

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.

ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1 Положение об обеспечении безопасности персональных данных в (далее – Положение) разработано в целях выполнения требований законодательства Российской Федерации в области защиты персональных данных.

2.2 Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности персональных данных в МАОУ "Средняя общеобразовательная школа № 2 с углубленным изучением английского языка» (далее – Оператор).

2.3 Настоящий документ учитывает положения основных нормативных правовых актов в области защиты персональных данных, а именно:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации №1119 от 1 ноября 2012 г. "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Нормативных актов ФСТЭК России:
 - «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 15 февраля 2008 г.;
 - «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 14 февраля 2008 г.;
 - Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. N 21 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Нормативных актов ФСБ России:
 - «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622;
 - «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.

2.4 Настоящее Положение предназначено для всех работников Оператора, а также третьих лиц, получающих временный или постоянный доступ к обрабатываемым у него ПДн на законном основании.

2.5 Настоящее Положение действует с момента его утверждения руководителем Оператора.

2.6 Актуализация настоящего Положения проводится не реже, чем два раза в год в соответствии с Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

2.7 Внесение изменений в настоящее Положение либо утверждение его новой редакции производится на основании соответствующего приказа руководителя Оператора.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1 ПДн, обрабатываемые у Оператора, цели, основание и сроки их обработки указаны в Перечне обрабатываемых персональных данных.

3.2 Обработка ПДн осуществляется Оператором с использованием средств автоматизации и без их использования.

3.3 Сроки хранения ПДн устанавливаются в письменном согласии субъекта ПДн на обработку его персональных данных, а также требованиями законодательства Российской Федерации, устанавливающими сроки хранения документов.

4. ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Под организацией работ по обеспечению безопасности ПДн понимается формирование и всестороннее обеспечение реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от реализации угроз безопасности ПДн, и осуществляемых в целях:

- предотвращения возможных (потенциальных) угроз безопасности ПДн;
- нейтрализации и/или парирования реализуемых угроз безопасности ПДн;
- ликвидации последствий реализации угроз безопасности ПДн.

4.2 Организация работ по обеспечению безопасности ПДн у Оператора должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по обеспечению безопасности ПДн Оператором.

4.3 Задачи по приведению деятельности Оператора в соответствие с требованиями законодательства Российской Федерации в области ПДн возлагаются на специально создаваемую для этих целей Комиссию и лиц, ответственных за организацию обработки и обеспечение безопасности ПДн, которые могут быть включены в состав данной Комиссии.

4.5 В случаях, когда Оператор на основании договора поручает обработку ПДн третьему лицу, Оператору необходимо заключить с данным лицом соглашение о соблюдении безопасности персональных данных, с возложением на третье лицо обязанности по обеспечению конфиденциальности и безопасности переданных Оператором ПДн (либо включить данное обязательство в заключаемый/действующий договор).

4.6 Работы по приведению деятельности Оператора в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям: обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации.

4.7 Работы по обеспечению безопасности ПДн, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:

- определение перечня лиц, допущенных к обработке ПДн;
- информирование работников Оператора об установленных правилах обработки ПДн и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности ПДн;
- учет и защита носителей ПДн;
- разграничение доступа к носителям ПДн;

- уничтожение ПДн.

5. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 В целях оценки уровня защищенности обрабатываемых у Оператора ПДн и своевременного устранения несоответствий требованиям законодательства РФ в области защиты ПДн у Оператора раз в год должен проводиться анализ изменений процессов защиты ПДн.

5.2 Анализ изменений проводится по следующим основным направлениям:

- перечень сотрудников и третьих лиц, допущенных в обработке ПДн, степень их участия в обработке ПДн и характер взаимодействия между собой;
- перечень и объем обрабатываемых ПДн;
- цели обработки ПДн;
- процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожения ПДн;
- способы обработки ПДн (автоматизированная, неавтоматизированная);
- перечень уполномоченных органов, в рамках отношений с которыми осуществляется обработка ПДн;
- перечень организационно-распорядительной документации, определяющей порядок обработки и защиты ПДн у Оператора;
- физические меры защиты ПДн, организация пропускного режима.

5.3 Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности ПДн, обрабатываемых с использованием средств автоматизации и без использования таких средств и при необходимости их уточнения.

5.4 Доступ к ПДн осуществляется в соответствии с Регламентом по допуску сотрудников и третьих лиц к обработке персональных данных, утвержденным Оператором.

5.5 Лица, допущенные к обработке ПДн, должны быть проинформированы:

- о допуске к обработке ПДн путем ознакомления с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным, обрабатываемым у Оператора;
- о категориях обрабатываемых ПДн путем ознакомления с утвержденным Перечнем обрабатываемых персональных данных;
- о правилах осуществления обработки ПДн путем ознакомления под роспись с документов Положением об обработке персональных данных.

5.6 Неавтоматизированная обработка ПДн должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения материальных носителей и установить перечень лиц, допущенных к обработке ПДн. У Оператора должен вестись учет носителей ПДн.

5.7 Фиксация ПДн должна осуществляться на отдельных материальных носителях (отдельных документах). ПДн должны отделяться от иной информации.

5.8 Фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы, не допускается. В случае если на одном материальном носителе все же зафиксированы ПДн, цели обработки которых несовместимы, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн осуществляется выборочное копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется);
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным выборочным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

5.10 Правила учета, хранения и уничтожения ПДн при неавтоматизированной обработке описаны в Регламенте по учёту, хранению и уничтожению носителей персональных данных.

5.9 При обработке ПДн, Оператор, должна иметь возможность и средства для восстановления ПДн, в случае их модификации или уничтожении вследствие несанкционированного доступа к ним. Правила резервного копирования и восстановления ПДн Оператором установлены в Регламенте по резервному копированию персональных данных.

5.10 Оператор определяет перечень помещений, используемых при обработке ПДн. При этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

5.11 Если при работе с ПДн работнику Оператора необходимо покинуть рабочее место, материальные носители ПДн должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители помещаются в отведенных для хранения места.

5.12 В случае достижения цели обработки ПДн Оператор прекращает обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. В случае если ПДн невозможно уничтожить, то они блокируются и уничтожаются в срок, не превышающий шести месяцев.

С Положением ознакомлены :

С.В. Майорова	_____	_____	2021 г.
В.Н.Евдокимова	_____	_____	2021 г.
В.Н.Григорова	_____	_____	2021 г.
Е.М.Пшеницына	_____	_____	2021 г.
Н.А.Иванова	_____	_____	2021 г.
С.В.Щедрина	_____	_____	2021 г.
Н.Ю.Власова	_____	_____	2021 г.
М.А.Бегунов	_____	_____	2021 г.
Г.Т.Пчёлкина	<i>Г.Т.Пчёлкина</i>	<i>16.06</i>	2021 г.
Т.В.Клаузер	_____	_____	2021г.