АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ «ОПЕРАТОР ГРАНТОВ ПО РАЗВИТИЮ ГРАЖДАНСКОГО ОБЩЕСТВА»

Ленина ул., 54, г. Майкоп, 385000
тел. 8 (8772) 52-78-19,
e-mail: nko01@adygheya.gov.ru

ФЕДЭХЭКЫПЭУ ЩЫМЫТ ХЭУШЪХЬАФЫКІЫГЪЭ ОРГАНИЗАЦИЕУ «ГРАЖДАНСКЭ ОБЩЕСТВЭМ ИХЭХЪОНЫГЪЭ ТЕГЪЭПСЫХЬЭГЪЭ ГРАНТХЭР ЗЫГОЩЫРЭ ОПЕРАТОР»

Ленин иур., 54, къ. Мыекъуапэ, 385000
тел. 8 (8772) 52-78-19,
e-mail: nko01@adygheya.gov.ru

ПРИКАЗ

«23» 03 2026г. № 9

г. Майкоп

О некоторых вопросах обработки персональных данных

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»,

приказываю:

1. Утвердить:

1.1. Политику Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества» в отношении обработки персональных данных, согласно приложению № 1 к настоящему приказу;

1.2. Положение о защите, хранении, обработке и передаче персональных данных работников Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества», согласно приложению № 2 к настоящему приказу;

1.3. Положение о работе с персональными данными работников Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества», согласно приложению № 3 к настоящему приказу

1.4. Форму согласия субъекта на обработку персональных данных, согласно приложению № 4 к настоящему приказу;

1.5. Форму обязательства о неразглашении персональных данных работников АНО «Оператор грантов по развитию гражданского общества», согласно приложению № 5 к настоящему приказу;

1.6. Меры по обеспечению безопасности автоматизированного рабочего места пользовательского сегмента Государственной информационной системы Республики Адыгея «Система электронного делопроизводства и документооборота «Дело» (вид 2) Автономной

некоммерческой организации «Оператор грантов по развитию гражданского общества, согласно приложению № 6 к настоящему приказу.

2. Контроль за исполнением настоящего приказа возложить на руководителя группы правового обеспечения, кадровой работы и делопроизводства Гонежук Заиру Нурбиевну.

Директор А.А. Бегеретов

Приложение № 1
к Приказу АНО «Оператор грантов по развитию гражданского общества «О персональных данных»
от 23.03 2026 № 9

Политика Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества» в отношении обработки персональных данных

1. Общие положения

1.1. Политика Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества» (оператор) в отношении обработки персональных данных (далее - Политика) разработана в целях обеспечения защиты прав и свобод субъекта персональных данных при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Основные понятия, используемые в Политике:

- **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- **оператор персональных данных (оператор)** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.3. Оператор, получивший доступ к персональным данным, обязан соблюдать конфиденциальность персональных данных - не раскрывать третьим лицам и не

распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.4. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные па основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных);
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Закона о персональных данных;
- иные сведения, предусмотренные Законом о персональных данных или другими федеральными законами.

1.5. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

1.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

1.7. Оператор персональных данных вправе:

- отстаивать свои интересы в суде;
- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;
- использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством.

1.8. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Закона о персональных данных.

1.9. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных,

находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Закона о персональных данных.

2. Цели сбора персональных данных

2.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2. Цели обработки персональных данных происходят в том числе из анализа правовых актов, регламентирующих деятельность оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных информационных системах персональных данных (по структурным подразделениям оператора и их процедурам в отношении определенных категорий субъектов персональных данных).

2.3. К целям обработки персональных данных оператора относятся:

- заключение, исполнение и прекращение гражданско-правовых договоров;
- организация кадрового учета организации, обеспечение соблюдения законов, заключение и исполнение обязательств по трудовым и гражданско-правовым договорам;
- ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, пользовании льготами;
- исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц, взносов во внебюджетные фонды и страховых взносов во внебюджетные фонды, пенсионного законодательства при формировании и передаче в СФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование;
- заполнение первичной статистической документации в соответствии с трудовым, налоговым законодательством и иными федеральными законами.

3. Правовые основания обработки персональных данных

3.1. Правовым основанием обработки персональных данных являются:

- совокупность правовых актов, во исполнение которых и в соответствии с которыми оператор осуществляет обработку персональных данных: Конституция Российской Федерации; статьи 86-90 Трудового кодекса Российской Федерации, (**федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью оператора**);
- уставные документы оператора;
- договоры, заключаемые между оператором и субъектом персональных данных;
- согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям оператора).

4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

4.1. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.2. Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Закона о персональных данных, при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

4.3. К категориям субъектов персональных данных относятся:

4.3.1. Работники оператора, бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников.

В данной категории субъектов оператором обрабатываются персональные данные:

- в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества:

Категория персональных данных	Перечень персональных данных	Способ обработки	Срок обработки и хранения
только общие персональные данные	- фамилия, имя, отчество; - пол; - гражданство; - дата и место рождения; - адрес места проживания; - сведения о регистрации по месту жительства или пребывания;	сбор, хранение, удаление, уничтожение	до 3 лет с согласия субъекта

	- номера телефонов (домашний, мобильный, рабочий); - адрес электронной почты; - замещаемая должность; - сведения о трудовой деятельности; - идентификационный номер налогоплательщика; - данные документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа; - данные полиса обязательного медицинского страхования; - данные паспорта или иного удостоверяющего личность документа; - данные паспорта, удостоверяющего личность гражданина Российской Федерации за пределами территории Российской Федерации; - данные трудовой книжки, вкладыша в трудовую книжку; - сведения о воинском учете; - сведения об образовании; - сведения о получении дополнительного профессионального образования; - сведения о владении иностранными языками; - сведения об участии в управлении хозяйствующим субъектом (за исключением жилищного, жилищно-строительного, гаражного кооперативов, садоводческого, огороднического, дачного потребительских кооперативов, товарищества собственников недвижимости и профсоюза, зарегистрированного в установленном порядке), занятии предпринимательской деятельностью; - сведения о наградах, иных поощрениях и знаках отличия;		

	- сведения о дисциплинарных взысканиях; - сведения, содержащиеся в материалах служебных проверок; - сведения о семейном положении; - сведения о близких родственниках, свойственниках; - сведения, содержащиеся в справках о доходах, расходах, об имуществе и обязательствах имущественного характера; - номер расчетного счета; - информация об оформленных допусках к государственной тайне; - иное.		

4.3.2. Клиенты и контрагенты оператора (физические лица).

В данной категории субъектов оператором обрабатываются персональные данные, полученные оператором:

- в целях исполнения договора, стороной которого является субъект персональных данных:

Категория персональных данных	Перечень персональных данных	Способ обработки	Срок обработки и хранения
только общие персональные данные	- фамилия, имя, отчество; - пол; - гражданство; - дата и место рождения; - адрес места проживания; - сведения о регистрации по месту жительства или пребывания; - номера телефонов (домашний, мобильный, рабочий); - адрес электронной почты; - замещаемая должность; - идентификационный номер налогоплательщика; - данные паспорта или иного удостоверяющего личность документа; - сведения об участии в управлении хозяйствующим субъектом (за исключением жилищного, жилищно-	сбор, хранение, удаление, уничтожение	до 3 лет с согласия субъекта

	строительного, гаражного кооперативов, садоводческого, огороднического, дачного потребительских кооперативов, товарищества собственников недвижимости и профсоюза, зарегистрированного в установленном порядке), занятии предпринимательской деятельностью; - номер расчетного счета; - иное.		

4.3.3. Представители/работники клиентов и контрагентов оператора (юридических лиц).

В данной категории субъектов оператором обрабатываются персональные данные, полученные оператором:

- в целях исполнения договора, стороной которого является клиент/контрагент (юридическое лицо):

Категория персональных данных	Перечень персональных данных	Способ обработки	Срок обработки и хранения
только общие персональные данные	- фамилия, имя, отчество; - пол; - номера телефонов (домашний, мобильный, рабочий); - адрес электронной почты; - замещаемая должность; - данные паспорта или иного удостоверяющего личность документа; - сведения об участии в управлении хозяйствующим субъектом (за исключением жилищного, жилищно-строительного, гаражного кооперативов, садоводческого, огороднического, дачного потребительских кооперативов, товарищества собственников недвижимости и профсоюза, зарегистрированного в установленном порядке), занятии предпринимательской деятельностью; - иное.	сбор, хранение, удаление, уничтожение	до 3 лет с согласия субъекта

4.4. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается:

- в случае, если субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

- в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации.

5. Порядок и условия обработки персональных данных

5.1. Оператор осуществляет обработку персональных данных - операции, совершаемые с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.2. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Законом о персональных данных.

5.3. Обработка персональных данных оператором ограничивается достижением конкретных, заранее определенных и законных целей. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

5.4. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.5. При осуществлении хранения персональных данных оператор персональных данных обязан использовать базы данных, находящиеся на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Закона о персональных данных.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков). При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

5.6. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

5.7. Оператор вправе поручить обработку персональных данных другому лицу на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных.

Кроме того, оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

5.8. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

5.9. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами. Состав и перечень мер оператор определяет самостоятельно.

5.10. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6. Порядок и условия обработки биометрических персональных данных

6.1. К биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

6.2. Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, связанных с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

6.3. Предоставление биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных пунктом 6.2 настоящей Политики. Оператор не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на обработку персональных данных, если в соответствии с федеральным законом получение оператором согласия на обработку персональных данных не является обязательным.

6.4. Обработка биометрических персональных данных осуществляется оператором в соответствии с требованиями к защите биометрических персональных данных, установленными в соответствии со статьей 19 Закона о персональных данных.

6.5. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

6.6. Под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность.

6.7. Оператор утверждает порядок передачи материальных носителей уполномоченным лицам.

6.8. Материальный носитель должен использоваться в течение срока, установленного оператором, осуществившим запись биометрических персональных данных на материальный носитель, но не более срока эксплуатации, установленного изготовителем материального носителя.

6.9. Оператор обязан:

- осуществлять учет количества экземпляров материальных носителей;
- осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

6.10. Технологии хранения биометрических персональных данных вне информационных систем персональных данных должны обеспечивать:

- доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц;
- применение средств электронной подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;
- проверку наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством Российской Федерации в сфере отношений, связанных с обработкой персональных данных.

6.11. При хранении биометрических персональных данных вне информационных систем персональных данных должна обеспечиваться регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных.

7. Обезличивание персональных данных при получении требования о предоставлении персональных данных, полученных в результате обезличивания персональных данных

7.1. При получении требования о предоставлении персональных данных, полученных в результате обезличивания персональных данных, оператор обезличивает обрабатываемые им персональные данные в соответствии с требованиями к обезличиванию персональных данных, методами обезличивания персональных данных и порядком обезличивания персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 августа 2025 г. № 1154.

7.2. При обезличивании персональных данных оператор обеспечивает:

- соблюдение Правил обезличивания персональных данных и методов обезличивания персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 августа 2025 г. № 1154;

- раздельное хранение персональных данных и обезличенных данных;

- принятие мер по обеспечению безопасности обезличенных данных в соответствии с Законом о персональных данных;

- исключение из обезличенных данных информации, доступ к которой ограничен федеральными законами;

- использование алгоритмов и программы для электронных вычислительных машин для обезличивания персональных данных, обеспечивающих возможность предоставления обезличенных данных из информационной системы оператора в государственную информационную систему Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, указанную в статье 13^1 Закона о персональных данных, без потери таких данных и (или) их изменения;

- возможность внесения изменений и дополнений в обезличенные данные, поддержку актуальности обезличенных данных и возможность повторного применения методов обезличивания персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 августа 2025 г. № 1154, без возможности преобразования обезличенных данных к исходному виду, позволяющему определить их принадлежность конкретному субъекту персональных данных, а также целостность массива обезличенных данных и их соответствие требованию о предоставлении обезличенных данных.

7.3. Выполнение оператором требований к обезличиванию должно исключить наличие в персональных данных, полученных в результате обезличивания, информации, доступ к которой ограничен федеральными законами.

7.4. Оператор в соответствии с требованием о предоставлении персональных данных, полученных в результате обезличивания персональных данных, предоставляет персональные данные, полученные в результате обезличивания персональных данных, в государственную информационную систему уполномоченного органа в сфере регулирования информационных технологий в порядке, установленном Правительством Российской Федерации по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

8. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

8.1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Закона о персональных данных, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта

персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

8.2. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

8.3. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

8.4. Оператор обязан прекратить обработку персональных данных или обеспечить прекращение обработки персональных данных лицом, действующим по поручению оператора:

- в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, в срок, не превышающий трех рабочих дней с даты этого выявления;

- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных;

- в случае достижения цели обработки персональных данных и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8.5. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с

уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

8.6. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор в срок, не превышающий десяти рабочих дней с даты получения им соответствующего требования, обязан прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных Законом о персональных данных.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

8.7. После истечения срока нормативного хранения документов, содержащих персональные данные субъекта, или при наступлении иных законных оснований документы подлежат уничтожению.

8.8. Оператор для этих целей создает экспертную комиссию и проводит экспертизу ценности документов.

8.9. По результатам экспертизы документы, содержащие персональные данные субъекта и подлежащие уничтожению:

- на бумажном носителе - уничтожаются путем сжигания;

- в электронном виде - стираются с информационных носителей либо физически уничтожаются сами носители, на которых хранится информация.

8.10. В случае если обработка персональных данных осуществлялась оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

8.11. В случае если обработка персональных данных осуществлялась оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных.

Приложение № 2
к Приказу АНО «Оператор грантов по развитию гражданского общества
«О персональных данных»
от 23.03. 2026 № 9

Положение
о защите, хранении, обработке и передаче персональных данных работников Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества»

1. Общие положения

1.1.Настоящее положение разработано в соответствии с положениями Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных) и определяет порядок сбора, учета, обработки, накопления, использования, распространения и хранения персональных данных работников Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества» (далее - организация, работодатель).

1.2. Целью настоящего положения является обеспечение защиты персональных данных работников организации от несанкционированного доступа и разглашения.

1.3. В целях настоящего положения под персональными данными понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных.

1.4. К персональным данным относятся:

- фамилия, имя, отчество;
- дата и место рождения;
- гражданство;
- сведения о знании иностранных языков;
- данные об образовании (наименование учебного заведения, год окончания, документ об образовании, квалификация, специальность);
- профессия;
- стаж работы (общий, непрерывный, дающий право на выслугу лет);
- семейное положение;
- данные о членах семьи (степень родства, Ф. И. О., год рождения, паспортные данные, включая прописку и место рождения);
- паспорт (номер, дата выдачи, кем выдан);
- адрес места жительства (по паспорту, фактический), дата регистрации по месту жительства;
- номер телефона (домашний, сотовый);
- сведения о воинском учёте;
- сведения о состоянии здоровья работника, необходимые работодателю для определения пригодности для выполнения поручаемой работы и предупреждения профессиональных заболеваний, предусмотренные действующим законодательством Российской Федерации;

- содержание заключенного с работником контракта или трудового договора;

- сведения об аттестации, повышении квалификации, профессиональной переподготовке работника;

- сведения об использованных отпусках;

- сведения об имеющихся наградах (поощрениях), почётных званиях;

- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;

- сведения об идентификационном номере налогоплательщика;

- сведения о социальных льготах (в соответствии с действующим законодательством Российской Федерации);

- данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения);

- иные сведения, необходимые работодателю в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

1.5. Все персональные данные работника работодатель может получить только от него самого. В случаях когда работодатель может получить необходимые персональные данные работника только у третьего лица, работодатель в обязательном порядке уведомляет об этом работника и получает от него письменное согласие.

1.6. Работодатель в обязательном порядке сообщает работнику о целях, способах и источниках получения персональных данных, а также о перечне подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение.

1.7. При изменении персональных данных работник письменно уведомляет работодателя о таких изменениях в срок, не превышающий 7 календарных дней

1.8. Персональные данные работника являются конфиденциальной информацией и не могут быть использованы работодателем или любым иным лицом в личных целях.

1.9. При определении объема и содержания персональных данных работника работодатель руководствуется настоящим положением, Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

1.10. Работодатель, работник и его представители совместно разрабатывают меры защиты персональных данных работника.

1.11. Работник не должен отказываться от своих прав на сохранение и защиту тайны.

2. Обработка, передача и хранение персональных данных работника

2.1. Обработка персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества работодателя.

2.8. Работодатель при обработке персональных данных работника на бумажных носителях в целях обеспечения их защиты:

- назначает должностное лицо (работника), ответственного за обработку персональных данных;

- ограничивает допуск в помещения, в которых хранятся документы, содержащие персональные данные работников.

2.9. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда работодателя.

2.10. Работники отдела кадров, бухгалтерии и службы охраны труда работодателя, допущенные к персональным данным работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников не допускаются.

2.11. Руководитель отдела кадров вправе передавать персональные данные работника в бухгалтерию организации в случаях, установленных законодательством, необходимых для исполнения обязанностей работников бухгалтерии.

2.12. Руководитель организации может передавать персональные данные работника третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных законодательством.

2.13. При передаче персональных данных работника руководитель отдела кадров и руководитель организации предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требуют от этих лиц письменное подтверждение соблюдения этого условия.

2.14. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных работника, определяются должностными инструкциями.

2.15. Все сведения о передаче персональных данных работника учитываются для контроля правомерности использования данной информации лицами, ее получившими.

2.16. Руководитель отдела кадров обязан предоставлять персональную информацию в Фонд пенсионного и социального страхования Российской Федерации, фонд обязательного медицинского страхования (ФОМС), по форме, в порядке и объеме, установленных законодательством Российской Федерации.

2.17. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.18. Передача информации, содержащей сведения о персональных данных работников, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

2.19. Персональные данные работника хранятся в отделе кадров, в сейфе на бумажных носителях: трудовая книжка, личная карточка, личное дело и на электронных носителях с ограниченным доступом.

Право доступа к персональным данным работника имеют:

- руководитель организации;
- руководитель отдела кадров организации;
- сотрудники отдела кадров;
- сотрудники службы охраны труда.

3. Требования к помещениям, в которых производится обработка персональных данных

3.1. Размещение оборудования информационных систем персональных данных, специального оборудования и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

3.2. Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных

данных, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

3.3. Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, реализуются дополнительные требования, определяемые методическими документами Федеральной службы безопасности России.

4. Права работника на защиту его персональных данных

4.1. Работник в целях обеспечения защиты своих персональных данных, хранящихся у работодателя, имеет право:

- получать полную информацию о своих персональных данных, их обработке, хранении и передаче;

- определять своих представителей для защиты своих персональных данных;

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушениями настоящего положения и законодательства Российской Федерации.

При отказе работодателя исключить или исправить персональные данные работника работник вправе заявить работодателю в письменном виде о своем несогласии с соответствующим обоснованием;

- требовать от работодателя извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

4.2. Если работник считает, что работодатель осуществляет обработку его персональных данных с нарушением требований Закона о персональных данных или иным образом нарушает его права и свободы, работник вправе обжаловать действия или бездействие работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

5. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

5.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

5.2. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Законом о персональных данных, а также требований к защите персональных данных, установленных в соответствии с названным Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

6. Заключительные положения

6.1. Настоящее положение вступает в силу с момента его утверждения.

6.2. Работодатель обеспечивает неограниченный доступ к настоящему документу.

6.3. Настоящее положение доводится до сведения всех работников персонально под роспись.

С положением ознакомлены:

№ п/п	Ф. И. О. работника	Дата	Подпись
1	2	3	4
	Белоусов Н.А.	23.03.26 г.	[signature]
	Гончарук З.Н.	23.03.26 г.	[signature]
	Кузнецова С.В.	23.03.26 г.	[signature]
	Гусаев А.А.	23.03.26 г.	[signature]

Приложение № 3
к Приказу АНО «Оператор грантов по развитию гражданского общества «О персональных данных»
от 23.03. 2026 № 9

Положение
о работе с персональными данными работников Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества»

1. Общие положения

1.1. Настоящее положение регулирует отношения, связанные с обработкой персональных данных, включающие в себя производимые АНО «Оператор грантов по развитию гражданского общества» (далее - организация, работодатель) действия по получению, обработке, хранению, передаче персональных данных работников или иному их использованию, с целью защиты персональных данных работников от несанкционированного доступа, а также неправомерного их использования и утраты.

1.2. Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных) и иными нормативно-правовыми актами в области обработки и защиты персональных данных.

2. Понятие и состав персональных данных

2.1. В целях настоящего положения под персональными данными понимается любая информация, прямо или косвенно относящаяся к работнику.

2.2. При заключении трудового договора лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку и (или) сведения о трудовой деятельности, за исключением случаев, если трудовой договор заключается впервые;
- документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании и (или) о квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);
- справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию);

- справку о том, является или не является лицо подвергнутым административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ (при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, подвергнутые административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ, до окончания срока, в течение которого лицо считается подвергнутым административному наказанию).

В отдельных случаях с учетом специфики работы может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

2.3. Запрещается требовать от лица, поступающего на работу, документы, помимо предусмотренных Трудовым кодексом Российской Федерации, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

2.4. К персональным данным работника относятся:

- анкетные и биографические данные;
- паспортные данные;
- страховой номер индивидуального лицевого счета;
- идентификационный номер налогоплательщика;
- номер полиса обязательного медицинского страхования;
- сведения о воинском учете;
- специальность и занимаемая должность;
- сведения о заработной плате;
- сведения о социальных льготах;
- адрес места жительства, контактный телефон;
- содержание трудового договора;
- приказы по личному составу;
- личное дело и трудовая книжка.

2.5. Указанные сведения и документы являются конфиденциальными. Работодатель как оператор персональных данных не вправе распространять персональные данные без согласия работника, если иное не предусмотрено федеральным законом.

3. Обработка персональных данных работника и гарантии их защиты

3.1. Под обработкой персональных данных понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

- обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и

продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;

- все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

- работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных настоящим Кодексом и другими федеральными законами;

- работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

- при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.3. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном Трудовым кодексом Российской Федерации, иными федеральными законами и настоящим положением.

3.4. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.5. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

3.6. Работодатель, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

3.7. Работодатель при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.8. Работодатель осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике работодателя в отношении обработки персональных данных, настоящему положению.

3.9. Работодатель знакомит работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику работодателя в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучает указанных работников.

3.10. Работодатель обеспечивает безопасность персональных данных работников следующими способами:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

- применением для уничтожения персональных данных, прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, в составе которых реализована функция уничтожения информации;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учетом машинных носителей персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3.11. Работодатель обрабатывает без использования средств автоматизации следующие категории персональных данных работника, обеспечивает их защиту, которые хранятся на бумажных носителях:

Цель обработки персональных данных: ведение кадрового и бухгалтерского учета, обеспечение соблюдения трудового законодательства РФ.

Категория персональных данных	Перечень персональных данных	Категория работников	Срок обработки и хранения
только общие персональные данные	- фамилия, имя, отчество; - год, месяц, дата рождения; - место рождения;	все работники	3 года с согласия

	- адрес; - семейное положение; - образование; - профессия; - социальное положение; - доходы.		физического лица

3.17. Работодатель при обработке персональных данных работника на бумажных носителях в целях обеспечения их защиты:

- назначает должностное лицо (работника), ответственного за обработку персональных данных;

- ограничивает допуск в помещения, в которых хранятся документы, содержащие персональные данные работников.

3.18. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда работодателя.

3.19. Работники отдела кадров, бухгалтерии и службы охраны труда работодателя, допущенные к персональным данным работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников не допускаются.

3.20. Персональные данные работника хранятся в отделе кадров, в сейфе на бумажных носителях: трудовая книжка, личная карточка, личное дело и на электронных носителях с ограниченным доступом.

Право доступа к персональным данным работника имеют:

- руководитель организации;
- руководитель отдела кадров организации;
- сотрудники отдела кадров;
- сотрудники службы охраны труда.

4. Передача персональных данных работника

4.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности);

- осуществлять передачу персональных данных работника в пределах организации в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только

те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.2. Все сведения о передаче персональных данных работника учитываются для контроля правомерности использования данной информации лицами, ее получившими.

4.3. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

4.4. Передача информации, содержащей сведения о персональных данных работников, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

4.5. Согласие на обработку персональных данных, разрешенных работником для распространения, оформляется отдельно от иных согласий работника на обработку его персональных данных. Работодатель обеспечивает работнику возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных этим работником для распространения.

4.6. В согласии на обработку персональных данных, разрешенных работником для распространения, он вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных работодателем неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

4.7. Передача (распространение, предоставление, доступ) персональных данных, разрешенных работником для распространения, должна быть прекращена в любое время по его требованию. Указанные в данном требовании персональные данные могут обрабатываться только работодателем.

5. Обезличивание персональных данных при получении требования о предоставлении персональных данных, полученных в результате обезличивания персональных данных

5.1. При получении требования о предоставлении персональных данных, полученных в результате обезличивания персональных данных, работодатель обезличивает обрабатываемые им персональные данные в соответствии с требованиями к обезличиванию персональных данных, методами обезличивания персональных данных и порядком обезличивания персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 августа 2025 г. № 1154.

5.2. При обезличивании персональных данных работодатель обеспечивает:

- соблюдение Правил обезличивания персональных данных и методов обезличивания персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 августа 2025 г. № 1154;

- раздельное хранение персональных данных и обезличенных данных;

- принятие мер по обеспечению безопасности обезличенных данных в соответствии с Законом о персональных данных;

- исключение из обезличенных данных информации, доступ к которой ограничен федеральными законами;

- использование алгоритмов и программы для электронных вычислительных машин для обезличивания персональных данных, обеспечивающих возможность предоставления обезличенных данных из информационной системы работодателя в государственную информационную систему Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, указанную в статье 13^1 Закона о персональных данных, без потери таких данных и (или) их изменения;

- возможность внесения изменений и дополнений в обезличенные данные, поддержку актуальности обезличенных данных и возможность повторного применения методов обезличивания персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 августа 2025 г. № 1154, без возможности преобразования обезличенных данных к исходному виду, позволяющему определить их принадлежность конкретному работнику, а также целостность массива обезличенных данных и их соответствие требованию о предоставлении обезличенных данных.

5.3. Выполнение работодателем требований к обезличиванию должно исключить наличие в персональных данных, полученных в результате обезличивания, информации, доступ к которой ограничен федеральными законами.

5.4. Работодатель в соответствии с требованием о предоставлении персональных данных, полученных в результате обезличивания персональных данных, предоставляет персональные данные, полученные в результате обезличивания персональных данных, в государственную информационную систему уполномоченного органа в сфере регулирования информационных технологий в порядке, установленном Правительством Российской Федерации по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

6. Порядок уничтожения персональных данных

6.1. В случае выявления неправомерной обработки персональных данных при обращении работника или его представителя либо по запросу работника или его представителя (далее - обращение работника) либо уполномоченного органа по защите прав субъектов персональных данных (далее - уполномоченный орган) работодатель осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому работнику, с момента такого обращения или получения указанного запроса на период проверки.

6.2. В случае выявления неточных персональных данных при обращении работника или по запросу уполномоченного органа работодатель осуществляет блокирование персональных данных, относящихся к этому работнику, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы работника, или третьих лиц.

6.3. В случае подтверждения факта неточности персональных данных работодатель на основании сведений, представленных работником либо уполномоченным органом, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.4. В случае выявления неправомерной обработки персональных данных, осуществляемой работодателем, работодатель в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

6.5. В случае если обеспечить правомерность обработки персональных данных невозможно, работодатель в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

6.6. Об устранении допущенных нарушений или об уничтожении персональных данных работодатель уведомляет работника, а также уполномоченный орган, если запрос был направлен этим органом.

6.7. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав работника, работодатель с момента выявления им такого инцидента, уполномоченным органом или иным заинтересованным лицом уведомляет уполномоченный орган:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав работника, и предполагаемом вреде, нанесенном правам работника, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном работодателем на взаимодействие с уполномоченным органом, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

6.8. В случае достижения цели обработки персональных данных работодатель прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

6.9. В случае отзыва работником согласия на обработку его персональных данных работодатель прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

6.10. В случае обращения работника к работодателю с требованием о прекращении обработки персональных данных работодатель в срок, не превышающий десяти рабочих дней с даты получения им соответствующего требования, прекращает их обработку, за исключением случаев, предусмотренных Законом о персональных данных.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления работодателем в адрес работника мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.11. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.4-6.10 настоящего положения, работодатель

осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.12. Работодатель уведомляет Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав работников, в порядке, утвержденном приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2022 г. № 187.

6.13. Работодатель передает в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, информацию о компьютерных инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных, в порядке, установленном совместно с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и уполномоченным органом.

6.14. После истечения срока нормативного хранения документов, содержащих персональные данные работников, или при наступлении иных законных оснований документы подлежат уничтожению.

6.15. Работодатель для этих целей создает экспертную комиссию и проводит экспертизу ценности документов.

6.16. По результатам экспертизы документы, содержащие персональные данные работника и подлежащие уничтожению:

- на бумажном носителе - уничтожаются путем измельчения в шредере или сжигания;

- в электронном виде - стираются с информационных носителей либо физически уничтожаются сами носители, на которых хранится информация.

6.17. В случае если обработка персональных данных осуществлялась работодателем без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных работников, является акт об уничтожении персональных данных.

6.18. В случае если обработка персональных данных осуществлялась работодателем с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных работников, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных.

7. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя

7.1. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

- полную информацию об их персональных данных и обработке этих данных, в том числе содержащую:

подтверждение факта обработки персональных данных работодателем;

правовые основания и цели обработки персональных данных;

цели и применяемые работодателем способы обработки персональных данных;

сроки обработки персональных данных, в том числе сроки их хранения;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

информацию о способах исполнения работодателем обязанностей при обработке персональных данных;

- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

- определение своих представителей для защиты своих персональных данных;

- доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

8.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

8.2. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Законом о персональных данных, а также требований к защите персональных данных, установленных в соответствии с названным Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

9. Заключительные положения

9.1. Настоящее положение вступает в силу с момента его утверждения.

9.2. Работодатель обеспечивает неограниченный доступ к настоящему документу.

9.3. Настоящее положение доводится до сведения всех работников персонально под подпись.

С положением ознакомлены:

№ п/п	Ф. И. О. работника	Дата	Подпись
1	2	3	4
	[illegible] А. А.	23.03.26	
	[illegible] З.Н.	23.03.26	
	[illegible] С.А.	23.03.26	
	[illegible] А.А.	23.03.26	

Приложение № 4
к Приказу АНО «Оператор грантов по развитию гражданского общества «О персональных данных»
от 23.03. 2026 № 9

Согласие субъекта на обработку персональных данных

Я, _____,
проживающий(ая) по адресу _____, основной документ, удостоверяющий личность (паспорт) серия_____ номер_____ дата выдачи _____, в лице моего представителя (если есть) _____, проживающего(ей) по адресу _____, основной документ, удостоверяющий личность (паспорт) серия_____ номер_____ дата выдачи _____, наименование выдавшего органа_____, действующего (ей) на основании _____, на основании статей 9, 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в целях ведение кадрового и бухгалтерского учета и обеспечения соблюдения трудового законодательства РФ даю свое согласие АНО «Оператор грантов по развитию гражданского общества» на автоматизированную, а также без использования средств автоматизации обработку своих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных.

Лицо, осуществляющее обработку персональных данных по поручению оператора - Руководитель группы правового обеспечения, кадровой работы и делопроизводства - ФИО.

Перечень персональных данных, на обработку которых дается согласие

N п/п	Персональные данные	Согласие	
		ДА	НЕТ
Общая информация			
	Фамилия		
	Имя		
	Отчество		
	Год, месяц, дата и место рождения		
	Адрес места жительства		
	Семейное положение		
	Социальное положение		
	Имущественное положение		
	Образование		
	Профессия		
	Другая информация		

Настоящее согласие действует 3 года.

Субъект персональных данных вправе отозвать данное согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные даняые или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев.

[подпись субъекта персональных данных]

[число, месяц, год]

Приложение № 5
к Приказу АНО «Оператор грантов по развитию гражданского общества «О персональных данных»
от 23.03. 2026 № 9

Обязательство
о неразглашении персональных данных работников АНО «Оператор грантов по развитию гражданского общества»

Я, _____,являясь работником АНО «Оператор грантов по развитию гражданского общества» и исполняющий(ая) обязанности по должности _____, понимаю, что получаю доступ к информации, содержащей персональные данные работников АНО «Оператор грантов по развитию гражданского общества», в частности к сведениям о (об):

- анкетных и биографических данных;
- паспортных данных;
- ИНН, СНИЛС;
- воинском учете;
- наличии судимостей;
- специальности и занимаемой должности;
- заработной плате;
- социальных льготах;
- адресе места жительства, контактном телефоне;
- содержании трудового договора;
- содержании приказов по личному составу;
- содержании личного дела и трудовой книжки;
- содержании отчетов, направляемых в органы статистики.

Я понимаю, что исполнение моих должностных обязанностей связано с обработкой персональных данных работников АНО «Оператор грантов по развитию гражданского общества», включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

При работе с персональными данными работников АНО «Оператор грантов по развитию гражданского общества» обязуюсь соблюдать требования Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Положения о работе с персональными данными работников АНО «Оператор грантов по развитию гражданского общества», а также иных нормативных правовых актов в области защиты персональных данных.

При передаче персональных данных работников АНО «Оператор грантов по развитию гражданского общества» обязуюсь соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами;

- осуществлять передачу персональных данных работника в пределах АНО «Оператор грантов по развитию гражданского общества» в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

До моего сведения также доведены (с разъяснениями) Положение о работе с персональными данными работников АНО «Оператор грантов по развитию гражданского общества», Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное постановлением Правительства РФ от 15 сентября 2008 г. № 687, Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства РФ от 1 ноября 2012 г. № 1119.

Я понимаю, что нарушение мной правил обработки персональных данных, установленных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Положением о работе с персональными данными работников АНО «Оператор грантов по развитию гражданского общества» а также требований к защите персональных данных, установленных в соответствии с названным Федеральным законом, приведет к нарушению прав работников АНО «Оператор грантов по развитию гражданского общества».

Я предупрежден(а) о том, что в случае нарушения положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работников, я могу быть привлечен к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлечен к гражданско-правовой,

административной и уголовной ответственности в порядке, установленном федеральными законами (статья 90 Трудового кодекса Российской Федерации).

[**должность, подпись, инициалы, фамилия**]

Дата:

Приложение № 6
к Приказу АНО «Оператор грантов по развитию гражданского общества «О персональных данных»
от 23 03. 2026 № 9

Описание мер по обеспечению безопасности автоматизированного рабочего места пользовательского сегмента Государственной информационной системы Республики Адыгея «Система электронного делопроизводства и документооборота «Дело» (вид 2) Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества

1. Общие положения

1.1 В соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» выбор мер по обеспечению безопасности информации, подлежащий реализации на автоматизированном рабочем месте (далее – АРМ) пользовательского сегмента Государственной информационной системы Республики Адыгея «Система электронного делопроизводства и документооборота «Дело» (вид 2) (далее – СЭД «Дело») Автономной некоммерческой организации «Оператор грантов по развитию гражданского общества (далее – Оператор грантов), включает:

1) определение базового набора мер по обеспечению безопасности информации для установленного класса защищенности в соответствии с базовыми наборами мер по обеспечению безопасности информации;

2) адаптацию базового набора мер по обеспечению безопасности информации с учетом структурно-функциональных характеристик АРМ СЭД «Дело», информационных технологий, особенностей функционирования АРМ (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми на абонентском пункте, или структурно-функциональными характеристиками, не свойственными ГИС СЭД «Дело»);

3) уточнение адаптированного базового набора мер по обеспечению безопасности информации с учетом не выбранных ранее мер, в результате чего определяются меры по обеспечению безопасности, направленные на нейтрализацию всех актуальных угроз безопасности для АРМ СЭД «Дело»;

4) дополнение уточненного адаптированного базового набора мер по обеспечению безопасности мерами, обеспечивающими выполнение требований к защите, установленными иными нормативными правовыми актами в области обеспечения безопасности информации и защиты информации.

1.2 Общий порядок определения мер по обеспечению безопасности информации для их реализации на АРМ СЭД «Дело» представлен на рисунке 1.

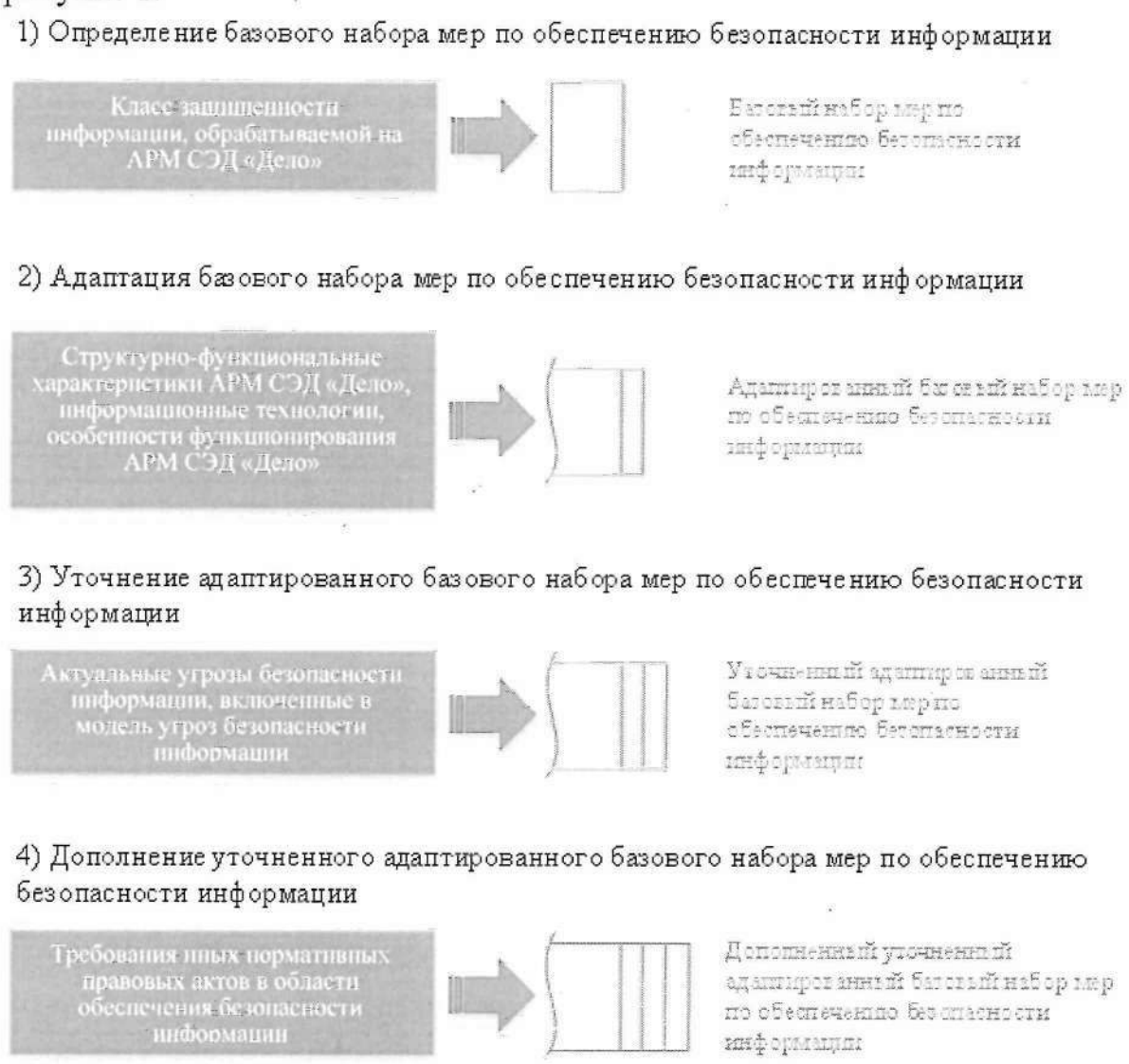

Рисунок 1 – Общий порядок определения мер по обеспечению безопасности информации для их реализации на АРМ СЭД «Дело»

1.3 При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности информации, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности.

2. Определение базового набора мер по обеспечению безопасности информации

2.1 Для установленного 3 класса защищенности АРМ СЭД «Дело», в базовый набор включены следующие меры:

- ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора;
- ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- ИАФ.5 Защита обратной связи при вводе аутентификационной информации;
- ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);
- УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей;
- УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
- УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- УПД.13 Реализация защищенного удаленного доступа к объектам доступа через внешние информационно-телекоммуникационные сети;

- УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа;

- УПД.15 Регламентация и контроль использования в информационной системе мобильных технических средств;

- УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);

- ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;

- ЗНИ.1 Учет машинных носителей информации;

- ЗНИ.2 Управление доступом к машинным носителям информации;

- ЗНИ.8 Уничтожение (стирание) или обезличивание информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания;

- РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения;

- РСБ.2 Определение состава и содержания информации о событиях безопасности, нодлежащих регистрации;

- РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения;

- РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;

- РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

- РСБ.6 Генерирование временных меток и (или) синхронизация системного времени в информационной системе;

- РСБ.7 Защита информации о событиях безопасности;

- АВЗ.1 Реализация антивирусной защиты;

- АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов);

- АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;

- АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

- АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

– АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации;

– АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе;

– ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;

– ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;

– ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

– ЗСВ.3 Регистрация событий в виртуальной инфраструктуре;

– ЗСВ.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре;

– ЗСВ.10 Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователям и (или) группой пользователей;

– ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования;

– ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;

– ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

– ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

– ЗИС.5 Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств;

– ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе;

– ЗИС.30 Защита мобильных технических средств, применяемых в информационной системе.

3. Адаптация базового набора мер по обеспечению безопасности информации

Ввиду особенностей технологического процесса обработки информации на АРМ СЭД «Дело» из базового набора мер обеспечения безопасности информации были исключены меры в соответствии с Таблицей 1.

Таблица 1- Адаптация базового набора мер по обеспечению безопасности

Обозначение меры	Меры защиты информации в информационных системах	Обоснование исключения меры
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Мера исключается из базового набора мер для АРМ СЭД «Дело» в связи с отсутствием внешних пользователей.
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Меры исключаются из базового набора в связи с отсутствием на АРМ СЭД «Дело» технологий виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;	
ЗСВ.3	Регистрация событий в виртуальной инфраструктуре	
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователям и (или) группой пользователей	
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	Мера исключается из базового набора мер для АРМ СЭД «Дело» в связи с отсутствием видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Мера исключается из базового набора мер для АРМ СЭД «Дело» в связи с отсутствием беспроводных соединений
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	Мера исключается из базового набора в связи с отсутствием на

Обозначение меры	Меры защиты информации в информационных системах	Обоснование исключения меры
		АРМ СЭД «Дело» мобильных технических средств

4. Уточнение адаптированного базового набора мер по обеспечению безопасности

Уточнение адаптированного базового набора мер защиты информации проводится с учетом результатов оценки возможности адекватно блокировать (нейтрализовать) угрозы безопасности. Исходными данными при уточнении адаптированного базового набора мер являются перечень угроз безопасности информации и характеристики нарушителя (потенциал, оснащенность, мотивация), включенные в Модели угроз безопасности информации, обрабатываемой на автоматизированном рабочем месте пользовательского сегмента Государственной информационной системы Республики Адыгея «Система электронного делопроизводства и документооборота «дело» (вид 2) Оператора грантов. Анализ мер, необходимых для нейтрализации актуальных угроз безопасности, представлен в таблице 2.

Таблица 2 – Анализ мер, необходимых для нейтрализации угроз безопасности

№ п/п	Наименование угрозы	Меры защиты информации
1.	УБИ.004. Угроза аппаратного сброса пароля BIOS	ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены.
2.	УБИ.006. Угроза внедрения кода или данных	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;

№ п/п	Наименование угрозы	Меры защиты информации
		УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ЗНИ.7 Контроль подключения машинных носителей информации
3.	УБИ.007. Угроза воздействия на программы с высокими привилегиями	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения; ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;
4.	УБИ.008. Угроза восстановления аутентификационной информации	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
5.	УБИ.022. Угроза избыточного выделения оперативной памяти	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

№ п/п	Наименование угрозы	Меры защиты информации
		АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ЗНИ.7 Контроль подключения машинных носителей информации.
6.	УБИ.023. Угроза изменения компонентов системы	ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ЗНИ.7 Контроль подключения машинных носителей информации.
7.	УБИ. 025. Угроза изменения системных и глобальных переменных	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ОПС.2 Управление установкой (инсталляцией)

№ п/п	Наименование угрозы	Меры защиты информации
		компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения; ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;
8.	УБИ.030. Угроза использования информации идентификации/аутентификации, заданной по умолчанию	ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов; ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
9.	УБИ.031. Угроза использования механизмов авторизации для повышения привилегий	УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
10.	УБИ.034. Угроза использования слабостей протоколов сетевого/локального обмена данными	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами; АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов.

№ п/п	Наименование угрозы	Меры защиты информации
		ЗИС.23 Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями. ЗИС.24 Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.
11.	УБИ. 063. Угроза некорректного использования функционала программного обеспечения	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
12.	УБИ.069 Угроза неправомерных действий в каналах связи	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами; ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи; ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты отподмены сетевых устройств и сервисов. ЗИС.23 Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями. ЗИС.24 Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.
13.	УБИ.071. Угроза несанкционированного восстановления удаленной защищаемой информации	ЗНИ.8 Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между

№ п/п	Наименование угрозы	Меры защиты информации
		пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
14.	УБИ.074. Угроза несанкционированного доступа к аутентификационной информации	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ЗНИ.7 Контроль подключения машинных носителей информации.
15.	УБИ.086. Угроза несанкционированного изменения аутентификационной информации	УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
16.	УБИ.089. Угроза несанкционированного редактирования реестра	УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы. ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения; ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.

№ п/п	Наименование угрозы	Меры защиты информации
17.	УБИ.090. Угроза несанкционированного создания учетной записи пользователя	ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов; ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
18.	УБИ.091. Угроза несанкционированного удаления защищаемой информации	УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
19.	УБИ.098. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами; ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи; ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты отподмены сетевых устройств и сервисов. ЗИС.23 Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями. ЗИС.24 Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.
20.	УБИ.099. Угроза обнаружения хостов	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами; ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи,

№ п/п	Наименование угрозы	Меры защиты информации
		имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи; ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов. ЗИС.23 Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями. ЗИС.24 Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.
21.	УБИ.100. Угроза обхода некорректно настроенных механизмов аутентификации	ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации; АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
22.	УБИ.115. Угроза перехвата вводимой и выводимой на периферийные устройства информации	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
23.	УБИ.116. Угроза перехвата данных, передаваемых по вычислительной сети	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы

№ п/п	Наименование угрозы	Меры защиты информации
		управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами; ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;
24.	УБИ.118. Угроза перехвата привилегированного процесса	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения; ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.
25.	УБИ.121. Угроза повреждения системного реестра	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям,

№ п/п	Наименование угрозы	Меры защиты информации
		администраторам и лицам, обеспечивающим функционирование информационной системы;
26.	УБИ.122. Угроза повышения привилегий	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения; ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.
27.	УБИ.131. Угроза подмены субъекта сетевого доступа	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены; ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов. ЗИС.23 Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями. ЗИС.24 Прекращение сетевых соединений по их

№ п/п	Наименование угрозы	Меры защиты информации
		завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.
28.	УБИ.132. Угроза получения предварительной информации об объекте защиты	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами; ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены; ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов. ЗИС.23 Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями. ЗИС.24 Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.
29.	УБИ.140. Угроза приведения системы в состояние «отказ в обслуживании»	УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу; ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов. ЗИС.24 Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.
30.	УБИ.143. Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям,

№ п/п	Наименование угрозы	Меры защиты информации
		администраторам и лицам, обеспечивающим функционирование информационной системы;
31.	УБИ.152. Угроза удаления аутентификационной информации	АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения; ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.
32.	УБИ.157. Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
33.	УБИ. 167. Угроза заражения компьютера при посещении неблагонадёжных сайтов	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы

№ п/п	Наименование угрозы	Меры защиты информации
		управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
34.	УБИ.170. Угроза неправомерного шифрования информации	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации. УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ОДТ.3 Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование; ОДТ.4 Периодическое резервное копирование информации на резервные машинные носители информации; ОДТ.5 Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала.
35.	УБИ.171. Угроза скрытного включения вычислительного устройства в состав бот-сети	АВЗ.1 Реализация антивирусной защиты;

№ п/п	Наименование угрозы	Меры защиты информации
		АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации. УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
36.	УБИ.176. Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.
37.	УБИ.178. Угроза несанкционированного использования системных и сетевых утилит	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
38.	УБИ.179. Угроза несанкционированной модификации защищаемой информации	ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора; УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;

№ п/п	Наименование угрозы	Меры защиты информации
		УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ЗНИ.1 Учет машинных носителей информации; ЗНИ.2 Управление доступом к машинным носителям информации; ЗНИ.7 Контроль подключения машинных носителей информации
39.	УБИ. 185. Угроза несанкционированного изменения параметров настройки средств защиты информации	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
40.	УБИ. 186. Угроза внедрения вредоносного кода через рекламу, сервисы и контент	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной; УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
41.	УБИ. 187. Угроза несанкционированного воздействия на средство защиты информации	АВЗ.1 Реализация антивирусной защиты;

№ п/п	Наименование угрозы	Меры защиты информации
		АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной; УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
42.	УБИ.189. Угроза маскирования действий вредоносного кода	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов). АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
43.	УБИ. 190. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

№ п/п	Наименование угрозы	Меры защиты информации
44.	УБИ.193. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
45.	УБИ. 197. Угроза хищения аутентификационной информации из временных файлов cookie	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов. ЗИС.23 Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями. ЗИС.24 Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.
46.	УБИ.198. Угроза скрытной регистрации вредоносной программой учетных записей администраторов	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;

№ п/п	Наименование угрозы	Меры защиты информации
		АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации; УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной; УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
47.	УБИ. 201. Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации; УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной; УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; УПД.5 Назначение минимально необходимых прав и привилегий пользователям,

№ п/п	Наименование угрозы	Меры защиты информации
		администраторам и лицам, обеспечивающим функционирование информационной системы.
48.	УБИ.208. Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения; ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;
49.	УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6 («Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» утверждены приказом ФСТЭК России от 18 февраля 2013 г. №21)
50.	УБИ.217: Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации; АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации; ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Меры, направленные на нейтрализацию всех актуальных угроз, выявленные при уточнении адаптированного базового набора, представлены в таблице 3.

Таблица 3 - Меры, направленные на нейтрализацию всех актуальных угроз

Обозначение меры	Меры защиты информации в информационных системах
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ОПС.2	Управление установкой (инсталляцией) компонентов ПО, в том числе определение компонентов, подлежащих установке, настройка

Обозначение меры	Меры защиты информации в информационных системах
	параметров установки компонентов, контроль за установкой компонентов программного обеспечения
ЗНИ.7	Контроль подключения машинных носителей информации
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.22	Защита государственной информационной системы от угроз безопасности информации, направленных на отказ в обслуживании государственной информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) государственной информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения

5. Усиление уточненного адаптированного базового набора мер по обеспечению безопасности информации

5.1 В соответствии с методическим документом «Меры защиты информации в государственных информационных системах», утвержденным ФСТЭК России, мерам по обеспечению безопасности информации могут предъявляться дополнительные требования к усилению в зависимости от класса защищенности информационной системы или ее сегментов.

5.2 Необходимость усиления отдельных мер по обеспечению безопасности информации при ее обработке на АРМ СЭД «Дело» 3-го класса защищенности (К3) приведена в таблице 4.

Таблица 4 – необходимость усиления отдельных мер по обеспечению безопасности информации на АРМ СЭД «Дело»

Обозначение меры	Мера защиты информации	Требования к усилению
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	1) оператором должно быть исключено повторное использование идентификатора пользователя в течение не менее одного года; 2) оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не более 90 дней
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	В случае использования в информационной системе механизмов аутентификации на основе пароля (иной последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими: длина пароля не менее шести символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	1) оператором должны использоваться автоматизированные средства поддержки управления учетными записями пользователей; 2) в информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной	1) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему;

Обозначение меры	Мера защиты информации	Требования к усилению
	метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	2) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам; 3) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	В информационной системе обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств в соответствии с ИАФ.2
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	1) оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации; 2) оператором должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации: перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием
АВЗ.1	Реализация антивирусной защиты	В информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности
АНЗ.1	Выявление, анализ уязвимостей информационной	1) оператором обеспечивается использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности),

Обозначение меры	Мера защиты информации	Требования к усилению
	системы и оперативное устранение вновь выявленных уязвимостей	имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей; 2) оператором предоставляется доступ только администраторам к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности)

6. Дополнение усиленного уточненного адаптированного базового набора мер по обеспечению безопасности информации

6.1 Для обеспечения защиты персональных данных при их обработке на АРМ СЭД «Дело», а также при необходимости использования СКЗИ на АРМ СЭД «Дело» должны дополнительно реализовываться организационные и организационно-технические меры по обеспечению безопасности информации, перечисленные в таблице № 5.

Таблица 5 – дополнительные меры по обеспечению безопасности информации при ее обработке на АРМ СЭД «Дело»

Обозначение меры	Меры защиты информации в информационных системах
«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21	
Выявление инцидентов и реагирование на них (приказ ФСТЭК 21)	
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов

Обозначение меры	Меры защиты информации в информационных системах
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
ИНЦ.5	Принятие мер по устранению последствий инцидентов
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов
Управление конфигурацией информационной системы и системы защиты информации (УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных
Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава 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»	
ДОП.1	Поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним
ДОП.2	Учет лиц, допущенных к работе с СКЗИ

Обозначение меры	Меры защиты информации в информационных системах
ДОП.3	Контроль над соблюдением условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним
ДОП.4	Разбирательство и составление заключений по фактам нарушения условий хранения носителей информации, использования СКЗИ, которые могут привести к нарушению конфиденциальности информации или другим нарушениям, приводящим к снижению уровня защищенности информации, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений
ДОП.5	Описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности КИ с использованием СКЗИ при ее обработке в информационных системах
ДОП.6	Обеспечение сохранности СКЗИ, носителей ключевой, аутентифицирующей и парольной информации СКЗИ
Постановление правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	
ДОП.7	Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения
ДОП.8	Обеспечение сохранности носителей персональных данных;
ДОП.9	Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей
ДОП.10	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
ДОП.11	Назначение должностного лица (работник), ответственного за обеспечение безопасности персональных данных в информационной системе

7. Итоговый набор мер по обеспечению безопасности информации

7.1 Итоговый набор мер по обеспечению безопасности информации при ее обработке на АРМ СЭД «Дело», приведен в таблице 6.

Таблица 6 - Итоговый набор мер по обеспечению безопасности информации при ее обработке на АРМ СЭД «Дело»

Условное обозначение и номер меры	Меры по обеспечению безопасности информации
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3 (усиленная 1а, 2а)	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4 (усиленная 1б)	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутептификационной информации
Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1 (усиленная 1, 2)	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2 (усиленная 1, 2, 3)	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование

Условное -обозначение и номер меры	Меры по обеспечению безопасности информации
	информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
Ограничение программной среды (ОПС)	
ОПС.2.	Управление установкой (инсталляцией) компонентов программного обеспечения (ПО), в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.7	Контроль подключения машинных носителей информации
ЗНИ.8 (усиленная 1, 5б)	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

Условное обозначение и номер меры	Меры по обеспечению безопасности информации
Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ. 5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
Антивирусная защита (АВЗ)	
АВЗ.1 (усиленная 1)	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.1 (усиленная 1, 4)	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации

Условное обозначение и номер меры	Меры по обеспечению безопасности информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
Обеспечение доступности информации (ОДТ)	
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
ОДТ.4.	Периодическое резервное копирование информации на резервные машинные носители информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала
Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены

Условное обозначение и номер меры	Меры по обеспечению безопасности информации
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.22	Защита государственной информационной системы от угроз безопасности информации, направленных на отказ в обслуживании государственной информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) государственной информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения
Выявление инцидентов и реагирование на них (ИНЦ)	
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
ИНЦ.5	Принятие мер по устранению последствий инцидентов
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов

Условное обозначение и номер меры	Меры по обеспечению безопасности информации
Управление конфигурацией информационной системы и системы защиты информации (УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных
Дополнительные меры (ДОП)	
ДОП.1	Поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним
ДОП.2	Учет лиц, допущенных к работе с СКЗИ
ДОП.3	Контроль над соблюдением условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним
ДОП.4	Разбирательство и составление заключений по фактам нарушения условий хранения носителей информации, использования СКЗИ, которые могут привести к нарушению конфиденциальности информации или другим нарушениям, приводящим к снижению уровня защищенности информации, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений
ДОП.5	Описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности КИ с использованием СКЗИ при ее обработке в информационных системах

Условное обозначение и номер меры	Меры по обеспечению безопасности информации
ДОП.6	Обеспечение сохранности СКЗИ, носителей ключевой, аутентифицирующей и парольной информации СКЗИ
ДОП.7	Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения
ДОП.8	Обеспечение сохранности носителей персональных данных;
ДОП.9	Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей
ДОП.10	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
ДОП.11	Назначение должностного лица (работник), ответственного за обеспечение безопасности персональных данных в информационной системе