

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



Приказ № 522 о/д от 29.10.2019

Инструкция **ответственного за обеспечение безопасности персональных данных в** **информационной системе персональных данных**

1. Общие положения

1.1. Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

1.2. Настоящая Инструкция разработана в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»,
- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»,
- Постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных",
- Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

1.3. Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

1.4. Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест:

2. Обязанности администратора информационной безопасности.

Администратор информационной безопасности обязан:

2.1. Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в

ИСПДн;

2.2. Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

2.3. Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

2.4. Ежедневно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

2.5. Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;

2.6. Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

2.7. Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

2.8. Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

2.9. Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

2.10. Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

2.11. Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

2.12. Обязан проводить мероприятия по организации антивирусной защиты;

2.13. Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;

2.14. Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

2.15. Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

2.16. Установить причины, по которым стал возможным НСД;

2.17. Установить последствия, к которым привел НСД;

2.18. Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

2.19. Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы

доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;

2.20. Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

3.1. Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

3.2. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

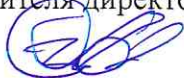
3.3. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн.

4. Ответственность администратора информационной безопасности

4.1. На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

4.2. Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Разработчик:
заместителя директора по общим вопросам



_____ / Ю.Ю. Алексеев /

