

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



**Правила оценки вреда, который может быть
причинен субъектам персональных данных в
случае нарушения требований по обработке и
обеспечению безопасности персональных данных в
информационной системы персональных данных**

1. Общие положения

1.1. Настоящие Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в информационной системы персональных данных (далее – Правила) в ГБПОУ «ТК им. Н.Д. Кузнецова» определяют порядок оценки вреда, который может быть причинён субъектам персональных в случае нарушения федерального законодательства по защите персональных данных, в частности Федерального закона № 152-ФЗ «О персональных данных» (далее - № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных № 152-ФЗ.

1.2. Настоящий Порядок разработан 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 Составы 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».

2. Термины и определения

2.1. В настоящих Правилах используются основные понятия:

2.1.1. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.1.2. Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

2.1.3. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2.1.4. Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.

2.1.5. Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

2.1.6. Убытки - расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.

2.1.7. Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

2.1.8. Оценка возможного вреда - определение уровня вреда на основании учёта причинённых убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

3. Описание вреда субъектам персональных данных

3.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

3.2.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных.

3.2.2. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных.

3.2.3. Неправомерное изменение персональных данных является нарушением целостности персональных данных.

3.2.4. Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации.

3.2.5. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных.

3.2.6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных.

3.2.7. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных.

3.2.8. Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

3.3. Субъекту персональных данных может быть причинён вред в форме:

3.3.1. Убытков - расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.

3.3.2. Морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

4. Методика оценки возможного вреда субъектам персональных данных

4.1. Оценка возможного вреда должна производиться коллегиально. В комиссии должно быть четыре человека.

4.2. В оценке возможного вреда исходить из учёта последствий допущенного нарушения принципов обработки персональных данных. Вводится четыре уровня возможного вреда:

нулевой - вред субъекту ПДн не причиняется;

низкий - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

средний - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;

высокий - во всех остальных случаях.

4.3. Каждому уровню возможного вреда сопоставляется числовая оценка Y_1 , а именно:

- 0 - при нулевом уровне вреда;
- 0,05 - при низком уровне вреда;
- 0,1 - при среднем уровне вреда;
- 0,2 - при высоком уровне вреда.

4.4. Каждым членом комиссии на основании собственного субъективного мнения выставляется одна из возможных оценок возможного вреда субъекту для каждой актуальной угрозы безопасности его ПДн из-за несанкционированного, в том числе случайного, доступа к его ПДн при их обработке в информационных системах.

4.5. Все коэффициенты оценок суммируются по каждой актуальной угрозе.

4.6. По значению суммарной оценки Y_2 определяется возможный вред следующим образом:

- если $Y_2 > 0,9$, то вред субъектам ПДн признается высоким;
- если $0,5 < Y_2 < 0,9$, то вред субъектам ПДн признается средним;
- если $0,2 < Y_2 < 0,5$, то вред субъектам ПДн признается низким;
- если $0 < Y_2 < 0,2$, то вред субъектам ПДн признается нулевым.

5. Требования к мерам защиты

С использованием данных об уровне защищенности ИСПДн ГБПОУ «ТК им. Н.Д.

П-155/2019

Кузнецова» и категориях персональных данных, обрабатываемых в них, на основе «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» формулируются и применяются конкретные организационные и технические меры защиты, которые могут быть использованы при эксплуатации ИСПДн.

Разработчик:

заместителя директора по общим вопросам



_____/ Ю.Ю. Алексеев /

АКТ**оценки возможного вреда субъектам, чьи персональные данные обрабатываются в информационной системе персональных данных.**

Комиссия в составе:

председатель комиссии: *Должность – Фамилия И.О.*

члены комиссии: *Должность – Фамилия И.О.*

Должность – Фамилия И.О.

Должность – Фамилия И.О.

Должность – Фамилия И.О.

Должность – Фамилия И.О.

Должность – Фамилия И.О.

с целью: самостоятельной экспертной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Обществом обязанностей, предусмотренных Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных» (далее Закон о ПДн) и принятыми в соответствии с ним нормативными правовыми актами,

рассмотрев результаты по сбору и анализу исходных данных на информационные системы персональных данных (далее по тексту - ИСПДн) Учреждения,

во исполнение требований пунктов 1 и 5 части 1 статьи 18.1 Федерального закона «О персональных данных», о том, что оператор персональных данных самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о ПДн, и, в частности, к таким мерам относится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Обществом законодательства в сфере персональных данных,

и в соответствии с нормами Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

с учетом правил оценки вреда, который может быть причинен субъектам персональных данных, ОПРЕДЕЛИЛА:

оценку возможного вреда коллегиально комиссией на основе следующей методологии: каждым членом комиссии на основании собственного субъективного мнения выставляется, в соответствии с показателями таблицы №1, одна из возможных оценок возможного вреда субъекту в случае реализации конкретного типа актуальной угрозы безопасности его ПДн из-за несанкционированного, в том числе случайного, доступа к его ПДн при их обработке в конкретной информационной системе. Затем все условные коэффициенты оценок суммируется, и определяется, что:

вред субъектам ПДн высокий, если суммарный $0,9 < V_p$

вред субъектам ПДн средний, если суммарный $0,5 < V_p < 0,9$

вред субъектам ПДн низкий, если суммарный $0,2 < V_p < 0,5$

вред субъектам ПДн нулевой, если суммарный $0 < V_p < 0,2$

Таблица №1

Определение возможного вреда (Vp)	Условный коэффициент
Нулевой	0
низкий	0,05
Средний	0,1
Высокий	0,2

определила:

I. В ИСПДн ГБПОУ «ТК им. Н.Д. Кузнецова» осуществляется автоматизация процесса ведения кадрового учета, расчета заработной платы, ведения бухгалтерского учета, и ведется обработка персональных данных работников и обучающихся ГБПОУ «ТК им. Н.Д. Кузнецова».

II. В случае реализации возможных типов актуальных угроз безопасности персональных данных из-за несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в ИСПДн, возможный вред субъектам ПДн членами комиссии определяется:

ТИПЫ актуальных угроз безопасности ПДн	ОЦЕНКИ возможного вреда субъекту ПДн, определенные членами комиссии							Определение возможного вреда (У2)
	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Эксперт 5	Эксперт 6	Эксперт 7	
Кража ПЭВМ	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	У2 = 0,7 вред субъектам ПДн средний
Кража носителей информации	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	У2 = 0,6 вред субъектам ПДн средний
Кража ключей и паролей доступа внутренними и внешними нарушителями	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	У2 = 1,4 вред субъектам ПДн высокий
Кража, модификация, уничтожение информации	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	У2 = 0,65 вред субъектам ПДн средний
Вывод из строя узлов ПЭВМ, каналов связи	Нулевой(0)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Нулевой(0)	Нулевой(0)	У2 = 0,2 вред субъектам ПДн низкий
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Нулевой (0)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Нулевой (0)	Нулевой (0)	У2 = 0,35 вред субъектам ПДн низкий
Несанкционированное отключение средств защиты	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	У2 = 0,5 вред субъектам ПДн средний
Действия вредоносных программ (вирусов)	Средний (0,1)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	У2 = 1,0 вред субъектам ПДн высокий

Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкий (0,05)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	У2 = 0,45 вред субъектам ПДн низкий
Установка ПО, не связанного с исполнением служебных обязанностей	Нулевой (0)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	У2 = 0,3 вред субъектам ПДн низкий
Внедрение аппаратных закладок	Нулевой (0)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	У2 = 0,4 вред субъектам ПДн низкий
Утрата паролей доступа к ИСПДн	Низкий (0,05)	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	У2 = 0,5 вред субъектам ПДн средний
Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкий (0,05)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	У2 = 0,4 вред субъектам ПДн низкий
Непреднамеренное отключение средств защиты	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	У2 = 0,55 вред субъектам ПДн средний
Выход из строя аппаратно-программных средств	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Низкий (0,05)	У2 = 0,4 вред субъектам ПДн низкий
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	У2 = 1,4 вред субъектам ПДн высокий

Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	У2 = 1,0 вред субъектам ПДн высокий
Удаленный запуск приложений	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	У2 = 0,6 вред субъектам ПДн средний
Сканирование сети	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Нулевой (0)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	У2 = 0,35 вред субъектам ПДн низкий

III. ВЫВОД:

На основании экспертных оценок, выставленных членами комиссии, комиссия по персональным данным определила, что в случае реализации актуальных угроз безопасности персональных данных, обработка которых осуществляется в ИСПДн субъектам персональных данных может быть причинен вред, который оценивается как средний ($Y2_{\text{среднее значение}} = 0,62$ вред субъектам ПДн).

Принимаемые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», считать достаточными.

Председатель комиссии:

_____ (И.О. Фамилия)
подпись

Члены комиссии

_____ (И.О. Фамилия)
подпись

_____ (И.О. Фамилия)
подпись

_____ (И.О. Фамилия)
подпись

_____ (И.О. Фамилия)
подпись

_____ (И.О. Фамилия)
подпись

_____ (И.О. Фамилия)
подпись

г. Самара

20.11.2019

Протокол № _____
оценки возможного вреда субъектам персональных данных

Комиссия в составе:

председатель комиссии: *Должность – Фамилия И.О.*члены комиссии: *Должность – Фамилия И.О.**Должность – Фамилия И.О.**Должность – Фамилия И.О.**Должность – Фамилия И.О.**Должность – Фамилия И.О.**Должность – Фамилия И.О.*

с целью самостоятельной экспертной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения ГБПОУ «ТК им. Н.Д. Кузнецова» (далее - Учреждение) обязанностей, предусмотренных Федеральным законом № 152-ФЗ от 27.07.2006 «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами,

рассмотрев результаты по сбору и анализу исходных данных на информационные системы персональных данных, во исполнение требований пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», о том, что оператор персональных данных самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о ПДн, и, в частности, к таким мерам относится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Учреждением законодательства в сфере персональных данных,

с учетом правил оценки вреда, который может быть причинен субъектам персональных данных, ОПРЕДЕЛИЛА:

ТИПЫ актуальных угроз безопасности ПДн	ОЦЕНКИ возможного вреда субъекту ПДн, определенные членами комиссии							Определение возможного вреда (Y2)	
	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Эксперт 5	Эксперт 6	Эксперт 7		
Кража ПЭВМ	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Y2 = 0,7 вред субъектам ПДн средний
Кража носителей информации	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Y2 = 0,6 вред субъектам ПДн средний
Кража ключей и паролей доступа внутренними и внешними нарушителями	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Y2 = 1,4 вред субъектам ПДн высокий
Кража, модификация, уничтожение информации	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Y2 = 0,65 вред субъектам ПДн средний
Вывод из строя узлов ПЭВМ, каналов связи	Нулевой(0)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Нулевой(0)	Нулевой(0)	Y2 = 0,2 вред субъектам ПДн низкий
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Нулевой (0)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Нулевой (0)	Нулевой (0)	Y2 = 0,35 вред субъектам ПДн низкий
Несанкционированное отключение средств защиты	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,5 вред субъектам ПДн средний
Действия вредоносных программ (вирусов)	Средний (0,1)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Y2 = 1,0 вред субъектам ПДн высокий

Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	У2 = 0,45 вред субъектам низкий
Установка ПО, не связанного с исполнением служебных обязанностей	Нулевой (0)	Средний (0,1)	Средний (0,1)	Нулевой (0)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	У2 = 0,3 вред субъектам низкий
Внедрение аппаратных закладок	Нулевой (0)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	У2 = 0,4 вред субъектам низкий
Утрата паролей доступа к ИСПДн	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	У2 = 0,5 вред субъектам средний
Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	У2 = 0,4 вред субъектам низкий
Непреднамеренное отключение средств защиты	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	У2 = 0,55 вред субъектам средний
Выход из строя аппаратно-программных средств	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	У2 = 0,4 вред субъектам низкий
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	У2 = 1,4 вред субъектам высокий

Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	У2 = 1,0 вред субъектам ПДн высокий
Удаленный запуск приложений	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	У2 = 0,6 вред субъектам ПДн средний
Сканирование сети	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Нулевой (0)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	У2 = 0,35 вред субъектам ПДн низкий

Вывод: На основании оценок, выставленных членами комиссии, данных об уровне защищенности информационной системы персональных данных ГБПОУ «ТК им. Н.Д. Кузнецова» и категориях персональных данных, обрабатываемых в них, с учетом требований, предусмотренных статьями 18.1 и 19 Федерального закона № 152-ФЗ от 27.07.2006. «О персональных данных» в ГБПОУ «ТК им. Н.Д. Кузнецова» приняты следующие меры:

1. Назначен ответственный за обработку персональных данных и администратор информационных систем персональных данных;
2. Осуществляется внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных;
3. Работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;
4. Разработаны правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
5. Обеспечивается учет машинных носителей персональных данных;
6. Обеспечивается восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
7. Определён перечень сотрудников, осуществляющих обработку персональных данных, сведения на бумажных носителях хранятся в сейфах или выделенных помещениях, определены места хранения персональных данных;
8. Ведётся учёт всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал учета с отметкой об их выдаче (приеме);
9. Утверждены инструкции, регламентирующие работу с персональными данными и информационными системами персональных данных:
 - 1)
10. Исключена возможность неконтролируемого пребывания посторонних лиц в помещениях где ведется обработка персональных данных.
11. На компьютерах установлено антивирусное программное обеспечение.
12. Пользователи работают под ограниченными учетными записями.
13. Вход в информационную систему осуществляется по буквенноцифровому паролю.
14. Используются средства резервного копирования.

Принимаемые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», считать достаточными.

Председатель комиссии:

_____ подпись (И.О. Фамилия)

Члены комиссии

_____ подпись (И.О. Фамилия)

_____ подпись (И.О. Фамилия)

_____ подпись (И.О. Фамилия)

П-155/2019

подпись

(И.О. Фамилия)

подпись

(И.О. Фамилия)

подпись

(И.О. Фамилия)

