

	<b>РУКОВОДСТВО ПО КАЧЕСТВУ РК ВНГ - 2018</b>	ПО.73.03-2021
		Страница 1 из 6

УТВЕРЖДАЮ  
 Директор  
 MAOY Вторая гимназия  
 И. М. Михно  
 «02» марта 2021 год

<b>ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИСПД ГИМНАЗИИ</b>	<b>ПО.73.03-2021</b>
--	----------------------

<b>Введено в действие приказом № 83 от «02» марта 2021 г.</b>	<b>экземпляр № 1</b>
---	----------------------

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных MAOY Вторая гимназия (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

Положение обязательно для исполнения всеми работниками MAOY Вторая гимназия (далее – Гимназия), непосредственно осуществляющими защиту ПДн, обрабатываемых в ИСПДн.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

**Основные технические средства и системы** – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи 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 обработ-



ки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

**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. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Основной целью обеспечения безопасности ПДн, при их обработке в ИСПДн, является защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Задачей, которую необходимо решить для достижения поставленной цели, является обеспечение безопасности ПДн при их обработке в ИСПДн с помощью системы защиты персональных данных (далее – СЗПДн), нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных».

СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

### 4. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

СЗПДн основывается на следующих принципах:

- **Принцип системности** – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.
- **Принцип комплексности** – предполагает, что СЗПДн должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности ПДн от возможных угроз всеми доступными законными средствами, методами и мероприятиями.
- **Принцип непрерывности защиты** – это процесс обеспечения безопасности ПДн, осуществляемый руководством, ответственным за обеспечение безопасности ПДн в ИСПДн и работниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность СЗИ, сколько процесс, который должен постоянно идти на всех уровнях внутри Гимназии, и каждый работник должен принимать участие в этом процессе.
- **Принцип разумной достаточности** – предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

- **Принцип гибкости** – СЗПДн должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.
- **Принцип простоты применения СЗИ** – механизмы защиты должны быть интуитивно понятны и просты в применении. Применение СЗИ не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

## 5. ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, проводятся следующие мероприятия:

- определение ответственных лиц за обеспечение защиты ПДн;
- определение актуальных угроз безопасности ПДн;
- определение уровня защищенности ПДн;
- реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн;
- ограничение доступа в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку ПДн;
- учет и хранение съемных машинных носителей ПДн;
- организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ;
- организация парольной защиты;
- организация антивирусной защиты;
- организация обновления программного обеспечения и СЗИ;
- использование СЗИ;
- использование средств шифровальной (криптографической) защиты информации (далее – СКЗИ);
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн;
- планирование мероприятий по защите ПДн в ИСПДн;
- управление (администрирование) СЗПДн;
- управление конфигурацией ИСПДн и СЗПДн;
- реагирование на инциденты;
- информирование и обучение персонала ИСПДн.

5.2. За вопросы обеспечения безопасности ПДн, обрабатываемых в ИСПДн, отвечают:

- директор Гимназии;
- ответственный за организацию обработки ПДн – работник, отвечающий за организацию и состояние процесса обработки ПДн;
- ответственный за обеспечение безопасности ПДн в ИСПДн – работник, отвечающий за правильность использования и нормальное функционирование установленной СЗПДн;



- администратор ИСПДн – работник, отвечающий за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки ПДн.

5.3. Актуальные угрозы безопасности ПДн, обрабатываемых в ИСПДн, определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей ИСПДн, возможных способов реализации угроз безопасности ПДн и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности). Для определения угроз безопасности ПДн и разработки «Модели угроз безопасности персональных данных» применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 п. 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. №1085.

5.4. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и оформляется в виде «Акта об определении уровня защищенности персональных данных».

5.5. Реализация правил разграничения доступа, к ПДн, обрабатываемым в ИСПДн, осуществляется в соответствии с «Положением о разрешительной системе доступа в информационных системах персональных данных МАОУ Вторая гимназия, утвержденным приказом директора Гимназии.

5.6. Основные технические средства и системы ИСПДн располагаются в помещениях, находящихся в пределах границы контролируемой зоны, определенной приказом директора Гимназии, с максимальным удалением от её границ.

5.7. Доступ в помещения, в которых ведется обработка ПДн, осуществляется в соответствии с действующими Правилами доступа работников в помещения, в которых ведется обработка персональных данных, утвержденными приказом директора Гимназии.

5.8. Работа со съемными машинными носителями ПДн в ИСПДн осуществляется в соответствии с «Порядком обращения со съемными машинными носителями персональных данных в МАОУ Вторая гимназия, утвержденным приказом генерального директора Гимназии.

5.9. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МАОУ Вторая гимназия, утвержденной приказом директора Гимназии.

5.10. Организация парольной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по парольной защите информации в МАОУ Вторая гимназия, утвержденной приказом директора Гимназии.

5.11. Организация антивирусной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по организации антивирусной защиты в МАОУ Вторая гимназия, утвержденной приказом директора Гимназии.

5.12. Организация обновления программного обеспечения и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных МАОУ Вторая



гимназия и «Инструкцией администратора информационных систем персональных данных МАОУ Вторая гимназия, утвержденные приказом директора Гимназии.

5.13. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, применяются СЗИ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации, в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании».

5.14. Установка и настройка СЗИ в ИСПДн проводится в соответствии с эксплуатационной документацией на СЗПДн и документацией на СЗИ.

5.15. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, при их передаче по открытым каналам связи, применяются СКЗИ. Обращение с СКЗИ, эксплуатируемыми в ИСПДн, осуществляется в соответствии с «Инструкцией по обращению со средствами криптографической защиты информации в МАОУ Вторая гимназия, утвержденной приказом директора Гимназии.

5.16. На этапах внедрения СЗПДн проводится оценка эффективности принимаемых мер по обеспечению безопасности ПДн, которая включает в себя:

- предварительные испытания СЗПДн;
- опытную эксплуатацию СЗПДн;
- анализ уязвимостей ИСПДн и принятие мер по их устранению;
- приемочные испытания СЗПДн.

5.17. Ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн должны сообщаться любые инциденты информационной безопасности, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн;
- факты попыток и успешной реализации несанкционированного доступа в помещения, в которых ведется обработка ПДн;
- факты сбоя или некорректной работы систем обработки ПДн;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн, обрабатываемых в ИСПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн в ИСПДн.

5.18. Разбор инцидентов информационной безопасности проводится в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных МАОУ Вторая гимназия, утвержденным приказом И. о. директора Гимназии.

5.19. Контроль за принимаемыми мерами по обеспечению безопасности ПДн осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в МАОУ Вторая гимназия», утвержденным приказом директора Гимназии.

5.20. Все работники, допущенные в установленном порядке к работе с ПДн, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации за необеспечение сохранности и несоблюдение правил работы с ПДн.

5.21. Ответственность за доведение требований настоящего Положения до работников Гимназии и обеспечение мероприятий по их реализации несет ответственный за обеспечение безопасности ПДн в ИСПДн.

## 6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

	<b>РУКОВОДСТВО ПО КАЧЕСТВУ РК ВНГ - 2018</b>	ПО.73.12-2020
		Страница 6 из 6

Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно. Изменения в Положение вносятся согласно установленному в Гимназии порядку.

Право ходатайствовать о внесении изменений в Положение имеет руководитель и заместители руководителя Гимназии. Разработка и актуализация документации, контроль применения внутренней документации осуществляется на основании п. 6.3.4 и п. 6.3.5 СМК.ДП.4.2.3-01.2018.