Министерство образования и науки Мурманской области

Государственное автономное профессиональное образовательное учреждение Мурманской области

"Оленегорский горнопромышленный колледж"

УТВЕРЖДАЮ
Директор ГАПОУ МО «ОГПК»
_____ Н.В. Панас
«25» августа 2025г.

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ГАПОУ МО «ОГПК»

1. Общие положения

1.1. Настоящая Инструкция разработана на основании:

— Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

— Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

— постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящая Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных ГАПОУ МО «Оленегорский горнопромышленный колледж» (далее – ответственное лицо, информационная система) определяет права, обязанности и ответственность ответственного лица.

1.3. Ответственное лицо относится к категории специалистов и непосредственно подчиняется директору колледжа.

1.4. На должность ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных назначается лицо, имеющее высшее образование без предъявления требований к стажу работы или среднее профессиональное образование и стаж работы в аналогичных должностях не менее одного года.

1.5. Ответственное лицо назначается директором колледжа

1.6. Ответственное лицо должно знать:

— законодательство Российской Федерации в области персональных данных;

— порядок систематизации, учета и ведения документации с использованием современных информационных технологий;

— основы экономики, организации труда, производства и управления;

— средства вычислительной техники, коммуникаций и связи;

— правила и нормы охраны труда;

— локальные нормативные акты образовательной организации, касающиеся его деятельности.

1.7. В своей деятельности ответственное лицо руководствуется Положением об обработке и защите персональных для сотрудников и обучающихся ГАПОУ МО

«ОГПК», настоящей Инструкцией и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.

1.8. Ответственное лицо несёт персональную ответственность за выполнение настоящей Инструкции в установленном законом порядке.

2.Организация работы

2.1. Ответственное лицо должно иметь специальное рабочее место, размещённое на территории колледжа таким образом, чтобы исключить несанкционированный доступ к нему посторонних лиц и других сотрудников.

2.2. Рабочее место Ответственного лица должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к информационной системе, средствами контроля технических средств защиты информации (далее – СЗИ).

2.3. Ответственное лицо может привлекать сторонних сотрудников к работам по организации разграничения доступа, настройке локальной сети, техническому обслуживанию и модернизации СЗИ. Указанные работы и допуск сторонних лиц согласовываются с директором колледжа в установленном порядке и проводятся только в присутствии ответственного лица.

2.4. Ответственное лицо взаимодействует с ответственными за эксплуатацию информационной системы и/или администратором информационной системы по вопросам обеспечения защиты информации и прав доступа пользователей к ней.

2.5. На время отсутствия Ответственного лица (отпуск, болезнь, пр.) его обязанности исполняет сотрудник, назначенный в установленном порядке, который приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

3. Обязанности

Ответственное лицо обязано:

3.1. Осуществлять внутренний контроль за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, в том числе:

— проводить инструктаж и консультации пользователей информационной системы по соблюдению установленного режима конфиденциальности;

— проводить плановый и внеочередной контроль выполнения пользователями информационной системы установленного режима конфиденциальности в том числе при обращении с персональными идентификаторами, съемными носителями информации, в процессе создания электронных документов, при процедурах обезвреживания администратором безопасности информации зараженных файлов и т.д.;

— принимать участие в процедурах контроля операций по безопасному удалению личных файлов пользователей при прекращении полномочий учетной записи, по уничтожению персональных идентификаторов/паролей и созданию новых персональных идентификаторов/паролей;

— контролировать порядок учёта, создания, хранения и использования резервных и архивных копий массивов данных, электронных документов;

— контролировать поддержание в актуальном состоянии действующих локальных нормативных актов, журналов и форм учета по работе с персональными данными;

— контролировать обеспечение соответствия работ с информационной системой технике безопасности, правилам и нормам охраны труда.

— 3.2. Доводить до сведения работников колледжа положения законодательства Российской Федерации о персональных данных, локальных актов

по вопросам обработки персональных данных, требований к защите персональных данных в том числе путем:

— разработки соответствующих инструкций, методических рекомендаций, а также внесения изменений в действующие локальные нормативные акты и методические материалы колледжа;

— формирования внутренней информационной рассылки об изменениях в действующем законодательстве;

— проведения специальных занятий (семинаров, консультаций), при необходимости – с участием приглашенных специалистов.

— 3.3. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

— 3.4. Проводить работы по технической защите информации и поддержанию необходимого уровня защищенности информационной системы при эксплуатации и модернизации последней, включая:

— контроль над процессом осуществления резервного копирования массивов данных, электронных документов;

— обеспечение антивирусной защиты всех элементов информационной системы;

— контроль за установкой и периодическим обновлением антивирусных средств в том числе на персональных компьютерах пользователей информационной системы;

— контроль соблюдения пользователями порядка и правил антивирусной защиты;

— проведение контрольных и тестовых испытаний и проверок элементов информационной системы.

— 3.5. Наделять и изменять права доступа всех групп пользователей информационной системы к персональным данным и защищаемым программным ресурсам, в том числе:

— организовать порядок доступа к работе с информационной системой;

— при необходимости организовать разграничение доступа сотрудников колледжа (чтение, запись, модификация, создание, удаление) к защищаемым программным ресурсам;

— осуществлять контроль смены паролей для доступа к информационной системе в установленном порядке.

— 3.6. Осуществлять установку, настройку и сопровождение программных и технических СЗИ, в том числе:

— участвовать в приемке новых программных и технических средств СЗИ;

— контролировать внесение изменений в конфигурацию программных, технических СЗИ;

— не допускать установку, использование, хранение и размножение в информационной системе программного обеспечения, не связанного с выполнением функциональных задач;

— обеспечивать восстановление программной среды, программных средств и настроек СЗИ при сбоях в работе информационной системы.

— 3.7. Контролировать неизменность состояния и физическую сохранность СЗИ и оборудования информационной системы, в том числе:

— обеспечивать эксплуатацию технических средств и оборудования в соответствии с их назначением;

— контролировать соблюдение требований по размещению и использованию оборудования информационной системы, указанные в технической документации;

— вести и хранить документацию на технических средства и оборудование в соответствии с установленными правилами;

— вести учёт, хранение и выдачу машинных носителей персональных данных;

— контролировать проведение технического обслуживания оборудования для доступа к информационной системе;

— при необходимости организовывать и участвовать в мероприятиях, связанных с вскрытием, опечатыванием, модификацией технических средств информационной системы; в ходе указанных мероприятий составлять акты о вскрытии и опечатывании корпусов технических средств;

— осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ.

— 3.8. Контролировать исполнение всеми группами пользователей правил работы с информационной системой и СЗИ, в том числе:

— контролировать качество и своевременность выполнения сотрудниками образовательной организации установленных требований по обеспечению безопасности персональных данных;

— контролировать соблюдение правил допуска сотрудников в помещения, где размещено оборудование, обеспечивающие работу информационной системы;

— контролировать соблюдение принятых в колледже правил использования паролей/персональных идентификаторов;

— не допускать к работе посторонних лиц;

— принимать участие в организации и проведении расследований по фактам нарушений в области защиты персональных данных и разработке предложений по устранению недостатков и предупреждению подобного рода нарушений.

— 3.9. Представлять руководству отчёт о состоянии информационной системы, в том числе:

— о состоянии материально-технической базы и программного обеспечения;

— о соблюдении сотрудниками колледжа правил работы с информационной системой персональных данных;

— о выявленных нарушениях, нештатных ситуациях и сбоях в работе СЗИ.

4. Права

Ответственное лицо имеет право:

4.1. Требовать от сотрудников колледжа выполнения положений действующего законодательства и локальных нормативных актов по обеспечению защиты персональных данных.

4.2. Требовать от пользователей и администраторов информационной системы своевременного информирования о возникновении сбоев в работе СЗИ и/или инцидентов, связанных с нарушением правил эксплуатации оборудования, правил доступа к информационной системе.

4.3. Давать сотрудникам колледжа обязательные для выполнения указания по работе с информационной системой.

4.4. Привлекать в установленном порядке сотрудников колледжа и сторонних специалистов для решения вопросов, связанных с эксплуатацией и модернизацией информационной системы.

4.5. Требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования СЗИ.

4.6. Осуществлять оперативное вмешательство в работу пользователя информационной системы при явной угрозе безопасности персональным данным с последующим докладом руководству.

4.7. Участвовать в анализе ситуаций, касающихся функционирования СЗИ, и в расследованиях по случаям несанкционированного доступа к персональным данным и другим случаям нарушения режима обработки персональных данных.

4.8. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности персональных данных, несанкционированного доступа, утраты, модификации, порчи персональных данных, правил эксплуатации технических средств.

4.9. Требовать от сотрудников колледжа письменных объяснений при проведении служебных расследований по вопросам нарушений требований обеспечения безопасности персональных данных.

4.10. Вносить предложения руководству колледжа об ограничении доступа/отстранении от работы с информационной системой сотрудников, систематически нарушающих требования обеспечения безопасности персональных данных

4.11. Требовать от руководства колледжа оказания содействия в исполнении своих должностных обязанностей и прав.

4.12. Знакомиться с проектами решений руководства колледжа, касающимися его деятельности.

4.13. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей Инструкцией.

4.14. Осуществлять взаимодействие с руководителями структурных служб колледжа, получать информацию и документы, необходимые для выполнения своих должностных обязанностей.

4.15. Подписывать и визировать документы в пределах своей компетенции.

4.16. Вести переписку со сторонними организациями по вопросам, входящим в его компетенцию.

5. Ответственность

Ответственное лицо несет ответственность за:

5.1. Неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации;

5.2. Причинение материального ущерба работодателю – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации;

5.3. Правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным, гражданским законодательством Российской Федерации.

5.4. Качество проводимых работ по контролю всех групп пользователей информационной системы в вопросах обеспечения безопасности персональных данных.

5.5. Обеспечение устойчивой работоспособности СЗИ информационной системы.

С инструкцией ознакомлен:  А.А. Соболев

(подпись) (фамилия, инициалы)