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
администратора информационной системы персональных данных

1. Общие положения

1.1. Инструкция определяет основные задачи, функции, обязанности, права и ответственность Администратора безопасности информационной системы персональных данных (далее - ИСПДн) ГБПОУ «ТК им. Н.Д. Кузнецова» (далее – Учреждение).

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»,
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.3. Администратор безопасности ИСПДн (далее - Администратор) назначается приказом Директора Учреждения и является лицом, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники ИСПДн, в пределах своей зоны ответственности.

1.4. Закрепление функциональных обязанностей и разделение зон ответственности производится приказом Директора Учреждения..

1.5. В своей деятельности Администратор руководствуется требованиями действующих федеральных законов, общегосударственных, ведомственных, а также

внутренних нормативных документов по вопросам защиты информации и обеспечивает их выполнение пользователями ИСПДн.

1.6. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

2. Задачи и функции администратора.

2.1. Основными задачами Администратора являются:

- сопровождение средств защиты информации (в том числе криптографических, шифровальных) от несанкционированного доступа (далее - СЗИ) и основных технических средств и систем (далее - ОТСС);
- организация разграничения доступа;
- контроль эффективности защиты информации.

2.2. Для выполнения поставленных задач на Администратора возлагаются следующие функции:

2.2.1. опуск пользователей (разработчиков, эксплуатационного персонала) к техническим, программным средствам и информационным ресурсам ИСПДн в соответствии с требованиями «Положения о разрешительной системе допуска пользователей к обрабатываемой в ИСПДн информации» на всех стадиях жизненного цикла ИСПДн.

2.2.2. Участие на стадии проектирования (внедрения) ИСПДн в разработке технологии обработки информации конфиденциального характера (далее - Информации) по вопросам:

- организация порядка учета, хранения и обращения с документами и носителями информации;
- подготовки инструкций, определяющих задачи, функции, ответственность, права и обязанности пользователей ИСПДн по вопросам защиты информации, а также ответственных по защите информации в процессе автоматизированной обработки информации;
- сопровождение СЗИ, в том числе средств криптографической защиты информации, на стадии эксплуатации ИСПДн, включая ведение служебной информации СЗИ (управление ключевой системой, сопровождение правил разграничения доступа), оперативный контроль за функционированием СЗИ;
- контроль выполнения требований действующих нормативных документов по вопросам защиты информации при обработке информации в ИСПДн;
- контроль соответствия общесистемной программной среды эталону (контроль целостности программного обеспечения) и проверка включаемых в ИСПДн новых программных средств.

3. Обязанности администратора.

3.1. Для реализации поставленных задач и возложенных функций Администратор обязан:

3.1.1. Сопровождать СЗИ и ОТСС:

- Вести учет (по вопросам обеспечения безопасности информации) и знать перечень установленных в подразделениях Учреждения СЗИ и перечень задач, решаемых с их использованием;
- Вести журнал учета эксплуатационной и технической документации СЗИ ИСПДн.
- Вести журнал учета машинных носителей персональных данных.
- Осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на автоматизированных рабочих местах (далее - АРМ) специальных

программных и программно-аппаратных СЗИ;

• Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов, осуществлять проверку работоспособности системы защиты после установки (обновления) программных средств ИСПДн;

• Периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование);

• Контролировать соответствие технического паспорта ИСПДн фактическому составу (комплектности) ИСПДн и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИСПДн);

• Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ;

• Вести журнал учета нештатных ситуаций, фактов вскрытия и опечатывания АРМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИСПДн;

• Проводить периодический инструктаж сотрудников подразделения (пользователей ИСПДн) по правилам работы с используемыми средствами и системами зашиты информации.

3.1.2. Организовывать разграничения доступа:

3.1.2.1. Участвовать в разработке и знать перечень защищаемых информационных ресурсов.

3.1.2.2. Разрабатывать для ИСПДн решения по:

• составу доменов сети, системы доверительных отношений между ними;

• составу групп (локальных и глобальных) каждого домена;

• приписке пользователей с одинаковыми правами, статусом безопасности и характером решаемых задач к соответствующим группам;

• определению информационных связей между сегментами сети и требований к изоляции сегментов с использованием средств аппаратной безопасности сегментов;

• вести учет заявок пользователей на допуск к информационным ресурсам ИСПДн;

• осуществлению контроля за наличием активных компьютеров сети, состоянием активных пользователей, использованием разделяемых ресурсов, процессом печати на общих принтерах;

• разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, проектированию системы почтовых ящиков, использованию СЗИ при передаче закрытых документов);

• разработке порядка выхода пользователей в сети связи общего пользования (далее - Сети) и использованию встроенных СЗИ в сервисных программах;

• определению режимов использования СЗИ: защита паролей, защита в протоколах передачи данных, кодирование файлов, подключение дополнительных алгоритмов криптографической защиты;

• разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита;

• осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ ИСПДн;

• контролировать и требовать соблюдения установленных правил по организации парольной защиты в ИСПДн Учреждения;

• осуществлять оперативный контроль за работой пользователей защищенных АРМ, анализировать содержимое журналов событий операционных систем (далее - ОС), систем управления базами данных (далее - СУБД), пакетов прикладных программ (далее -

Лист
ознакомления с «Инструкцией администратора информационной системы персональных данных»

№ п/п	ФИО	Должность	Подпись, дата