РОССИЙСКАЯ ФЕДЕРАЦИЯ
УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ ГОРОДА ТУЛЫ

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ – ЦЕНТРАЛИЗОВАННАЯ БУХГАЛТЕРИЯ ПО МУНИЦИПАЛЬНЫМ ОБРАЗОВАТЕЛЬНЫМ УЧРЕЖДЕНИЯМ ГОРОДА ТУЛЫ

ПРИКАЗ

20 января 2022 г. **№5-а**

г. Тула

О защите персональных данных
в МКУ-ЦБ по МОУ г.Тулы

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», 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 Российской Федерации от 15.09.2008 №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», локальными нормативными актами

ПРИКАЗЫВАЮ:

1. Утвердить инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах (Приложение №1).
2. Утвердить правила обработки персональных данных в МКУ-ЦБ по МОУ г.Тулы (Приложение №2).
3. Утвердить Политику МКУ-ЦБ по МОУ г.Тулы в отношении обработки персональных данных (Приложение №3).
4. Утвердить Положение о порядке организации и проведения работ по защите конфиденциальной информации в МКУ-ЦБ по МОУ г.Тулы (Приложение №4).
5. Утвердить перечень сведений конфиденциального характера в МКУ-ЦБ по МОУ г.Тулы (Приложение №5).
6. Утвердить инструкцию по обработке персональных данных, осуществляемой без использования средств автоматизации, в МКУ-ЦБ по МОУ г.Тулы (Приложение №6).
7. Утвердить инструкцию по антивирусной защите в информационных системах МКУ-ЦБ по МОУ г.Тулы (Приложение №7).
8. Утвердить инструкцию по организации парольной защиты в информационных системах МКУ-ЦБ по МОУ г.Тулы (Приложение №8).

9. Утвердить регламент резервного копирования и восстановления информации МКУ-ЦБ по МОУ г.Тулы (Приложение №9).
10. Утвердить инструкцию пользователя информационных систем МКУ-ЦБ по МОУ г.Тулы (Приложение №10).
11. Специалисту по кадрам отдела правовой, кадровой работы и делопроизводства Пономаревой М.О. ознакомить с документами, утвержденными настоящим приказом, работников, на которых распространяется их действие под подпись в течение 5 (пяти) рабочих дней.
12. Специалисту по кадрам отдела правовой, кадровой работы и делопроизводства Пономаревой М.О. организовать ознакомление с документами, утвержденными настоящим приказом, вновь принимаемых работников, на которых распространяется их действие под подпись.
13. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник - главный бухгалтер
МКУ - ЦБ по МОУ г. Тулы Л.А. Скалина

Приложение №1

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

Инструкция
ответственного за обеспечение безопасности персональных данных в информационных системах МКУ-ЦБ по МОУ г.Тулы

1. Общие положения.

1.1. Ответственный за обеспечение безопасности персональных данных в информационных системах МКУ-ЦБ по МОУ г.Тулы (далее Ответственный) — сотрудник МКУ-ЦБ по МОУ г.Тулы, обеспечивающий защиту информации, обрабатываемой в информационных системах МКУ-ЦБ по МОУ г.Тулы, отвечающий за защиту информационных систем и содержащейся в них информации от несанкционированного доступа, осуществляет функции контроля за соблюдением режима защиты конфиденциальной информации (в т. ч. персональных данных), корректировку разрешительной системы доступа к информационным системам (ресурсам), ведение и поддержание в актуальном состоянии документации по вопросам защиты информации в информационных системах МКУ-ЦБ по МОУ г.Тулы.

1.2. Ответственный осуществляет взаимодействие по вопросам технической защиты конфиденциальной информации (в т. ч. персональных данных) с организацией - лицензиатом ФСТЭК России на деятельность по технической защите конфиденциальной информации, осуществлявшей аттестацию объектов информатизации МКУ-ЦБ по МОУ г.Тулы (орган по аттестации) на соответствие этих объектов требованиям законодательства Российской Федерации.

1.3. Ответственный в своей работе руководствуется положениями настоящей Инструкции, требованиями других нормативных правовых и нормативно-методических документов, регламентирующих защиту информации, требованиями эксплуатационной документации средств защиты информации, используемых в МКУ-ЦБ по МОУ г.Тулы, технических и программных средств, имеющих встроенные механизмы защиты.

2. В обязанности Ответственного входит:

2.1. Ведение учета перечня категорий персональных данных, обрабатываемых в МКУ-ЦБ по МОУ г.Тулы;

2.1. Ведение учета лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ;

2.2. Ведение учета лиц, допущенных к работе со средствами криптографической защиты информации;

2.3. Разработка и поддержание в актуальном состоянии разрешительной системы доступа к локальным и сетевым ресурсам информационных систем МКУ-ЦБ по МОУ г.Тулы;

2.4. Разработка и поддержание в актуальном состоянии технических паспортов информационных систем МКУ-ЦБ по МОУ г.Тулы;

2.5. Согласование вносимых изменений в технический паспорт аттестованных информационных систем с органом по аттестации;

2.6. Участие в проведении мероприятий внутреннего контроля по вопросам обработки и защиты конфиденциальной информации, в том числе персональных данных;

2.7. Ведение учета средств защиты информации, эксплуатационной и технической документации к ним;

2.8. Ведение учета съемных носителей персональных данных (в т. ч. маркировка учтенных съемных носителей).

3. Ответственный имеет право:

3.1. Требовать от пользователей информационных систем МКУ-ЦБ по МОУ г.Тулы выполнения установленной технологии обработки информации, локальных актов в сфере информационной безопасности МКУ-ЦБ по МОУ г.Тулы;

3.2. Останавливать обработку информации информационных системах МКУ-ЦБ по МОУ г.Тулы в случае подтверждения нарушений установленной технологии обработки данных, приводящих к нарушению функционирования средств защиты информации;

3.3. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам защиты информации;

4. Ответственный несет персональную ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с настоящей инструкцией.

5. Ответственный несет ответственность по законодательству РФ за нарушение требований нормативно-методических документов по защите информации и настоящей инструкции.

Приложение №2

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

ПРАВИЛА
обработки персональных данных МКУ-ЦБ по МОУ г.Тулы

I. Общие положения

1. Настоящие Правила обработки персональных данных (далее Правила) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн), а также определяют цели обработки ПДн, содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2. Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных».

3. Обработка ПДн в МКУ-ЦБ по МОУ г.Тулы осуществляется как с использованием средств автоматизации, так и без использования средств автоматизации.

4. Руководитель МКУ-ЦБ по МОУ г.Тулы с целью выполнения требований законодательства Российской Федерации в сфере защиты информации назначает ответственного за организацию обработки ПДн в МКУ-ЦБ по МОУ г.Тулы, а также ответственного за обеспечение безопасности ПДн в информационных системах МКУ-ЦБ по МОУ г.Тулы, утверждает локальные документы, регламентирующие порядок обработки и защиты информации в МКУ-ЦБ по МОУ г.Тулы.

II. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере ПДн

5. Для выявления и предотвращения нарушений законодательства Российской Федерации в сфере ПДн реализуются следующие процедуры:

5.1. Принятие мер, направленных на обеспечение выполнения обязательных требований при обработке ПДн и соблюдения прав субъектов ПДн;

5.2. Организация внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным действующим законодательством в

области ПДн и регламентирующими документами МКУ-ЦБ по МОУ г.Тулы;

5.3. Ознакомление сотрудников, осуществляющих обработку ПДн, с законодательством Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, настоящими Правилами и (или) обучение сотрудников;

5.4. Ограничение обработки ПДн достижением конкретных, заранее определенных и законных целей;

5.5. Осуществление обработки ПДн в соответствии с принципами и условиями обработки ПДн, установленными законодательством Российской Федерации в области ПДн;

5.6. Недопущение обработки ПДн, несовместимых с целями сбора ПДн;

5.7. Недопущение объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

5.8. Соответствие содержания и объема обрабатываемых ПДн заявленным целям обработки (обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки);

5.9. Обеспечение при обработке ПДн точности ПДн, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки ПДн.

III. Цели и содержание обрабатываемых ПДн в МКУ-ЦБ по МОУ г.Тулы

№ п./п.	Цели обработки ПДн	Субъекты ПДн	Перечень категорий ПДн	Места хранения бумажных носителей ПДн	Перечень лиц, имеющих доступ к ПДн	Правовое основание обработки ПДн
1.	Ведение кадрового учета, заключение и исполнение трудовых договоров	Сотрудники, их близкие родственники	Ф.И.О.; должность; адрес; число, месяц, год рождения; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; образование; трудовая деятельность	Отдел кадров, архив	Специалист отдела кадров, бухгалтер по расчету заработной платы, начальник отдела правовой, кадровой работы и делопроизводства	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», локальные акты
2.	Ведение воинского учета	Сотрудники	Ф.И.О.; должность; адрес; число, месяц, год рождения; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; образование; трудовая деятельность	Отдел кадров, архив	Специалист отдела кадров, начальник отдела правовой, кадровой работы и делопроизводства	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», локальные акты
3.	Предоставление отчетности (индивидуальных сведений в ПФР; справок о доходах в ИФНС), возмещение расходов по страхованию в ФСС, подготовка и выдача справок (2-НДФЛ, для расчета пособий, для центра занятости, для назначения пенсии за выслугу лет и т.п.)	Сотрудники, их близкие родственники	Ф.И.О.; должность; адрес; число, месяц, год рождения; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; образование; трудовая деятельность	Кабинет бухгалтера по расчету заработной платы, архив	Специалист отдела кадров, бухгалтер по расчету заработной платы, начальник отдела правовой, кадровой работы и делопроизводства	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», локальные акты
4.	Перечисление заработной платы через банк	Сотрудники	Ф.И.О.; должность; адрес; число, месяц, год рождения; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; образование; трудовая деятельность	Кабинет бухгалтера по расчету заработной платы, архив	Бухгалтер по расчету заработной платы	Согласие на обработку (передачу) ПДн
5.	Ведение кадрового резерва	Претенденты на замещение вакантных должностей	Ф.И.О.; должность; адрес; число, месяц, год рождения; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; образование; трудовая деятельность	Отдел кадров	Специалист отдела кадров, начальник отдела правовой, кадровой работы и делопроизводства	Согласие на обработку ПДн
6.	Рассмотрение кандидатур на замещение вакантных должностей (работа с резюме претендентов)	Претенденты на замещение вакантных должностей в Администрации	Ф.И.О.; должность; адрес; число, месяц, год рождения; вид, серия, номер документа, удостоверяющего	Отдел кадров	Специалист отдела кадров	Согласие на обработку ПДн

			личность, наименование органа, выдавшего его, дата выдачи; образование; трудовая деятельность			
7.	Деятельность в соответствии с полномочиями МКУ-ЦБ по МОУ г.Тулы	Физические лица и представители юридических лиц, состоящие в договорных отношениях с МКУ-ЦБ по МОУ г.Тулы	Ф.И.О.; должность; адрес; число, месяц, год рождения; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; образование; трудовая деятельность	Приемная руководителя МКУ-ЦБ по МОУ г.Тулы	Специалист отдела кадров, бухгалтер по расчету заработной платы, начальник отдела правовой, кадровой работы и делопроизводства	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», локальные акты
8.	Рассмотрение обращений граждан	Лица, направившие обращение	Фамилия, имя, отчество, адрес, номер контактного телефона или сведения о других способах связи, информация, сообщаемая в обращении	Приемная руководителя МКУ-ЦБ по МОУ г.Тулы	Начальник отдела правовой, кадровой работы и делопроизводства	Федеральный закон от 02.05.2006 N 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», локальные акты
9.	Рассмотрение запросов от органов, осуществляющих контрольные и надзорные функции	Органы, направившие обращение	Фамилия, имя, отчество, адрес, номер контактного телефона или сведения о других способах связи, информация, сообщаемая в обращении	Отдел кадров	Специалист отдела кадров, начальник отдела правовой, кадровой работы и делопроизводства	Согласно действующему законодательству РФ. согласие на обработку персональных данных для предоставления информации в надзорные и контрольные органы не требуется.

VII. Порядок уничтожения ПДн при достижении целей обработки или при наступлении иных законных оснований

6. Уничтожению подлежат ПДн при достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

7. Уничтожение ПДн может быть произведено любым способом, исключающим возможность восстановления ПДн.

8. Уничтожение бумажных носителей ПДн осуществляется соответствующей комиссией и фиксируется актом об уничтожении ПДн.

9. Уничтожение ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Приложение №3

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

Политика
МКУ-ЦБ по МОУ г.Тулы в отношении обработки персональных данных

1. Общие положения

1.1. Настоящая Политика МКУ-ЦБ по МОУ г.Тулы в отношении обработки персональных данных (далее - Политика) разработана в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

1.2. Политика определяет цели, принципы обработки и реализуемые требования к защите персональных данных в МКУ-ЦБ по МОУ г.Тулы.

1.3. Персональные данные являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации.

2. Основные понятия

2.1. В настоящей Политике используются следующие основные понятия:

2.1.1. Субъектами персональных данных МКУ-ЦБ по МОУ г.Тулы являются:

- работники МКУ-ЦБ по МОУ г.Тулы;
- претенденты на замещение вакантной должности;
- студенты, проходящие практику в МКУ-ЦБ по МОУ г.Тулы;
- контрагенты МКУ-ЦБ по МОУ г.Тулы;
- лица, передавшие персональные данные в МКУ-ЦБ по МОУ г.Тулы в своих обращениях и заявлениях, в том числе при оформлении пропуска на территорию или в помещения МКУ-ЦБ по МОУ г.Тулы;
- лица, состоящие в договорных или иных отношениях с МКУ-ЦБ по МОУ г.Тулы.

2.1.2. В соответствии со ст. 86 ТК РФ МКУ-ЦБ по МОУ г.Тулы предоставлено право обрабатывать персональные данные сотрудника Учреждения исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получения образования и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.1.3. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.1.4. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств

автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.1.5. Конфиденциальность персональных данных – обязанность оператора и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Принципы и цели обработки персональных данных

3.1. МКУ-ЦБ по МОУ г.Тулы в своей деятельности по обработке персональных данных руководствуется следующими принципами:

3.1.1. Обработка персональных данных осуществляется на законной и справедливой основе.

3.1.2. Цели обработки персональных данных соответствуют полномочиям МКУ-ЦБ по МОУ г.Тулы.

3.1.3. Содержание и объем обрабатываемых персональных данных соответствуют целям обработки персональных данных.

3.1.4. Достоверность персональных данных, их актуальность и достаточность для целей обработки, недопустимость обработки избыточных по отношению к целям сбора персональных данных.

3.1.5. Ограничение обработки персональных данных при достижении конкретных и законных целей, запрет обработки персональных данных, несовместимых с целями сбора персональных данных.

3.1.6. Запрет объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.1.7. Осуществление хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем это требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством.

3.1.8. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

3.2. Обработка персональных данных работников МКУ-ЦБ по МОУ г.Тулы осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, заключения и исполнения трудовых договоров, ведения воинского учета, исполнения требований по охране труда.

3.3. Обработка персональных данных граждан, не являющихся работниками МКУ-ЦБ по МОУ г.Тулы, осуществляется с целью реализации полномочий МКУ-ЦБ по МОУ г.Тулы в соответствии с Уставом, а также с целью отбора претендентов на замещение вакантных должностей МКУ-ЦБ по МОУ г.Тулы.

4. Перечень мер по обеспечению безопасности персональных данных при их обработке

4.1. МКУ-ЦБ по МОУ г.Тулы при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

4.1.1. Назначением ответственного за организацию обработки персональных данных.

4.1.2. Утверждением локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

4.1.3. Осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных.

4.1.4. Ознакомлением работников МКУ-ЦБ по МОУ г.Тулы, непосредственно осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных работников.

4.1.5. Выполнением требований, установленных постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» при обработке персональных данных, осуществляемой без использования средств автоматизации.

4.1.6. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

4.1.7. Учетом машинных носителей персональных данных.

4.1.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием мер.

4.1.9. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.1.10. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых в информационной системе персональных данных.

4.2. Работники МКУ-ЦБ по МОУ г.Тулы, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную,

административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение №4

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите конфиденциальной информации в МКУ-ЦБ по МОУ г.Тулы

I. Общие положения

1. Настоящее Положение устанавливает порядок организации и проведения работ по защите конфиденциальной информации в МКУ-ЦБ по МОУ г.Тулы (далее – Учреждение).

2. Действие настоящего Положения не распространяется на правоотношения, связанные с обращением со сведениями, составляющими государственную тайну.

3. В настоящем Положении под конфиденциальной информацией (информацией конфиденциального характера, сведениями конфиденциального характера) понимается информация ограниченного доступа, свободный доступ к которой ограничен в соответствии с федеральным законодательством, а также служебная информация, доступ к которой ограничен обладателем информации.

4. В настоящем Положении используются основные понятия в значении, определенном Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также следующие понятия:

автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

допуск к конфиденциальной информации – процедура оформления права граждан на доступ к сведениям конфиденциального характера;

защищаемые помещения (ЗП) – помещения (кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, конференций, переговоров и т.п.), связанных с обсуждением и (или) оглашением информации конфиденциального характера;

контролируемая зона (КЗ) – пространство (территория, здание, помещение или их часть), в котором исключено неконтролируемое пребывание лиц, не имеющих допуска, а также транспортных, технических и иных материальных средств;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по функциональному предназначению и техническим

характеристикам;

носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информационных сигналов;

ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;

служебная информация ограниченного распространения – информация, касающаяся деятельности Учреждения, ограничение на распространение которой диктуются служебной необходимостью;

средство защиты информации (СЗИ) – техническое, программное, программно-техническое средство, предназначенное (используемое) для защиты информации;

утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

5. Защита конфиденциальной информации осуществляется на основании действующего законодательства Российской Федерации.

6. Доступ к сведениям конфиденциального характера Учреждение, в том числе содержащимся в информационных системах, может быть предоставлен с согласия обладателя информации и (или) в случаях, установленных законодательством.

7. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

8. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

9. Согласие на обработку персональных данных может быть отозвано

субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, предусмотренных действующим законодательством Российской Федерации Федерального закона.

10. В Учреждении осуществляется разрешение или ограничение доступа к информации, определяется порядок и условия такого доступа.

11. Сведения конфиденциального характера, в том числе служебную информацию, ставшие известными работнику вследствие выполнения должностных обязанностей, запрещается использовать в личных целях и в целях причинения имущественного ущерба, морального вреда.

II. Принципы ограничения доступа к сведениям

9. Основными принципами ограничения доступа являются законность, обоснованность и своевременность.

10. Законность ограничения доступа заключается в выполнении требований законодательства при отнесении сведений к категории конфиденциальной информации. При этом учитываются как нормы, предписывающие налагать ограничения на доступ к этим сведениям, так и запрещающие такие ограничения.

11. Обоснованность ограничения доступа заключается в установлении путем экспертной оценки целесообразности ограничения доступа, вероятных последствий этого акта, исходя из законных интересов Учреждения.

12. Своевременность ограничения доступа заключается в установлении ограничений на разглашение и (или) распространение сведений с момента их получения (разработки) или заблаговременно.

III. Порядок отнесения сведений к категории конфиденциальной информации

13. Решение об отнесении сведений к категории конфиденциальной информации принимает руководитель Учреждения путем утверждения перечня сведений конфиденциального характера (далее – Перечень сведений).

14. Для включения в Перечень сведений осуществляется анализ информации, содержащейся в утверждаемых руководителем документах, документах текущей деятельности (информационных потоках), обрабатываемых как в интересах обладателя информации, так и в интересах других лиц.

15. С целью обеспечения принципа обоснованности рассматривается возможный ущерб, который может быть нанесен государству, Учреждению, иным лицам в результате разглашения или распространения конфиденциальной информации, с затратами, необходимыми на ограничение доступа к ней.

16. Возможный ущерб оценивается исходя из наличия материальных, финансовых, репутационных и иных рисков или морального вреда в результате несанкционированного разглашения или распространения конфиденциальной информации.

17. При определении размера (степени) ущерба прогнозируются возможные потери и риски, возникающие не только в настоящее время, но и те, которые могут возникнуть в будущем.

18. При рассмотрении вопросов отнесения сведений к категории конфиденциальной информации учитываются следующие отрицательные факторы разглашения конфиденциальной информации:

нарушение федеральных законов и иных нормативных правовых актов по ограничению доступа к информации;

разрыв отношений (или их осложнение) с деловыми партнерами, юридическими и физическими лицами по причине разглашения сведений;

срыв или невыполнение договорных обязательств, контрактов;

создание трудностей при взаимодействии;

экономические, судебные и иные санкции со стороны юридических и физических лиц за незаконное разглашение сведений о них;

потеря, блокирование или искажение информации в базах данных;

несанкционированная передача баз данных или их части;

раскрытие действующей системы защиты информации.

19. Информация, полученная в результате взаимодействия Учреждения с контрагентами в процессе хозяйственной деятельности, может быть отнесена к категории конфиденциальной положениями заключаемых договоров, соглашений, в которых также отражаются взаимные обязательства и ответственность сторон за сохранность этой информации.

Такая информация в Перечень сведений не включается.

IV. Обязанности по защите конфиденциальной информации и ответственность

20. В Учреждении назначается лица, ответственные:

за организацию обработки персональных данных;

за обеспечение безопасности конфиденциальной информации (в том числе персональных данных).

21. Указанные в пункте 20 ответственные лица в пределах своей компетенции организуют:

контролируемый допуск работников Учреждения к информации конфиденциального характера;

учет, хранение и уничтожение документов и машинных носителей с конфиденциальной информации;

обработку конфиденциальной информации с помощью средств вычислительной техники;

выполнение мероприятий по защите конфиденциальной информации;

контроль соблюдения порядка работы с конфиденциальной информацией.

22. Не допускается хранение и обработка конфиденциальной информации на территории иностранных государств, если иное не предусмотрено действующими международными соглашениями Российской Федерации.

23. Доступ к конфиденциальной информации осуществляется в соответствии с разрешительной системой доступа (матрицей доступа), утверждаемой руководителем Учреждения.

24. За разглашение конфиденциальной информации, а также нарушение порядка обращения с ней, работник Учреждения может быть привлечен к дисциплинарной и (или) иной ответственности, предусмотренной действующим законодательством.

25. Не реже одного раза в год в Учреждении осуществляется контроль (аудит) соблюдения порядка работы с конфиденциальной информацией.

V. Порядок обмена конфиденциальной информации

26. Предоставление (передача) конфиденциальной информации может производиться только на основании решения руководителя Учреждения при условии соблюдения требований по защите информации.

27. Информация конфиденциального характера предоставляется органам государственной власти, государственным учреждениям и органам местного самоуправления Тульской области на безвозмездной основе.

28. Предоставление конфиденциальной информации иным лицам, если иное не установлено законодательством, регулируется заключаемыми договорами, устанавливающими права, обязанности и ответственность сторон, перечень предоставляемых конфиденциальных сведений и компенсацию за разглашение и иное распространение указанных сведений.

29. При направлении сторонним организациям (учреждениям, предприятиям) сведений и документов, содержащих конфиденциальную информацию, в сопроводительном письме необходимо уведомлять (информировать) получателя о законном требовании соблюдения конфиденциальности полученной им информации и ответственности за ее разглашение или распространение. При обмене конфиденциальной информацией между органами власти, учреждениями делать указанное уведомление не обязательно.

30. Передача конфиденциальной информации в электронном виде разрешается только по защищенным каналам связи, оборудованным сертифицированными средствами защиты.

31. Не допускается речевая передача конфиденциальной информации по открытым проводным каналам связи, выходящим за пределы КЗ, и радиоканалам. При необходимости передачи конфиденциальной информации следует использовать защищенные линии связи.

32. Проведение конфиденциальных мероприятий (в том числе совещаний, комиссий, собраний, обсуждений и т. п.) разрешается только в ЗП, исключающих возможность перехвата речевой информации конфиденциального характера.

33. При необходимости ЗП оборудуются сертифицированными средствами защиты информации. ЗП должны быть аттестованы по требованиям безопасности информации и размещаться в пределах контролируемой зоны органа власти.

34. В Учреждении в соответствии с установленными требованиями по защите информации определяется перечень ЗП и лиц, ответственных за их эксплуатацию.

35. Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, устройств сотовой, пейджинговой и транкинговой связи.

VI. Организация и проведение работ по защите конфиденциальной информации

36. Проведение работ по защите конфиденциальной информации осуществляется путем:

выполнения комплекса мероприятий (правовых, организационных, технических), направленных на предотвращение утечки информации (в том числе по техническим каналам), несанкционированного доступа к ней, преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения;

проведения специальных работ, порядок организации и выполнения которых определяется Правительством Российской Федерации и федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

37. Организация мероприятий по защите конфиденциальной информации возлагается на ответственных лиц, указанных в пункте 20 настоящего Положения.

38. Обработка конфиденциальной информации допускается только на АС Учреждения, оснащенных сертифицированными по требованию законодательства программными, техническими и программно-техническими средствами защиты информации.

39. АС обработки такой информации должны быть аттестованы по требованиям безопасности информации, а применяемое в них программное обеспечение должно быть лицензионным.

40. При обработке конфиденциальной информации с использованием АС необходимо неукоснительно выполнять требования утвержденных руководителем Учреждения локальных актов, регламентирующих:

антивирусную защиту информации;

использование программного обеспечения;

применение машинных носителей информации;

организацию сетевой защиты информации;

авторизацию пользователей;

иные аспекты защиты информации.

Приложение №5

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

ПЕРЕЧЕНЬ

сведений конфиденциального характера в МКУ-ЦБ по МОУ г.Тулы

№ п/п	Сведения, отнесенные к категории ограниченного доступа	Основание отнесения сведений к категории ограниченного доступа
1	Персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу)	Статья 7 Федерального закона от 27 июня 2006 года №152-ФЗ «О персональных данных»
2	Сведения, ставшие известными в связи с исполнением должностных обязанностей, в том числе сведения, касающиеся частной жизни и здоровья граждан или затрагивающие их честь и достоинство	Пункт 6 статьи 12 Федерального закона от 02.03.2007 N 25-ФЗ «О муниципальной службе в Российской Федерации»
3	Сведения о личной и семейной тайне. Сведения о частной жизни. Сведения, раскрывающие тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.	Статья 23 Конституции Российской Федерации, принятой всенародным голосованием 12 декабря 1993 года
4	Сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния	Статья 12 Федерального закона от 15.11.1997 N 143-ФЗ «Об актах гражданского состояния»
5	Сведения, предоставляемые участниками торгов в соответствии с правилами организованных торгов	Статья 23 Федерального закона от 21.11.2011 N 325-ФЗ «Об организованных торгах»
6	Сведения, содержащиеся в проектах документов и (или) прилагаемых к ним материалах на любом носителе информации до официальной публикации	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
7	Сведения, содержащиеся в материалах служебных расследований (проверок) до издания соответствующих распорядительных документов	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
8	Сведения о системах защиты информации (средства, методы и способы защиты информации, реквизиты доступа, матрицы доступа и процедуры доступа к информационным системам и ресурсам). Сведения об оценке эффективности защиты информации.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
9	Сведения об информационно-телекоммуникационных сетях и каналах связи, компьютерных сетях, средствах вычислительной техники, программном обеспечении, системах и средствах охранно-тревожной, пожарной сигнализации и видеонаблюдения	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
10	Сведения, раскрывающие бюджетные проектировки финансирования правительства и органов исполнительной власти Тульской области, а также подведомственных государственных учреждений до момента утверждения объемов финансирования	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»

№ п/п	Сведения, отнесенные к категории ограниченного доступа	Основание отнесения сведений к категории ограниченного доступа
11	Сведения о деятельности конкурсных, аукционных и других подобных комиссий и об оценке предложений до момента утверждения победителя закупочной процедуры	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
12	Сведения, раскрывающие вопросы защиты объектов от чрезвычайных ситуаций техногенного характера и террористических проявлений	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
13	Несекретная информация, касающаяся деятельности органа местного самоуправления, ограничения на распространение которой диктуются служебной необходимостью	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
14	Сведения об организации внутренних контрольных мероприятий и проверок до их завершения	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
15	Сведения, раскрывающие: -штатные расписания; -распоряжения по личному составу	Пункт 3 статьи 6 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
16	Данные, содержащиеся в паспорте безопасности МКУ-ЦБ по МОУ г. Тулы от 15.10.2018	Постановление Правительства РФ от 25 марта 2015 г. N 272 "Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)".

Приложение №6

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

ИНСТРУКЦИЯ
по обработке персональных данных, осуществляемой без использования средств автоматизации, МКУ-ЦБ по МОУ г.Тулы

I. Общие положения

1. Настоящая инструкция по обработке персональных данных, осуществляемой без использования средств автоматизации, в МКУ-ЦБ по МОУ г.Тулы (далее - Инструкция) устанавливают порядок обработки персональных данных, осуществляемой без использования средств автоматизации, а также порядок заполнения типовых форм документов МКУ-ЦБ по МОУ г.Тулы (далее – Учреждение), характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма).

2. Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных».

II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

4. Работники Учреждения, осуществляющие обработку персональных данных без использования средств автоматизации, а также лица, осуществляющие такую обработку по договору с Учреждением, информируются о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти Тульской области, а также локальными правовыми актами Учреждения. По факту информирования указанные лица подписывают обязательства о неразглашении персональных данных.

5. При хранении материальных носителей персональных данных, обрабатываемых без использования средств автоматизации, с целью соблюдения условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ, применяются следующие муры:

5.1. Хранение материальных носителей персональных данных, обрабатываемых без использования средств автоматизации, осуществляется в местах, установленных локальными актами Учреждения.

5.2. Обеспечивается раздельное хранение персональных данных, обработка которых осуществляется в несовместимых целях.

5.3. Руководитель Учреждения устанавливает перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

6. Работник Учреждения, ответственный за организацию обработки персональных данных, совместно с администратором безопасности контролирует реализацию мер, указанных в п.п. 5.1.-5.3. Инструкции, а также порядок их принятия.

III. Порядок заполнения типовых форм

7. Учреждение является оператором, осуществляющим обработку персональных данных, адрес: г. Тула, ул. Гоголевская, д. 92.

Целями обработки персональных данных является осуществление деятельности, реализация полномочий Учреждения, в том числе кадровый учет, исполнение трудовых договоров, рассмотрение кандидатур на замещение вакантных должностей, антикоррупционная деятельность, воинский учет, ведением бухгалтерского, налогового и иных видов учета и пр.

Источником получения персональных данных, обрабатываемых без использования средств автоматизации, является непосредственно субъект персональных данных, либо его официальный представитель.

Сроки обработки персональных данных устанавливаются локальными актами Учреждения.

Персональные данные в администрации обрабатываются смешанным образом. Перечень действий с персональными данными, обрабатываемыми без использования средств автоматизации: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, удаление, уничтожение персональных данных.

Приложение №7

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

ИНСТРУКЦИЯ
по антивирусной защите в информационных системах МКУ-ЦБ по МОУ г.Тулы

1. Настоящая инструкция предназначена для ответственного за обеспечение безопасности персональных данных в информационных системах МКУ-ЦБ по МОУ г.Тулы (далее – Ответственный) и пользователей, обрабатывающих персональные данные на автоматизированных рабочих местах (далее АРМ) информационных систем МКУ-ЦБ по МОУ г.Тулы.
2. В целях обеспечения антивирусной защиты на АРМ производится антивирусный контроль.
3. Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах МКУ-ЦБ по МОУ г.Тулы.
4. К применению на АРМ допускаются только лицензионные и сертифицированные ФСТЭК России антивирусные средства.
5. На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций МКУ-ЦБ по МОУ г.Тулы.
6. Пользователи АРМ при работе с носителями информации обязаны перед началом работы осуществить проверку их на предмет отсутствия компьютерных вирусов.
7. Обновление антивирусных баз осуществляется ежедневно путем настройки в антивирусном средстве доступа к серверам обновлений разработчика антивирусного средства. В случае невозможности настроить доступ к серверам обновлений разработчика антивирусного средства, Ответственный один раз в неделю осуществляет установку пакетов обновлений антивирусных баз, осуществляет контроль их подключения к антивирусному программному обеспечению и проверку жесткого диска и съемных носителей на наличие вирусов.
8. При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность Ответственного и прекратить какие-либо действия на АРМ.
9. Ответственный проводит расследование факта заражения АРМ компьютерным вирусом. «Лечение» зараженных файлов осуществляется путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль.
10. В случае обнаружения вируса, не поддающегося лечению, Ответственный обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность АРМ. В случае

отказа АРМ – произвести восстановление соответствующего программного обеспечения.

11. Обо всех фактах заражения АРМ, Ответственный обязан ставить в известность ответственного за организацию обработки персональных данных и своего непосредственного руководителя.

Приложение №8

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

Инструкция
по организации парольной защиты
в информационных системах МКУ-ЦБ по МОУ г.Тулы

1. Инструкция по организации парольной защиты в информационных системах МКУ-ЦБ по МОУ г.Тулы регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах МКУ-ЦБ по МОУ г.Тулы, а также контроль за действиями пользователей при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) информационных систем МКУ-ЦБ по МОУ г.Тулы и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение защиты персональных данных в информационных системах МКУ-ЦБ по МОУ г.Тулы (далее Ответственный).

3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями АРМ самостоятельно с учетом следующих требований:

3.1. Длина пароля должна быть не менее 7 символов;

3.2. В числе символов пароля необходимо использовать буквы в верхнем и/или нижнем регистрах и цифры;

3.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.);

3.4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 3-х позициях;

3.5. Личный пароль пользователь не имеет права сообщать никому.

4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного.

6. Для генерации стойких значений паролей могут применяться специальные программные средства.

7. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 180 дней.

8. Внеплановая смена личного пароля или удаление (блокирование) учетной записи пользователя в случае прекращения его полномочий (увольнение и т. п.) должна производиться Ответственным немедленно после окончания последнего сеанса работы данного пользователя с системой.

9. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) Ответственного.

10. В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 8 или п. 9 настоящей инструкции в зависимости от полномочий владельца скомпрометированного пароля.

11. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у Ответственного или руководителя подразделения в опечатанном личной печатью (штампом организации) конверте.

Приложение №9

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

РЕГЛАМЕНТ
резервного копирования и восстановления информации в МКУ-ЦБ по МОУ г.Тулы

I. Общие положения

1. Настоящий Регламент резервного копирования и восстановления информации в МКУ-ЦБ по МОУ г.Тулы (далее – Регламент), хранящихся на серверах и автоматизированных рабочих местах (далее – АРМ) МКУ-ЦБ по МОУ г.Тулы, разработан в соответствии с требованиями Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации.

2. Настоящий регламент разработан с целью:

определения порядка резервирования информации;

определения порядка восстановления информации в случае ее искажения или утраты, в связи с попытками несанкционированного доступа, сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

упорядочения работы сотрудников, связанной с резервным копированием и восстановлением информации;

3. В настоящем Регламенте определены действия при выполнении следующих мероприятий:

резервное копирование;

контроль резервного копирования;

хранение резервных копий;

восстановление информации.

II. Порядок резервного копирования

4. Резервному копированию подлежит информация следующих основных категорий:

информация ограниченного доступа, в том числе персональные данные (далее – ПДн), хранящаяся на серверах МКУ-ЦБ по МОУ г.Тулы (базы данных, файлы и каталоги);

информация ограниченного доступа, в том числе ПДн, хранящаяся на АРМ МКУ-ЦБ по МОУ г.Тулы.

5. Резервное копирование/восстановление информации, хранящейся на серверах МКУ-ЦБ по МОУ г.Тулы, осуществляется штатными средствами операционных систем с использованием Veeam Annual Basic Maintenance Renewal – Veeam Backup Essential Standard 2 socket bundle.

6. Контроль результата процедур резервного копирования, а также восстановление информации ограниченного доступа, хранящейся на серверах МКУ-ЦБ по МОУ г.Тулы, осуществляет ответственный за обеспечение безопасности персональных данных в информационных системах МКУ-ЦБ по МОУ г.Тулы (далее – Ответственный).

7. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) носителей резервных копий без потерь информации, а также обеспечивать восстановление информации в случае отказа любого из устройств резервного копирования.

8. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

9. Резервное копирование/восстановление информации, хранящейся на АРМ МКУ-ЦБ по МОУ г.Тулы, осуществляется пользователями на учтенные съемные носители.

10. Необходимость и периодичность резервного копирования информации, хранящейся на АРМ МКУ-ЦБ по МОУ г.Тулы, а также срок хранения резервных копий такой информации на съемных носителях определяется пользователями самостоятельно.

11. Резервное копирование информации может осуществляться исключительно на съемные машинные носители информации, учтенные в журнале учета съемных носителей информации МКУ-ЦБ по МОУ г.Тулы.

12. Не допускается создание резервных копий на неучтенные и личные носители информации. При использовании съемных машинных носителей как носителей ПДн запись в журнале учета должна содержать отметку «Конфиденциально».

13. Хранение съемных машинных носителей ПДн должно осуществляться в сейфах (металлических шкафах), оборудованных внутренними замками и приспособлениями для опечатывания замочных скважин.

14. В случае отсутствия сейфа (металлического шкафа) у пользователя, осуществляющего хранение, допускается осуществлять хранение в сейфе Ответственного.

15. Носители с ПДн, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения, реализующим полное физическое уничтожение данных.

16. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, должно быть немедленно сообщено Ответственному.

III. Восстановление информации из резервной копии

17. В случае необходимости, восстановление информации, хранящейся на серверах МКУ-ЦБ по МОУ г.Тулы, может производиться Ответственным на основании заявки пользователя.

18. В случае повреждения или утраты информации, хранящейся на АРМ МКУ-ЦБ по МОУ г.Тулы до начала восстановления их со съемного носителя пользователь должен определить причину утраты или повреждения файлов, содержащих ПДн.

19. Если повреждение или удаление информации вызвано действиями самого пользователя (непреднамеренное удаление файла), восстановление информации со съёмного носителя может осуществляться пользователем незамедлительно.

20. В случае повреждения файловой системы АРМ или работоспособности жесткого диска в результате системного сбоя АРМ пользователь должен обратиться к Ответственному.

Перенос файлов из резервной копии может выполняться пользователем только после восстановления работоспособности АРМ.

21. В случае повреждения или утраты файлов, содержащих конфиденциальную информацию, в том числе ПДн, вследствие несанкционированного доступа (далее – НСД) к АРМ МКУ-ЦБ по МОУ г.Тулы пользователь незамедлительно сообщает о данном факте Ответственному.

Восстановление файлов из резервной копии может осуществляться только после проведения расследования инцидента безопасности НСД с соответствующим устранением угрозы дальнейших инцидентов НСД.

22. Если утрата файлов на АРМ МКУ-ЦБ по МОУ г.Тулы произошла в результате вирусного заражения, восстановление файлов возможно только после выполнения мероприятий в соответствии с инструкцией антивирусной защиты МКУ-ЦБ по МОУ г.Тулы.

Приложение №10

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 20.01.2022 №5-а

ИНСТРУКЦИЯ
пользователя информационных систем МКУ-ЦБ по МОУ г.Тулы

1. Пользователями информационных систем (далее – ИС) МКУ-ЦБ по МОУ г.Тулы являются сотрудники, в установленном порядке допущенные к работе в ИС.

2. Настоящая инструкция определяет обязанности, права и ответственность пользователей, допущенных к работе в ИС, в области обеспечения безопасности конфиденциальной информации, в том числе персональных данных (далее – ПДн).

3. При эксплуатации ИС пользователь обязан:

а) соблюдать конфиденциальность при работе с информацией в ИС;

б) руководствоваться требованиями настоящей инструкции, а также иных документов МКУ-ЦБ по МОУ г.Тулы, регламентирующих обработку и защиту конфиденциальной информации, в том числе ПДн:

в) помнить свои личные пароли и идентификаторы;

г) руководствоваться требованиями инструкций по эксплуатации установленных средств вычислительной техники и средств защиты информации (далее – СЗИ);

д) блокировать ввод-вывод информации на своем автоматизированном рабочем месте ИС (далее – АРМ) перед оставлением своего рабочего места (перерыва в работе) или выключать АРМ;

е) блокировать вывод информации на монитор АРМ при выходе в течение рабочего дня из помещения, в котором размещается ИС.

4. При эксплуатации ИС пользователю запрещается:

а) самостоятельно подключать к АРМ нештатные устройства;

б) самостоятельно вносить изменения в состав, конфигурацию и размещение АРМ;

в) самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в АРМ;

г) самостоятельно вносить изменения в размещение и настройку СЗИ;

д) сообщать устно, письменно или иным способом другим лицам пароли, передавать личные идентификаторы, ключевые дискеты и другие реквизиты доступа к ресурсам ИС.

5. Пользователь ИС имеет право:

а) обращаться к ответственному за обеспечение безопасности ПДн по вопросам защиты обрабатываемой в ИС информации и эксплуатации установленных СЗИ, а также с просьбой об оказании технической и методической помощи по использованию ИС;

б) обращаться к ответственному за организацию обработки ПДн по вопросам, связанным с выполнением требований законодательства РФ в области защиты конфиденциальной информации, в том числе ПДн.

6. Пользователь несет персональную ответственность за соблюдение требований законодательства РФ и документов МКУ-ЦБ по МОУ г.Тулы, определяющих порядок обработки и защиты конфиденциальной информации, в том числе ПДн.