

## **ИНСТРУКЦИЯ**

### **Ответственного за организацию обработки персональных данных в МОУ «Средняя общеобразовательная школа № 5 г. Надыма»**

#### **1. Общие положения**

1.1. Настоящая Инструкция определяет основные обязанности и права лица, ответственного за организацию обработки, хранения, использования и защиты персональных данных в МОУ «Средняя общеобразовательная школа № 5 г. Надыма» (далее – Образовательная организация).

1.2. Ответственный за организацию обработки персональных данных в Образовательной организации назначается приказом директора Образовательной организации из числа заместителей Образовательной организации.

1.3. Ответственный за организацию обработки персональных данных в Образовательной организации (далее – Ответственный) подчиняется директору Образовательной организации, в части вопросов, касающихся обработки и обеспечения безопасности персональных данных в Образовательной организации, ему подчиняются все остальные ответственные лица.

1.4. Ответственный отвечает за организацию и состояние процесса обработки персональных данных в Образовательной организации.

1.5. Ответственный осуществляет руководство должностными лицами Образовательной организации по вопросам организации обработки и обеспечения безопасности персональных данных.

1.6. Все сотрудники Образовательной организации обязаны выполнять требования Ответственного за организацию обработки персональных данных в части вопросов, касающихся обработки и обеспечения безопасности персональных данных в Образовательной организации.

1.7. Ответственный за организацию обработки персональных данных в Образовательной организации отвечает за качество проводимых им работ по контролю действий при работе с персональными данными, состояние и поддержание установленного уровня защищенности персональных данных при их обработке.

## **2. Обязанности Ответственного за организацию обработки персональных данных**

2.1. Обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации информационных систем, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью.

2.2. Знать и предоставлять ответственными лицами за информационную безопасность изменения к списку лиц, доступ которых к информации ограниченного доступа необходим для выполнения трудовых обязанностей.

2.3. Проводить инструктаж и консультации по соблюдению режима конфиденциальности.

2.4. Организовывать периодический контроль по соблюдению режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению мер по защите информации, а также принимать участие в проведении проверок уполномоченными органами.

2.5. Взаимодействовать с ответственными лицами за информационную безопасность по вопросам обеспечения и выполнения требований обработки персональных данных.

2.6. Контролировать осуществление мероприятий по установке и настройке средств защиты.

2.7. Организовывать работы по плановому контролю работоспособности технических средств защиты информации, охраны объекта, средств защиты информации от несанкционированного доступа.

2.8. Контролировать периодическое резервирование копирование баз данных и сопутствующей защищаемой информации.

2.9. По указанию руководства своевременно и точно отражать изменения в локальных актах по управлению средствами защиты информации и по правилам обработки информации ограниченного доступа.

2.10. Знать перечень и условия обработки персональных данных.

2.11. Знать перечень установленных в образовательной организации технических средств и перечень задач, решаемых с их использованием.

2.12. Обеспечивать соблюдение сотрудниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов.

2.13. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационной системы и осуществления несанкционированного доступа к защищаемой информации и техническими средствами, сообщать о них руководителю.

2.14. Инструктировать сотрудников по вопросам обеспечения информационной безопасности и правами работы с применениями средств защиты информации.

2.15. Знать Законодательство РФ о персональных данных, следить за его изменениями.

2.16. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей защищаемой информации, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

2.17. Проводить иные мероприятия, требуемые нормативными документами по защите информации.

### **3. Права Ответственного за организацию обработки персональных данных**

3.1. Требовать от всех пользователей персональных данных в Образовательной организации выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

3.2. Инициировать блокирование доступа сотрудников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.3. Учувствовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

3.4. Инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных, и технических средств или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.5. обращаться с предложением о приостановке процесса обработки персональных данных или отстранению от работы в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

3.6. Подавать свои предложения по совершенствованию мер защиты персональных данных, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

### **4. Действия при обнаружении попыток несанкционированного доступа**

4.1. К попыткам несанкционированного доступа относятся:

— сеансы работы с персональными данными пользователями, не имеющими на это право, пользователями, нарушивших установленную периодичность доступа. Или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

— действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к персональным данным, при использовании учетной записи, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа Ответственный обязан:

— по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

— доложить служебной запиской о факте несанкционированного доступа, его результате (успешный, не успешный) и предпринятых действиях;

— известить директора Образовательной организации о факте несанкционированного доступа.

## **5. Ответственность**

5.1. Ответственный несет персональную ответственность за:

- соблюдения требований настоящей Инструкции;
- правильность и объективность принимаемых решений;
- качество и своевременность проводимых им работ по обеспечению безопасности персональных данных.

5.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.