**АДМИНИСТРАЦИЯ КУЙБЫШЕВСКОГО ВНУТРИГОРОДСКОГО РАЙОНА ГОРОДСКОГО ОКРУГА САМАРА**

# ПОСТАНОВЛЕНИЕ

23.12.2022 № 409

Об определении политики Администрации Куйбышевского внутригородского района городского округа Самара в отношении защиты и обработки персональных данных

С целью принятия мер, необходимых для обеспечения выполнения обязанностей связанных с обработкой персональных данных, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 14.07.2022), постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», руководствуясь Уставом Куйбышевского внутригородского района городского округа Самара, ПОСТАНОВЛЯЮ:

1. Утвердить:

1.2. Правила осуществления политики в отношении защиты и обработки персональных данных в Администрации Куйбышевского внутригородского района городского округа Самара согласно приложению № 1 к настоящему постановлению;

002967

1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных согласно приложению № 2 к настоящему постановлению;

1.4. Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных согласно приложению № 3 к настоящему постановлению;

1.5. Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, согласно приложению № 4 к настоящему постановления;

1.6. Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные согласно приложению № 5 к настоящему постановления;

1.7. Типовое обязательство муниципального служащего, работника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, согласно приложению № 6 к настоящему постановления;

1.8. Типовую форму согласия на обработку персональных данных работников Администрации, иных субъектов персональных данных согласно приложению № 7 к настоящему постановлению;

1.9. Порядок доступа в помещения, где размещены используемые средства криптографической защиты информации, обрабатываются и хранятся персональные данные, а также средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации, согласно приложению № 8 к настоящему постановлению;

1.10. Перечень информационных систем персональных данных Администрации согласно приложению № 9 к настоящему постановлению;

1.11. Должностную инструкцию ответственного за организацию обработки персональных данных в Администрации согласно приложению № 10 к настоящему постановлению;

1.12. Перечень помещений Администрации Куйбышевского внутригородского района городского округа Самара, где размещены используемые средства криптографической защиты информации, обрабатываются и хранятся персональные данные, а также средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации, согласно приложению № 11 к настоящему постановлению;

1.13. Журнал учета лиц, имеющих право доступа в помещения Администрации Куйбышевского внутригородского района городского округа Самара, где размещены используемые средства криптографической защиты информации, обрабатываются и хранятся персональные данные, а также средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации, согласно приложению № 12 к настоящему постановлению;

1.14. Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов, согласно приложению № 13 к настоящему постановлению;

1.15. Инструкция ответственного пользователя средств криптографической защиты информации Администрации Куйбышевского внутригородского района городского округа Самара согласно приложению № 14 к настоящему постановлению;

1.16. Инструкция пользователя средств криптографической защиты информации Администрации Куйбышевского внутригородского района городского округа Самара согласно приложению № 15 к настоящему постановлению;

1.17. Перечень должностей сотрудников Администрации Куйбышевского внутригородского района городского округа Самара, допущенных к работе со средствами криптографической защиты информации согласно приложению № 16 к настоящему постановлению.

2. Произвести закладку журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

3. Заместителю главы Куйбышевского внутригородского района городского округа Самара по информационной политике в срок до 31.01.2023 обеспечить ревизию средств криптографической защиты информации, в том числе с учетом данных журнала регистрации поэкземплярного учета средств криптографической защиты информации, заложенного распоряжением Администрации Куйбышевского внутригородского района городского округа Самара от 21.12.2017 № 497 «Об организации в Администрации Куйбышевского внутригородского района городского округа Самара поэкземплярного учета средств криптографической защиты информации», с внесением (переносом) данных в журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов, заложенный настоящим постановлением.

4. Признать утратившими силу:

4.1. Постановление Администрации Куйбышевского внутригородского района городского округа Самара от 31.12.2015 № 3 «Об утверждении политики в отношении обработки персональных данных в Администрации Куйбышевского внутригородского района городского округа Самара»;

4.2. Постановление Администрации Куйбышевского внутригородского района городского округа Самара от 31.12.2015 № 32 «Об организации обработки и защиты персональных данных в Администрации Куйбышевского внутригородского района городского округа Самара»;

4.3. Распоряжение Администрации Куйбышевского внутригородского района городского округа Самара от 16.04.2020 № 120 «Об утверждении Порядка доступа в помещения, где размещены используемые средства криптографической защиты информации, обрабатываются и хранятся персональные данные, а также средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации»;

4.4. Распоряжение Администрации Куйбышевского внутригородского района городского округа Самара от 21.12.2017 № 497 «Об организации в Администрации Куйбышевского внутригородского района городского округа Самара поэкземплярного учета средств криптографической защиты информации»;

4.5. Распоряжение Администрации Куйбышевского внутригородского района городского округа Самара 09.07.2019 № 305 «Об организации в Администрации Куйбышевского внутригородского района городского округа Самара поэкземплярного учета средств криптографической защиты информации»

5. Начальнику отдела муниципальной службы и кадров правового управления Администрации Куйбышевского внутригородского района городского округа Самара в срок до 31.01.2023 довести настоящее постановление до сведения всех работников Администрации.

6. Настоящее постановление вступает в силу с момента его официального опубликования.

7. Контроль за выполнением настоящего постановления оставляю за собой.

Глава Куйбышевского внутригородского
района городского округа Самара А.А.Коробков

Дугушова
3303890

ПРИЛОЖЕНИЕ № 1
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Правила осуществления политики в отношении защиты и обработки персональных данных в Администрации Куйбышевского внутригородского района городского округа Самара

I. Общее положение.

1. Правила осуществления политики в отношении защиты и обработки персональных данных в Администрации Куйбышевского внутригородского района городского округа Самара (далее - Правила) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок их уничтожения при достижении целей обработки или при наступлении иных законных оснований в Администрации Куйбышевского внутригородского района городского округа Самара (далее – Администрация).

1.2. Администрация как оператор осуществляет обработку персональных данных, определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.3. Обработка персональных данных в Администрации осуществляется с соблюдением принципов и условий, установленных законодательством Российской Федерации в области персональных данных, а также Правилами.

1.4. В настоящих Правилах используются следующие основные понятия:

1) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор – Администрация, организующая и осуществляющая обработку персональных данных по роду своей деятельности;

3) обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых оператором 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;

4) автоматизированная обработка персональных данных – обработка персональных данных с помощью средств автоматизации оператора;

5) распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в

информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных – совокупность содержащихся в базах данных оператора персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

## II. Правовое основание обработки персональных данных.

2.1. Правовым основанием обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, в том числе:

1) Конституция Российской Федерации;

2) Гражданский кодекс Российской Федерации;

3) Трудовой кодекс Российской Федерации;

4) Налоговый кодекс Российской Федерации;

5) Кодексом об административных правонарушениях в Российской Федерации;

6) Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных);

7) Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации»;

8) Федеральным законом от 27.06.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

9) Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

10) Федеральный закон от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»;

11) Федеральный закон от 21.07.1993 № 5485-1 «О государственной тайне»;

12) Закон Самарской области от 09.10.2007 № 96-ГД «О муниципальной службе в Самарской области»;

13) Закон Самарской области от 06.07.2015 № 74-ГД «О разграничении полномочий между органами местного самоуправления городского округа Самара и внутригородских районов городского округа Самара по решению вопросов местного значения внутригородских районов»;

14) Устав Куйбышевского внутригородского района городского округа Самара, утвержденный Решением Совета депутатов Куйбышевского внутригородского района городского округа Самара от 22.10.2015 № 17.

## III. Информация об операторе.

3.1. Наименование: Администрация Куйбышевского внутригородского района городского округа Самара.

ИНН: 6314041182

Адрес местонахождения: 443004, г.Самара, ул.Зеленая, 14.

Почтовый адрес: 443004, г.Самара, ул.Зеленая, 14.

Тел. факс: 8 /846/ 330-34-06, 8 /846/ 264-12-00

E-mail: kujadm@samadm.ru

Регистрационный номер записи в Реестре операторов: 63-16-001964

## IV. Основные права и обязанности Оператора и Субъекта персональных данных.

4.1. Оператор имеет право:

1) самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;

2) поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;

3) 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, указанных в Законе о персональных данных.

4.2. Оператор обязан:

1) организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;

2) отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;

3) сообщать в уполномоченный орган по защите прав субъектов персональных данных (Федеральную службу по надзору в сфере связи,

информационных технологий и массовых коммуникаций, далее - Роскомнадзор) по запросу этого органа необходимую информацию в течение 10 рабочих дней с даты получения такого запроса. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору необходимо направить в Роскомнадзор мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации;

4) в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование его о компьютерных инцидентах, которые повлекли неправомерную передачу (предоставление, распространение, доступ) персональных данных.

4.3. Субъект персональных данных имеет право:

1) получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;

2) требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

3) дать предварительное согласие на обработку персональных данных в целях продвижения на рынке товаров, работ и услуг;

4) обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных.

## V. Категории субъектов персональных данных.

5.1. К категориям субъектов, персональные данные которых обрабатываются в соответствии с Правилами, относятся:

1) муниципальные служащие и работники Оператора;

2) физические лица, состоящие в договорных и иных гражданско-правовых отношениях с Оператором;

3) уволенные муниципальные служащие и работники Оператора;

4) родственники муниципального служащего, работника, депутата представительного органа муниципального образования;

5) Глава муниципального образования;

6) граждане, включенные в кадровый резерв, резерв для замещения вакантных должностей муниципальной службы, граждане, претендующие на включение в кадровый резерв, резерв для замещения вакантных должностей муниципальной службы;

7) граждане, представленные к награждению почетными званиями;

8) граждане, персональные данные которых необходимы для оказания муниципальных и государственных услуг, а также выполнения возложенных на Оператора функций, полномочий и обязанностей;

9) граждане, обратившиеся к Оператору в порядке, предусмотренном Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

10) граждане, являющиеся пользователями сайта Оператора;

11) депутаты представительного органа муниципального образования и их помощники;

12) физические лица – участники административного производства.

## VI. Цели сбора персональных данных.

6.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

6.2. Обработка Оператором персональных данных осуществляется в следующих целях:

1) осуществление своей деятельности в соответствии с Уставом Куйбышевского внутригородского района городского округа Самара при выполнении возложенных на Оператора функций, полномочий, обязанностей;

2) исполнение трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, законодательства о муниципальной службе в;

3) исполнение налогового, гражданского законодательства Российской Федерации;

4) рассмотрение обращений граждан;

5) административное производство;

6) исполнения требований о государственной тайне, о противодействии коррупции;

7) ведение официального сайта Оператора.

## VII. Перечень (категории) обрабатываемых персональных данных.

7.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в разделе VI настоящей Политики. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

7.2. Оператор обрабатывает следующие персональные данные категорий субъектов, указанных в разделе V настоящих Правил:

1) фамилия, имя, отчество, в том числе прежние, а также в случае их изменения – сведения о том, когда и по какой причине они изменились;

2) паспортные данные;

3) гражданство и подданство;

4) дата и место рождения;

5) сведения о семейном положении, в том числе данные о регистрации (расторжении) брака;

6) сведения об образовании, опыте работы, квалификации, профессиональной подготовке, повышении квалификации, чине, аттестации,

7) сведения о владении иностранными языками и языками народов РФ;

8) сведения о пребывании за границей РФ, период пребывания за границей РФ;

9) сведения о трудовой деятельности, наличии поощрений, наград, дисциплинарных взысканий, проверках и их результатах;

10) данные о включении в кадровый резерв;

11) сведения о временной нетрудоспособности;

12) сведения о наличии (отсутствии)заболеваний, препятствующих поступлению на муниципальную службу или ее прохождению;

13) сведения о состоянии здоровья, об инвалидности, сроки действия установленной инвалидности;

14) сведения о судимости (отсутствии судимости);

15) сведения о допуске к государственной тайне;

16) сведения, сообщаемые в резюме и сопроводительных письмах;

17) изображения (фотографии);

18) адрес регистрации по месту жительства (пребывания);

19) индивидуальный номер налогоплательщика;

20) сведения о воинском учете;

21) СНИЛС;

22) сведения о членах семьи и близких родственниках, в том числе проживающих за границей, включая место работы и анкетные данные;

23) сведения о доходах, расходах, об имуществе, обязательствах имущественного характера, в том числе супругов и несовершеннолетних детей;

24) сведения об адресах сайтов и страниц сайтов в информационно-телекоммуникационной сети Интернет;

25) адрес электронной почты;

26) номера контактных телефонов;

27) реквизиты полисов обязательного и добровольного медицинского страхования и содержащиеся в них сведения;

28) сведения о реквизитах банковских счетов для выплаты денежного содержания и о размере заработной платы;

29) политические взгляды, партийная принадлежность, участие в выборных компаниях;

30) сведения об участии в органах управления некоммерческих организаций;

31) иные персональные данные, предоставляемые субъектом персональных данных в соответствии с требованиями трудового законодательства, законодательства о муниципальной службе, а также сведения, которые субъект персональных данных пожелал сообщить о себе;

32) cookie-файлы.

7.3. Оператор не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством Российской Федерации.

## VIII. Порядок и условия обработки персональных данных.

8.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

8.2. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

8.3. Оператор осуществляет обработку персональных данных для каждой цели их обработки способом смешанной обработки персональных данных (без передачи по внутренней сети Оператора, с передачей по сети Интернет).

8.4. К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

8.5. Обработка персональных данных для каждой цели обработки, указанной в п. 6.2. Правил, осуществляется путем:

1) получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных;

2) внесения персональных данных в журналы, реестры и информационные системы Оператора;

3) использования иных способов обработки персональных данных.

8.6. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

8.7. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы

исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

8.8. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

1) определяет угрозы безопасности персональных данных при их обработке;

2) принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;

3) назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Оператора;

4) создает необходимые условия для работы с персональными данными;

5) организует учет документов, содержащих персональные данные;

6) организует работу с информационными системами, в которых обрабатываются персональные данные;

7) хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;

8) организует обучение работников Оператора, осуществляющих обработку персональных данных.

8.9. Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требует каждая цель обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

8.9.1. Персональные данные на бумажных носителях хранятся в Администрации в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ

(Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Приказом Росархива от 20.12.2019 № 236)).

8.9.2. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

8.10. Оператор прекращает обработку персональных данных в следующих случаях:

1) выявлен факт их неправомерной обработки (в течение трех рабочих дней с даты выявления);

2) достигнута цель их обработки;

3) истек срок действия или отозвано согласие субъекта персональных данных на обработку указанных данных, когда по Закону о персональных данных обработка этих данных допускается только с согласия.

8.11. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку Оператор прекращает обработку этих данных, если:

1) иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

2) Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

3) иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

8.12. При обращении субъекта персональных данных к Оператору с требованием о прекращении обработки персональных данных в срок, не превышающий 10 рабочих дней с даты получения Оператором

соответствующего требования, обработка персональных данных прекращается, за исключением случаев, предусмотренных Законом о персональных данных. Указанный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору необходимо направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока.

8.13. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

8.14. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

8.14.1. При эксплуатации автоматизированных систем необходимо соблюдать требования:

1) к работе допускаются только назначенные лица;

2) на ПЭВМ, дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);

3) на период обработки защищаемой информации в помещении могут находиться лица, допущенные в установленном порядке к обрабатываемой информации.

8.15. Обработка персональных данных без использования средств автоматизации (или неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

8.15.1. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

8.15.2. При неавтоматизированной обработке персональных данных на бумажных носителях:

1) не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;

2) персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

3) документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

4) дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

8.15.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовые формы), должны соблюдаться следующие условия:

1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными

данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

2) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

3) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

4) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

8.15.4. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

8.15.5. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

1) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется

копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

2) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

8.15.6. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

8.15.7. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

## XI. Порядок рассмотрения запросов субъектов персональных данных.

9.1. Субъект персональных данных, указанный в разделе V настоящих Правил, имеет право на получение информации, касающейся обработки его персональных данных, указанной в части 7 статьи 14 Закона о персональных данных.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Закона о персональных данных.

9.2. Субъект персональных данных имеет право требовать от Оператора уточнения его персональных данных, их блокирования или

уничтожения, в случае если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

9.3. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Оператором субъекту персональных данных или его представителю в течение 10 рабочих дней с момента обращения либо получения запроса субъекта персональных данных или его представителя. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору следует направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации.

9.4. В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

9.5. При обращении либо при получении запроса субъекта персональных данных или его представителя сведения должны быть предоставлены в доступной форме. Запрос регистрируется в день поступления по правилам делопроизводства.

9.6. Запрос должен содержать:

1) номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

2) сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо

сведения, иным образом подтверждающие факт обработки персональных данных Оператором;

3) подпись субъекта персональных данных или его представителя.

9.7. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Оператор предоставляет сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

9.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

## X. Порядок блокировки, уничтожения и обезличивания персональных данных.

10.1. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

10.2. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.

10.3. При выявлении Оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Оператор:

1) в течение 24 часов - уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;

2) в течение 72 часов - уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

10.4. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных

данных или в результате которых уничтожаются материальные носители персональных данных.

10.5. Условия и сроки уничтожения персональных данных Оператором:

1) достижение цели обработки персональных данных либо утрата необходимости достигать эту цель - в течение 30 дней;

2) достижение максимальных сроков хранения документов, содержащих персональные данные, - в течение 30 дней;

3) предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки, - в течение семи рабочих дней;

4) отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, - в течение 30 дней.

10.6. При достижении цели обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

1) иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

2) оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

3) иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

10.7. Уничтожение персональных данных осуществляет комиссия, созданная распоряжением Администрации.

10.8. Способы уничтожения персональных данных устанавливаются в локальных нормативных актах Оператора.

10.9. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса используемых информационных систем персональных данных и по достижению сроков обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством Российской Федерации.

10.10. К способам обезличивания персональных данных при условии дальнейшей обработки персональных данных относятся:

1) уменьшение перечня обрабатываемых сведений;

2) замена части сведений идентификаторами;

3) обобщение (понижение) точности некоторых сведений;

4) деление сведений на части и обработка их в разных информационных системах;

5) другие способы.

К способам обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

10.11. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо:

1) использование паролей;

2) использование антивирусных программ;

3) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

1) хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;

2) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

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

10.13. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

## XI. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Должностные лица Администрации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

ПРИЛОЖЕНИЕ № 2
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Правила осуществления в Администрации Куйбышевского внутригородского района городского округа Самара контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации организовывается проведение периодических проверок условий обработки персональных данных на предмет соответствия Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам Администрации.

2. Проверки осуществляются ответственным за организацию обработки персональных данных в Администрации в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям. Ответственный за организацию обработки персональных данных в Администрации назначается Главой Куйбышевского внутригородского района городского округа Самара.

3. Лицо, ответственное за организацию обработки персональных данных, обязано:

3.1. осуществлять внутренний контроль за соблюдением Администрацией и ее работниками законодательства Российской Федерации

о персональных данных, в том числе требований к защите персональных данных;

3.2. доводить до сведения работников Администрации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3.3. организовывать и контролировать прием и обработку обращений и запросов субъектов пересыльных данных или их представителей.

4. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, ответственный за организацию обработки персональных данных в Администрации докладывает Главе Куйбышевского внутригородского района городского округа Самара.

ПРИЛОЖЕНИЕ № 3
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Перечень должностей муниципальных служащих Администрации Куйбышевского внутригородского района городского округа Самара, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных

1. Первый заместитель главы Куйбышевского внутригородского района городского округа Самара;

2. заместитель главы Куйбышевского внутригородского района городского округа Самара;

3. руководитель управления Администрации Куйбышевского внутригородского района городского округа Самара;

4. начальник отдела Администрации Куйбышевского внутригородского района городского округа Самара.

ПРИЛОЖЕНИЕ № 4
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Перечень должностей Администрации Куйбышевского внутригородского района городского округа Самара, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1. Глава Куйбышевского внутригородского района городского округа Самара;
2. первый заместитель главы Куйбышевского внутригородского района городского округа Самара;
3. заместитель главы Куйбышевского внутригородского района городского округа Самара;
4. руководитель управления;
5. начальник отдела;
6. председатель административной комиссии;
7. заместитель начальника отдела;
8. заведующий сектором;
9. консультант;
10. главный специалист;
11. инспектор;
12. архивариус;
13. инженер;
14. специалист-эксперт;
15. управляющий микрорайоном.

ПРИЛОЖЕНИЕ № 5
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Типовая форма разъяснения субъекту персональных данных
юридических последствий отказа предоставить свои персональные данных

В соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» уведомляем Вас, что обязанность представления Вами персональных данных установлена статьей 29 Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации» в связи с поступлением и прохождением муниципальной службы.

Администрацией Куйбышевского внутригородского района городского округа Самара определен перечень персональных данных, которые субъект персональных данных обязан представить уполномоченным лицам Администрации Куйбышевского внутригородского района городского округа Самара в связи с поступлением на муниципальную службу, ее прохождением и увольнением с муниципальной службы.

Без представления Вами обязательных для заключения трудового договора сведений данный договор не может быть заключен.

Мне, _____,

(фамилия, имя, отчество (при наличии))

Разъяснены юридические последствия отказа предоставить свои персональные данные уполномоченным лицам Администрации Куйбышевского внутригородского района городского округа Самара.

«_____» _____ 20____ г. _____ _____

(дата) (подпись) (Ф.И.О.)

ПРИЛОЖЕНИЕ № 6
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Типовое обязательство муниципального служащего, работника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним муниципального контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____

(фамилия, имя, отчество – при наличии)

обязуюсь прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей в Администрации Куйбышевского внутригородского района городского округа Самара, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

Положения законодательства Российской Федерации, предусматривающие ответственность за нарушение требований Федерального закона 27.07.2006 № 152-ФЗ «О персональных данных» мне разъяснены.

«_____» _____ 20____ г. _____

(дата) (подпись)

ПРИЛОЖЕНИЕ № 7
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Типовая форма согласия на обработку персональных данных работников Администрации Куйбышевского внутригородского района городского округа Самара, иных субъектов персональных данных

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)

проживающий (-ая) по адресу: _____
(индекс, страна, субъект РФ, город, район, улица, дом, квартира),

_____
(паспорт серия, №, кем, когда выдан)

в лице представителя _____,

действующего на основании _____

_____
(фамилия, имя, отчество; адрес представителя субъекта персональных данных;
номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе; реквизиты доверенности (номер доверенности, когда и кем выдана) или иного документа, подтверждающего полномочия представителя
(при получении согласия от представителя субъекта персональных данных))

даю согласие на обработку моих персональных данных, перечисленных в настоящем согласии.

Перечень персональных данных, на обработку которых дается согласие:

- фамилия, имя, отчество, в том числе прежние, а также в случае их изменения – сведения о том, когда и по какой причине они изменились;
- паспортные данные;
- гражданство и подданство;
- дата и место рождения;

- сведения о семейном положении, в том числе данные о регистрации (расторжении) брака;
- сведения об образовании, опыте работы, квалификации, профессиональной подготовке, повышении квалификации, чине, аттестации,
- сведения о владении иностранными языками и языками народов РФ;
- сведения о пребывании за границей РФ, период пребывания за границей РФ;
- сведения о трудовой деятельности, наличии поощрений, наград, дисциплинарных взысканий, проверках и их результатах;
- данные о включении в кадровый резерв;
- сведения о временной нетрудоспособности;
- сведения о наличии (отсутствии)заболеваний, препятствующих поступлению на муниципальную службу или ее прохождению;
- сведения о состоянии здоровья, об инвалидности, сроки действия установленной инвалидности;
- сведения о судимости (отсутствии судимости);
- сведения о допуске к государственной тайне;
- сведения, сообщаемые в резюме и сопроводительных письмах;
- изображения (фотографии);
- адрес регистрации по месту жительства (пребывания);
- индивидуальный номер налогоплательщика;
- сведения о воинском учете;
- СНИЛС;
- сведения о членах семьи и близких родственниках, в том числе проживающих за границей, включая место работы и анкетные данные;
- сведения о доходах, расходах, об имуществе, обязательствах имущественного характера, в том числе супругов и несовершеннолетних детей;

- сведения об адресах сайтов и страниц сайтов в информационно-телекоммуникационной сети Интернет;
- адрес электронной почты;
- номера контактных телефонов;
- реквизиты полисов обязательного и добровольного медицинского страхования и содержащиеся в них сведения;
- сведения о реквизитах банковских счетов для выплаты денежного содержания и о размере заработной платы;
- политические взгляды, партийная принадлежность, участие в выборных компаниях;
- сведения об участии в органах управления некоммерческих организаций;
- иные сведения, которые я пожелал(а) сообщить о себе.

Действия с персональными данными, на совершение которых даётся согласие:

- обработка (любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение в установленных федеральными законами случаях, предоставление, доступ), блокирование, удаление, уничтожение).

Обработка персональных данных осуществляется в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Согласие выдается оператору (наименование): Администрация Куйбышевского внутригородского района городского округа Самара.

Адрес оператора: 443004, г. Самара, ул. Зелёная, д. 14.

Срок действия настоящего согласия и порядок его отзыва:

- согласие на обработку персональных данных действует с даты подписания настоящего согласия и в течение всего срока трудовых и непосредственно связанных с ними отношений;

- после прекращения трудовых и непосредственно связанных с ними отношений персональные данные будут храниться в Администрации Куйбышевского внутригородского района городского округа Самара в течение предусмотренного законодательством Российской Федерации и иными нормативными правовыми актами Российской Федерации срока хранения документов;

- согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме.

_____

(подпись)

Субъект или его представитель при обращении или по запросу (в письменной или в электронной форме) имеет право на получение информации, касающейся обработки его персональных данных (в соответствии со статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

«_____» _____ 20____ г. _____ _____

(дата) (подпись) (Ф.И.О.)

Подтверждаю, что ознакомлен(-а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

«_____» _____ 20____ г. _____ _____

(дата) (подпись) (Ф.И.О.)

ПРИЛОЖЕНИЕ № 8
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Порядок доступа в помещения, где размещены используемые средства криптографической защиты информации, обрабатываются и хранятся персональные данные, а также средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации

1. Порядок доступа в помещения Администрации, где размещены используемые средства криптографической защиты информации, обрабатываются и хранятся персональные данные, а также средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации (далее – Порядок), разработан во исполнение требований постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами», а также Приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

2. Порядок регламентирует условия и порядок осуществления доступа в помещения Администрации, где размещены используемые средства

криптографической защиты информации (далее - СКЗИ), обрабатываются и хранятся персональные данные, а также СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - Помещения) в целях организации режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

3. Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

4. Помещения должны оснащаться входными дверьми с замками, должно обеспечиваться постоянное закрытие дверей Помещений на замок и их открытие только для санкционированного прохода. Ключи от этих Помещений выдаются уполномоченным лицам на время рабочего дня и сдаются на пост охраны по окончанию периода пребывания в Помещении.

5. Доступ в Помещения, разрешается только работникам, чьи должности определены Перечнем должностей работников Администрации, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (далее - уполномоченные лица).

6. Уполномоченными лицами организуется и осуществляется контроль за доступом в Помещения посторонних лиц. Под посторонними лицами понимаются лица, не уполномоченные на обработку персональных данных. Пребывание посторонних лиц в Помещениях, допускается только в присутствии уполномоченных лиц. При этом должен быть исключен просмотр обрабатываемых персональных данных, обеспечена сохранность материальных носителей персональных данных и исключен несанкционированный доступ к ним.

7. О попытках неконтролируемого проникновения посторонних лиц в Помещения необходимо незамедлительно сообщать руководителю структурного подразделения Администрации.

8. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать руководителю структурного подразделения Администрации.

9. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения Администрации.

10. Уборка помещений, в которых ведется обработка персональных данных и хранятся документы и носители информации, содержащие персональные данные, должна производиться в присутствии работников, проводящих обработку персональных данных.

11. Установка оборудования, его замена или ремонт в помещениях, в которых ведется обработка персональных данных, хранятся документы и носители информации, содержащие персональные данные, должны проводиться по согласованию с руководителем структурного подразделения Администрации.

ПРИЛОЖЕНИЕ № 9
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Перечень информационных систем персональных данных Администрации Куйбышевского внутригородского района городского округа Самара

1. Автоматизированная информационная система «СБИС»;

2. Автоматизированная информационная система «Электронный муниципальный архив»;

3. Единая автоматизированная система консолидированного бухгалтерского и бюджетного учёта и отчётности городского округа Самара;

4. Закрытая система (каналы) связи по передачи отчетности;

5. Реестр контрактов на официальном сайте Единой Информационной системы в сфере закупок в рамках Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

6. Реестр незаконно установленных на территории Куйбышевского внутригородского района городского округа Самара временных построек, за исключением нестационарных торговых объектов;

7. Реестр самовольно установленных объектов, не являющихся объектами капитального строительства, на территории Куйбышевского внутригородского района городского округа Самара;

8. Официальный сайт Администрации Куйбышевского внутригородского района городского округа Самара;

9. Система электронного документооборота и управления электронным документооборотом АИС «САМАРА»;

10. Федеральная государственная информационная система «Федеральный реестр государственных и муниципальных услуг (функций)»;

11. Электронная почта Администрации Куйбышевского внутригородского района городского округа Самара.

ПРИЛОЖЕНИЕ № 10
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Должностная инструкция ответственного за организацию обработки персональных данных в Администрации Куйбышевского внутригородского района городского округа Самара

Настоящая должностная инструкция разработана и утверждена в соответствии с положениями Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и иных нормативных актов, регулирующих трудовые правоотношения в Российской Федерации.

## I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за организацию обработки персональных данных Администрации назначается и освобождается распоряжением Главы Куйбышевского внутригородского района городского округа Самара из лиц с высшим профессиональным образованием и стажем работы в области обработки персональных данных не менее трёх лет.

1.2. Ответственный за организацию обработки персональных данных Администрации подчиняется непосредственно Главе Куйбышевского внутригородского района городского округа Самара.

1.3. Ответственный за организацию обработки персональных данных Администрации в своей деятельности руководствуется:

- законодательством Российской Федерации;

- Уставом Куйбышевского внутригородского района городского округа Самара;

- Правилами внутреннего трудового распорядка Администрации Куйбышевского внутригородского района городского округа Самара;

- трудовым договором;

- настоящей должностной инструкцией.

1.4. Ответственный за организацию обработки персональных данных Администрации должен знать: трудовое законодательство; руководящие документы по организации труда; документы, определяющие политику Администрации в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений; методы применения правовых, организационных и технических мер по обеспечению безопасности персональных данных; меры осуществления внутреннего контроля и (или) аудита соответствия обработки персональных данных; порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством; алгоритм ознакомления работников Администрации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников; организацию труда и управления; методы учета кадров; порядок разработки нормативных материалов для защиты персональных данных;

передовой отечественный и зарубежный опыт в области обработки персональных данных.

1.5. Особые условия допуска к работе: прохождение обязательных предварительных - при поступлении на муниципальную службу (работу) и периодических медицинских осмотров (обследований), а также внеочередных медицинских осмотров (обследований) в порядке, установленном действующими законодательным и нормативно-правовыми актами, прохождение инструктажа по технике безопасности на рабочем месте.

1.6. Ответственный за организацию обработки персональных данных под роспись знакомится с должностной инструкцией ответственного за организацию обработки персональных данных в Администрации.

## II. ОБЯЗАННОСТИ

2.1. Организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

2.2. Организовывать и осуществлять внутренний контроль за соблюдением уполномоченными на обработку персональных данных требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных.

2.3. Организовывать доведение до сведения уполномоченных на обработку персональных данных положений законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.4. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.5. В случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

2.6. Осуществлять внутренний контроль за соблюдением Администрацией и ее работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

2.7. Доводить до сведения работников Администрации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.8. Блокировать неправомерно обрабатываемые персональные данные, прекращать обработку персональных данных в соответствии с законодательством Российской Федерации.

2.9. Уведомлять субъектов персональных данных об устранении допущенных нарушений при обработке их персональных данных.

2.10. Проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации о персональных данных, соотношения указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации в области обработки и защиты персональных данных.

2.11. Участвовать в рассмотрении проектов решений по вопросам своей компетенции.

2.12. Руководить подчиненными и координировать деятельность Администрации в области обработки персональных данных.

## III. ПРАВА

3. Ответственный за организацию обработки персональных данных Администрации имеет право:

3.1. На предоставление ему работы, обусловленной трудовым договором.

3.2. Рабочее место, соответствующее государственным нормативным требованиям охраны труда и условиям, предусмотренным трудовым договором.

3.3. Своевременную и в полном объёме выплату заработной платы в соответствии со своей квалификацией, сложностью труда, количеством и качеством выполненной работы.

3.4. Отдых, обеспечиваемый установлением нормальной продолжительности рабочего времени, предоставлением еженедельных выходных дней, нерабочих праздничных дней, оплачиваемых ежегодных отпусков.

3.5. Полную достоверную информацию об условиях труда и требованиях охраны труда на рабочем месте.

3.6. Защиту своих трудовых прав, свобод и законных интересов всеми не запрещёнными законом способами.

3.7. Возмещение вреда, причиненного ему в связи с исполнением трудовых обязанностей, и компенсацию морального вреда в порядке, установленном Трудовым кодексом Российской Федерации, иными федеральными законами.

3.8. Обязательное социальное страхование в случаях, предусмотренных федеральными законами.

3.9. Повышение своей квалификации.

3.10. Ознакомление с проектами решений Главы Куйбышевского внутригородского района городского округа Самара, касающимися его деятельности.

3.11. Представление на рассмотрение предложений Главе Куйбышевского внутригородского района городского округа Самара, по вопросам деятельности Администрации.

3.12. Получение от работников Администрации информации, необходимой для осуществления своей деятельности.

3.13. Объединение, включая право на создание профессиональных союзов и вступление в них для защиты своих трудовых прав, свобод и законных интересов.

3.14. Взаимодействие с другими отделами Администрации для решения оперативных вопросов своей профессиональной деятельности.

3.15. Доступ к информации, касающейся обработки персональных данных.

3.16. Неотложное принятие мер по защите персональных данных.

## IV. ОБЯЗАННОСТИ

4. Ответственный за организацию обработки персональных данных Администрации обязан:

4.1. Выполнять работу в соответствии со своей квалификацией, должностными инструкциями, служебными и должностными обязанностями.

4.2. Соблюдать служебную тайну.

4.3. Совершенствовать в установленном порядке профессиональные знания и навыки путем обучения по дополнительным профессиональным программам в образовательных и научных организациях.

4.4. Также ответственный за организацию обработки персональных данных Администрации принял на себя обязательства:

- добросовестно исполнять свои трудовые обязанности, возложенные на него трудовым договором и должностной инструкцией;

- в положенные сроки отчитываться о результатах своей деятельности по утверждённым формам;

- соблюдать Правила внутреннего трудового распорядка Администрации Куйбышевского внутригородского района городского округа Самара;

- соблюдать трудовую дисциплину;

- соблюдать требования по охране труда и обеспечению безопасности труда;

- бережно относиться к имуществу Администрации (в том числе к имуществу третьих лиц, находящемуся у Главы Куйбышевского внутригородского района городского округа Самара, если Глава Куйбышевского внутригородского района городского округа Самара несёт ответственность за сохранность этого имущества) и других работников;

- незамедлительно сообщить Главе Куйбышевского внутригородского района городского округа Самара о возникновении ситуации, представляющей угрозу жизни и здоровью людей, сохранности имущества Администрации (в том числе к имуществу третьих лиц, находящемуся у Главы Куйбышевского внутригородского района городского округа Самара, если Глава Куйбышевского внутригородского района городского округа Самара несёт ответственность за сохранность этого имущества).

## V. УСЛОВИЯ РАБОТЫ

5.1. Режим работы ответственного за организацию обработки персональных данных Администрации определяется в соответствии с Правилами внутреннего трудового распорядка Администрации Куйбышевского внутригородского района городского округа Самара, а также трудовым договором.

5.2. В связи со служебной необходимостью ответственный за организацию обработки персональных данных Администрации обязан выезжать в служебные командировки (в том числе местного значения).

5.3. Ответственный за организацию обработки персональных данных Администрации ознакомлен с Уставом Куйбышевского внутригородского района городского округа Самара, обязуется не разглашать служебную тайну Администрации.

## VI. ОТВЕТСТВЕННОСТЬ

6. Ответственный за организацию обработки персональных данных Администрации несет ответственность:

6.1. За ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей должностной инструкцией.

6.2. Недостоверную информацию о состоянии выполнения работы.

6.3. Невыполнение распоряжений и поручений Главы Куйбышевского внутригородского района городского округа Самара, не противоречащих законодательству.

6.4. Правонарушения, совершённые в процессе осуществления своей деятельности.

6.5. Причинение материального ущерба.

6.6. Нарушение правил техники безопасности и инструкции по охране труда, непринятие мер по пресечению выявленных нарушений правил техники безопасности, противопожарных и других правил.

6.7. Несоблюдение трудовой дисциплины.

6.8. Непринятие мер по устранению недостатков, выявленных в ходе независимой оценки качества выполненной работы.

ПРИЛОЖЕНИЕ № 11
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

Перечень помещений Администрации Куйбышевского внутригородского района городского округа Самара, где размещены используемые средства криптографической защиты информации, обрабатываются и хранятся персональные данные, а также средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации

1. 443004, г. Самара, ул. Зеленая, д. 14, кабинеты 2, 4, 9 – 29, 31 – 34, 36, 37, 39 – 41.
2. 443004, г. Самара, ул. Зеленая, д. 14а.
3. 443004, г. Самара, ул. Калининградская, д. 28, кабинеты 3, 8.
4. 443065, г. Самара, ул. Бакинская, д. 22а, кабинеты, 7, 18, 23.
5. 443065, г. Самара, ул. Бакинская, д. 20.

ПРИЛОЖЕНИЕ № 12
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 №409

Журнал учета лиц, имеющих право доступа в помещения Администрации Куйбышевского внутригородского района городского округа Самара, где размещены используемые средства криптографической защиты информации, обрабатываются и хранятся персональные данные, а также средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации

Начат «__»___20__г.
Окончен «__»___20__г.
Журнал составлен на ___листах

| № п/п | ФИО пользователя СКЗИ | Должность | Структурное подразделение | Отметка о добавлении сотрудника | | Отметка об ознакомлении с Порядком доступа в Помещения, где обрабатываются и хранятся персональные данные | | Отметка об исключении сотрудника | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Дата | Подпись ответственного лица | Дата | Подпись сотрудника | Причина исключения | Дата | Подпись ответственного лица |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | | | | | | | | | |

ПРИЛОЖЕНИЕ № 13
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

# Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Начат «__»___20__г.
Окончен «__»___20__г.
Журнал составлен на ___листах

| № п/п | Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов | Серийный номер СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов | Номера экземпляров (криптографические номера) ключевых документов | Отметка о получении | | Отметка о выдаче | |
|---|---|---|---|---|---|---|---|
| | | | | От кого получено | Дата и номер сопроводительного письма | ФИО пользователя СКЗИ | Дата и расписка в получении |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | | | | | | | |

| Отметка о подключении (установки СКЗИ) | | | Отметка об изъятии СКИЗ из аппаратных средств, уничтожении ключевых документов | | | Примечание |
|---|---|---|---|---|---|---|
| ФИО сотрудников криптографической защиты, пользователя СКИЗ, произведших подключение (установку) | Дата подключения (установки) и подписи лиц, произведших подключение (установку) | Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ | Дата изъятия (уничтожения) | ФИО сотрудников криптографической защиты, пользователя СКИЗ, производивших изъятие (уничтожение) | Номер акта или расписка об уничтожении | |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | | | | | | |

ПРИЛОЖЕНИЕ № 14
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

# Инструкция ответственного пользователя средств криптографической защиты информации Администрации Куйбышевского внутригородского района городского округа Самара

## 1. Общее положение.

1.1. Настоящая инструкция ответственного пользователя средств криптографической защиты информации Администрации Куйбышевского внутригородского района городского округа Самара (далее – инструкция) определяет основные правила и обязанности ответственного пользователя средств криптографической защиты информации (далее – ответственный пользователь СКЗИ).

1.2. Ответственный пользователь СКЗИ отвечает за организацию, обеспечение функционирования и безопасность средств криптографической защиты информации (далее – СКЗИ), предназначенные для защиты информации, не содержащей сведения, составляющие государственную тайну.

1.3. Ответственный пользователь СКЗИ должен знать нормы действующего законодательства РФ в сфере обработки и обеспечения безопасности защищаемой информации, а также в области защиты

информации при ее передаче по открытым каналам связи с использованием СКЗИ.

1.4. В своей деятельности ответственный пользователь СКЗИ руководствуется настоящей инструкцией.

## 2. Обязанности ответственный пользователь СКЗИ.

2.1. Ответственный пользователь СКЗИ обязан соблюдать требования правовых актов, устанавливающих порядок работы с защищаемой информацией.

2.2. Осуществлять контроль за организацией, обеспечением функционирования и безопасности СКЗИ, предназначенных для обеспечения безопасности защищаемой информации:

2.2.1. Контролировать соблюдение условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ней.

2.2.2. Обеспечивать надежное хранение эксплуатационной и технической документации к СКЗИ, ключевых документов, носителей информации ограниченного распространения.

2.2.3. Вносить предложения по режиму охраны помещений, в которых установлены СКЗИ или хранятся ключевые документы к ним.

2.2.4. Вести журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (далее – журнал).

2.2.5. Выдавать пользователям СКЗИ экземпляры СКЗИ, эксплуатационной и технической документации к ним под расписку в соответствующем журнале.

2.2.6. Контролировать получение и доставку СКЗИ, эксплуатационной и технической документации к ним.

2.2.7. Контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в срок, указанный в эксплуатационной и технической документации к соответствующим СКЗИ, или, если срок

уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) под расписку с соответствующем журнале.

2.3. Осуществлять контроль за организацией, обеспечением функционирования и безопасности квалифицированных электронных подписей (далее – КЭП), содержащихся на носителях ключевой информации:

2.3.1. Отправлять запросы на получение КЭП служащими Администрации.

2.3.2. Осуществлять подготовку рабочего места пользователя СКЗИ.

2.3.3. Проводить инструктаж пользователей СКЗИ по правилам работы с СКЗИ и КЭП под подпись.

2.3.4. Вести журналы учета выдачи носителей с ключевой информацией, пользователей СКЗИ.

2.3.5. Осуществлять временное хранение носителей ключевой информации пользователей в период длительного отсутствия на рабочем месте (отпуск, болезнь и т.п.) с занесением соответствующей записи в журнал.

2.3.6. Выводить из действия носители ключевой информации, в отношении которой возникло подозрение в компрометации.

2.3.7. Контролировать уничтожение ключей КЭП, действие которых прекращено или в случае увольнения пользователей ключа КЭП.

2.3.8. Принимать решение об уничтожении или сохранения ключей КЭП при переводе пользователя КЭП на другую должность.

2.4. Участвовать в анализе ситуаций, касающихся нарушения условий хранения носителей защищаемой информации, использования СКЗИ, которые могут привести к нарушению конфиденциальности защищаемой информации.

2.5. Контролировать исполнение пользователями СКЗИ требований Инструкции пользователя СКЗИ, а также требований действующего законодательства РФ в сфере обработки и обеспечения безопасности защищаемой информации.

2.6. Вести учет помещений, в которых установлены СКЗИ, а также мест хранения СКЗИ и ключевых документов.

## 3. Действия ответственный пользователь СКЗИ в случае получения информации о компрометации ключевой информации.

3.1. Принимать все необходимые меры для обеспечения безопасности защищаемой информации, в случае получения от пользователей информации о фактах утраты, компрометации ключевой информации, в частности, обеспечить выполнение следующих мероприятий:

3.1.1. В каждом случае, по факту (или предполагаемой) компрометации ключевых документов, проводить служебное расследование, результатом которого является квалификация или не квалификация данного события как компрометации.

3.1.2. О факте компрометации ключевой информации производить информирование всех заинтересованных участников информационного обмена.

3.1.3. Выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожить с занесением соответствующей записи в журнал.

3.1.4. Пользователю СКЗИ выдать новый носитель ключевой информации для своевременного восстановления связи.

3.2. Своевременно информировать ответственного за организацию обработки пересыльных данных о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой информации.

## 4. Права ответственный пользователь СКЗИ.

4.1. Ответственный пользователь СКЗИ имеет право знакомиться с правовыми актами, регламентирующими процессы обработки защищаемой информации.

4.2. Требовать от пользователей СКЗИ соблюдения требований действующего законодательства РФ в сфере обработки и обеспечения безопасности защищаемой информации.

4.3. Требовать прекращения работы в информационных системах, как в целом, так и отдельных пользователей СКЗИ, в случае выявления нарушений требований по работе с СКЗИ, предназначенными для обеспечения безопасности защищаемой информации, или в связи с нарушением функционирования СКЗИ.

ПРИЛОЖЕНИЕ № 15
к постановлению
Администрации
Куйбышевского
внутригородского района
от «23» 12 2022 № 409

# Инструкция пользователя средств криптографической защиты информации Администрации Куйбышевского внутригородского района городского округа Самара

## 1. Общее положение.

1.1. Настоящая инструкция пользователя средств криптографической защиты информации Администрации Куйбышевского внутригородского района городского округа Самара (далее – инструкция) определяет порядок обращения пользователей со средствами криптографической защиты информации (далее – СКЗИ), а также определяет порядок восстановления связи в случае компрометации действующих ключей.

1.2. Пользователя средств криптографической защиты информации Администрации (далее – пользователи СКЗИ) являются сотрудники Администрации, включенные в перечень сотрудников, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну.

1.3. Непосредственно к работе с СКЗИ пользователя допускаются только после ознакомления с настоящей инструкцией. Ознакомление пользователей с настоящей инструкцией осуществляет под роспись

ответственный пользователь средств криптографической защиты информации (далее - ответственный пользователь СКЗИ).

1.4. Пользователь СКЗИ должен знать нормы действующего законодательства РФ в области обработки и обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, а также в области защиты информации при ее передаче по открытым каналам связи с использованием СКЗИ.

1.5. В своей деятельности, связанной с обработкой защищаемой информации с использованием СКЗИ, пользователь СКЗИ руководствуется настоящей инструкцией.

1.6. Пользователи СКЗИ несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту носителей ключевой информации от несанкционированного использования.

## 2. Порядок обращения с СКЗИ.

2.1. Пользователи СКЗИ обязаны осуществлять эксплуатацию СКЗИ в соответствии с документацией СКЗИ, а также в соответствии с иными нормативно правовыми актами, регулирующими отношения по вопросу обращения с СКЗИ.

2.1.1. Не разглашать информацию ограниченного доступа, к которой они допущены.

2.1.2. Сохранять носители ключевой информации и другие документы о ключах, выдаваемые с ключевыми носителями.

2.1.3. Соблюдать требования к обеспечению безопасности информации ограниченного доступа с использованием СКЗИ.

2.1.4. Получать экземпляры СКЗИ, эксплуатационной и технической документации к ним под расписку в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

2.1.5. Нести персональную ответственность за сохранность доверенных пользователю СКЗИ экземпляров СКЗИ.

2.1.6. Сдавать СКЗИ, эксплуатационной и технической документации к ним, ключевую документацию при увольнении или отстранении от исполнения от обязанностей, связанной с использованием СКЗИ.

2.1.7. Сообщать ответственному пользователю СКЗИ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним.

2.1.8. Немедленно уведомлять ответственного пользователя СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

2.1.9. При обнаружении на ПК, оборудованном СКЗИ, посторонних программ или вирусов, необходимо прекратить работу с СКЗИ на данном рабочем месте и сообщать ответственному пользователю СКЗИ.

2.2. Пользователям СКЗИ запрещается:

2.2.1. Разглашать информацию ограниченного доступа, к которой был допущен пользователь СКЗИ.

2.2.2. Разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным.

2.2.3. Осуществлять несанкционированное копирование ключевых носителей.

2.2.4. Вносить какие-ибо изменения в программное обеспечение СКЗИ.

## 3. Порядок обращения с квалифицированными электронными подписями, содержащимися на носителях ключевой информации.

3.1. При работе с квалифицированной электронной подписью (далее – КЭП) пользователь СКЗИ обязать знать и следовать положениям следующих организационно-распорядительных документов:

3.1.1. руководства по обеспечению безопасности использования КЭП с СКЗИ;

3.1.2. настоящей инструкции;

3.1.3. правила по организации парольной защиты;

3.1.4. правил доступа в помещения, в которых размещены СКЗИ.

3.2. Ознакомление пользователей КЭП осуществляется ответственным пользователем СКЗИ под роспись.

3.3. При эксплуатации КЭП пользователь СКЗИ обязан следовать правилам:

3.3.1. Получить КЭП на носителе ключевой информации под роспись в соответствующем журнале, убедившись, то они правильно маркированы (имеют серийный номер).

3.3.2. Нести ответственность за конфиденциальность сохранения пароля (ПИН-кода) ключа КЭП (если таковой имеется).

3.3.3. Нести персональную ответственность за сохранность носителя ключевой информации в месте, не доступным третьим лицам.

3.3.4. Не допускать использования КЭП третьими лицами.

3.3.5. Вставлять носитель ключевой информации в считывающее устройство только на время использования КЭП.

3.3.6. Знать и соблюдать меры по исключению несанкционированного доступа в помещения, в которых размещены средства КЭП.

3.3.7. Исключить присутствие третьих лиц, а в случае необходимости их присутствия обеспечить контроль за их действиями во избежание негативных воздействий на средства КЭП и СКЗИ.

3.3.8. Сдавать на временное хранение ответственному пользователю СКЗИ носители ключевой информации в период длительного отсутствия на рабочем месте, в период отпуска, болезни и т.п. под роспись.

3.4. При работе с КЭП пользователю СКЗИ запрещается:

3.4.1. Осуществлять несанкционированное копирование КЭП.

3.4.2. Разглашать содержимое носителей ключевой информации.

3.4.3. Передавать носители лицам, к ним не допущенным.

3.4.4. Выводить ключевую информацию на дисплей, принтер и иные средства отображения информации.

3.4.5. Использовать носители ключевой информации в режимах, не предусмотренных штатным режимом использования.

3.4.6. Вносить какие-либо изменения в программное обеспечение средств КЭП.

3.4.7. Записывать на носители ключевой информации постороннюю информацию (в том числе рабочие или личные файлы).

3.4.8. Оставлять средства вычислительной техники с установленными средствами КЭП без контроля после ввода ключевой информации.

3.4.9. Использовать КЭП и соответствующий сертификат ключа проверки КЭП, заявление на изменение статуса которого подано, в течение времени, исчисляемого с момента подачи заявления на изменение статуса сертификата по момент официального информирования об изменении статуса сертификата, либо об отказе в изменении статуса.

3.4.10. Использовать КЭП, сертификат ключа проверки которого аннулирован, действие которого прекращено или приостановлено.

3.4.11. Удалять ключевую информацию с носителей ключевой информации до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки КЭП.

3.4.12. Пересылать файлы с ключевой информацией по электронной почте сети Интернет или по внутренней электронной почте.

3.5. Пользователь СКЗИ обязан уведомить ответственного пользователя СКЗИ за 30 дней до окончания срока действия сертификата проверки КЭП и получить дальнейшие инструкции о выпуске нового

сертификата проверки КЭП либо об уничтожении ключевой информации в связи с отсутствием необходимости дальнейшего использования КЭП.

3.6. При увольнении пользователь СКЗИ сдает носить ключевой информации ответственного пользователя СКЗИ под роспись в соответствующем журнале.

3.7. При переназначении пользователя СКЗИ проводится анализ должностных обязанностей пользователя СКЗИ, требующих использования КЭП. На основе данных анализа принимается решение об уничтожении КЭП или о продолжении эксплуатации КЭП пользователем с занесением соответствующей записи в журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

## 4. Восстановление связи в случае компрометации действующих ключей к СКЗИ.

4.1. Под компрометацией ключа КЭП понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца носителя ключевой информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих ключей КЭП, относятся:

4.1.1. Утрата (хищение) носителя ключевой информации, в том числе – с последующим его обнаружение.

4.1.2. Увольнение (переназначение) сотрудников, использующих КЭП.

4.1.3. Передача ключей по линии связи в открытом виде.

4.1.4. Нарушение правил хранения носителей ключевой информации.

4.1.5. Вскрытие фактов утечки передаваемой информации или ее искажения (подмены, подделки).

4.1.6. Ошибка при совершении криптографической операции.

4.1.7. Несанкционированное или без учетное копирование ключевой информации.

4.1.8. Все случаи, когда нельзя достоверно установить, что произошло с носителем ключевой информации, в том числе случаи, когда носитель ключевой информации вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий.

4.2. При наступлении любого из перечисленных выше событий пользователь СКЗИ должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) руководителю подразделения и ответственному пользователю СКЗИ любым доступным способом.

4.3. При подтверждении факта компрометации действующих КЭП пользователь СКЗИ обязан обеспечить немедленное изъятие из обращения скомпрометированных КЭП и сдачу ответственному пользователю СКЗИ в течении 3 рабочих дней под роспись в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

4.4. Следует немедленно обратиться удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата.

4.5. Для восстановления конфиденциальной связи после компрометации действующей КЭП пользователь СКЗИ получает у ответственного пользователя СКЗИ новый ключ.

ПРИЛОЖЕНИЕ № 16
к постановлению
Администрации
Куйбышевского
внутригородского района
от «26» 12 2022 № 409

Перечень должностей сотрудников Администрации Куйбышевского внутригородского района городского округа Самара, допущенных к работе со средствами криптографической защиты информации

1. Глава Куйбышевского внутригородского района городского округа Самара;
2. первый заместитель главы Куйбышевского внутригородского района городского округа Самара;
3. заместитель главы Куйбышевского внутригородского района городского округа Самара;
4. руководитель управления;
5. начальник отдела;
6. председатель административной комиссии;
7. заместитель начальника отдела;
8. заведующий сектором;
9. консультант;
10. главный специалист;
11. инспектор;
12. архивариус;
13. инженер;
14. специалист-эксперт.