

Итого в документе пронумеровано, прошнуровано
и скреплено печатью 5 (пять) страниц
Директор МБОУ Школа № 10 «Успех»
г.о.Самара С.А.Терентьев



Утверждено
директором МБОУ Школа № 10 «Успех» г. о. Самара
(Приказ от 17.08.2020 г. № 335-од.)

**Положение
об обеспечении безопасности персональных данных
при их обработке в информационных системах персональных данных
МБОУ Школа № 10 «Успех» г. о. Самара
(новая редакция)**

1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в образовательном учреждении.

Настоящее Положение разработано в соответствии с Федеральным законом "О персональных данных", Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 01.11.2012 № 1119.

2. Основные термины, используемые в настоящем Положении:

1) персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

2) обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

3) распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

4) использование персональных данных – действия (операции) с персональными данными, совершаемые в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

5) блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

6) уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

7) информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств (далее - информационная система)

8) технические средства, позволяющие осуществлять обработку персональных

Согласовано
Педагогическим советом
Протокол № 3 от 31.05.2020

Утверждено
директором МБОУ Школа № 10 «Успех» г. о.
Самара
(Приказ от 17.08.2020 г. № 335-од.)

данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

3. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

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

5. Информационные системы классифицируются в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

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

7. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность

носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8. Образовательное учреждение обязано обеспечивать безопасность персональных данных при их обработке в информационной системе

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

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

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

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

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

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

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

11. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе назначается

должностное лицо (работник), ответственный за обеспечение безопасности персональных данных.

12. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного руководителем образовательного учреждения.

13. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 12 настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется должностным лицом (работником), ответственным за обеспечение безопасности персональных данных.

14. При обнаружении нарушений порядка предоставления персональных данных образовательное учреждение незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

15. Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

16. К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий.

17. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

18. Уничтожение персональных данных или завершение использования персональных данных субъектов персональных данных Оператор обязан осуществлять в следующих случаях:

- выявление неправомерной обработки персональных данных, в том числе по обращению субъекта персональных данных или его представителя либо запросу уполномоченного органа по защите прав субъектов персональных данных, если обеспечить правомерность обработки персональных данных невозможно;
- требование субъекта персональных данных, если его персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- отзыв субъектом персональных данных согласия на обработку его персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных;
- достижение цели обработки персональных данных или утрата необходимости в достижении этих целей;
- истечения сроков хранения персональных данных, установленных нормативно-правовыми актами Российской Федерации и нормативно-правовыми актами Самарской области;
- признание недостоверности персональных данных или получения их незаконным путем по требованию уполномоченного органа по защите прав субъектов персональных данных;
- в иных, установленных законодательством случаях.

19. Сотрудники Школы, уполномоченные на получение, обработку, хранение, передачу и любое другое использование персональных данных осуществляют:

- контроль наступления случаев, указанных в пункте 18 настоящего положения;
- подготовку и представление комиссии по проведению мероприятий по защите персональных данных, а также по контролю за соблюдением порядка обращения с документами, содержащими персональные данные, в Школе (далее — Комиссия) пакета документов, содержащего персональные данные, подлежащие уничтожению, с описью, на утилизацию.

20. Директор Школы осуществляет контроль обоснованности уничтожения или завершения использования персональных данных.

21. Решение об уничтожении или о завершении использования персональных данных принимается Комиссией.

22. В зависимости от типа носителя информации (бумажный или электронный) выделяются два способа уничтожения персональных данных:

- физическое уничтожение носителя (уничтожение через shredding, сжигание);
- уничтожение информации с носителя.

23. Уничтожение части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

24. Уничтожение персональных данных производится в срок, не превышающий трех рабочих дней с момента наступления случаев, указанных в пункте 18 настоящего положения.

25. После уничтожения персональных данных составляется Акт об обработке персональных данных (далее — Акт).

26. Акт подписывается членами Комиссии.