

**ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ РАБОТ ПО  
ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ  
ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В  
ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ  
ДАННЫХ  
В ЛГ МАОУ «СОШ № 4»**

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Положение определяет основные мероприятия и порядок проведения работ по обеспечению безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) Лангепасское городское муниципальное автономное образовательное учреждение «Средняя общеобразовательная школа № 4».

1.2. В ЛГ МАОУ «СОШ № 4» обработка ПДн осуществляется в следующих информационных системах (далее - ИС):

- Система по начислению заработной платы, учета персональных данных работников, воинского учета. (ИС: Предприятия «Заработная плата и кадры»);
- Система учета персональных данных учеников и родителей;
- Система для автоматизации печати аттестатов школы и приложений к ним (Аттестат школы);
- «АРМ-К СОШ №4» / Информационно-аналитическая система "АВЕРС: Управление образовательным учреждением" (КРМ "Директор").

1.3. Все работники учреждения, участвующие в обработке ПДн в ИС учреждения, должны быть ознакомлены с Положением.

**2. ПОРЯДОК ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ  
ПЕРСОНАЛЬНЫХ ДАННЫХ**

2.1. С целью организации работ по защите ПДн (приказ от 01.09.2016 г. № 177/1 о.) назначается должностное лицо, ответственное за обеспечение безопасности ПДн.

2.2. В обязанности ответственного за обеспечение безопасности ПДн входит:

- контроль и организация работ по обеспечению безопасности ПДн;
- утверждение организационно-распорядительных документов по вопросам обеспечения безопасности ПДн;
- утверждение перечня подразделений, работникам которых необходим доступ к ПДн для выполнения служебных обязанностей;
- утверждение списка лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и системы защиты ПДн (далее – СЗПДн) учреждения;
- проведение разбирательств по фактам возникновения событий, которые могут привести к снижению уровня защищенности ПДн.

2.3. Ответственным за выполнение работ по обеспечению безопасности ПДн при их обработке в ИС учреждения является ответственный за

информационную безопасность, назначаемый (приказ от 01.09.2016 г. № 177/1 о.) .

2.4. Реализация требований по обеспечению безопасности ПДн осуществляется администраторами, разработчиками и пользователями информационных систем учреждения.

### **3. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

3.1. Требования по обеспечению безопасности ПДн при их обработке в ИС учреждения формируются на основании установленного уровня защищенности ИСПДн и перечня актуальных угроз безопасности ПДн.

3.2. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн реализуются комплексом организационных и технических мер, средств и механизмов защиты информации, определенных в Техническом задании на создание СЗПДн.

3.3. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн Организации реализуются в рамках следующих направлений:

- организация системы допуска и учета лиц, допущенных к работе с ПДн;
- организация системы защиты межсетевое взаимодействия;
- организация режима безопасности помещений ИСПДн;
- организация безопасного хранения и уничтожения носителей ПДн;
- организация защиты от вредоносного кода;
- организация парольной защиты;
- организация управления инцидентами информационной безопасности и реагирования на них;
- организация управления конфигурацией ИСПДн и СЗПДн учреждения;
- организация системы криптографической защиты информации;
- организация системы резервного копирования и восстановления;
- организация управления СЗПДн учреждения;
- организация контроля эффективности мер защиты ПДн;
- организация системы обучения по вопросам обеспечения безопасности ПДн.

### **4. СИСТЕМА ДОПУСКА И УЧЕТА ЛИЦ**

4.1. Ответственным за организацию системы допуска к ПДн является ответственный за обеспечение безопасности ПДн.

4.2. Работники учреждения допускаются к обработке ПДн в ИСПДн, использование которых необходимо для выполнения их функциональных обязанностей.

4.3. Приказом директора учреждения утверждается Перечень ПДн, обрабатываемых в учреждении. Обработка ПДн, не включенных в Перечень, не допускается.

4.4. Перечень определяется и пересматривается в установленном в учреждении порядке не реже, чем один раз в три года.

4.5. Доступ работников учреждения к ПДн, обрабатываемым в ИСПДн учреждения, определяется перечнем подразделений, работники которых имеют доступ к ПДн, утверждаемым приказом по учреждению.

4.6. Права доступа пользователей ИСПДн учреждения определяются в соответствии с Матрицами доступа, разрабатываемыми администратором ИБ для каждой ИСПДн учреждения.

4.7. Управление учетными записями пользователей и распределение прав доступа к информационным ресурсам ИСПДн учреждения, внешним носителям информации и периферийным устройствам осуществляется администратором ИСПДн учреждения, назначаемым приказом директора учреждения, по согласованию с администратором ИБ.

4.8. Общий порядок предоставления доступа, изменения и отмены доступа к информационным ресурсам ИСПДн учреждения устанавливается организационно-распорядительными документами учреждения.

4.9. Ответственный за ИБ осуществляет оценку необходимости запрашиваемого уровня доступа к ПДн.

4.10. Ответственный за ИБ осуществляет учет лиц, допущенных к работе с ПДн в ИСПДн учреждения.

4.11. Ответственный за ИБ осуществляет контроль за своевременным блокированием доступа (изменением прав доступа) при увольнении пользователя ИСПДн учреждения (изменении должностных обязанностей).

4.12. В пределах контролируемой зоны учреждения запрещено подключение к информационной сети мобильных технических средств, портативных рабочих станций и внешних носителей информации.

## **5. СИСТЕМА ЗАЩИТЫ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ**

5.1. Обеспечение защиты межсетевого взаимодействия реализуется по следующим направлениям:

- выделение сетевых сегментов обработки ПДн в информационной сети учреждения;
- межсетевое экранирование выделенных сегментов обработки ПДн Организации;
- разграничение доступа пользователей к ресурсам сетей связи общего пользования.

5.2. В информационной сети учреждения должны быть выделены:

- сегменты серверов ИСПДн;
- сегменты пользователей ИСПДн;
- сегмент локальной вычислительной сети (далее – ЛВС) учреждения;
- сегмент СЗПДн.

5.3. Включение новых серверов и рабочих станций в сегменты ИСПДн должно осуществляться только после выполнения требований по защите ПДн.

5.4. Доступ к сегментам ИСПДн из других сегментов информационной сети учреждения должен ограничиваться межсетевыми экранами.

5.5. Межсетевое экранирование сегментов ИСПДн учреждение должно обеспечивать:

- 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);
- 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 аппаратного отключения межсетевого экрана);
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- защиту беспроводных соединений, применяемых в ИСПДн.

5.6. Серверы, доступные из сетей связи общего пользования, должны быть размещены в выделенном сегменте демилитаризованной зоны. Доступ к таким серверам из сетей связи общего пользования разрешается только по необходимым сетевым портам.

5.7. Используемые межсетевые экраны должны быть сертифицированы в соответствии с требованиями к средствам межсетевого экранирования, установленными Приказом ФСТЭК России № 21 от 18.02.2013.

5.8. Управление сетевым оборудованием учреждения осуществляется инженером-электроникой и инженером-программистом.

5.9. Доступ к сетевому оборудованию разрешен только инженеру-электронику и инженеру-программисту.

5.10. В случае производственной необходимости пользователям ИСПДн учреждения может предоставляться доступ:

-к сети Интернет;

-к сервисам внешней электронной почты.

5.11. Правила работы пользователей ИСПДн с ресурсами сети Интернет и электронной почты устанавливаются организационно-распорядительными документами учреждения.

## **6. РЕЖИМ БЕЗОПАСНОСТИ ПОМЕЩЕНИЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1. Обеспечение безопасности помещений ИСПДн направлено на исключение возможности несанкционированного доступа к техническим средствам ИСПДн, их хищения и нарушения работоспособности, хищения носителей информации.

6.2. Приказом директора учреждения определяются границы контролируемой зоны учреждения, на территории которой исключено бесконтрольное пребывание посторонних лиц.

6.3. Реализация режима безопасности помещений ИСПДн возлагается на лица, работающие в данных помещениях.

## **7. БЕЗОПАСНОСТЬ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ**

7.1. Безопасность информации, хранящейся на бумажных и отчуждаемых электронных носителях ПДн, обеспечивается путем организации системы учета и безопасного хранения носителей ПДн.

7.2. Ответственным за учет и соблюдение условий хранения электронных носителей ПДн является ответственный за ИБ.

7.3. При уничтожении носителя ПДн должны обеспечиваться и контролироваться гарантированное уничтожение (стирание) ПДн.

## **8. ЗАЩИТА ОТ ВРЕДОНОСНОГО КОДА**

8.1. Средства защиты от вредоносного кода должны быть установлены на всех рабочих станциях и серверах учреждения.

8.2. Средства защиты от вредоносного кода должны обеспечивать:

- автоматическое блокирование или удаление обнаруженного вредоносного программного обеспечения;
- регулярную проверку программных модулей рабочих станций и серверов ИСПДн учреждения на предмет наличия в них вредоносного программного обеспечения по типовым шаблонам и с помощью эвристического анализа;

- возможность отката операций удаления вредоносного программного обеспечения путем помещения файлов, содержащих вредоносное программное обеспечение, в карантин;
- своевременное обновление антивирусных баз (сигнатур угроз) и программных модулей.

8.3. При выявлении фактов заражения вредоносным программным обеспечением ответственным за обеспечение безопасности ПДн проводится разбирательство с целью установления причин возникновения заражения.

8.4. Обязанности по устранению последствий заражения вредоносным программным обеспечением возлагаются на ответственного за ИБ.

## **9. ПАРОЛЬНАЯ ЗАЩИТА**

9.1. Парольная защита применяется для исключения возможности получения несанкционированного доступа к элементам ИСПДн учреждения (рабочим станциям, серверам, активному сетевому оборудованию) в целях недопущения утечки, а также несанкционированной модификации или уничтожения ПДн.

9.2. Парольная защита применяется:

- при доступе пользователей к операционным системам рабочих станций и серверов, прикладному программному обеспечению ИСПДн учреждения, средствам защиты информации;
- при доступе системных администраторов к средствам управления сетевым и серверным оборудованием, операционным системам серверов и рабочих станций, специальному программному обеспечению ИСПДн учреждения, средствам защиты информации.

9.3. Требования парольной защиты определяются организационно-распорядительными документами учреждения.

9.4. При выявлении фактов нарушения требований парольной защиты ответственным за обеспечение безопасности ПДн проводится разбирательство.

## **10. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА НИХ**

10.1. Для регистрации и учета событий, которые могут привести к снижению уровня защищенности ПДн (далее – инцидентов), должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также применяться средства (системы) анализа защищенности.

10.2. Средства (системы) анализа защищенности должны обеспечивать, в том числе:

- выявление и анализ уязвимостей, связанных с ошибками в конфигурации операционных систем и программного обеспечения рабочих станций и серверов ИСПДн учреждения;
- контроль установки обновлений программного обеспечения рабочих станций и серверов ИСПДн учреждения.

10.3. В учреждении должен быть обеспечен контроль заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн учреждения.

10.4. Анализ инцидентов осуществляется:

- Ответственным за ИБ при просмотре журналов событий, формируемых средствами защиты информации;
- Ответственным за ИСПДн при просмотре журналов событий, формируемых программным обеспечением ИСПДн и системами управления базами данных;
- Инженером-программистом и инженером-электронником при просмотре журналов событий сетевого и серверного оборудования, операционных систем и системного программного обеспечения.

10.5. О фактах обнаружения инцидентов ответственные работники должны немедленно сообщать ответственному за ИБ.

10.6. Права доступа на модификацию и удаление журналов событий безопасности должны быть ограничены для всех пользователей ИСПДн учреждения.

## **11. СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

11.1. Система криптографической защиты информации предназначена для криптографической защиты информации, передаваемой по каналам связи, расположенным вне контролируемой зоны учреждения.

11.2. Криптографическая защита должна реализовываться алгоритмами, определяемыми ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 с применением программно-технических средств шифрования и/или специального прикладного программного обеспечения, сертифицированных в установленном порядке ФСБ России.

11.3. Эксплуатация СКЗИ должна осуществляться в полном соответствии с эксплуатационной и технической документацией к ним.

11.4. Допуск работников учреждения к работе с СКЗИ должен осуществляться в соответствии со списком лиц, допущенных к СКЗИ, утвержденным ответственным за обеспечение безопасности ПДн.

11.5. Допуск работников учреждения к работе с СКЗИ должен осуществляться после проведения ответственным за ИБ обучения и ознакомления с требованиями по работе с СКЗИ.

11.6. Ответственный за ИБ должен вести учет используемых СКЗИ, технической и эксплуатационной документации к ним в Журнале учета СКЗИ.

11.7. Контроль выполнения требований по эксплуатации СКЗИ осуществляет ответственный за ИБ. При выявлении фактов нарушения требований по эксплуатации СКЗИ ответственным за обеспечение безопасности ПДн проводится разбирательство.

## **12. ОРГАНИЗАЦИЯ СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ**

12.1. Для обеспечения возможности восстановления функционирования и работоспособности ИСПДн учреждения и средств защиты информации при возникновении аварийных ситуаций должна быть реализована система резервного копирования и восстановления.

12.2. Резервному копированию подлежат информация следующих основных категорий:

- ПДн, хранящиеся в виде отдельных файлов, каталогов или баз данных ИСПДн;
- системные и конфигурационные файлы операционных систем и специального программного обеспечения серверов;

-конфигурационные файлы сетевого оборудования;

-системные и конфигурационные файлы средств защиты информации.

12.3. Ответственными за осуществление резервного копирования являются инженер-программист и инженер-электроник соответствующих информационных ресурсов.

12.4. Требования к периодичности и способам осуществления резервного копирования информационного ресурса определяются особенностями функционирования соответствующего информационного ресурса.

12.5. Ответственный за ИБ должен осуществлять регулярные проверки выполнения требований резервного копирования информационных ресурсов.

### **13. УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

13.1. В учреждении должно обеспечиваться управление конфигурацией ИСПДн и СЗПДн учреждения.

13.2. В учреждении допускается использование ограниченного набора программного обеспечения (ПО), формирующего базовую конфигурацию ИСПДн учреждения.

13.3. При первоначальной настройке рабочих станций и серверов инженером-программистом и инженер-электроником производится установка ПО на основании перечня разрешенного ПО.

13.4. Пересмотр базовой конфигурации осуществляется ответственным за ИБ при возникновении необходимости.

13.5. При согласовании внесения изменений в конфигурацию ИСПДн учреждения ответственному за ИБ необходимо учитывать потенциальное воздействие планируемых изменений на возникновение дополнительных угроз безопасности информации и на работоспособность ИСПДн учреждения.

13.6. ПО, используемое в ИСПДн учреждения, должно регулярно обновляться. Получение обновлений должно осуществляться из официальных источников производителя ПО. Получение обновлений ПО сертифицированных средств защиты информации должно осуществляться из специализированных источников обновления производителей средств в соответствии с эксплуатационной документацией к ним.

13.7. ПО, используемое в учреждении, приобретается в соответствии с лицензионной политикой разработчика.

13.8. Установка обновлений ПО не считается внесением изменений в конфигурацию ИСПДн и СЗПДн учреждения и не требует заполнения заявки на внесение изменений.

### **14. УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ**

14.1. СЗПДн должна обеспечивать управление:

- заведением и удалением учетных записей пользователей, полномочиями пользователей и поддержанием правил разграничения доступа в ИСПДн учреждения;
- резервным копированием и восстановлением работоспособности ИСПДн и СЗПДн учреждения;
- обновлением программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации;

- регистрацией и анализом инцидентов ИБ.

14.2. Администрирование СЗПДн осуществляет ответственный за ИБ.

## **15. КОНТРОЛЬ ПРИНЯТЫХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

15.1. Ответственным за контроль выполнения принятых мер по обеспечению безопасности ПДн является ответственный за обеспечение безопасности ПДн.

15.2. ответственный за ИБ осуществляет постоянный контроль выполнения требований по обеспечению безопасности ПДн в рамках выполнения своих обязанностей.

## **16. ОБУЧЕНИЕ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ**

16.1. Ответственный за ИБ должен регулярно проходить обучение на курсах повышения квалификации по вопросам защиты информации (не реже одного раза в три года).

16.2. Ознакомление работников учреждения с правилами работы с ПДн осуществляется:

- путем проведения ответственным за ИБ в учреждении, в которое принят работник, первичных инструктажей с вновь принятым работником учреждения по соблюдению установленных правил работы с ПДн;
- путем проведения обучения работников (пользователей средств вычислительной техники) ответственным за ИБ правилам работы с используемыми средствами защиты информации и СКЗИ;
- путем самостоятельного изучения работником учреждения организационно-распорядительных документов, регламентирующих вопросы обеспечения безопасности ПДн.

16.3. Допуск работников учреждения к ресурсам ИСПДн осуществляется только после прохождения первичного инструктажа и ознакомления с организационно-распорядительными документами учреждения по вопросам обеспечения безопасности ПДн.

16.4. При проведении первичного инструктажа нового пользователя ИСПДн должны быть разъяснены:

- права и обязанности пользователя ИСПДн;
- действия, которые запрещены при обработке ПДн;
- возможные последствия и ответственность в случае нарушения правил работы с ПДн.