МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ ГОРОДСКОЙ ОКРУГ ГОРОД ЛАНГЕПАС
ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА-ЮГРЫ
ЛАНГЕПАССКОЕ ГОРОДСКОЕ МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
«СПОРТИВНАЯ ШКОЛА»
(ЛГ МАУ «Спортшкола»)

ПРИКАЗ

«_30_» __июля__ 2018г. № _247_ - ОД

Об обеспечении безопасности конфиденциальной информации

В соответствии с Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных (ред. от 25.07.2011), Постановлением Правительства Российской Федерации от 17.11.2007 №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», письмом руководителя Аппарата Губернатора-заместителя Губернатора Ханты-Мансийского автономного округа - Югры от 20.10.2011 №ВЕ-21623 «Об обеспечении безопасности конфиденциальной информации», распоряжением администрации города Лангепас от 12.12.2011 №460-р «Об обеспечении безопасности конфиденциальной информации», Уставом учреждения, в целях обеспечения требуемого уровня безопасности конфиденциальной информации в ЛГ МАУ «Спортшкола»,

ПРИКАЗЫВАЮ:

1. Утвердить Положение по организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ЛГ МАУ «Спортшкола». Приложение 1.
2. Утвердить Положение о порядке обработки персональных данных без использования средств автоматизации в ЛГ МАУ «Спортшкола». Приложение 2.
3. Утвердить Положение о защите персональных данных спортсменов и их родителей (законных представителей) в ЛГ МАУ «Спортшкола». Приложение 3.
4. Техническое обслуживание и ремонт автоматизированных систем с машинными носителями конфиденциальной информации осуществлять специалистами (согласно договора) в присутствии должностного лица, ответственного за выполнение мероприятий по защите информации.
5. При передаче автоматизированных систем сторонним организациям для проведения профилактических или ремонтно-восстановительных работ изымать из состава автоматизированных систем машинные носители конфиденциальной информации.
6. В случае принятия решения о завершении обработки информации на автоматизированной системе с машинными носителями конфиденциальной информации по причине неисправности (списания) или приобретения новой автоматизированной системы:

6.1. Исключить повторное использование машинных носителей конфиденциальной информации в автоматизированных системах, обрабатывающих общедоступную информацию.

6.2. Выполнить стирание (форматирование) машинного носителя конфиденциальной информации с оформлением Акта о стирании информации ограниченного доступа.

6.3. Отформатированный документ и учтенный машинный носитель конфиденциальной информации использовать повторно только на автоматизированных системах, обрабатывающих конфиденциальную информацию.

6.4. Уничтожать машинные носители конфиденциальной информации в случае, если стереть информацию не предоставляется возможным или при условии, что данный носитель не будет использоваться на автоматизированных системах, обрабатывающих конфиденциальную информацию, с оформлением Акта об уничтожении машинного носителя и с отметкой в журнале учета машинных носителей конфиденциальной информации.

7. Ответственному за защиту информации в ЛГ МАУ «Спортшкола», заведующему отделом И.В. Радостевой:
7.1. организовать учет машинных носителей конфиденциальной информации (винчестеры, flash-накопители) в соответствии с Перечнем мероприятий согласно Приложению 4;
7.2. оформлять сведения о ремонтных (профилактических) работах, в том числе сведения об установке и модификации аппаратных и программных средств, по журналу учета ремонтных (профилактических) работ, выполненных на автоматизированных системах, обрабатывающих конфиденциальную информацию, согласно Приложению 5.
8. Контроль исполнения приказа оставляю за собой.

И.о. директора **О.А. Хабаров**

При проведении антикоррупционной экспертизы приказа (проекта приказа) признаки коррупциогенности не выявлены (выявлены, не выявлены)

Председатель Комиссии _____ М.А. Марочкина

С приказом ознакомлен (а) и согласен(а):

«30»	07	2018г.	(Ю.В. Найбауэр)
«30»	07	2018г.	(И.В. Федотова)
«30»	07	2018г.	(Е.Р. Ковалёв)
«30»	07	2018г.	(С.В. Медведев)
«30»	07	2018г.	(К.В. Тюленева)
«01»	08	2018г.	(О.В. Копалова)
«07»	08	2018г.	(М.Г. Махмудова)
«07»	08	2018г.	(Г.Р. Шарнас)
«19»	08	2018г.	(И.В. Радостева)
«___»		2018г.	(_____)
«___»		2018г.	(_____)
«___»		2018г.	(_____)

Приложение 1
к приказу ЛГ МАУ «Спортшкола»
№247- ОД от 30 июня 2018г.

Положение по организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

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) Лангепасского городского муниципального автономного учреждния «Спортвная школа» (далее – Учреждение).

1.2. В Учреждении обработка ПДн осуществляется в следующих информационных системах (далее - ИС):

- *Система по начислению заработной платы (1С: Бухгалтерия);*
- *Система учета персональных данных работников (1С: Предприятие – зарплата, кадры);*

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

1. Порядок организации работ по обеспечению безопасности персональных данных

1.1. С целью организации работ по защите ПДн приказом «О назначении ответственного лица» от 20.03.2018 №92 назначен ответственный за обеспечение безопасности ПДн.

1.2. 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;
- утверждение базовой конфигурации ИС и СЗПДн Учреждения;
- проведение разбирательств по фактам возникновения событий, которые могут привести к снижению уровня защищенности ПДн.

1.3. Ответственным за выполнение работ по обеспечению безопасности ПДн при их обработке в ИС Учреждения является администратор информационной безопасности (далее – администратор ИБ), назначаемый приказом директора учреждения.

1.4. Реализация требований по обеспечению безопасности ПДн осуществляется администраторами, разработчиками и пользователями информационных систем Учреждения.

2. Требования по обеспечению безопасности персональных данных

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

2.2. 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.

2.3. Применение средства защиты информации разрешается после проверки корректности его функционирования и оформления заключения о готовности средства защиты информации к эксплуатации (форма заключения приведена в приложении №1). Требования по обеспечению безопасности ПДн при их обработке в ИСПДн Учреждения реализуются в рамках следующих направлений:

- организация системы допуска и учета лиц, допущенных к работе с ПДн;
- организация системы защиты межсетевого 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.

3. Система допуска и учета лиц

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

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

3.3. Приказом директора Учреждение утверждается Перечень ПДн, обрабатываемых в Учреждении. Обработка ПДн, не включенных в Перечень, не допускается.

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

3.5. Доступ работников Учреждения к ПДн, обрабатываемым в ИСПДн Учреждения, определяется перечнем подразделений, работники которых имеют доступ к ПДн, утверждаемым приказом по Учреждению.

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

3.7. 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.

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

3.9. Администратор ИБ осуществляет оценку необходимости запрашиваемого уровня доступа к ПДн.

3.10. Администратор ИБ осуществляет учет лиц, допущенных к работе с ПДн в ИСПДн Учреждения.

3.11. Администратор ИБ осуществляет контроль за своевременным блокированием доступа (изменением прав доступа) при увольнении пользователя ИСПДн Учреждения (изменении должностных обязанностей).

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

4. Система защиты межсетевого взаимодействия

4.1. Обеспечение защиты межсетевого взаимодействия реализуется по следующим направлениям:

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

4.2. В корпоративной информационной сети Учреждения должны быть выделены:

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

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

4.4. Доступ к сегментам ИСПДн из других сегментов корпоративной информационной сети Организации должен ограничиваться межсетевыми экранами.

4.5. Межсетевое экранирование сегментов ИСПДн Учреждения 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.

4.6. Межсетевое экранирование должно обеспечивать отделение ЛВС и сети среды виртуализации от сетей связи общего пользования.

4.7. 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.

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

4.9. Управление сетевым оборудованием Учреждения осуществляется системным администратором.

4.10. В случае производственной необходимости пользователям ИСПДн Учреждения может предоставляться доступ:

- к сети Интернет;
- к сервисам внешней электронной почты.

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

5. Режим безопасности помещений информационных систем персональных данных

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

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

5.3. Режим безопасности помещений ИСПДн реализуется в соответствии с Положением об организации режима безопасности помещений ИСПДн.

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

6. Безопасность носителей персональных данных

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

6.2. Ответственным за учет и соблюдение условий хранения электронных носителей ПДн является администратор ИБ.

6.3. Порядок учета, хранения и уничтожения носителей ПДн регламентируется Положением об учете, порядке хранения и уничтожения носителей ПДн.

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

7. Защита от вредоносного кода

7.1. Средства защиты от вредоносного кода должны быть установлены на всех рабочих станциях и серверах Учреждения.

7.2. 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 обеспеченияпо типовым шаблонам и с помощью эвристического анализа;
- возможность отката операций удаления вредоносного программного обеспечения путем помещения файлов, содержащих вредоносное программного обеспечение, в карантин;
- своевременное обновление антивирусных баз (сигнатур угроз) и программных модулей.

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

7.4. Обязанности по устранению последствий заражения вредоносным программным обеспечением возлагаются на администратора ИБ.

8. Парольная защита

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

8.2. Парольная защита применяется:

- при доступе пользователей к операционным системам рабочих станций и серверов, прикладному программному обеспечению ИСПДн Учреждение, 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.

8.3. Требования парольной защиты определяются организационно-распорядительными документами Учреждения.

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

9. Управление инцидентами информационной безопасности и реагирование на них

9.1. 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.

9.2. 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.

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

9.4. Анализ инцидентов осуществляется:

- администратором ИБ при просмотре журналов событий, формируемых средствами защиты информации;
- администратором ИСПДн при просмотре журналов событий, формируемых программным обеспечением ИСПДн и системами управления базами данных;
- системными администраторами при просмотре журналов событий сетевого и серверного оборудования, операционных систем и системного программного обеспечения.

9.5. Журналы аудита должны просматриваться ответственными работниками регулярно (не реже одного раза в неделю).

9.6. О фактах обнаружения инцидентов ответственные работники должны немедленно сообщать администратору ИБ.

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

10. Система криптографической защиты информации

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

10.2. 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.

10.3. Эксплуатация СКЗИ должна осуществляться в полном соответствии с эксплуатационной и технической документации к ним.

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

10.5. Допуск работников Учреждения к работе с СКЗИ должен осуществляться после проведения администратором ИБ обучения и ознакомления с требования по работе с СКЗИ.

10.6. Администратор ИБ должен вести учет используемых СКЗИ, технической и эксплуатационной документации к ним в Журнале учета СКЗИ и Журнале учета приема-выдачи СКЗИ.

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

10.8. Порядок использования СКЗИ в Учреждении определяется Положением о контроле использования СКЗИ.

11. Организация системы резервного копирования и восстановления

11.1. 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.

11.2. Резервному копированию подлежит 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.

11.3. Ответственными за осуществление резервного копирования являются системные администраторы соответствующих информационных ресурсов.

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

11.5. Администратор ИБ должен осуществлять регулярные проверки выполнения требований резервного копирования информационных ресурсов.

12. Управление конфигурацией информационных систем персональных данных и системы защиты персональных данных

12.1. В Учреждении должно обеспечиваться управление конфигурацией ИСПДн и СЗПДн Учреждения.

12.2. В Учреждении допускается использование ограниченного набора программного обеспечения (ПО), формирующего базовую конфигурацию ИСПДн Учреждения.

12.3. Состав базовой конфигурации ПО на рабочих станциях и серверах ИСПДн Учреждения утверждается приказом директора Учреждения (форма состава базовой конфигурации ПО приведена в приложении №2). Установка на рабочих станциях и серверах ИСПДн Учреждения ПО, не входящего в состав разрешенного ПО, не допускается.

12.4. Состав базовой конфигурации ПО СЗПДн Учреждения устанавливается эксплуатационной документацией на СЗПДн Учреждения.

12.5. При первоначальной настройке рабочих станций и серверов системными администраторами производится установка ПО на основании перечня разрешенного ПО.

12.6. Пересмотр базовой конфигурации осуществляется администратором ИБ при возникновении необходимости по согласованию с ответственным за обеспечение безопасности ПДн. Пересмотренная базовая конфигурация доводится до сведения всех работников Учреждения путем рассылки по электронной почте с обязательным запросом уведомления о прочтении письма.

12.7. Внесение изменений в конфигурацию ИСПДн Учреждения осуществляется на основании заявки заинтересованного лица, согласованной с руководителем структурного подразделения (форма заявки приведена в приложении №3).

12.8. При согласовании внесения изменений в конфигурацию ИСПДн Учреждения администратору ИБ необходимо учитывать потенциальное воздействие планируемых

изменений на возникновение дополнительных угроз безопасности информации и на работоспособность ИСПДн Учреждения.

12.9. 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.

12.10. ПО, используемое в Учреждении, приобретается в соответствии с лицензионной политикой разработчика.

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

13. Управление системой защиты информации информационной системы

13.1. СЗПДн должна обеспечивать управление:

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

13.2. Администрирование СЗПДн осуществляет администратор ИБ.

14. Контроль принятых мер по обеспечению безопасности персональных данных

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

14.2. Администратор ИБ осуществляет постоянный контроль выполнения требований по обеспечению безопасности ПДн в рамках выполнения своих обязанностей.

14.3. Мероприятия по контролю мер выполнения требований по обеспечению безопасности ПДн проводятся в соответствии с Планом внутренних проверок, утвержденным приказом директора Организации.

14.4. Контроль эффективности мер защиты информации должен осуществляться в соответствии с Положением по организации контроля эффективности защиты информации.

15. Обучение по вопросам обеспечения безопасности

15.1. Администратор ИБ должен регулярно проходить обучение на курсах повышениякваликации по вопросам защиты информации (не реже одного раза в три года).

15.2. Ознакомление работников Организации с правилами работы с ПДн осуществляется:

- путем проведения руководителем структурного подразделения Организации, в которое принят работник, первичных инструктажей с вновь принятым работником Организации по соблюдению установленныхправил работы с ПДн;
- путем проведения обучения работников (пользователей средств вычислительной техники) администратором ИБ правилам работы с используемыми средствами защиты информации и СКЗИ;
- путем самостоятельного изучения работником Организацииорганизационно-распорядительных документов, регламентирующих вопросы обеспечения безопасности ПДн.

15.3. Допуск работников Организации к ресурсам ИСПДн осуществляется только после прохождения первичного инструктажа и ознакомления с организационно-распорядительными документами Организациипо вопросам обеспечения безопасности ПДн.

15.4. 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.