

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в
информационных системах персональных данных
МКОУ «Кашкентская СОШ»

1. Термины и определения

1.1. Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие право доступа к информации в соответствии с локальными актами и законодательством Российской Федерации, могут беспрепятственно реализовывать данное право.

1.2. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.3. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.4. Конфиденциальность информации – свойство безопасности информации, при котором доступ к информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации.

1.5. 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.

1.6. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.7. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

- 6.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.
- 6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.
- 6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.

1.8. Целостность информации – свойство безопасности информации, при котором изменение информации осуществляют только те субъекты доступа, которые имеют на это право в соответствии с локальными актами и законодательством Российской Федерации.

2. Общие положения

2.1. Настоящая Инструкция определяет функции, обязанности и права ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – Ответственный) ГБУ ДО РД «МАН РД» (далее – Учреждение).

2.2. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных (далее – ПДн), не исключает обязательного выполнения их требований.

2.3. Ответственный назначается приказом Директора Учреждения.

2.4. На время отсутствия (болезнь, отпуск, пр.) Ответственного его обязанности возлагаются на работника, назначенного и допущенного в установленном порядке.

3. Функциональные обязанности

3.1. Ответственный выполняет следующие функции:

- 3.1.1. Управляет доступом пользователей в ИСПДн;
- 3.1.2. Управляет полномочиями пользователей в ИСПДн;
- 3.1.3. Поддерживает установленные правила разграничения доступа в ИСПДн;
- 3.1.4. Управляет (администрирует) системой защиты информации (далее – СиЗИ) ИСПДн:
 - управляет средствами защиты информации (далее – СЗИ)
 - управляет программным обеспечением СЗИ;
 - восстанавливает работоспособность СЗИ;
 - устанавливает обновления программного обеспечения СЗИ, выпускаемых разработчиками (производителями) СЗИ;
 - анализирует события в ИСПДн, связанные с защитой информации (события безопасности);
 - информирует пользователей об угрозах безопасности информации;
 - информирует пользователей о правилах эксплуатации СЗИ;
 - обучает пользователей работе со СЗИ;
 - управляет доступом к съемным машинным носителям информации, используемым в ИСПДн (определяет должностных лиц, имеющих доступ к съемным машинным носителям информации);
 - сопровождает функционирование СиЗИ в ходе ее эксплуатации;
 - поддерживает конфигурацию СиЗИ (структуру СиЗИ, состав, места установки и параметры настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СиЗИ (поддержание базовой конфигурации СиЗИ);
 - определяет лиц, которым разрешены действия по внесению изменений в базовую конфигурацию СиЗИ;
 - управляет изменениями базовой конфигурации СиЗИ, в том числе:
 - определяет типы возможных изменений;

- разрешает или отказывает во внесении изменений;
- документирует действия по внесению изменений;
- хранит данные об изменениях.

3.1.5. Поддерживает конфигурацию ИСПДн (структуру ИСПДн, состав, места установки и параметры программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на ИСПДн;

3.1.6. Анализирует потенциальные воздействия планируемых изменений в базовой конфигурации СиЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

3.1.7. Определяет параметры настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и СиЗИ;

3.1.8. Выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИСПДн и (или) к возникновению угроз безопасности информации (далее – Инциденты), и реагирует на них.

3.1.9. Обнаруживает и идентифицирует Инциденты, в том числе:

- отказы в обслуживании;
- сбои (перезагрузки) в работе СЗИ;
- нарушения правил разграничения доступа;
- неправомерные действия по сбору информации;
- иные события, приводящие к возникновению Инцидентов.

3.1.10. Анализирует Инциденты, в том числе определяет источники и причины возникновения Инцидентов, а также оценивает их последствия;

3.1.11. Планирует меры по устранению Инцидентов, в том числе:

- по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев;
- устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению Инцидентов.

3.1.12. Планирует и принимает меры по предотвращению повторного возникновения Инцидентов.

3.1.13. Контролирует обеспечение уровня защищенности ПДн, обрабатываемых в ИСПДн:

- контролирует события безопасности и действия пользователей в ИСПДн;
- контролирует (анализирует) уровень защищенности ПДн;
- контролирует перемещение съемных машинных носителей информации за пределы контролируемой зоны лицами, которым оно необходимо для выполнения своих должностных обязанностей (функции);
- анализирует и оценивает функционирование СиЗИ ИСПДн, включая выявление, анализ и устранение недостатков в функционировании СиЗИ ИСПДн;

- выполняет периодический анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности ПДн;
- документирует процедуры и результаты контроля (мониторинга) за обеспечением уровня защищенности ПДн, содержащихся в ИСПДн;
- принимает решения по результатам контроля (мониторинга) за обеспечением уровня защищенности ПДн о доработке (модернизации) СиЗИ ИСПДн.

3.1.14. Ведет учет:

- используемых шифровальных (криптографических) СЗИ в ИСПДн, эксплуатационной и технической документации к ним;
- съемных машинных носителей (при их наличии), используемых в ИСПДн для хранения и обработки ПДн.

3.1.15. Обеспечивает защиту информации при выводе из эксплуатации ИСПДн или после принятия решения об окончании обработки информации:

- обеспечивает архивирование информации, содержащейся в ИСПДн (архивирование должно осуществляться при необходимости дальнейшего использования);
- обеспечивает уничтожение (стирание) данных и остаточной информации со съемных машинных носителей информации, при необходимости передачи съемного машинного носителя информации другому пользователю ИСПДн или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения;
- при выводе из эксплуатации съемных машинных носителей информации, на которых осуществлялись хранение и обработка ПДн, осуществляет физическое уничтожение этих съемных машинных носителей информации.

4. Права

4.1. Ответственный имеет право:

- требовать от работников – пользователей ИСПДн соблюдения установленной технологии обработки ПДн и выполнения требований локальных нормативных актов и иной организационно-распорядительной документации по обеспечению безопасности ПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи информации ограниченного доступа и технических средств, входящих в состав ИСПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования СиЗИ;
- участвовать в анализе ситуаций, касающихся функционирования СЗИ и расследования фактов несанкционированного доступа к ПДн;
- подавать свои предложения по совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

- 5.1. Ответственному категорически запрещается:
- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных (личных) целях;
 - умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках СЗИ, которые могут привести к инцидентам информационной безопасности.
- 5.2. На Ответственного возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты ПДн.
- 5.3. Ответственный несет ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

- 6.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.
- 6.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.
- 6.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.