П-150/2019

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

Протокол заседания Совета Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета обучающихся
Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета родителей
Учреждения
от 29.10.2019г. № 20

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»
_____А.Н. Сакеев
«29» октября 2019г.
Приказ № 522 о/д от 29.10.2019

Инструкция
по управлению доступом к персональным данным

1. Общие положения

1.1 Настоящая инструкция определяет в ГБПОУ «ТК им. Н.Д. Кузнецова» управление доступом к персональным данным обрабатываемым в информационной системе персональных данных (далее - ИСПДн) на основе обеспечения реализациии правил разграничения доступа, на основе установленной в ГБПОУ «ТК им. Н.Д. Кузнецова» (далее - Организация) матрицы доступа.

1.2 Настоящая Инструкция разработана на основе следующих нормативных документов:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- Приказ ФСТЭК России от 18.02.2013 года №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3 Правила разграничения доступа должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты персональных данных и иной информации о функционировании системы защиты, а также иным объектам доступа.

1.4 Права доступа должны назначаться исходя из принципа предоставления минимально необходимых прав для осуществления пользователями своих должностных обязанностей.

1.5 Средства управления доступом должны быть защищены от модификации

пользователем.

1.6 Все пользователи ИСПДн должны быть предупреждены об ответственности за нарушение требований настоящей инструкции.

1.7 Пользователи ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы с ИСПДн под роспись.

1.8 Обязанность ознакомления пользователей с настоящей инструкцией лежит на **ответственном за организацию обработки ПДн.**

2. Порядок предоставления прав доступа к ресурсам ИСПДн

2.1 Разграничение доступа к ресурсам ИСПДн осуществляет и контролирует **администратор безопасности** путём настройки программно-технических средств ИСПДн и средств защиты информации (далее - СЗИ).

2.2 Регистрация новых пользователей ИСПДн, изменение и отмена прав доступа существующих пользователей осуществляется администратором безопасности на основании заявки непосредственного руководителя пользователя в которой указываются права пользователя по доступу к ресурсам ИСПДн.

2.3 В случае необходимости, заявки согласуются с владельцем информационного ресурса ИСПДн к которому пользователю предоставляется доступ.

2.4 Все поступающие заявки должны храниться у администратора безопасности.

2.5 Предоставление пользователям удалённого доступа к ресурсам ИСПДн, а также предоставление права использования мобильных технических средств производится по согласованию с ответственным за организацию обработки персональных данных.

2.6 Порядок регистрации новых пользователей в ИСПДн приведён в Инструкции по идентификации и аутентификации пользователей информационной системы персональных данных.

3. Матрица доступа

3.1 Все изменения прав доступа к информационным ресурсам ИСПДн регистрируются администратором безопасности в **матрице доступа** (приложение1).

3.2 Сохранность, конфиденциальность и актуальность матрицы доступа обеспечивает администратор безопасности.

4. Порядок контроля и пересмотра прав доступа пользователей

4.1 Контроль и актуализацию прав доступа пользователей к ресурсам ИСПДн, а также контроль соответствующих настроек программно-технических средств ИСПДн и СЗИ осуществляет администратор безопасности не реже **одного раза в месяц.**

4.2 Проверку и пересмотр прав доступа пользователей к информационным ресурсам ИСПДн проводит владелец информационного ресурса не реже **одного раза в год.**

5. Порядок предоставления пользователям доступа к ресурсам ИСПДн до прохождения процедур идентификации и аутентификации

5.1 Действия с ресурсами ИСПДн до прохождения процедур идентификации и аутентификации разрешены администратору безопасности и ответственным пользователям для проведения работ по восстановлению работоспособности ИСПДн после сбоев и аварий технических средств ИСПДн.

5.2 Проведение работ по восстановлению работоспособности ИСПДн только с письменного разрешения ответственного за организацию обработки персональных данных. В разрешении должны быть кратко описаны необходимые действия с ресурсами ИСПДн. Срок действия разрешения заканчивается в момент запуска ИСПДн после восстановления.

5.3 Доступ к ресурсам ИСПДн до момента прохождения процедур идентификации, аутентификации остальным пользователям запрещён.

6 . Порядок предоставления удалённого доступа к ресурсам ИСПДн

6.1 Удалённый доступ к информационным ресурсам ИСПДн предоставляется только пользователям, которым он необходим для выполнения должностных обязанностей.

6.2 Права пользователей на осуществление удалённого доступа к ресурсам ИСПДн должны отражаться администратором безопасности в матрице доступа.

6.3 Удалённый доступ возможен только с помощью технических средств (персональный компьютер, ноутбук, планшет, сотовый телефон) внесённых в **журнал учета разрешённых средств удалённого доступа** (приложение 2).

6.4 Защита информации при осуществлении удалённого доступа к ресурсам ИСПДн должна обеспечиваться с помощью штатных средств криптографической защиты информации, входящих в состав системы защиты персональных данных ИСПДн.

6.5 Выдачу, учёт, хранение, настройку программного обеспечения, установку программного обеспечения, в том числе программного обеспечения средств защиты информации и его обновление, антивирусную защиту технических средств удалённого доступа осуществляет **администратор безопасности.**

6.6 При настройке средств удалённого доступа к ресурсам ИСПДн администратор безопасности осуществляет их настройку таким образом, чтобы обеспечивалась автоматическая аутентификация средств удалённого доступа при доступе к ресурсам ИСПДн.

7. Порядок использования в ИСПДн мобильных технических средств

7.1 К мобильным техническим средствам относятся: съёмные машинные носители информации (флэш-накопители, внешние накопители на жёстких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

7.2 Все мобильные технические средства Организации должны быть учтены и идентифицированы.

7.3 Учёт мобильных технических средств осуществляет администратор безопасности в **журнале учёта разрешённых мобильных технических средств** (приложение 3).

7.4 Права по использованию мобильных технических средств предоставляются пользователю в порядке, предусмотренном п.3 настоящий инструкции и отражаются администратором безопасности в **матрице доступа.**

7.5 Контроль за правильностью использования мобильных технических средств, а также контроль исправности мобильных технических средств производит **администратор безопасности.**

7.6 В случае выявления фактов использования мобильных технических средств не по назначению, мобильное устройство изымается у пользователя и о данном факте ставятся в известность непосредственный руководитель пользователя и ответственный за организацию обработки персональных данных.

7.7 В случае обнаружения неисправности администратор безопасности принимает меры по ремонту мобильного устройства.

7.8 При передаче мобильных технических средств на ремонт или техническое обслуживание **администратор безопасности** полностью очищает их от информации, имеющей отношение к ИСПДн.

8. Порядок взаимодействия с внешними информационными системами

8.1 Информационное взаимодействие с внешними информационными системами (информационными системами сторонних организаций) должно осуществляться в строгом соответствии с требованиями Федерального закона «О персональных данных».

8.2 Организацию информационного взаимодействия с внешней информационной системой обеспечивает администратор безопасности на основании распоряжения руководителя Организации.

8.3 В случае необходимости, для организации информационного взаимодействия с внешней информационной системой администратор безопасности может привлекать системных администраторов.

8.4 Доступ к ресурсам ИСПДн пользователям внешних информационных систем предоставляется в порядке, предусмотренном п.3 настоящей инструкции.

8.5 В случае если информационное взаимодействие осуществляется по каналам связи выходящим за границы контролируемой зоны Организации (по каналам связи общего пользования) должна обеспечиваться защита передаваемой информации с помощью штатных средств криптографической защиты информации, входящих в состав системы защиты персональных данных ИСПДн.

Разработчик:
заместителя директора по общим вопросам

_____/ Ю.Ю. Алексеев /

Приложение 1

Форма матрицы доступа

Матрица доступа ИСПДн

№	Наименование информационных ресурсов, используемых в ИСПДн	Тип информационного ресурса	Тип доступа	Уровень доступа		
				Пользователь	Администратор (системный)	Администратор (безопасности)

Приложение 2

Журнал учета разрешённых средств удалённого доступа

Уч. №_____ 20__ год.

№ п/п	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ подпись	Дата возврата/ подпись	Примечание

Приложение 3

Журнал учёта разрешённых мобильных технических средств

Уч. №

20____ год.

№ п/п	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ подпись	Дата возврата/ подпись	Примечание

Лист
ознакомления с «Инструкцией по управлению доступом к персональным данным»

№ п/п	ФИО	Должность	Подпись, дата