

Инструкция по работе ответственного лица за обеспечение безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности, права и ответственность ответственного лица за обеспечение безопасности персональных данных МОУ «ООШ №4 г. Катав-Ивановска» (далее – Учреждение).

1.2. Ответственное лицо за обеспечение безопасности персональных данных является штатным работником Учреждения и назначается Приказом Руководителя Учреждения.

1.3. Ответственное лицо за обеспечение безопасности персональных данных (далее - Ответственный) - лицо, отвечающее за организацию и состояние процесса обработки персональных данных в информационных системах персональных данных.

1.4. Решение вопросов организации защиты персональных данных, обрабатываемых в информационных системах Учреждения, входит в прямые трудовые обязанности Ответственного.

1.5. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

1.6. Ответственный в своей работе руководствуется Федеральным законом от 27.07.2006

№ 152-ФЗ «О персональных данных», постановлениями Правительства, руководящими и нормативными документами ФСТЭК России, а также другими нормативными правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами Учреждения.

1.7. Требования Ответственного, связанные с выполнением им своих трудовых обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к персональным данным.

1.8. Ответственный обладает правами доступа к любым носителям персональных данных Учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Блокирование персональных данных** - временное прекращение обработки персональных данных.

2.2. Доступ к информации – возможность получения информации и ее использования.

2.3. Защита информации — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.4. Информация - сведения (сообщения, данные) независимо от формы их представления.

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

2.6. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.7. Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

2.8. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.9. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.10. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

Ответственный обязан:

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

3.2. Знать и предоставлять ответственному за организацию обработки персональных данных изменения к списку лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей.

3.3. Проводить инструктаж и консультации пользователей ПЭВМ по соблюдению режима конфиденциальности.

3.4. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

3.5. Организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами.

3.6. Взаимодействовать с администратором безопасности по вопросам обеспечения и выполнения требований обработки персональных данных.

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

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

3.9. Контролировать периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации.

3.10. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и по правилам обработки персональных данных.

3.11. Знать перечень и условия обработки персональных данных в Учреждении.

3.12. Знать перечень установленных в подразделениях технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

3.13. Обеспечивать соблюдение работниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационных систем.

3.14. Осуществлять контроль за порядком учета, создания, хранения и использования машинных носителей, содержащих персональные данные.

3.15. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем подразделения, сообщать о них Руководителю Учреждения.

3.16. Инструктировать работников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами защиты информации.

3.17. Знать законодательство Российской Федерации о персональных данных, следить за его изменениями.

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

3.19. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

4. ПРАВА ОТВЕТСТВЕННОГО

Ответственный имеет право:

4.1. Требовать от всех пользователей ИСПДн выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

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

4.3. Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

4.4. Инициировать проведение служебных расследований 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 из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

4.5. Обращаться к руководителю подразделения с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

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

5. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

5.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа Ответственный обязан:

5.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

5.2.2. доложить Руководителю Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

5.2.4. известить ответственного за организацию обработки персональных данных и администратора безопасности о факте несанкционированного доступа.

6. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный несет персональную ответственность за:

6.1.1. соблюдение требований настоящей Инструкции,

6.1.2. правильность и объективность принимаемых решений,

6.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных,

6.1.4. за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

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