

Согласовано

на заседании Управляющего совета
МБОУ «Уньюганская СОШ № 2
им. Альшевского М.И.»
Протокол №3 от «24» марта 2022 г.

Принято

на заседании педагогического совета
МБОУ «Уньюганская СОШ № 2
им. Альшевского М.И.»
Протокол № 6 от «25» марта 2022 г

Утверждаю

директор
МБОУ «Уньюганская СОШ № 2
им. Альшевского М.И.»

О.А.Каратаева
Приказ №394 -од
от «31» марта 2022 г.

Согласовано

Общее собрание
работников
МБОУ «Уньюганская
СОШ № 2
им. Альшевского
М.И.»
Протокол № 3 от «10» марта 2022 г.

Регистрационный номер 316

**ПОЛОЖЕНИЕ
ОБ ОТВЕТСТВЕННОМ ЛИЦЕ, ОСУЩЕСТВЛЯЮЩЕМ
ФУНКЦИИ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ
ДАНЫХ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ
ОБЩЕОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ «УНЬЮГАНСКАЯ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №2 ИМЕНИ ГЕРОЯ
СОЦИАЛИСТИЧЕСКОГО ТРУДА АЛЬШЕВСКОГО МИХАИЛА
ИВАНОВИЧА»**

п. Уньюган
2022

1. Положение об ответственном лице, осуществляющем функции по организации защиты персональных данных (далее – ПДн) в Муниципальном бюджетном общеобразовательном учреждении «Уньюганская средняя общеобразовательная школа №2 имени Героя Социалистического труда Альшевского Михаила Ивановича» (далее — Положение) разработано на основании ст.24 Конституции РФ, Закона «Об информации, информационных технологиях и защите информации» №249-ФЗ от 27.07.2006 г. (с изменениями), Федерального закона РФ «О персональных данных» №152-ФЗ от 27.07.2006 г., Федерального закона РФ от 21.07.2014 г. №242-ФЗ «о внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». (с изменениями, Устава Муниципального бюджетного общеобразовательного учреждения «Уньюганская средняя общеобразовательная школа №2 имени Героя Социалистического труда Альшевского Михаила Ивановича» (далее- Школа).
2. Настоящее Положение устанавливает требования к полномочиям и обязанностям ответственного за обеспечение защиты ПДн должностного лица (далее – ответственное лицо) в Школе при их обработке в информационных системах персональных данных (далее ИСПДн) в Школе. При этом, обрабатываемые ПДн представляют собой совокупность ПДн, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации (далее информационные системы) или без использования таковых.
3. Под техническими средствами, позволяющими осуществлять обработку ПДн, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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.
4. Ответственное лицо назначается приказом директора и обеспечивает безопасность ПДн путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.
5. Ответственное лицо обеспечивает безопасность ПДн при их обработке в информационных системах с помощью системы защиты ПДн, 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 ПДн), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.
6. Для обеспечения безопасности ПДн, при их обработке в информационных системах, ответственное лицо обеспечивает защиту 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.
7. Методы и способы защиты информации в ИСПДн устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой

- безопасности Российской Федерации в пределах их полномочий.
8. Ответственное лицо обеспечивает достаточность принятых мер по организации безопасной обработки ПДн в информационных системах, оцениваемой при проведении государственного контроля и надзора. Работы по обеспечению безопасности ПДн при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.
 9. Ответственное лицо обеспечивает применение средств защиты информации в информационных системах, прошедших в установленном порядке процедуру оценки соответствия.
 10. Ответственное лицо обеспечивает и организует разработку организационной, технической документации на ИСПДн и подготовку информационной системы к проведению оценки соответствия (аттестации).
 11. При проведении классификации ИСПДн ответственное лицо руководствуется порядком проведения классификации ИСПДн устанавливаемым совместно Федеральной службой по техническому и экспортному контролю Российской Федерации.
 12. Ответственное лицо обеспечивает обмен персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.
 13. Ответственное лицо обеспечивает размещение информационных систем, специального оборудования и охрану помещений, в которых ведется работа с ПДн, организацию режима безопасности в этих помещениях при котором обеспечивается сохранность носителей ПДн и средств защиты информации, а также исключается возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.
 14. Возможные каналы утечки информации при обработке ПДн в информационных системах определяются Федеральной службой по техническому и экспортному контролю Российской Федерации и Федеральной службой безопасности Российской Федерации в пределах их полномочий.
 15. Пользователями ИСПДн являются сотрудники, обрабатывающие ПДн в информационной системе, отвечающие за обеспечение конфиденциальности ПДн и безопасности ПДн в информационной системе на своем рабочем месте.
 16. При обработке ПДн в информационной системе
 - ответственное лицо обеспечивает и требует от пользователей ИСПДн в рамках их компетенции:
 - а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
 - б) своевременное обнаружение фактов несанкционированного доступа к ПДн;
 - в) недопущение воздействия на технические средства автоматизированной обработки ПДн в результате которого может быть нарушено их функционирование;
 - г) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
 - д) постоянный контроль за обеспечением уровня защищенности ПДн.
 17. Мероприятия по обеспечению безопасности ПДн при их обработке в информационных системах организуются и проводятся ответственным лицом и включают в себя:
 - а) определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;
 - б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов

- защиты ПД, 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 Пользователей ИСПДн, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
 - е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
 - ж) учет Пользователей ИСПДн, допущенных к работе с ПДн 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 ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
 - к) описание системы защиты ПДн.
18. Сотрудники, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании списка, утвержденного ответственным лицом и согласованного с администратором информационной безопасности ИСПДн.
19. Ответственное лицо обеспечивает регистрацию запросов Пользователей информационной системы на получение ПДн, а также факты предоставления ПДн по этим запросам в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется ответственным лицом и администратором информационной безопасности ИСПДн.
20. При обнаружении нарушений порядка предоставления ПДн администратор информационной безопасности ИСПДн по распоряжению ответственного лица незамедлительно приостанавливает предоставление ПДн пользователям информационной системы до выявления причин нарушений и устранения этих причин.