Утверждаю
Директор
ФГБПОУ «ГУЦЭИ им. М.Н. Румянцева (Карандаша)»
_____ Е.В. Шевченко
«29» ноября 2023 г.

ПОЛОЖЕНИЕ *

Об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ФГБПОУ «ГУЦЭИ им. М.Н. Румянцева (Карандаша)»

1. Общие положения

1.1. Настоящее Положение разработано 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. Положение определяет порядок организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, а также основные обязанности, права и ответственность руководителя образовательной организации, сотрудников образовательной организации и ответственных лиц, допущенных к работе с информационной системой персональных данных (далее - информационная система, пользователь).

1.3. Пользователями являются сотрудники образовательной организации, в силу своих функциональных обязанностей участвующие в процессах обработки персональных данных и имеющие доступ к информационной системе.

1.4. Допуск пользователей к работе с информационной системой осуществляется на основании распоряжения руководителя образовательной организации и в соответствии со списком лиц, допущенных к работе с персональными данными и сведениями конфиденциального характера.

1.5. Общее руководство организацией работ по обеспечению безопасности персональных данных при их обработке в информационных системах осуществляет руководитель образовательной организации.

1.6. Методическое руководство работой пользователей осуществляют ответственные лица, назначенные приказом руководителя образовательной организации в соответствии с локальными нормативными актами.

1.7. Требования настоящего Положения обязательны для исполнения всеми пользователями/ответственными лицами и доводятся под роспись.

1.8. Контроль выполнения требований настоящего Положения осуществляется руководителем образовательной организации и/или уполномоченным сотрудником.

2. Общие правила работы в информационной системе

2.1. Работа в информационной системе производится пользователями для выполнения возложенных на них должностных обязанностей на закрепленных за ними персональных компьютерах/автоматизированных рабочих местах (далее - АРМ).

2.2. Запрос на установку АРМ, его настройку и установку сетевого программного обеспечения осуществляется с санкции руководителя образовательной организации по предварительной заявке/служебной записке на имя руководителя образовательной организации.

2.3. Для идентификации пользователя сотруднику администратором выдается уникальное имя (учетная запись) и пароль. Имя и пароль необходимы для получения доступа к ресурсам сети (сетевым дискам, принтерам и программам).

2.4. При увольнении сотрудника его учетная запись и пароль уничтожаются.

2.5. АРМ размещается таким образом, чтобы исключить визуальный просмотр экрана видеомонитора лицами, не имеющими отношения к обрабатываемой информации.

2.6. Пользователь взаимодействует с ответственными за эксплуатацию информационной системы по вопросам обеспечения защиты информации и подчиняется их распоряжениям.

2.7. Поддержка и сопровождение установленного системного и сетевого программного обеспечения осуществляется техническими специалистами.

2.8. Несогласованное подключение внешних устройств и установка программного оборудования запрещены.

2.9. При нарушении нормальной работы сети и в случае обнаружения неисправности любого компьютерного и сетевого оборудования, а также при сбое или неправильной работе программного обеспечения пользователь обязан немедленно сообщить техническим специалистам.

3. Правила организации парольной защиты информационной системы

3.1. Личные пароли выбираются пользователями самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- среди символов пароля обязательно должны присутствовать буквы и цифры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, и т.д.);

личный пароль пользователь не имеет права сообщать никому;

смена паролей пользователей должна проводиться регулярно в соответствии с установленным порядком.

3.2. Внеплановая смена личного пароля или удаление учетной записи пользователя компьютерной сети в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) производится администратором после окончания последнего сеанса работы данного пользователя по распоряжению руководителя образовательной организации.

3.3. Хранение пользователями значений своих действующих паролей на бумажном носителе допускается только в местах, защищенных от несанкционированного доступа третьих лиц.

3.4. Повседневный контроль при работе пользователей информационной системы с паролями, соблюдением порядка их смены хранения и использования возлагается на администратора информационной системы.

4. Правила организации антивирусной защиты

4.1. К использованию в информационной системе образовательной организации допускаются только лицензионные антивирусные средства.

4.2. Установка средств антивирусного контроля осуществляется техническими специалистами по распоряжению руководителя образовательной организации.

4.3. В начале работы при включении АРМ, а также при первом доступе к файлам в автоматическом режиме проводится их антивирусный контроль.

4.4. Не реже одного раза в неделю в автоматическом режиме производится полная проверка дисков персональных компьютеров, подключенных к информационной системе, на наличие вирусов.

4.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).

4.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщение о системных ошибках и т.п.), пользователь вместе с техническим специалистом должен провести внеочередной антивирусный контроль.

4.7. В случае обнаружения зараженных компьютерными вирусами файлов пользователь обязан:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов непосредственное руководство, владельца зараженных файлов, а также других пользователей, использующие эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- вместе с техническим специалистом провести лечение или уничтожение зараженных файлов.

5. Обязанности пользователя - сотрудника образовательной организации

Пользователь обязан:

5.1. Строго соблюдать изложенные выше:

- правила обеспечения безопасности при работе с информационной системой;
- правила парольной защиты;
- правила антивирусной защиты.

5.2. Хранить в тайне свои идентификационные данные(имена, пароли и т.д.) и осуществлять вход в информационную систему только под своими идентификационными данными в разрешенный период времени.

5.3. Немедленно вызывать администратора информационной системой и ставить в известность руководителя образовательной организации при:

- подозрении о компрометации личных идентификаторов и паролей;
- обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа;
- обнаружении несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
- обнаружении некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключенных устройств;
- выходе из строя или неустойчивом функционировании узлов АРМ или периферийных устройств, а также перебоях в системе электроснабжения.

5.4. Немедленно выполнять предписания администраторов информационной системы.

5.5. Предоставлять свое АРМ администратору информационной системы для планового и внеочередного контроля.

5.6. Проводить полное или частичное резервное копирование служебной информации в соответствии с установленным порядком.

5.7. Осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ.

5.8. Уважать права других пользователей на конфиденциальность и право пользования общими ресурсами.

Пользователям запрещается:

5.9. Самостоятельно переставлять и передвигать, а также подключать компьютерную технику в помещении (в том числе при проведении генеральных уборок, перестановке мебели и пр.).

5.10. Самостоятельно производить установку, настройку, модификацию и тестирование сетевого аппаратного или программного обеспечения.

6. Обязанности ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных

Ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных (далее - ответственное лицо) обязан:

6.1. Осуществлять внутренний контроль соблюдения 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.

6.2. Доводить до сведения работников организации 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 образовательной организации;
- формирования внутренней информационной рассылки об изменениях в действующем законодательстве;
- проведения специальных занятий (семинаров, консультаций), при необходимости - с участием приглашенных специалистов.

6.3. 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.

6.4. 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.

6.5. 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 образовательной организации (чтение, запись, модификация, создание, удаление) к защищаемым программным ресурсам;
- организовать своевременное внесение и удаление учетных записей сотрудников образовательной организации при изменении прав доступа;
- осуществлять контроль смены паролей для доступа к информационной системе в установленном порядке.

6.6. Осуществлять установку, настройку и сопровождение программных и технических

средств защиты информации (далее - СЗИ), в том числе:

- участвовать в приемке новых программных и технических средств СЗИ;
- контролировать внесение изменений в конфигурацию программных, технических СЗИ;
- проводить анализ воздействия изменений в конфигурации информационной системы на обеспечение безопасности персональных данных;
- обеспечивать документальное оформление изменений в конфигурации информационной системы;
- 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.

6.7. 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 информационной системы;
- 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.

6.8. 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 образовательной организации 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.

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

- о состоянии материально-технической базы и программного обеспечения;
- о соблюдении сотрудниками образовательной организации правил работы с информационной системой персональных данных;
- о выявленных нарушениях, нештатных ситуациях и сбоях в работе СЗИ.

7. Обязанности пользователя - руководителя образовательной организации

Руководитель для обеспечения безопасности персональных данных обязан:

7.1. Организовывать и контролировать вопросы обеспечения безопасности персональных данных в образовательной организации в соответствии с действующим законодательством.

7.2. Издать соответствующий распорядительный документ, в котором предусмотрено:

- определение круга лиц, допущенных к работе в информационной системе;

- назначение ответственных лиц;
- полномочия ответственного лица и технических специалистов;
- порядок осуществления антивирусного контроля;
- ознакомление под роспись лиц, допущенных к работе с персональными данными, с перечисленными выше правилами и предупреждение об ответственности за их нарушение.

7.3. Контролировать работы по внесению изменений в аппаратно-программную конфигурацию компьютеров в образовательной организации.

7.4. Контролировать соблюдение требований по обеспечению безопасности персональных данных при проведении технического обслуживания и ремонтных работ.

7.5. Организовать инструктаж сотрудников по правилам работы с используемыми аппаратно-программными средствами.

7.6. Осуществлять контроль соблюдения пользователями требований настоящего Положения.

8. Права пользователя - сотрудника образовательной организации

Пользователь имеет право:

8.1. Осуществлять доступ к программным и аппаратным средствам информационной системы в пределах предоставленных полномочий и в соответствии с закрепленными за ним обязанностями.

8.2. Обращаться к техническим специалистам и руководству за необходимой технической и методической помощью.

8.3. Участвовать в анализе ситуаций, касающихся функционирования закрепленного за ним АРМ и рабочих программ.

8.4. Знакомиться с проектами решений руководства организации, касающимися его деятельности.

8.5. Вносить на рассмотрение руководства предложения по совершенствованию работы информационной системы и закрепленного за ним АРМ.

9. Права ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных

Ответственное лицо имеет право:

9.1. Требовать от сотрудников образовательной организации выполнения положений действующего законодательства и локальных нормативных актов по обеспечению защиты персональных данных.

9.2. 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.

9.3. Давать сотрудникам образовательной организации обязательные для выполнения указания по работе с информационной системой.

9.4. Привлекать в установленном порядке сотрудников образовательной организации и сторонних специалистов для решения вопросов, связанных с эксплуатацией и модернизацией информационной системы.

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

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

9.7. 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.

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

9.9. Требовать от сотрудников образовательной организации письменных объяснений при проведении служебных расследований по вопросам нарушений требований обеспечения безопасности персональных данных.

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

9.11. Требовать от руководства организации оказания содействия в исполнении своих должностных обязанностей и прав.

9.12. Знакомиться с проектами решений руководства организации, касающимися его деятельности.

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

9.14. Осуществлять взаимодействие с руководителями структурных служб образовательной организации, получать информацию и документы, необходимые для выполнения своих должностных обязанностей.

9.15. Подписывать и визировать документы в пределах своей компетенции.

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

10. Права пользователя - руководителя образовательной организации

Руководитель имеет право на все перечисленные выше права пользователя - сотрудника образовательной организации и в дополнение к ним:

10.1. Требовать от сотрудников образовательной организации выполнения положений действующего законодательства и локальных нормативных актов по обеспечению информационной безопасности.

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

10.3. Давать сотрудникам образовательной организации обязательные для выполнения указания по работе с информационной системой.

10.4. Инициировать и проводить служебные расследования по фактам нарушения установленных требований обеспечения безопасности персональных данных, несанкционированного доступа, утраты, модификации, порчи программных и аппаратных элементов информационной системы, правил эксплуатации технических средств.

10.5. Привлекать сотрудников образовательной организации к проведению плановых и внеочередных работ по обеспечению безопасности персональных данных, установке и модернизации программных и аппаратных средств.

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

11. Ответственность

Пользователи и ответственные лица несут ответственность за:

11.1. Неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящим Положением, - в пределах, определенных действующим трудовым законодательством Российской Федерации.

11.2. Причинение материального ущерба работодателю - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

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

11.4. Качество проводимых работ по обеспечению безопасности персональных данных.

11.5. Обеспечение устойчивой работоспособности информационной системы.

12. Заключительные положения

12.1. В Положение могут вноситься изменения, дополнения в связи с совершенствованием образовательного процесса и изменениями в законодательстве Российской Федерации. Внесение изменений и дополнений в настоящее Положение осуществляется путем подготовки проекта Положения в новой редакции, согласованного в установленном порядке.

12.2. Настоящее Положение вступает в юридическую силу со дня его утверждения руководителем образовательной организации и действует без ограничения срока действия.