояние	Вывод
а) Организация режима безопасности помещений, препятствующего неконтролируемому проникновению посторонних лиц	Офис закрывается на ключ. Доступ посторонних лиц в помещение, где размещены ИСПД, ограничен. Ключи хранятся у директора.	Выполнено
б) Обеспечение сохранности носителей персональных данных	Бумажные документы хранятся в запираемых шкафах. Рабочая станция директора защищена паролем на вход в ОС и блокировкой экрана.	Выполнено
в) Утверждение перечня лиц, имеющих доступ к персональным данным	Доступ к ИСПД имеет исключительно директор ООО «ЗАКОН.ГУРУ». Перечень лиц, имеющих доступ к персональным данным, определён приказом директора.	Выполнено
г) Использование СЗИ при необходимости для нейтрализации актуальных угроз	Применяются: Windows Defender с автообновлением баз; шифрование HTTPS при передаче данных; автообновление ОС.	Выполнено

**Часть IV. Оценка эффективности мер защиты
(Приложение к Приказу № 21)**

Базовый набор мер адаптирован в соответствии с пунктом 9 Приказа № 21 с учётом структурно-функциональных характеристик ИСПД. Меры, связанные с информационными технологиями, не используемыми в ИСПД (виртуализация, беспроводные сети, мобильные устройства), исключены из базового набора.

Код меры	Содержание меры	Фактическое состояние	Вывод
ИАФ.1	Идентификация и аутентификация пользователей —	Доступ к рабочей станции, СДО и почте — по логину и паролю.	Выполнено

	работников оператора		
ИАФ.3	Управление идентификаторами	Учётные записи созданы только для директора. Учётные записи посторонних на рабочей станции отсутствуют.	Выполнено
ИАФ.4	Управление средствами аутентификации	Пароль устанавливается при создании учётной записи; при необходимости производится смена.	Выполнено
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Поле ввода пароля скрывает символы средствами ОС и веб-браузера.	Выполнено
ИАФ.6	Идентификация и аутентификация внешних пользователей	Слушатели получают персональные учётные записи в СДО.	Выполнено
УПД.1	Управление учётными записями пользователей	Учётные записи в СДО создаются и удаляются директором.	Выполнено
УПД.2	Реализация методов разграничения доступа	Директор — полный доступ; слушатели — доступ только к своим материалам в СДО.	Выполнено
УПД.5	Назначение минимально необходимых прав	Слушателям назначены минимальные права в СДО.	Выполнено
УПД.10	Блокирование сеанса после бездействия	На рабочей станции включена блокировка экрана по бездействию.	Выполнено
УПД.13	Защищённый удалённый доступ через внешние сети	Доступ к СДО и почте — через веб-интерфейс по протоколу HTTPS.	Выполнено
АВЗ.1	Реализация антивирусной защиты	На рабочей станции установлен и включён Windows Defender.	Выполнено
АВЗ.2	Обновление баз данных признаков вредоносных программ	Обновление баз Windows Defender — автоматически.	Выполнено
АНЗ.2	Контроль установки обновлений ПО	Автообновление ОС включено.	Выполнено
РСБ.1–3,	Регистрация и защита	Журнал событий	Выполнено

РСБ.7	событий безопасности	безопасности ведётся средствами ОС рабочей станции директора. Доступ к журналу — только у директора.	
ЗТС.3	Контроль физического доступа к техническим средствам	Рабочая станция размещена в офисе с ограниченным доступом.	Выполнено
ЗТС.4	Размещение устройств отображения информации	Монитор ориентирован так, чтобы исключить просмотр ПД посторонними.	Выполнено
ЗИС.3	Защита ПД при передаче по каналам связи	Все передачи через интернет (СДО, почта) — по протоколу HTTPS.	Выполнено
ЗНИ.8 (адаптировано)	Уничтожение ПД на носителях при передаче или утилизации	Бумажные носители с персональными данными уничтожаются способом, исключающим возможность восстановления персональных данных, с составлением акта уничтожения.	Выполнено

Часть V. Общие выводы

1. Установить уровень защищённости ИСПД — 4-й (четвёртый) (подпункт «б» пункта 12 ПП № 1119).
2. Установить степень вреда субъектам персональных данных — НИЗКАЯ (пункт 2 Требований № 178).
3. Все четыре требования 4-го уровня защищённости, предусмотренные пунктом 13 ПП № 1119, выполнены в полном объёме.
4. Базовый набор мер для 4-го уровня защищённости (Приложение к Приказу № 21) реализован применительно к структурно-функциональным характеристикам ИСПД. Нарушений не выявлено.
5. Следующее плановое обследование провести не позднее чем через 3 года с даты настоящего акта (пункт 17 ПП № 1119, пункт 6 Приказа № 21).

Лицо, ответственное за организацию обработки персональных данных,

директор ООО «ЗАКОН.ГУРУ»: _____ / Лутикова В.Г. /



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 02D11A8D00DBB2579C4D76098EE40514D3
Владелец: ЛУТИКОВА ВИКТОРИЯ ГАРОВНА
Действителен: с 12.05.2025 до 12.08.2026