

Утверждено приказом директора
МУК «Кассельская ЦКС»
от 02.07.2025 г. № 15

Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных

1. Общие положения

1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) Муниципальном учреждении культуры «Кассельская централизованная клубная система» Нагайбакского муниципального района Челябинской области (далее – Учреждение).

2. Настоящий документ разработан в соответствии с Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные.

4. Изменения и дополнения к настоящему документу утверждаются в установленном порядке.

2. Термины и определения

5. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

6. 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.

7. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

8. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

9. Технические средства, позволяющие осуществлять обработку персональных данных, – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах

10. 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.

3. Особенности обеспечения безопасности персональных данных при их обработке в ИСПДн

11. Меры по обеспечению безопасности персональных данных принимаются 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.

12. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных». Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

13. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

14. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

15. В ИСПДн Учреждения устанавливаются уровни защищенности персональных данных в зависимости от угроз безопасности этих данных в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 1 ноября 2012г. № 1119.

16. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

17. В Учреждении организован режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

18. Безопасность персональных данных при их обработке в ИСПДн обеспечивают ответственный за обеспечение безопасности персональных данных и администратор безопасности.

4. Требования по обеспечению безопасности

19. При обработке персональных данных в информационной системе должно быть обеспечено:

1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

5) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

6) постоянный контроль над обеспечением уровня защищенности персональных данных.

20. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

1) определение угроз безопасности персональных данных при их обработке в ИСПДн;

2) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

4) учет машинных носителей персональных данных;

5) установление правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;

6) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн;

7) ознакомление Работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных Работников.

21. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе возлагается на администратора безопасности.

22. Список лиц, имеющих право доступа к персональным данным, уполномоченных на обработку этих данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных, утверждается директором.

23. Работники Учреждения, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей, для получения доступа к информационной системе обращаются с устным запросом к ответственному за обеспечение безопасности персональных данных.

24. При обнаружении нарушений порядка предоставления персональных данных администратор безопасности незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

25. Иные требования по обеспечению безопасности информации и средств защиты информации в Учреждении выполняются в соответствии с требованиями федеральных органов исполнительной власти и на основании нормативно-правовых документов субъекта федерации.

5. Регистрация событий безопасности ИСПДн

26. В ИСПДн подлежат регистрации следующие события:

1) вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;

2) подключение машинных носителей информации и вывод информации на носители информации;

3) запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

4) попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

5) попытки удаленного доступа.

27. Сроки хранения событий безопасности определяются заданными настройками средств защиты информации от несанкционированного доступа. При их отсутствии, определяются штатными средствами журналирования операционной системы.

28. Состав и содержание информации о событиях безопасности:

1) типы события;

2) дата и время события;

3) идентификационной информации источника события безопасности;

4) результат события безопасности (успешно или неуспешно);

5) субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

29. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения предусматривает:

1) возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени: обеспечивается возможностями операционной системы и средств защиты информации от несанкционированного доступа;

2) генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с п. 26 настоящего Положения с составом и содержанием информации, определенными в соответствии с п. 28 настоящего Положения;

3) хранение информации о событиях безопасности в течение времени, установленного в соответствии с п. 27 настоящего Положения.

30. Доступ к записям регистрации событий и функциям управления механизмами регистрации предоставляется только администратору безопасности и обслуживающему персоналу под контролем администратора безопасности.

6. Ответственность

31. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, Работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.