

ПРИНЯТО  
на заседании  
педагогического совета  
МБОУ «Школа № 6»  
Протокол № 5 от 09.02.2023

УТВЕРЖДАЮ  
Директор МБОУ «Школа № 6»

\_\_\_\_\_  
Е.В. Мещанкина  
Приказ № 54 от 09.02.2023

**Положение**  
**о комиссии по приведению деятельности муниципального бюджетного**  
**общеобразовательного учреждения города Ростова-на-Дону «Школа № 6**  
**имени Героя Советского Союза Самохина Н.Е.»**  
**в соответствии с требованиями законодательства Российской Федерации в**  
**области обработки персональных данных**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о комиссии по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Положение) определяет основные задачи, функции и права комиссии, в обязанности которой входит проведение работ по обеспечению безопасности и организации обработки персональных данных в МБОУ «Школа № 6» (далее – Оператор).

1.2. Комиссия по приведению Оператора в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Комиссия), назначается на весь период обработки персональных данных у Оператора приказом руководства Оператора.

1.3. Состав Комиссии назначается приказом руководства Оператора.

1.4. Из состава Комиссии работники исключаются на основании приказа руководства Оператора.

1.5. Основной задачей Комиссии является приведение деятельности Оператора в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Требования законодательства) и контроль над исполнением основных положений законодательства.

1.6. Свою деятельность Комиссия осуществляет в соответствии с «Планом мероприятий по приведению МБОУ «Школа № 6» в соответствие с требованиями законодательства Российской Федерации в области персональных данных», утверждаемым руководством Оператора.

1.7. Комиссия самостоятельно разрабатывает «План мероприятий по приведению деятельности МБОУ «Школа № 6» в соответствие с требованиями законодательства Российской Федерации в области персональных данных» и передает руководству Оператора на утверждение.

1.8. В своей деятельности Комиссия руководствуется законодательными и нормативно-правовыми актами Российской Федерации в области персональных данных, настоящим Положением и иными нормативными актами Оператора.

## **2. ОРГАНИЗАЦИОННАЯ СТРУКТУРА КОМИССИИ**

- 2.1. Комиссия состоит из Председателя Комиссии и членов Комиссии.
- 2.2. Комиссия возглавляется Председателем Комиссии.
- 2.3. Комиссия подчиняется руководству Оператора.
- 2.4. Из состава Комиссии назначается лицо, ответственное за организацию обработки персональных данных, и администратор безопасности информационных систем персональных данных.

## **3. ОСНОВНЫЕ ФУНКЦИИ КОМИССИИ**

3.1. Разработка проектов документов, необходимых для выполнения Требования законодательства.

3.2. Организация и проведение работ по обеспечению безопасности помещений, в которых производится обработка персональных данных, а также находятся на хранении материальные носители персональных данных.

3.3. Анализ и оценка соответствия внутренних нормативных документов Оператора, в части касающейся обработки персональных данных, а в случае выявления несоответствий – внесение необходимых изменений.

3.4. Организация и проведение работ по обучению и повышению осведомленности персонала в области персональных данных.

3.5. Анализ изменений законодательства Российской Федерации в области персональных данных.

3.6. Оценка выполнения Оператором обязанностей, установленных законодательством Российской Федерации в области персональных данных, а в случае выявления несоответствий – выработка рекомендаций по их устранению.

3.7. Организация подготовки и направления в уполномоченный орган по защите прав субъектов персональных данных Уведомления об обработке персональных данных, а в случае изменения сведений, содержащихся в Реестре операторов, осуществляющих обработку персональных данных, направление сведений о таких изменениях.

3.8. В случае выявления неправомерных действий с персональными данными, Комиссия направляет уведомление об устранении нарушений.

3.9. Анализ и оценка соответствия Требованиям законодательства типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, а в случае выявления несоответствий – выработка рекомендаций по их устранению.

3.10. Анализ и оценка соответствия договорной базы Оператора Требованиям законодательства, а в случае выявления несоответствий – внесение соответствующих изменений и дополнений.

3.11. Контроль выполнения Требований законодательства, в части касающейся согласия субъектов персональных данных на обработку их персональных данных.

3.12. Общий контроль соблюдения Оператором требований по обеспечению безопасности персональных данных и соблюдения Требований законодательства.

3.13. Организация работ и сбор необходимых документов при прохождении федерального государственного контроля (надзора) за соответствием обработки персональных данных Требованиями законодательства.

3.14. Ведение журнала по учету проверок в соответствии с Требованиями законодательства.

3.15. Организация работ по разработке моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных Оператора, в том числе:

3.15.1. оценка полноты и правильности определения угроз безопасности;

3.15.2. плановый и внеплановый пересмотр.

3.16. Организация работ по созданию системы защиты персональных данных (комплекса организационно-технических мер), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищенности информационных систем персональных данных.

3.17. Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.

3.18. Обучение лиц, применяющих средства защиты информации, правилам работы с ними.

3.19. Организация учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

3.20. Контроль выполнения мероприятий по защите персональных данных, реализуемых в рамках подсистем защиты с учетом уровня защищенности информационной системы персональных данных (не реже 1 раза в 3 года):

3.20.1. идентификация и аутентификация субъектов доступа и объектов доступа;

3.20.2. управление доступом субъектов доступа к объектам доступа;

3.20.3. ограничение программной среды;

3.20.4. защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

3.20.5. регистрация событий безопасности;

3.20.6. антивирусная защита;

3.20.7. обнаружение (предотвращение) вторжений;

3.20.8. контроль (анализ) защищенности персональных данных;

3.20.9. обеспечение целостности информационной системы и персональных данных;

3.20.10. обеспечение доступности персональных данных;

3.20.11. защита среды виртуализации;

3.20.12. защита технических средств;

3.20.13. защита информационной системы, ее средств, систем связи и передачи данных;

3.20.14. выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

3.20.15. управление конфигурацией информационной системы и системы защиты персональных данных.

3.21. Контроль за соответствием условий эксплуатации информационных систем персональных данных требованиям организационно-технической и эксплуатационной документации.

3.22. Контроль соблюдения работниками Оператора установленных требований по обеспечению безопасности персональных данных, проведение разбирательств и составление заключений по фактам несоблюдения данных требований.

3.23. Проведение внутренних проверок состояния защиты персональных данных.

3.24. Анализ эффективности и достаточности принятых мер и применяемых средств защиты персональных данных.

3.25. Разработка предложений по совершенствованию системы защиты персональных данных.

3.26. Решение вопросов, связанных с обслуживанием и эксплуатацией информационных систем:

3.26.1. эксплуатация информационных систем персональных данных в соответствии с организационно-технической и эксплуатационной документацией;

3.26.2. обеспечение работоспособности системы защиты персональных данных, реализуемой в рамках подсистем защиты с учетом уровня защищенности информационной системы;

3.26.3. организация мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

3.26.4. организация учета и использования машинных носителей информации;

3.26.5. организация работ по привлечению сторонних организаций для формирования и сопровождения баз данных и информационного взаимодействия (центров обработки информации), выполняющих функции операторов и администраторов системы централизованной обработки данных;

3.26.6. установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

3.26.7. учет лиц, допущенных к работе с персональными данными в информационных системах персональных данных.

3.27. Организация работ по размещению оборудования информационных систем персональных данных в части выполнения требований по сохранности носителей персональных данных и средств защиты информации, а также исключения возможности проникновения и неконтролируемого пребывания посторонних лиц на охраняемую территорию.

3.28. Уточнение персональных данных субъектов.

3.29. Блокирование обработки персональных данных субъектов.

3.30. Уничтожение персональных данных (по достижении целей обработки или в случае утраты необходимости в их достижении) при их автоматизированной обработке.

3.31. Обеспечение безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

3.32. Организация работ по ознакомлению работников Оператора, осуществляющих обработку персональных данных без использования средств автоматизации, а также лиц, осуществляющих такую обработку по договору с Оператором, о факте обработки ими персональных данных без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

3.33. Обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.34. Организация работ по уничтожению материальных носителей персональных данных в случае достижения целей обработки или в случае утраты необходимости в их достижении с составлением актов об уничтожении.

3.35. Контроль выполнения требований настоящего Положения.

3.36. Определение уровня защищенности информационных систем персональных данных.

#### **4. ПРАВА КОМИССИИ**

4.1. Запрос и получение необходимых материалов для организации и проведения работ по вопросам обеспечения безопасности персональных данных у Оператора.

4.2. Привлечение к проведению работ по защите персональных данных на договорной основе сторонних организаций.

4.3. Контроль деятельности структурных подразделений Оператора в части выполнения ими требований по обеспечению безопасности персональных данных.

5. Внесение предложений руководству Оператора о приостановке работ в случае обнаружения несанкционированного доступа, утечки персональных данных, а также в случае предпосылок нарушения безопасности персональных данных.

#### **5. Ответственность**

5.1. Председатель Комиссии и члены Комиссии несут ответственность в соответствии с законодательством Российской Федерации.

#### **6. Срок действия настоящего Положения**

6.1. Срок действия настоящего Положения не ограничен.

6.2. При изменении законодательства в настоящее Положение могут быть внесены дополнения и изменения, которые рассматриваются на заседании педагогического совета школы и утверждаются приказом МБОУ «Школа № 6».