УТВЕРЖДЕНЫ
приказом контрольно-счётной
комиссии Мирного
от 10 октября 2022 г. № 33-ос

Положение
о защите персональных данных работников

I. Общие положения

1.1. Положение о защите персональных данных работников (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории России.

1.2. Цель настоящего Положения – защита персональных данных работников контрольно-счётной комиссии Мирного от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

1.3. В целях настоящего Положения:

- под персональными данными понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных;

- под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

- под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационной системе.

II. Защита персональных данных

2.1. Работодатель принимает следующие меры по защите персональных данных:

2.1.1. Назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и внутренний контроль за соблюдением работниками требований к защите персональных данных.

2.1.2. Разработка политики в отношении обработки персональных данных.

2.1.3. Установление правил доступа к персональным данным, обеспечение регистрации и учета всех действий, совершаемых с персональными данными.

2.1.4. Установление индивидуальных паролей доступа работников контрольно-счётной комиссии Мирного в информационную систему в соответствии с их должностными обязанностями.

2.1.5. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

2.1.7. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ.

2.1.8. Обнаружение фактов несанкционированного доступа к персональным данным.

2.1.9. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.1.10. Обучение работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Работодателя в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

2.1.11. Осуществление внутреннего контроля и аудита.

2.1.12. Определение типа угроз безопасности и уровней защищенности персональных данных, которые хранятся в информационных системах.

2.2. Угрозы защищенности персональных данных.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

2.3. Уровни защищенности персональных данных.

2.3.1. Первый уровень защищенности. Если работодатель отнес информационную систему к первому типу угрозы или если тип угрозы второй, но работодатель обрабатывает специальные категории персональных данных более 100 тыс. физических лиц без учета работников.

2.3.2. Второй уровень защищенности. Если тип угрозы второй и работодатель обрабатывает специальные категории персональных данных работников вне зависимости от их количества или специальные категории персо-

нальных данных менее чем 100 тыс. физических лиц, или любые другие категории персональных данных более чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

2.3.3. Третий уровень защищенности. Если при втором типе угрозы работодатель обрабатывает общие персональные данные работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории персональных данных работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает биометрические персональные данные, или при третьем типе угрозы работодатель обрабатывает общие персональные данные более чем 100 тыс. физических лиц.

2.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие персональные данные работников или менее чем 100 тыс. физических лиц.

2.4. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;

- обеспечивает сохранность носителей информации;

- утверждает перечень работников, допущенных до персональных данных;

- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

2.5. При третьем уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 2.4 настоящего Положения, работодатель назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

2.6. При втором уровне защищенности персональных данных дополнительно к мерам, перечисленным в пунктах 2.4, 2.5 настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

2.7. При первом уровне защищенности персональных данных дополнительно к мерам, перечисленным в пунктах 2.4-2.6 настоящего Положения, работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к персональным данным в системе;

- создает отдел, ответственный за безопасность персональных данных в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

2.8. В целях защиты персональных данных на бумажных носителях работодатель:

- приказом назначает ответственного за обработку персональных данных;

- ограничивает допуск в помещение, где хранятся документы, которые содержат персональные данные работников;

- хранит документы, содержащие персональные данные работников в шкафах, запирающихся на ключ;

- хранит трудовые книжки работников в сейфе.

2.9. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только председателем контрольно-счётной комиссии Мирного, ведущим специалистом аппарата контрольно-счётной комиссии Мирного и уполномоченным лицом МКУ «Управление по обеспечению деятельности ОМСУ».

2.10. Работники, допущенные к персональным данным работников контрольно-счётной комиссии Мирного, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников контрольно-счётной комиссии Мирного не допускаются.

2.11. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.12. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

III. Гарантии конфиденциальности персональных данных

3.1. Все работники контрольно-счётной комиссии Мирного, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с Положением, требованиями законодательства Российской Федерации.

3.2. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

3.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников контрольно-счётной комиссии Мирного, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.