ОБЩИЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИБ

ПРАВОВЫЕ НОРМЫ И ТРЕБОВАНИЯ

При появлении модуля аналитики/идентификации пользователя – это идентифицируется как обработка ПДн с соответствующими требованиями.

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями на 14 июля 2022 года). *[Регулирует деятельность по обработке (использованию) персональных данных и определяет требования по их защите.]*

2. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21.07.2014 № 242-ФЗ. *[Определяет требования к хранению и отдельным процессам обработки персональных данных российских граждан на территории России.]*

3. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" *[Определяет требования к защите и уровни защищенности персональных данных.]*

4. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 05.12.2022) "Об информации, информационных технологиях и о защите информации" *[Регулирует отношения в сфере информации, информационных технологий и защиты информации.]*

5. Приказ ФСТЭК РФ от 18.02.2013 N 21 Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных *[Определяет организационно-технические меры и средства]*

6. "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)

7. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)

8. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ [*только если организация, которой принадлежит склад, является субъектом КИИ*].

ОРГАНИЗАЦИОННЫЕ МЕРЫ

1. Разработка и внедрение в организации пакета локальной организационно-распорядительной документации, регламентирующей порядок обработки и защиты персональных данных, ознакомление с документами сотрудников и ответственных лиц;
2. Введение физической охраны территории, внедрение систем видеонаблюдения, охранной сигнализации, усиление дверей и замков в помещения, установку решеток на окна первого и последнего этажей здания;
3. Организация хранения материальных носителей ПДн в сейфах, металлических запираемых шкафах;
4. Внедрение пропускной системы на территорию организации и в помещения, в которых хранятся и/или обрабатываются ПДн, установление контролируемой зоны;

5. Обучение, периодическое повышение квалификации сотрудников, ответственных за организацию системы защиты ПДн, проведение для всех сотрудников обзорных лекций, семинаров по вопросам обработки и защиты ПДн;
6. Проведение внешнего аудита или внутреннего контроля обработки ПДн на соответствие принятым в организации мерам, нормативным и локальным актам;
7. Организация постоянного контроля защищенности персональных данных, работоспособности средств защиты, исполнения обязанностей ответственными сотрудниками;
8. Расследование инцидентов, связанных с нарушением безопасности ПДн, и привлечение виновных лиц к дисциплинарной, административной и другим видам ответственности и т.п.

ТЕХНИЧЕСКИЕ МЕРЫ

ИСПДн обрабатывает биометрические персональные данные (2 группа) и для неё актуальны угрозы 2-го типа. Следовательно, **уровень защищенности нашей ИСПДн должен соответствовать 2-му уровню**.

Базовый набор мер в ИСПДн 2-го уровня защищенности персональных данных

Требования к системам 2-го уровня защищенности:

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах необходимо,

а) 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;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) 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;

д) назначить должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе;

е) доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Адаптация базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с

информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе).

Базовый набор мер:

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

1. Идентификация и аутентификация пользователей, являющихся работниками оператора

2. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

4. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

5. Защита обратной связи при вводе аутентификационной информации

6. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

II. Управление доступом субъектов доступа к объектам доступа (УПД)

Подсистема управления доступом

1. Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

2. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

3. Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

5. Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

6. Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

10. Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

11. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации

13. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

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

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

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

17. Обеспечение доверенной загрузки средств вычислительной техники

III. Ограничение программной среды (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

IV. Защита машинных носителей персональных данных (ЗНИ)

1. Учет машинных носителей персональных данных

2. Управление доступом к машинным носителям персональных данных

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

V. Регистрация событий безопасности (РСБ)

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

2. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

3. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

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

7. Защита информации о событиях безопасности

VI. Антивирусная защита (АВЗ)

1. Реализация антивирусной защиты

2. Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

VII. Обнаружение вторжений (СОВ)

1. Обнаружение вторжений

2. Обновление базы решающих правил

VIII. Контроль (анализ) защищенности персональных данных (АРЗ)

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

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

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

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

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

IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)

1. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации

4. Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)

X. Обеспечение доступности персональных данных (ОДТ)

4. Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных

5. Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала

XI. Защита среды виртуализации (ЗСВ)

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

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

3. Регистрация событий безопасности в виртуальной инфраструктуре

6. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных

7. Контроль целостности виртуальной инфраструктуры и ее конфигураций

8. Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры

9. Реализация и управление антивирусной защитой в виртуальной инфраструктуре

10. Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей

XII. Защита технических средств (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

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

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

3. Обеспечение защиты персональных данных 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

11. Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов

15. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных

17. Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы

20. Защита беспроводных соединений, применяемых в информационной системе

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

Компенсирующие меры:

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

II. Управление доступом субъектов доступа к объектам доступа (УПД)

7. Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных

8. Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему

9. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы

12. Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки

III. Ограничение программной среды (ОПС)

1. Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения

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

4. Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов

IV. Защита машинных носителей персональных данных (ЗНИ)

3. Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны

4. Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах

5. Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных

6. Контроль ввода (вывода) информации на машинные носители персональных данных

7. Контроль подключения машинных носителей персональных данных

V. Регистрация событий безопасности (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

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

VI. Антивирусная защита (АВЗ)

VII. Обнаружение вторжений (СОВ)

VIII. Контроль (анализ) защищенности персональных данных (АРЗ)

IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)

2. Контроль целостности персональных данных, содержащихся в базах данных информационной системы

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

5. Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы

6. Ограничение прав пользователей по вводу информации в информационную систему

7. Контроль точности, полноты и правильности данных, вводимых в информационную систему

8. Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях

X. Обеспечение доступности персональных данных (ОДТ)

1. Использование отказоустойчивых технических средств

2. Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы

3. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование

XI. Защита среды виртуализации (ЗСВ)

4. Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

5. Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией

XII. Защита технических средств (ЗТС)

1. Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам

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

5. Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

1. Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы

2. Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом

4. Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)

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

6. Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами

7. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода

8. Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи

9. Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации

10. Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам

12. Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю

13. Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя

14. Использование устройств терминального доступа для обработки персональных данных

16. Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов

18. Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения

19. Изоляция процессов (выполнение программ) в выделенной области памяти

Требования ФСТЭК России к технической защите информации в ИСПДн 2-го уровня защищенности персональных данных

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в ИСПДн применяются сертифицированные по требованиям безопасности информации средства защиты информации не ниже 5 класса

Обязательные средства защиты информации:

а) средства контроля съемных машинных носителей информации 5 класса, профиль защиты (ИТ.СКН.П5.ПЗ);

б) средства антивирусной защиты не ниже 5 класса, профиль защиты (ИТ.САВЗ.А5.ПЗ, ИТ.САВЗ.Б5.ПЗ, ИТ.САВЗ.В5.ПЗ, ИТ.САВЗ.Г5.ПЗ);

в) системы обнаружения вторжений не ниже 5 класса, профиль защиты (ИТ.СОВ.С5.ПЗ, ИТ.СОВ.У5.ПЗ);

г) межсетевой экран не ниже 5 класса, профиль защиты (ИТ.МЭ.А5.ПЗ, ИТ.МЭ.Б5.ПЗ, ИТ.МЭ.В5.ПЗ, ИТ.МЭ.Г5.ПЗ, ИТ.МЭ.Д5.ПЗ).

Средства защиты информации для усиления:

а) средства вычислительной техники не ниже 5 класса;

б) операционная система не ниже 5 класса, профиль защиты (ИТ.ОС.А5.ПЗ);

в) средства доверенной загрузки не ниже 5 класса, профиль защиты (ИТ.СДЗ.З35.ПЗ).

Применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Для нейтрализации актуальных атак в ИСПДн применяют СКЗИ класса КВ и выше.

Доверенные компоненты и подсистемы ИСПДн

Компоненты являются доверенными, если они удовлетворяют требованиям к защите информации в ИСПДн 2-го уровня защищенности персональных данных. Например, СЗИ от НСД Secret Net Studio, маршрутизаторы и межсетевые экраны Eltex, антивирусное ПО «Лаборатории Касперского», имеющие сертификаты соответствия ФСТЭК России.

Для обеспечения 2-го уровня защищенности персональных данных в ИСПДн на уровне компонентов и архитектуры требуется реализовать следующие подсистемы:

Подсистема управления доступом

1. Идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов

Возможности Secret Net Studio по обеспечению управления доступом:

1. Задание количества неудачных попыток аутентификации, после чего компьютер будет блокирован.
2. Задание интервала блокировки компьютера в случае достижения установленного максимального количества неуспешных попыток аутентификации - временная блокировка.

Подсистема регистрации и учета

1. Регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы
2. Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета

Подсистема обеспечения целостности

1. Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ
2. Физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации
3. Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа
4. Наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности

Возможности Secret Net Studio по обеспечению целостности данных:

1. Замкнутая программная среда с возможностью контроля целостности модулей.
2. Контроль целостности (файлы, папки, реестр).
3. Контроль целостности файлов и папок.

Межсетевое экранирование

Безопасное межсетевое взаимодействие для информационных систем 2 класса при их подключении к сетям международного информационного обмена, а также для распределенных информационных систем 2 класса при их разделении на подсистемы достигается путем применения средств межсетевого экранирования (межсетевых экранов), которые обеспечивают:

1. Фильтрацию на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
2. Фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
3. Фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
4. Фильтрацию с учетом любых значимых полей сетевых пакетов;
5. Регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
6. Идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
7. Регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
8. Регистрацию запуска программ и процессов (заданий, задач);
9. Контроль целостности своей программной и информационной части;
10. Восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
11. Регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

В распределенных информационных системах 2 и 1 классов при их разделении на отдельные части применяются межсетевые экраны, которые обеспечивают:

1. Фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
2. Идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
3. Регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
4. Контроль целостности своей программной и информационной части;
5. Фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
6. Восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
7. Регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

При разделении информационной системы при помощи межсетевых экранов на отдельные части системы для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом.

Анализ защищенности

1. Анализ защищенности проводится для распределенных информационных систем и информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности.
2. Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.
3. Обнаружение вторжений проводится для информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.

ПОРЯДОК ВЫПОЛНЕНИЕ 152-ФЗ

1. Обеспечить защиту данных

Основные требования общие для всех операторов персональных данных:

1. Обеспечить аутентификацию, чтобы к данным имели доступ только те, у кого есть на это право.
2. Поставить серверы с данными в защищенном месте, чтобы посторонний не мог войти в помещение и подключиться к серверу напрямую.
3. Использовать для защиты информации ПО, сертифицированное ФСТЭК (антивирусные программы, межсетевые экраны и другое ПО). При использовании ПО собственной разработки на него можно получить сертификат самостоятельно.

2. Разработать документы, описывающие порядок работы с персональными данными

Публичные документы: для предъявления тем, у кого берутся персональные данные

Согласие работника на обработку персональных данных. Согласие сотрудника на обработку должно быть конкретным, информированным, сознательным, предметным и однозначным. Это значит, что формулировки целей в согласии должны быть максимально точными и понятными.

Согласие работника на обработку биометрических персональных данных. Биометрические персональные данные лиц, не достигших возраста 18 лет, не могут обрабатываться. По общему правилу сдать биометрию работник может только по своему желанию. Работодатель в свою очередь не вправе обязать его это сделать. Кроме того, оператор по общему правилу не может обрабатывать биометрические персональные данные без согласия их субъекта.

Положение об обработке и защите персональных данных. Этот документ нужно показывать тем, кто лично подписывает согласие на обработку персональных данных. В

положении о персональных данных прописывают цель и сроки обработки и хранения данных, порядок их уничтожения.

Внутренние документы компании: описывается корпоративный порядок работы с персональными данными

Модель угроз безопасности. Этот документ показывает, какие опасности угрожают вашей системе хранения и обработки персональных данных. При составлении нужно ориентироваться на базовую модель от ФСТЭК.

Приказ о назначении ответственного за безопасность персональных данных. Если ООО, в нем должен быть ответственный — должностное лицо, которое следит за персональными данными. Его требуется назначить приказом.

Приказ о допуске к обработке персональных данных. В этом документе прописаны все сотрудники, которые имеют доступ к персональным данным. Доступ к системам видеонаблюдения и архивам должны иметь только специально уполномоченные лица. При этом обращаться им можно лишь к тем данным, которые необходимы для выполнения конкретных должностных обязанностей.

Инструкция пользователя системы персональных данных. В этой инструкции нужно прописать, как правильно общаться с персональными данными. С ней должны ознакомиться все, кто имеет доступ к данным.

3. Уведомить Роскомнадзор об обработке персональных данных и сообщать о возникновении инцидентов

При работе с персональными данными клиентов требуется отправить уведомление в Роскомнадзор — зарегистрироваться как оператор персональных данных. Отправить уведомление можно онлайн на сайте Роскомнадзора.

Кроме того, если работодатель обнаружил, что к ПД его сотрудников получили доступ третьи лица и нарушили их права, он обязан сообщить в Роскомнадзор в течение 24 часов. А в течение 72 часов — провести расследование инцидента и сообщить о его результатах. В сообщении нужно указать, кто именно из сотрудников компании виноват в происшествии и какие меры приняли.

4. Подключиться к Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКа)

ГосСОПКа расследует инциденты кибератак, выявляет уязвимости информационных систем безопасности. Если в организации произошло что-то из перечисленного, то обязана передать сведения в ГосСОПКу.

5. Подключиться к единой биометрической системе (ЕБС)

С июля 2022 любые организации, работающие с биометрией, обязаны передать все эти данные в единую биометрическую систему. В единую систему включаются только биометрические сведения, собранные с согласия человека.

5. Получить согласие на хранение и обработку персональных данных

Необходимо получить согласие от каждого человека, чьи персональные данные собираются, хранятся и обрабатываются. По закону о защите персональных данных 152-ФЗ

каждый клиент или сотрудник будет субъектом персональных данных и должен быть в курсе о том, что о нем ведется сбор персональной информации.

Получить согласие можно подписав письменное соглашение.

Кроме того, требуется уведомлять посетителей и сотрудников о том, что на территории ведется видеонаблюдение. Для этого достаточно повесить табличку "Ведется видеонаблюдение" на видном месте.

ПОЛИТИКА «ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В {НАЗВАНИЕ ОРГАНИЗАЦИИ}»

1. Информация о документе

Цель документа	• Защита прав и законных интересов субъектов персональных данных. • Выполнение {НАЗВАНИЕ ОРГАНИЗАЦИИ} требований законодательства в области персональных данных.
Краткое описание документа	Политика «Обработка персональных данных в {НАЗВАНИЕ ОРГАНИЗАЦИИ} (далее – Политика) определяет принципы, порядок и условия обработки персональных данных клиентов, работников {НАЗВАНИЕ ОРГАНИЗАЦИИ} и иных лиц, чьи персональные данные обрабатываются {НАЗВАНИЕ ОРГАНИЗАЦИИ}, лицами по поручению {НАЗВАНИЕ ОРГАНИЗАЦИИ}, а также в случаях обработки {НАЗВАНИЕ ОРГАНИЗАЦИИ} ПДн по поручению.
Ограничение доступа	Нет.

2. Ответственность и область применения

Настоящий документ регламентирует деятельность должностных лиц, имеющих доступ к персональным данным, собранным посредством системы видеонаблюдения с распознаванием лиц.

3. Определения терминов и сокращений

Наименование термина	**Сокращение**	**Определение термина (расшифровка сокращения)**
Вводимые определения:	**ПДн**	
Персональные данные		Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Биометрические персональные данные		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.

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.
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.
Распространение персональных данных		Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
Предоставление персональных данных		Действия, направленные на раскрытие персональных данных неопределенному 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.
Информационная система	**ИСПДн**	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их

персональных данных		обработку информационных технологий и технических средств.

4. Общие положения

Деятельность {НАЗВАНИЕ ОРГАНИЗАЦИИ} в соответствии с настоящей политикой обеспечивает защиту прав и свобод человека и гражданина при обработке его ПДн, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

Настоящая Политика разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных») и действует в отношении всех ПДн, обрабатываемых в {НАЗВАНИЕ ОРГАНИЗАЦИИ}. Политика распространяется на ПДн, полученные как до, так и после ввода в действие настоящей Политики.

ПДн являются информацией ограниченного доступа (конфиденциального характера) в соответствии с законодательством РФ, если иное не установлено законом. ПДн могут обрабатываться самостоятельно или в составе другой информации конфиденциального характера, порядок обработки которой устанавливается отраслевыми федеральными законами, в частности, о коммерческой тайне (коммерческая тайна), о связи (сведения об абоненте), о банках (банковская тайна), об архивном деле и другими (далее – отраслевое законодательство). Порядок обработки ПДн в {НАЗВАНИЕ ОРГАНИЗАЦИИ} регулируется настоящей Политикой в соответствии с требованиями действующего законодательства РФ в области ПДн и отраслевого законодательства РФ, если в нем установлен порядок обработки информации конфиденциального характера.

Организация хранения, учета и использования ПДн в {НАЗВАНИЕ ОРГАНИЗАЦИИ} осуществляется в соответствии с ФЗ «О персональных данных» и нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ}.

В соответствии с п. 2 ч. 2 ст. 1 ФЗ «О персональных данных» обращение с документами, переданными на хранение в соответствии с архивным законодательством, не регулируется настоящей Политикой.

Настоящая Политика распространяется на все процессы {НАЗВАНИЕ ОРГАНИЗАЦИИ}, связанные с обработкой ПДн субъектов, и обязательна для применения всеми работниками {НАЗВАНИЕ ОРГАНИЗАЦИИ}, осуществляющими обработку ПДн в силу своих должностных обязанностей.

Во всех случаях, не урегулированных настоящей Политикой, необходимо руководствоваться действующим законодательством РФ.

5. Конфиденциальность персональных данных

{НАЗВАНИЕ ОРГАНИЗАЦИИ} и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

6. Обработка персональных данных

{НАЗВАНИЕ ОРГАНИЗАЦИИ} является оператором ПДн, самостоятельно обрабатывает ПДн, и определяет цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн, или обрабатывает ПДн по поручению других Операторов.

Обработка ПДн субъектов ПДн осуществляется в {НАЗВАНИЕ ОРГАНИЗАЦИИ} в следующих целях:

- Видеонаблюдение и видеоаналитика для отслеживания и контроля пропускного режима для физических лиц,
- Видеонаблюдение и видеоаналитика для отслеживания и контроля пропускного режима для автомобилей, въезжающих и выезжающих на территорию склада

Обработка ПДн должна осуществляться на законной и справедливой основе. Обработке подлежат только ПДн, которые отвечают целям их обработки. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, не совместимая с целями сбора ПДн. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. В {НАЗВАНИЕ ОРГАНИЗАЦИИ} должны приниматься необходимые меры по удалению или уточнению неполных, или неточных данных. Ответственность за своевременное предоставление в {НАЗВАНИЕ ОРГАНИЗАЦИИ} сведений об изменении ПДн, обрабатываемых в {НАЗВАНИЕ ОРГАНИЗАЦИИ}, возлагается на субъектов ПДн, которым они принадлежат.

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

Обработка в {НАЗВАНИЕ ОРГАНИЗАЦИИ} специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается только в случаях, предусмотренных федеральным законодательством. Обработка указанных специальных категорий ПДн должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась их обработка, если иное не установлено федеральным законом.

Биометрические ПДн, которые используются {НАЗВАНИЕ ОРГАНИЗАЦИИ} для установления личности субъекта ПДн, могут обрабатываться в {НАЗВАНИЕ ОРГАНИЗАЦИИ} только при наличии согласия в письменной форме субъекта ПДн, за исключением случаев, предусмотренных ч. 2 ст. 11 ФЗ «О персональных данных».

Обработка ПДн в {НАЗВАНИЕ ОРГАНИЗАЦИИ} может осуществляться:

- работниками {НАЗВАНИЕ ОРГАНИЗАЦИИ};
- другими лицами, осуществляющими обработку ПДн по поручению {НАЗВАНИЕ ОРГАНИЗАЦИИ}.

Обработка ПДн другими лицами может осуществляться на основании соответствующего договора с {НАЗВАНИЕ ОРГАНИЗАЦИИ}, в котором содержится поручение на обработку ПДн. В поручении должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 ФЗ «О персональных данных».

Обработка ПДн в {НАЗВАНИЕ ОРГАНИЗАЦИИ} может осуществляться как с использованием, так и без использования средств автоматизации.

Автоматизированная обработка ПДн должна осуществляться в ИСПДн {НАЗВАНИЕ ОРГАНИЗАЦИИ} в строгом соответствии с настоящей политикой.

В {НАЗВАНИЕ ОРГАНИЗАЦИИ} запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных законодательством РФ.

Неавтоматизированная обработка ПДн должна осуществляться таким образом, чтобы ПДн обособлялись от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков) и иным способом.

Лица, осуществляющие обработку ПДн без использования средств автоматизации (работники {НАЗВАНИЕ ОРГАНИЗАЦИИ} и другие лица, осуществляющие обработку ПДн по поручению {НАЗВАНИЕ ОРГАНИЗАЦИИ}), должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется {НАЗВАНИЕ ОРГАНИЗАЦИИ} без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ}.

При неавтоматизированной обработке ПДн, предполагающей использование типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), необходимо выполнять следующие условия:

1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:

- сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации;
- реквизиты {НАЗВАНИЕ ОРГАНИЗАЦИИ} (наименование и адрес);
- фамилию, имя, отчество и адрес субъекта ПДн;

- источник получения ПДн, сроки обработки ПДн;
- перечень действий с ПДн, которые будут совершаться в процессе их обработки;
- общее описание используемых оператором способов обработки ПДн;

2. Типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПДн;

3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

4. Типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

При сохранении ПДн на материальных носителях при не автоматизированной обработке ПДн, не допускается сохранение на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн следует использоваться отдельный материальный носитель.

7. Права субъекта персональных данных

Субъект ПДн принимает решение о предоставлении его ПДн и даёт согласие на их обработку свободно, своей волей и в своём интересе. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в ФЗ «О персональных данных», возлагается на {НАЗВАНИЕ ОРГАНИЗАЦИИ}, либо на лицо, по поручению которого {НАЗВАНИЕ ОРГАНИЗАЦИИ} обрабатывает ПДн.

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, если такое право не ограничено в соответствии с федеральными законами. Субъект ПДн вправе требовать от {НАЗВАНИЕ ОРГАНИЗАЦИИ} уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8. Получение персональных данных

Получение ПДн в {НАЗВАНИЕ ОРГАНИЗАЦИИ} организуется таким способом, чтобы не нарушить конфиденциальность собираемых ПДн.

Перечень случаев, когда необходимо получить письменное согласие субъекта ПДн на обработку его ПДн, а также порядок и форма получения согласия определяются нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ} в соответствии с положениями ФЗ «О персональных данных».

В случае недееспособности субъекта ПДн письменное согласие на обработку его ПДн получается от его законного представителя.

ПДн могут быть получены {НАЗВАНИЕ ОРГАНИЗАЦИИ} от лица, не являющегося субъектом ПДн, при условии предоставления оператору подтверждения наличия оснований, указанных в пп. 2-11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 ФЗ «О персональных данных».

При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети «Интернет», запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации должны осуществляться в {НАЗВАНИЕ ОРГАНИЗАЦИИ} с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных ФЗ «О персональных данных».

Порядок получения ПДн определяется нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ}.

9. Сроки обработки (хранения) персональных данных

Порядок хранения ПДн, обрабатываемых в {НАЗВАНИЕ ОРГАНИЗАЦИИ}, определяется нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ} в соответствии с положениями ФЗ «О персональных данных».

Сроки обработки (хранения) ПДн определяются в соответствии со сроком действия договора с субъектом ПДн, приказом Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», сроками исковой давности, а также иными сроками, установленными законодательством РФ и нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ}.

ПДн, срок обработки (хранения) которых истек, должны быть уничтожены, если иное не предусмотрено федеральным законом или нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ}. Хранение ПДн после истечения срока хранения допускается только после их обезличивания.

10. Уточнение персональных данных

Уточнение ПДн, обрабатываемых в {НАЗВАНИЕ ОРГАНИЗАЦИИ}, осуществляется по запросам субъектов ПДн, их законных представителей или в случае обращения уполномоченного органа по защите прав субъектов ПДн.

Уточнение ПДн при осуществлении их обработки без использования средств автоматизации следует производить путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

11. Предоставление и передача персональных данных

При предоставлении ПДн третьей стороне должны выполняться следующие условия:

- передача (предоставление доступа) ПДн третьей стороне осуществляется на основании договора, существенным условием которого является обеспечение третьей стороной конфиденциальности ПДн и безопасности ПДн при их обработке;
- передача (предоставление доступа) ПДн третьей стороне осуществляется на основании действующего законодательства РФ;
- наличие согласия субъекта ПДн, на передачу его ПДн третьей стороне, в случаях, предусмотренных законодательством РФ наличия согласия в письменной форме.

В целях информационного обеспечения в {НАЗВАНИЕ ОРГАНИЗАЦИИ} могут создаваться специализированные справочники (телефонные, адресные книги и др.), содержащие ПДн, к которым с письменного согласия субъекта ПДн может предоставляться доступ неограниченному кругу лиц.

Сведения о субъекте ПДн должны быть в любое время исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

12. Блокирование персональных данных

Основанием блокирования {НАЗВАНИЕ ОРГАНИЗАЦИИ} ПДн, относящихся к соответствующему субъекту ПДн, является:

- обращение или запрос субъекта ПДн при условии подтверждения факта недостоверности, устаревания, неполноты ПДн, отсутствия необходимости в них для заявленной цели обработки, неправомерных действий с ними, незаконного их получения;
- обращение или запрос законного представителя субъекта при условии подтверждения факта недостоверности, устаревания, неполноты ПДн, отсутствия необходимости в них для заявленной цели обработки, неправомерных действий с ними, незаконного их получения;
- обращение или запрос уполномоченного органа по защите прав субъектов ПДн при условии подтверждения факта недостоверности, устаревания, неполноты ПДн, отсутствия необходимости в них для заявленной цели обработки, неправомерных действий с ними, незаконного их получения.

13. Уничтожение персональных данных

Основанием для уничтожения ПДн, обрабатываемых в {НАЗВАНИЕ ОРГАНИЗАЦИИ}, является:

- достижение цели обработки ПДн;
- утрата необходимости в достижении цели обработки ПДн;
- отзыв субъектом ПДн согласия на обработку своих ПДн за исключением случаев, когда обработка указанных ПДн является обязательной в соответствии с законом РФ или договором;

- выявление неправомерных действий с ПДн и невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты такого выявления;
- истечение срока хранения ПДн, установленного законодательством РФ и нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ};
- предписание уполномоченного органа по защите прав субъектов ПДн, Прокуратуры России или решение суда.

Оператор должен исполнить требование субъекта ПД о прекращении их обработки в срок 10 рабочих дней с даты получения обращения. Такой срок можно продлить, но не более чем на пять рабочих дней. Для этого нужно направить в адрес субъекта ПД мотивированное уведомление с указанием причин продления срока.

При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, и при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Уничтожение части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

14. Обеспечение безопасности персональных данных при их обработке

При обработке ПДн {НАЗВАНИЕ ОРГАНИЗАЦИИ} принимает правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Обеспечение безопасности ПДн осуществляется в рамках установления в {НАЗВАНИЕ ОРГАНИЗАЦИИ} режима безопасности информации конфиденциального характера.

Обеспечение безопасности ПДн, в частности, достигается:

- определением угроз безопасности ПДн при их обработке в ИСПДн;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПДн;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- учетом машинных носителей ПДн;
- обнаружением фактов несанкционированного доступа к ПДн;

- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ПДн в ИСПДн.

Уровни защищенности ПДн при их обработке в ИСПДн {НАЗВАНИЕ ОРГАНИЗАЦИИ}, требования к защите ПДн, обеспечивающих уровни защищенности ПДн, определяются в зависимости от актуальных угроз безопасности персональным данным с учетом возможного вреда субъекту ПДн, объема и содержания обрабатываемых ПДн, вида деятельности, при осуществлении которого обрабатываются ПДн в соответствии с требованиями Постановлений Правительства РФ, подзаконных нормативных правовых актов ФСТЭК, ФСБ, а также договорами между {НАЗВАНИЕ ОРГАНИЗАЦИИ}, операторами ПДн и субъектами ПДн.

Использование и хранение биометрических ПДн вне ИСПДн осуществляется только с применением материальных носителей информации и технологии хранения, которые обеспечивают защиту биометрических ПДн от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления и распространения.

Защита ПДн при неавтоматизированной обработке осуществляется в соответствии с требованиями подзаконных нормативных правовых актов РФ и нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ} по работе с материальными носителями информации.

15. Права субъекта персональных данных

Субъект ПДн, чьи ПДн обрабатываются в {НАЗВАНИЕ ОРГАНИЗАЦИИ}, имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн оператором;
- правовые основания и цели обработки ПДн;
- цели и способы обработки ПДн;
- сроки обработки ПДн, в том числе сроки их хранения;
- наименование и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

Сведения, указанные в настоящем пункте, предоставляются субъекту ПДн {НАЗВАНИЕ ОРГАНИЗАЦИИ} в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Все сведения предоставляются в соответствии с формой запроса в течении 10 рабочих дней.

16. Ответственность за нарушение норм, регулирующих обработку персональных данных

{НАЗВАНИЕ ОРГАНИЗАЦИИ} и/или работники {НАЗВАНИЕ ОРГАНИЗАЦИИ}, виновные в нарушении требований законодательства РФ в области ПДн, а также положений настоящей Политики, несут предусмотренную законодательством Российской Федерации ответственность.

Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн, подлежит возмещению в соответствии с законодательством Российской Федерации.

17. Заключительные положения

Настоящая Политика является общедоступной.

Настоящая Политика подлежит пересмотру в соответствии с нормативными документами {НАЗВАНИЕ ОРГАНИЗАЦИИ}.

Лица, чьи ПДн обрабатываются {НАЗВАНИЕ ОРГАНИЗАЦИИ}, могут получить разъяснения по вопросам обработки своих ПДн, направив соответствующий письменный запрос по почтовому адресу: {АДРЕС ОРГАНИЗАЦИИ}.

18. Нормативные ссылки

Внешние документы:

№ п/п	**Наименование документа**
1	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
2	Приказ Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения».