Подписано цифровой подписью: Подзорова Елена Александровна
Дата: 2023.02.07 13:28:32 +03'00'

Муниципальное бюджетное общеобразовательное учреждение "Гимназия имени А.П.Чехова"
наименование организации

ПРИКАЗ

Об утверждении инструкции по информационной безопасности в пользовательском сегменте РИСО

от 06.02.2023 — дата приказа

36-ОД — № приказа

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" и в целях выполнения организационных требований для подключения автоматизированного рабочего места к региональной информационной системе Ростовской области "Образование" пользовательский сегмент (далее - РИСО),

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Инструкцию по информационной безопасности РИСО.
2. Установить на территории МБОУ "Гимназия им. А.П.Чехова" контролируемую зону, включающую в себя помещения с ограниченным доступом. Помещением с ограниченным доступом является помещение, в котором постоянно размещается автоматизированное рабочее место РИСО.
3. Запретить нахождение работников в помещениях с ограниченным доступом, в целях, не связанных со служебной деятельностью.
4. Установить, что ответственность за организацию режима обеспечения безопасности помещений и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает - заместитель директора по УВР Венжик Тамара Дмитриевна.
5. При входе в помещение необходимо проверить отсутствие несанкционированного доступа в помещение, а при его обнаружении немедленно сообщить об этом факте ответственному за обработку персональных данных в МБОУ "Гимназия им. А.П.Чехова"
6. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель: Директор
должность
Подзорова Елена Александровна
ФИО (расшифровка подписи) — подпись

Ответственный(ая): Венжик Т.Д.
ФИО (расшифровка подписи) — подпись

УТВЕРЖДЕНА
приказом МБОУ «Гимназия им. А.П.Чехова»
от «06» 02 2023 г. № 36-ОД

Инструкция по информационной безопасности пользовательского сегмента региональной информационной системы Ростовской области «Образование»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет обязанности должностного лица, (далее – пользователя), обрабатывающего информацию (в том числе персональных данных (далее – ПДн), в пользовательском сегменте региональной информационной системы Ростовской области «Образование» (далее – РИСО) в МБОУ «Гимназия им. А.П. Чехова» (далее – Организация).

2. ОБЩИЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ОБРАБОТКИ ИНФОРМАЦИИ В РИСО

2.1. К защищаемой информации, обрабатываемой в РИСО, относятся персональные данные (далее –ПДн), служебная (технологическая) информация системы защиты, другая информация конфиденциального характера.

2.2. Обработка защищаемой информации в РИСО разрешается на основании приказа руководителя Организации.

2.3. Ответственность за организацию защиты информации в РИСО и выполнение установленных условий ее функционирования возлагается на ответственного за обработку персональных данных в Организации.

2.4. Ответственность за выполнение мероприятий безопасности информации возлагается на лицо, производящее ее обработку (пользователя РИСО).

2.5. Допуск пользователей к работе в РИСО осуществляется только для выполнения ими трудовых обязанностей в Организации.

2.6. К самостоятельной работе на автоматизированных рабочих местах (далее – АРМ), входящих в состав РИСО, допускаются лица, изучившие требования настоящей Инструкции и освоившие правила эксплуатации АРМ и технических средств защиты. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

2.7. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в нем работникам, а также лицам, привлекаемым к проведению ремонтных, наладочных и других работ и посетителей в сопровождении работников Организации.

2.8. Техническое обслуживание АРМ, уборка помещения и т.п. проводятся только под контролем уполномоченного лица Организации. При проведении этих работ обработка защищаемой информации запрещается.

2.9. По фактам и попыткам несанкционированного доступа к защищаемой информации, а также в случаях ее утечки и (или) модификации (уничтожения) проводятся служебные расследования.

3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

3.1. При первичном допуске к работе в РИСО пользователь знакомится с требованиями руководящих, нормативно–методических и организационно–распорядительных (регламентирующих) документов по вопросам безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию.

3.2. Каждый работник Организации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным РИСО, несет персональную ответственность за свои действия и обязан:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами РИСО;

– знать и строго выполнять правила работы со средствами защиты информации, установленными в РИСО;

– хранить в тайне свой пароль;

– передавать для хранения установленным порядком при необходимости свои реквизиты разграничения доступа только ответственному за обработку персональных данных в Организации;

– выполнять требования по антивирусной защите в части, касающейся действий пользователей.

3.3. Немедленно ставить в известность ответственного за обработку персональных данных в Организации в следующих случаях:

– при подозрении компрометации личного пароля;

– обнаружения фактов совершения в отсутствие пользователя попыток несанкционированного доступа (далее – НСД) к ресурсам РИСО;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств РИСО;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию РИСО, выхода из строя или неустойчивого функционирования узлов или периферийных устройств, а также перебоев в системе электроснабжения;

– некорректного функционирования установленных средств защиты на АРМ;

– обнаружения непредусмотренных отводов кабелей и подключенных устройств;

– обнаружения фактов и попыток НСД и случаев нарушения установленного порядка обработки защищаемой информации.

3.4. Пользователю категорически запрещается:

– использовать компоненты программного и аппаратного обеспечения РИСО в неслужебных целях.

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств РИСО или устанавливать дополнительно любые программные и аппаратные средства;

– записывать и хранить защищаемую информацию на неучтенных носителях информации;

– оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД;

– оставлять без личного присмотра на АРМ или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц;

– производить перемещения технических средств АРМ без согласования с ответственным за обработку персональных данных в Организации;

– вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с ответственным за обработку персональных данных в Организации и без оформления соответствующего Акта. Подключать к АРМ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию;

– осуществлять ввод пароля в присутствии посторонних лиц, если есть риск его компрометации;

– оставлять без контроля АРМ в процессе обработки конфиденциальной информации;

– привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств АРМ.

4. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ В ЧАСТИ РИСО

4.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в РИСО;

4.2. Знать перечень установленных в подразделениях Организации объектов вычислительной техники (далее – ОВТ), АРМ и перечень задач, решаемых с их использованием в РИСО;

4.3. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных ОВТ РИСО;

4.4. Осуществлять периодический контроль внесения изменений в конфигурацию (модификации) аппаратно-программных средств, защищенных ОВТ, устанавливать и осуществлять контроль за настройкой средств защиты ОВТ РИСО.

4.5. Периодически проверять состояние используемых СЗИ РИСО, осуществлять проверку правильности их настройки (выборочное тестирование).

4.6. Проводить периодическое тестирование функций средств защиты РИСО при изменении программной среды и персонала, с помощью тест-программ, имитирующих попытки НСД.

4.7. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования РИСО и осуществления НСД к информации и ОВТ.

4.8. Контролировать своевременное и точное отражение изменений в организационно–распорядительных и нормативных документах по управлению средствами защиты РИСО.

4.9. Проводить занятия с системными администраторами (при наличии) по правилам работы на ОВТ РИСО, оснащенных СЗИ;

4.10. Разрабатывать инструкции и памятки для пользователей, обрабатывающих ПДн в РИСО.

4.11. Разрабатывать регламенты проведения работ по обеспечению безопасности ПДн, обрабатываемых в РИСО.

4.12. Участвовать в работе Организации по пересмотру планов защиты;

4.13. Обеспечить автоматическую проверку (один раз в неделю), на наличие вирусов на объектах вычислительной техники, подключенных к РИСО;

4.14. Осуществлять учет и периодический контроль действий системных администраторов, касающихся обеспечения информационной безопасности.

4.15. Участвовать в установке, настройке и сопровождении программных средств защиты информации РИСО.

4.16. Участвовать в приемке новых программных средств обработки информации РИСО.

4.17. Обеспечивать доступ к защищаемой информации пользователям РИСО согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

4.18. Уточнять в установленном порядке обязанности пользователей РИСО при обработке ПДн.

4.19. Вести контроль осуществления резервного копирования информации РИСО.

4.20. Контролировать правильность функционирования средств защиты информации РИСО и неизменность их настроек.

4.21. Контролировать физическую сохранность технических средств обработки информации РИСО.

4.22. Контролировать исполнение пользователями РИСО введенного режима безопасности, а также правильность работы с элементами РИСО и средствами защиты информации.

4.23. Контролировать исполнение пользователями правил парольной политики.

4.24. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

4.25. Не допускать установку, использование, хранение и размножение в РИСО программных средств, не связанных с выполнением функциональных задач.

4.26. Осуществлять периодические контрольные проверки АРМ РИСО.

4.27. Оказывать помощь пользователям РИСО в части применения средств защиты и консультировать по вопросам введенного режима защиты.

4.28. Периодически представлять руководству отчет о состоянии защиты РИСО и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации, об имевших место попытках несанкционированного доступа к информации и ОВТ РИСО;

4.29. В случае отказа работоспособности технических средств и программного обеспечения РИСО, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

4.30. В случае выявления нарушений режима безопасности информации (ПДн), а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий;

4.31. Принимать участие в проведении работ по оценке соответствия РИСО требованиям безопасности информации.

4.32. Соблюдать требования режима конфиденциальности информации, содержащей персональные данные работников, а также третьих лиц, ставшей ему известной в связи с исполнением своих должностных обязанностей, и не использовать ее в интересах, не связанных с исполнением указанных обязанностей.

5. ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В РИСО

5.1. В процессе обработки информации РИСО участвуют следующие группы пользователей:

– ответственный за обработку персональных данных – обладает всей полнотой доступа к ресурсам объекта вычислительной техники, организует и контролирует работу ОВТ объектов информатизации, других пользователей.

– пользователи – имеющие доступ к АРМ объектов информатизации на основании приказа о допуске к АРМ в соответствии со своими ролями в РИСО.

5.2. Перечень объектов доступа:

– жесткие магнитные диски (ЖМД);

– штатное программное обеспечение (ПО).

5.3. К работе в РИСО допускаются только работники, допущенные к обработке персональных данных (далее - информации) и зарегистрированные в установленной системе защиты информации от несанкционированного доступа (далее – СЗИ НСД) и после изучения организационно-распорядительной документации РИСО.

5.4. Обработка информации осуществляется только на предварительно учтенных носителях информации, прошедших антивирусный контроль, причем каждый исполнитель для обработки информации использует только свой профиль пользователя, в котором закреплены правила разграничения доступа: возможность доступа к дискам, папкам и файлам, возможность записи и чтения информации и т.д.

5.5. Ответственный за обработку ПДн организует и контролирует доступ пользователей к ресурсам АРМ и состояние информации на носителях.

5.6. По окончании рабочего дня все съемные учтенные носители информации, документы и материалы запираются в сейфе, либо сдаются на хранение ответственному за обработку персональных данных.

5.7. Пользователи обязаны предъявлять, по требованию ответственного за обработку персональных данных, для проверки все числящиеся за ними носители информации.

5.8. Пользователю запрещается:

– обрабатывать информацию при наличии оснований полагать, что информация может быть просмотрена посторонними лицами;

– записывать информацию на неучтенных носителях информации, листах бумаги и т. д.;

– использовать в работе пароли, если есть подозрение на их компрометацию;

– разглашать сведения о применяемой системе защиты и содержании информации;

– изменять и тиражировать программное обеспечение;

– вводить персональные данные под диктовку;

– производить передачу персональных данных по каналам связи, имеющим выход за пределы контролируемой зоны РИСО, без использования средств криптографической защиты;

– производить печать персональных данных при помощи не предназначенного для этого оборудования.

6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА

6.1. Предоставление доступа работникам к РИСО осуществляется в соответствии с правилами и регламентами, действующими в Организации.

6.2. Перед предоставлением работнику доступа к РИСО, необходимо:

– отразить в трудовом договоре с работником обязательства о неразглашении защищаемой информации, которая будут ему известна при исполнении трудовых обязанностей, и о соблюдении требований локальных нормативных актов, регулирующих порядок обращения с защищаемой информацией;

– ознакомить работника под подпись с организационно-распорядительной документацией РИСО.

6.3. На основании решения руководителя Организации (в случае необходимости) осуществляется допуск пользователя к РИСО, в объеме, необходимом для выполнения им своих функциональных обязанностей.

6.4. При переводе на другую должность основанием для допуска служит приказ о переводе. В этом случае допуск работника по предыдущей должности прекращается, и он допускается к сведениям по новой должности.

6.5. Состав допущенных работников к РИСО необходимо держать в актуальном состоянии.

7. ПОРЯДОК ПРЕКРАЩЕНИЯ ДОСТУПА

7.1. Прекращение предоставления доступа пользователям к РИСО осуществляется в следующих случаях:

– увольнение работника;

– перевод работника на другую должность, не предусматривающую необходимости доступа к РИСО;

– компрометация аутентификационных данных пользователя либо нарушение пользователем требований информационной безопасности.

7.2. В случае компрометации аутентификационных данных пользователя работник извещает в письменном виде ответственного за обработку персональных данных в организации факте компрометации. Ответственный за обработку персональных данных в организации должен уведомить в письменном виде оператора РИСО, о необходимости отключения доступа пользователя к ресурсу и инициировать служебное расследование.

8. ОТВЕТСТВЕННОСТЬ

8.1. Работники, виновные в нарушении режима защиты ПДн, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

С инструкцией ознакомлен:

_____ _____ Венжик Т.Д.
(подпись) (расшифровка подписи)

«____» _____20___г.

_____ _____ _____
(подпись) (расшифровка подписи)

«____» _____20___г.